思科 ASA 系列命令参考，S 命令

更新日期：2014 年 11 月 5 日

Cisco Systems, Inc.
www.cisco.com

思科在全球设有 200 多个办事处。
地址、电话号码和传真号码
在思科网站上列出，网址为：
www.cisco.com/go/offices。

文本部件号：不适用，仅限在线使用

本手册中有关产品的规格和信息如有更改，恕不另行通知。我们相信本手册中的所有声明、信息和建议均准确可靠，但不提供任何明示或暗示的担保。用户应承担使用产品的全部责任。

产品配套的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您找不到软件许可或有限担保，请与思科代表联系以索取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。版权所有。版权所有 © 1981，加利福尼亚州大学董事。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问以下 URL： www.cisco.com/go/trademarks 。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并不代表实际地址和电话号码。本文档中包括的任何示例、命令显示输出、网络拓扑图和其他图形仅用于说明目的。在图示内容中使用的 IP 地址或电话号码纯属虚构，如有雷同，纯属巧合。

思科 ASA 系列命令参考，S 命令
© 2014 思科系统公司。版权所有。

第 1 章

same-security-traffic 至 shape 命令

same-security-traffic

要允许同等安全级别的接口之间的通信，或者让进入 anciscoasad 的流量从同一接口退出，请在全局配置模式下使用 **same-security-traffic** 命令。要禁用 same-security 流量，请使用此命令的 **no** 形式。

same-security-traffic permit {**inter-interface** | **intra-interface**}

no same-security-traffic permit {**inter-interface** | **intra-interface**}

语法说明

inter-interface	允许具有相同安全级别的不同接口之间通信。
intra-interface	允许通信进出同一接口。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	**intra-interface** 关键字现在允许所有流量（不只是 IPsec 流量）进入和退出同一接口。

使用指南

允许具有相同安全性的各接口之间通信（通过 **same-security-traffic inter-interface** 命令启用）有以下优点：

- 可以配置超过 101 个通信接口。如果对每个接口使用不同的级别，则每个级别只能配置一个接口 (0-100)。
- 可以允许流量在所有具有相同安全性的各接口之间自由流动，而无需访问列表。

same-security-traffic intra-interface 命令可让流量进入和退出同一接口（一般不允许这种情况）。此功能可能适用于进入某接口但然后又从同一接口流出的 VPN 流量。VPN 流量在这种情况下可能不加密，也可能对另一个 VPN 连接重新加密。例如，如果您有一个轴辐型 VPN 网络，其中 ASA 是轴，远程 VPN 网络是辐，要使一个辐与另一个辐通信，流量必须进入 ASA，然后再从中流出到另一个辐。

注　**same-security-traffic intra-interface** 命令允许的所有流量仍需遵守防火墙规则。小心不要造成可能导致返回流量不流经 ASA 的非对称路由情况。

示例

以下示例展示如何启用 same-security 接口通信：

```
ciscoasa(config)# same-security-traffic permit inter-interface
```

以下示例展示如何让流量能够进入和退出同一接口：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

相关命令

命令	说明
show running-config same-security-traffic	显示 **same-security-traffic** 配置。

sasl-mechanism

要指定用于向 LDAP 验证 LDAP 身份的 SASL（简单身份验证和安全层）机制，请在 aaa-server 主机配置模式下使用 **sasl-mechanism** 命令。SASL 身份验证机制选项为 **digest-md5** 和 **kerberos**。

要禁用身份验证机制，请使用此命令的 **no** 形式。

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

注　由于 ASA 用作 VPN 用户连接 LDAP 服务器的客户端代理，因此在这里引用的 LDAP 客户端是 ASA。

语法说明

digest-md5	ASA 使用从用户名和密码计算的 MD5 值响应。
kerberos	ASA 使用 GSSAPI（通用安全服务应用程序编程接口）Kerberos 机制发送用户名和领域来响应。
server-group-name	指定 Kerberos aaa 服务器组，最多 64 个字符。

默认值

没有默认行为或值。ASA 将身份验证参数以明文形式传递到 LDAP 服务器。

注　如果尚未配置 SASL，建议使用 **ldap-over-ssl** 命令通过 SSL 保护 LDAP 通信。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
aaa-server 主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用此命令指定 ASA 使用 SASL 机制向 LDAP 服务器进行身份验证。

ASA 和 LDAP 服务器可以支持多种 SASL 身份验证机制。在协商 SASL 身份验证时，ASA 将检索服务器上配置的 SASL 机制列表，并且将身份验证机制设置为 ASA 和服务器上配置的最强机制。Kerberos 机制强度高于 Digest-MD5 机制。为便于说明，如果 LDAP 服务器和 ASA 都支持两种机制，ASA 选择 Kerberos（相对更强的机制）。

禁用 SASL 机制时，必须为要禁用的每个机制输入单独的 **no** 命令，因为它们都是单独配置的。您未明确禁用的机制仍然有效。例如，您必须输入以下两个命令才可禁用两个 SASL 机制：

no sasl-mechanism digest-md5

no sasl-mechanism kerberos *server-group-name*

示例

以下示例在 aaa 服务器主机配置模式下输入，为 IP 地址为 10.10.0.1 的 LDAP 服务器 ldapsvr1 进行身份验证启用 SASL 机制。本示例启用 SASL digest-md5 身份验证机制：

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism digest-md5
```

以下示例启用 SASL Kerberos 身份验证机制，将 kerb-servr1 指定为 Kerberos AAA 服务器：

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

相关命令

命令	说明
ldap-over-ssl	指定以 SSL 保护 LDAP 客户端 - 服务器连接。
server-type	指定 Microsoft 或 Sun 作为 LDAP 服务器供应商。
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于将用户定义的属性名称映射到思科 LDAP 属性名称。

sast

要指定在 CTL 记录中创建的 SAST 证书数量，请在 ctl 文件配置模式下使用 **sast** 命令。要将 CTL 文件中的 SAST 证书数量恢复为默认值 2，请使用此命令的 **no** 形式。

sast *number_sasts*

no sast *number_sasts*

语法说明

number_sasts	指定要创建的 SAST 密钥数。默认值为 2。允许的最大值为 5。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CTL 文件配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

CTL 文件由系统管理员安全令牌 (SAST) 签名。

由于电话代理生成 CTL 文件，因此需要创建 SAST 密钥对 CTL 文件本身签名。此密钥可在 ASA 上生成。SAST 创建为自签证书。

通常，CTL 文件包含多个 SAST。当一个 SAST 不可恢复时，可使用另一个对文件签名。

示例

以下示例展示使用 **sast** 命令在 CTL 文件中创建 5 个 SAST 证书：

```
ciscoasa(config-ctl-file)# sast 5
```

相关命令

命令	说明
ctl-file (global)	指定要创建电话代理配置的控制文件或 CTL 文件，以解析从闪存。
ctl-file (phone-proxy)	指定要用于电话代理配置的控制文件。
phone-proxy	配置电话代理实例。

scansafe

要对某个情景启用云网络安全检查，请在情景配置模式下使用 **scansafe** 命令。要禁用云网络安全，请使用此命令的 **no** 形式。

scansafe [**license** *key*]

no scansafe [**license** *key*]

语法说明

license *key*	输入此情景的身份验证密钥。如果不指定密钥，该情景将使用系统配置中配置的许可证。ASA 将身份验证密钥发送到 云网络安全 代理服务器，指出请求来自哪个组织。身份验证密钥是一个 16 字节的十六进制数。

命令默认

默认情况下，情景使用在系统配置中输入的许可证。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

在多情景模式下，对每个情景都必须允许云网络安全。

示例

以下示例配置在使用默认许可证的情景一 (context one) 和使用许可证密钥覆盖的情景二 (context two) 中启用云网络安全。

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
```

```
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

scansafe general-options

要配置与云网络安全代理服务器通信，请在全局配置模式下使用 **scansafe general-options** 命令。要删除服务器配置，请使用此命令的 **no** 形式。

scansafe general-options

no scansafe general-options

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您可以为云网络安全配置主要和备用代理服务器。

示例

以下示例配置主要服务器：

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。

命令	说明
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

scep-enrollment enable

要对隧道组启用或禁用简单证书注册协议，请在隧道组常规属性模式下使用 **scep-enrollment enable** 命令。

要从配置中删除此命令，请使用此命令的 **no** 形式。

scep-enrollment enable

no scep-enrollment enable

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，此命令在隧道组配置中不存在。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

只有 Cisco AnyConnect 安全移动客户端 3.0 版和更高版本支持此功能。

ASA 可以代理 AnyConnect 与第三方证书颁发机构之间的 SCEP 请求。如果证书颁发机构用作代理，只需要它可供 ASA 访问即可。为使 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用 AAA 支持的任何方法进行身份验证。您还可以使用主机扫描和动态访问策略执行注册资格规则。

ASA 仅对 AnyConnect SSL 或 IKEv2 VPN 会话支持此功能。它支持所有 SCEP 标准的证书颁发机构，包括 IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。

无客户端（基于浏览器）访问不支持 SCEP 代理，但 WebLaunch - 无客户端发起的 AnyConnect - 支持此代理。

ASA 不支持轮询证书。

ASA 支持此功能的负载平衡。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的远程访问隧道组并对组策略启用 SCEP：

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

相关命令

命令	说明
crypto ikev2 enable	在 IPsec 对等设备通信的接口上启用 IKEv2 协商。
scep-forwarding-url	注册组策略的 SCEP 证书颁发机构。
secondary-pre-fill-username clientless	当证书不适用于 SCEP 代理的 WebLaunch 支持时，提供通用辅助密码。
secondary-authentication-server-group	当证书不可用时，提供用户名。

scep-forwarding-url

要为组策略注册 SCEP 证书颁发机构，请在组策略配置模式下使用 **scep-forwarding-url** 命令。要从配置中删除此命令，请使用此命令的 **no** 形式。

scep-forwarding-url {**none** | **value** [*URL*]}

no scep-forwarding-url

语法说明

none	不为组策略指定证书颁发机构。
URL	指定证书颁发机构的 SCEP URL。
value	为无客户端连接启用此功能。

默认值

默认情况下，此命令不存在。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

为每个组策略输入一次此命令，以支持第三方数字证书。

示例

以下示例在全局配置模式下输入，创建名为 FirstGroup 的组策略，并且为组策略注册证书颁发机构：

```
ciscoasa(config)# group-policy FirstGroup internal
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL.Please wait ...
```

相关命令

命令	说明
crypto ikev2 enable	在 IPsec 对等设备通信的接口上启用 IKEv2 协商。
scep-enrollment enable	对隧道组启用简单证书注册协议。

命令	说明
secondary-pre-fill-username clientless	当证书不适用于 SCEP 代理的 WebLaunch 支持时，提供通用辅助密码。
secondary-authentication-server-group	当证书不可用时，提供用户名。

secondary

要在故障切换组中为辅助设备指定较高优先级，请在故障切换组配置模式下使用 **secondary** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

secondary

no secondary

语法说明

此命令没有任何参数或关键字。

默认值

如果未为故障切换组指定 **primary** 或 **secondary**，则故障切换组将默认为 **primary**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

将主要优先级或次要优先级分配给故障切换组，指定当两个设备同时启动时（在设备轮询时间内），故障切换组在哪个设备上激活。如果一个设备在另一个设备前启动，则两个故障切换组都会在该设备上激活。当另一个设备联机时，以第二个设备优先的任何故障切换组都不会在第二个设备上激活，除非使用 **preempt** 命令对故障切换组进行配置，或使用 **no failover active** 命令手动强制该故障切换组在另一个设备上激活。

示例

以下示例将主要设备作为更高优先级来配置故障切换组 1，将辅助设备作为更高优先级来配置故障切换组 2。使用 **preempt** 命令对这两个故障切换组进行了配置，因此在设备可用后，这两个组将会自动在其首选设备上激活。

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

相关命令

命令	说明
failover group	为 Active/Active（主用 / 主用）故障切换定义故障切换组。
preempt	在设备可用后，强制故障切换组自动在其首选设备上激活。
primary	为主要设备指定高于辅助设备的优先级。

secondary-authentication-server-group

要指定辅助身份验证服务器组在双重身份验证启用时与会话关联，请在隧道组常规属性模式下使用 **secondary-authentication-server-group** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

secondary-authentication-server-group [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**]}

no secondary-authentication-server-group

语法说明

interface_name	（可选）指定 IPsec 隧道终止的接口。
LOCAL	（可选）如果服务器组中的所有服务器因通信失败而停用，需要根据本地用户数据库进行身份验证。如果服务器组名称为 **LOCAL** 或 **NONE**，请不要在此使用 **LOCAL** 关键字。
none	（可选）将服务器组名称指定为 **NONE**，表示不需要身份验证。
groupname [**LOCAL**]	标识先前配置的身份验证服务器或服务器组。这也可以是 LOCAL 组。
use-primary-username	将主要用户名用作辅助身份验证的用户名。

默认值

默认值为 **none**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

只有启用双重身份验证，此命令才有意义。**secondary-authentication-server-group** 命令指定辅助 AAA 服务器组。辅助服务器组不能是 SDI 服务器组。

如果配置 use-primary-username 关键字，则在登录对话中只要求一个用户名。

如果用户名提取自数字证书，则只有主要用户名用于身份验证。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的远程访问隧道组，并且将使用的组 sdi_server 指定为主要服务器组，将组 ldap_server 指定为连接的辅助身份验证服务器组：

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-server-group sdi_server
ciscoasa(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
pre-fill-username	启用预填充用户名功能。
show running-config tunnel-group	显示指示的隧道组配置。
tunnel-group general-attributes	指定命名的隧道组的常规属性。
username-from-certificate	在证书中指定要用作用于授权的用户名的字段。

secondary-color

要设置用于 WebVPN 登录、主页和文件访问页面的辅助颜色，请在 webvpn 配置模式下使用 **secondary-color** 命令。要从配置中删除颜色并重置默认值，请使用此命令的 **no** 形式。

secondary-color [*color*]

no secondary-color

语法说明

color	（可选）指定颜色。您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。 • RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。 • HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。 • 名称长度最多为 32 个字符

默认值

默认辅助颜色是 HTML #CCCCFF（淡紫色）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

建议使用的 RGB 值数量是 216，远远少于数学概率。许多显示器只能处理 256 色，其中 40 色在 MAC 和 PC 上分别呈现出不同的外观。为获得最佳效果，请检查发布的 RGB 表。要线上查找 RGB 表，请在搜索引擎中输入 RGB。

示例

以下示例展示如何设置 HTML 颜色值 #5F9EAO（青色）：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-color #5F9EAO
```

相关命令

命令	说明
title-color	设置用于登录、主页和文件访问页面中 WebVPN 标题栏的颜色。

secondary-pre-fill-username

要启用从客户端证书提取用户名以用于无客户端或 AnyConnect 连接的双重身份验证，请在隧道组 webvpn 属性模式下使用 **secondary-pre-fill-username** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

secondary-pre-fill-username {**clientless** | **ssl-client**} [**hide**]

secondary-pre-fill-username {**clientless** | **ssl-client**} **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]

no secondary-no pre-fill-username

语法说明

clientless	为无客户端连接启用此功能。
hide	对 VPN 用户隐藏要用于身份验证的用户名。
password	输入密码字符串。
ssl-client	为 AnyConnect VPN 客户端连接启用此功能。
type_num	输入以下选项之一： • 0（如果要输入的密码是明文）。 • 8（如果要输入的密码已加密）。密码在您键入时显示为星号。
use-common-password	指定使用通用辅助身份验证密码，而不提示用户输入。
use-primary-password	对辅助身份验证重新使用主要身份验证密码，而不提示用户输入。

默认值

默认禁用此功能。输入不带 **hide** 关键字的此命令将会向 VPN 用户显示提取的用户名。如果 **use-primary-password** 和 **use-common-password** 关键字都未指定，用户会收到密码提示。*type_num* 的默认值为 8。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组 WebVPN 属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。
8.3(2)	为命令增加了 [**use-primary-password** | **use-common-password** [*type_num*] *password*]。

使用指南

要启用此功能，还必须在隧道组常规属性模式下输入 **secondary-username-from-certificate** 命令。

此命令仅在启用了双重身份证时才有意义。通过 **secondary-pre-fill-username** 命令，可以将从 **secondary-username-from-certificate** 命令指定的证书字段中提取的用户名作为辅助用户名 / 密码身份验证的用户名。要使用这项从证书预填辅助用户名的功能，必须同时配置这两个命令。

注　无客户端连接和 SSL 客户端连接不是互斥选项。每个命令行只能指定一个选项，但两个选项可以同时启用。

如果隐藏第二个用户名并且使用主要或通用密码，用户体验类似于单身份验证。使用主要或通用密码时，使用设备证书对设备进行身份验证会获得无缝的用户体验。

use-primary-password 关键字指定将主要密码用作所有身份验证的辅助密码。

use-common-password 关键字指定对所有辅助身份验证使用通用辅助密码。如果终端上安装的设备证书包含 BIOS ID 或其他标识符，辅助身份验证请求可以使用预填的 BIOS ID 作为第二个用户名，并且使用为该隧道中所有身份验证配置的通用密码。

示例

以下示例创建名为 remotegrp 的 IPsec 远程访问隧道组，并且指定将终端上数字证书中的名称重新用作在连接基于浏览器时要用于身份验证或授权查询的名称。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

以下示例执行与上一个命令相同的功能，但会对用户隐藏用户名：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

以下示例执行与上一个命令相同的功能，不同之处是它只适用于 AnyConnect 连接：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

以下示例隐藏用户名，并且对辅助身份验证重新使用主要身份验证密码，而不提示用户：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-primary-password
```

以下示例隐藏用户名，并且对辅助身份验证使用您输入的密码：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password **********
```

相关命令

命令	说明
pre-fill-username	启用预填充用户名功能。
show running-config tunnel-group	显示指示的隧道组配置。
tunnel-group general-attributes	指定命名的隧道组的常规属性。
username-from-certificate	在证书中指定要用作用于授权的用户名的字段。

secondary-text-color

要设置 WebVPN 登录、主页和文件访问页面的辅助文本颜色，请在 webvpn 模式下使用 **secondary-text-color** 命令。要从配置中删除颜色并重置默认值，请使用此命令的 **no** 形式。

secondary-text-color [*black* | *white*]

no secondary-text-color

语法说明

auto	根据 text-color 命令的设置选择 black 或 white。也就是说，如果主要颜色为黑色，则该值为 white。
black	默认辅助文本颜色为黑色。
white	您可以将文本颜色更改为白色。

默认值

默认辅助文本颜色为黑色。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何将辅助文本颜色设置为白色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-text-color white
```

相关命令

命令	说明
text-color	为登录、主页和文件访问页面中 WebVPN 标题栏的文本设置颜色

secondary-username-from-certificate

要指定证书字段用作无客户端或 AnyConnect（SSL 客户端）连接双重身份验证的辅助用户名，请在隧道组常规属性模式下使用 **secondary-username-from-certificate** 命令。

要从配置中删除属性并还原默认值，请使用此命令的 **no** 形式。

secondary-username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**}

no secondary-username-from-certificate

语法说明

primary-attr	指定用于获得从证书进行授权查询的用户名的属性。如果启用了 pre-fill-username，则获得的名称也可在身份验证查询中使用。
secondary-attr	（可选）指定与主要属性一起使用的附加属性，用于得出进行身份验证或从数字证书进行授权查询的用户名。如果启用了 pre-fill-username，则获得的名称也可在身份验证查询中使用。
use-entire-name	指定 ASA 必须使用完整主题 DN (RFC1779) 得出从数字证书进行授权查询的名称。
use-script	指定使用 ASDM 生成的脚本文件从证书提取 DN 字段用作用户名。

默认值

此功能默认禁用，仅在双重身份验证启用时才有意义。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

只有启用双重身份验证，此命令才有意义。

在双重身份验证启用时。此命令选择一个或多个证书字段用作用户名。**secondary-username-from-certificate** 命令强制安全应用将指定的证书字段用作第二个用户名 / 密码身份验证的第二个用户名。

要将这项从证书预填用户名推导用户名的功能用于辅助用户名 / 密码身份验证或授权，还必须在隧道组 webvpn 属性模式下配置 **pre-fill-username** 和 **secondary-pre-fill-username** 命令。也就是说，要使用辅助预填用户名功能，必须配置这两个命令。

主要和辅助属性可能的值包括：

属性	定义
C	国家 / 地区：两个字母的国家 / 地区缩写。这些代码符合 ISO 3166 国家 / 地区缩写。
CN	公用名称：人员、系统或其他实体的名称。不可用作辅助属性。
DNQ	域名限定符。
EA	邮件地址。
GENQ	世代限定符。
GN	指定名称。
I	缩写。
L	区域：组织所在的城市或城镇。
N	名称。
O	组织：公司、机构、办事处、协会或其他实体的名称。
OU	组织单位：组织 (O) 内的子组。
SER	序列号。
SN	姓氏。
SP	省 / 自治区 / 直辖市：组织所在的省 / 自治区 / 直辖市
T	称谓。
UID	用户标识符。
UPN	用户主体名称。
use-entire-name	使用完整 DN 名称。不可用作辅助属性。
use-script	使用 ASDM 生成的脚本文件。

注　如果还指定 **secondary-authentication-server-group** 命令及 **secondary-username-from-certificate** 命令，则只有主要用户名用于身份验证。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的远程访问隧道组，并且指定将 CN（公用名称）用作主要属性，将 OU 用作辅助属性，以从数字证书推导授权查询的名称：

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN
ciscoasa(config-tunnel-general)# secondary-username-from-certificate OU
ciscoasa(config-tunnel-general)#
```

以下示例展示如何修改隧道组属性以配置预填充用户名。

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

相关命令

命令	说明
pre-fill-username	启用预填充用户名功能。
secondary-pre-fill-username	为无客户端或 AnyConnect 客户端连接启用用户名提取。
username-from-certificate	在证书中指定要用作用于授权的用户名的字段。
show running-config tunnel-group	显示指示的隧道组配置。
secondary-authentication-server-group	指定辅助 AAA 服务器组。如果用户名提取自数字证书，则只有主要用户名用于身份验证。

secure-unit-authentication

要启用安全设备身份验证，请在组策略配置模式下使用 **secure-unit-authentication enable** 命令。要禁用安全设备身份验证，请使用 **secure-unit-authentication disable** 命令。要从运行配置删除安全设备身份验证属性，请使用此命令的 **no** 形式。

secure-unit-authentication {enable | disable}

no secure-unit-authentication

语法说明

disable	禁用安全设备身份验证。
enable	启用安全设备身份验证。

默认值

安全设备身份验证已禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

安全设备身份验证要求您已为硬件客户端使用的隧道组配置身份验证服务器组。

如果在主要 ASA 上需要安全设备身份验证，请确保同时在所有备用服务器上配置它。

no 选项允许从另一个组策略继承安全设备身份验证的值。

安全设备身份验证要求 VPN 硬件客户端在每次客户端发起隧道时验证用户名和密码，从而提供额外的安全性。启用此功能后，硬件客户端没有保存的用户名和密码。

注　在此功能启用后，要启动 VPN 隧道，用户必须存在才可输入用户名和密码。

示例

以下示例展示如何对名为 FirstGroup 的组策略启用安全设备身份验证：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# secure-unit-authentication enable
```

相关命令

命令	说明
ip-phone-bypass	无需经过用户身份验证即可让 IP 电话连接。安全设备身份验证仍然有效。
leap-bypass	启用后，LEAP 数据包在用户身份验证之前可从 VPN 硬件客户端后面的无线设备通过 VPN 隧道。这样就可让使用思科无线接入点设备的工作站建立 LEAP 身份验证。然后，它们将根据用户身份验证再次进行验证。
user-authentication	要求硬件客户端后面的用户确定自己针对 ASA 的身份，然后才能连接。

security-group

要向安全对象组添加安全组以用于 Cisco TrustSec，请在对象组安全配置模式下使用 **security-group** 命令。要删除安全组，请使用此命令的 **no** 形式。

security-group {**tag** *sgt#* | **name** *sg_name*}

no security-group {**tag** *sgt#* | **name** *sg_name*}

语法说明

tag *sgt#*	将安全组对象指定为内联标记。为 Tag 安全类型输入 1-65533 的数字。 SGT 通过 IEEE 802.1X 身份验证、网络身份验证或 MAC 身份验证旁路 (MAB) 由 ISE 分配到设备。安全组名称创建于 ISE 上，为安全组提供便于用户使用的名称。该安全组表将 SGT 映射到安全组名称。
name ***sg_name***	将安全组对象指定为命名对象。为 Name 安全类型输入区分大小写的 32 字节字符串。*sg_name* 可以包含任何字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.]。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
对象组安全配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

例如，您可以通过在扩展 ACL 中包含组来创建用于支持 Cisco TrustSec 的功能的安全组对象组，该组然后又可用于访问规则。

与 Cisco TrustSec 集成时，ASA 将从 ISE 下载安全组信息。ISE 用作身份存储库，向用户身份映射提供 Cisco TrustSec 标记，向服务器资源映射提供 Cisco TrustSec 标记。在 ISE 上集中调配和管理安全组访问列表。

但是，ASA 可能有未在全局定义的本地化网络资源，需要具有本地化安全策略的本地安全组。本地安全组可能包含下载自 ISE 的嵌套安全组。ASA 将合并本地和中心安全组。

要在 ASA 上创建本地安全组，需创建本地安全对象组。本地安全对象组可以包含一个或多个嵌套的安全对象组或安全 ID 或安全组名称。用户还可以创建 ASA 上不存在的新安全 ID 或安全组名称。

您可以使用在 ASA 上创建的安全对象组来控制对网络资源的访问。您可以将安全对象组用作访问组或服务策略的一部分。

示例

以下示例展示如何配置安全组对象：

```
ciscoasa(config)# object-group security mktg-sg
ciscoasa(config)# security-group name mktg
ciscoasa(config)# security-group tag 1
```

以下示例展示如何配置安全组对象：

```
ciscoasa(config)# object-group security mktg-sg-all
ciscoasa(config)# security-group name mktg-managers
ciscoasa(config)# group-object mktg-sg // nested object-group
```

相关命令

命令	说明
object-group security	创建安全组对象。

security-group-tag value

要在 LOCAL 用户数据库以及 VPN 会话的组策略中配置安全组标记属性，请在组策略配置模式下使用 **security-group-tag value** 命令。要删除安全组标记属性，请使用此命令的 **no** 形式。

security-group-tag value *sgt*

no security-group-tag value *sgt*

语法说明

sgt	指定安全组标记编号。

命令默认

此命令的默认形式为 **security-group-tag none**，这意味着此属性集中没有安全组标记。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(1)	我们引入了此命令。

使用指南

ASA 9.3(1) 版完全支持 VPN 会话的安全组标记。安全组标记 (SGT) 可以分配到使用外部 AAA 服务器的 VPN 会话，或通过本地用户数据库配置分配。此标记然后可在第二层以太网上通过 Cisco TrustSec 系统传播。安全组标记适用于组策略，当 AAA 服务器无法提供 SGT 时可用于本地用户。

如果在 AAA 服务器的属性中没有 SGT 可分配到 VPN 用户，ASA 将使用默认组策略中的 SGT。如果组策略中也没有 SGT，则会分配标记 0x0。

远程用户连接服务器的常见步骤

1. 用户连接到 ASA。
2. ASA 向 ISE 请求 AAA 信息，其中可能包括 SGT。ASA 同时为用户的隧道流量分配 IP 地址。
3. ASA 使用 AAA 信息进行身份验证和创建隧道。
4. ASA 使用 AAA 信息中的 SGT 和分配的 IP 地址在第 2 层报头中添加 SGT。
5. 包含 SGT 的数据包传递到 Cisco TrustSec 网络中的下一个对等设备。

示例

以下示例展示如何为指定的组策略或 LOCAL 用户名属性集配置 SGT 属性：

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

相关命令

命令	说明
show asp table cts sgt-map	显示数据路径内维护的 IP 地址安全组表映射数据库中的 IP 地址安全组表映射条目。
show cts sgt-map	显示控制路径中的 IP 地址安全组表管理器条目。

security-level

要设置接口的安全级别，请在接口配置模式下使用 **security-level** 命令。要将安全级别设置为默认值，请使用此命令的 **no** 形式。安全级别在安全性较高的网络与安全性较低的网络之间实施额外保护，阻止两者之间互相通信。

security-level *number*

no security-level

语法说明

number	0（最低）到 100 的整数（最高）。

默认值

默认情况下，安全级别为 0。

如果将接口命名为 “inside”，但未明确设置安全级别，则 ASA 会将安全级别设置为 100（请参阅 **nameif** 命令）。需要时可以更改此级别。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	此命令已从 **nameif** 命令的关键字移至接口配置模式命令。

使用指南

此级别控制以下行为：

- 网络访问 - 默认情况下，默许从安全级别较高的接口访问安全级别较低的接口（出站）。高安全级别接口上的主机可以访问低安全级别接口上的所有主机。您可以通过向接口应用访问列表来限制访问。

  对于安全级别相同的接口，默许接口访问安全级别相同或更低的其他接口。

- 检测引擎 - 有些检测引擎取决于安全级别。对于安全级别相同的接口，检测引擎应用于任一方向的流量。
  - NetBIOS 检测引擎 - 只应用于出站连接。
  - OraServ 检测引擎 - 如果 OraServ 端口的控制连接存在于一对主机之间，则只允许入站数据连接通过 ASA。
- 过滤 - HTTP(S) 和 FTP 过滤只应用于出站连接（从高安全级别到低安全级别）。

  对于安全级别相同的接口，您可以过滤任一方向的流量。

- NAT 控制 - 启用 NAT 控制后，当高安全级别接口上的主机（内部）访问低安全级别接口上的主机（外部）时，您必须为高安全级别接口上的主机配置 NAT。

  若未启用 NAT 控制，或者是安全级别相同的接口，您可以选择在任何接口之间使用 NAT，或者选择不使用 NAT。请记住，对外部接口配置 NAT 可能需要特殊关键字。

- **established** 命令 - 如果高安全级别主机到低安全级别主机已建立连接，此命令允许从低安全级别主机到高安全级别主机的返回连接。

  对于安全级别相同的接口，您可以对两个方向配置 **established** 命令。

通常，安全级别相同的接口无法通信。如果希望安全级别相同的接口进行通信，请参阅 **same-security-traffic** 命令。如果要创建 101 个以上的通信接口，或者希望将保护功能同等应用到两个接口之间的流量，您可能需要将两个接口分配到同一级别，并且允许它们通信；例如，您有两个安全性完全一样的部门。

如果您要更改接口的安全级别，并且不希望等到现有连接超时后才使用新安全信息，可以使用 **clear local-host** 命令清除连接。

示例

以下示例将两个接口的安全级别配置为 100 和 0：

```
ciscoasa(config)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

相关命令

命令	说明
clear local-host	重置所有连接。
interface	配置接口并进入接口配置模式。
nameif	设置接口名称。
vlan	将 VLAN ID 分配给子接口。

send response

要将 RADIUS 记账响应开始和记账响应停止消息发送到 RADIUS 记账响应开始和停止消息的发送方，请在 RADIUS 记账参数配置模式（使用 **inspect radius-accounting** 命令访问）下使用 **send response** 命令。

默认情况下该选项处于禁用状态。

send response

no send response

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Radius-accounting 参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何发送 RADIUS 记账响应：

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# send response
ciscoasa(config-pmap-p)# send response
```

相关命令

命令	说明
inspect radius-accounting	设置 RADIUS 记账的检查。
parameters	设置检查策略映射的参数。

seq-past-window

要对序列号超过窗口的数据包（收到的 TCP 数据包的序列号超过 TCP 接收窗口的右边）设置操作，请在 tcp-map 配置模式下使用 **seq-past-window** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令是使用 **set connection advanced-options** 命令启用的 TCP 规范化策略的一部分。

seq-past-window {**allow** | **drop**}

no seq-past-window

语法说明

allow	允许序列号超过窗口的数据包。仅当 **queue-limit** 命令设置为 0（禁用）时才允许此操作。
drop	丢弃序列号超过窗口的数据包。

默认值

默认操作是丢弃序列号超过窗口的数据包。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TCP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。

使用指南

要启用 TCP 规范化，请使用模块化策略框架：

1. **tcp-map** - Identifies the TCP normalization actions.
   a. **seq-past-window** - 在 tcp-map 配置模式下，可以输入 **seq-past-window** 命令等。
2. **class-map** - Identify the traffic on which you want to perform TCP normalization.
3. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced-options** - 确定创建的 tcp 映射。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

示例

以下示例将 ASA 设置为允许序列号超过窗口的数据包。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# seq-past-window allow
ciscoasa(config)# class-map cmap
```

```
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

相关命令

命令	说明
class-map	为服务策略标识流量。
policy-map	标识要应用于服务策略中的流量的操作。
queue-limit	设置无序数据包限制。
set connection advanced-options	启用 TCP 规范化。
service-policy	将服务策略应用于接口。
show running-config tcp-map	显示 TCP 映射配置。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

serial-number

要在注册时将 ASA 序列号包含在证书中，请在 crypto ca trustpoint 配置模式下使用 **serial-number** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

serial-number

no serial-number

语法说明

此命令没有任何参数或关键字。

默认值

默认设置不包含序列号。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入信任点中心的 crypto ca trustpoint 配置模式，并且在信任点中心的注册请求中包含 ASA 序列号：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# serial-number
```

相关命令

命令	说明
crypto ca trustpoint	进入 trustpoint 配置模式。

server (pop3s, imap4s, smtps)

要指定默认邮件代理服务器，请在适用的邮件代理配置模式下使用 **server** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。当用户连接到邮件代理但未指定服务器时，ASA 会将请求发送到默认邮件服务器。如果未配置默认服务器，而且用户也不指定服务器，ASA 将返回错误。

server {*ipaddr or hostname*}

no server

语法说明

hostname	默认邮件代理服务器的 DNS 名称。
ipaddr	默认邮件代理服务器的 IP 地址。

默认值

默认情况下没有默认邮件代理服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Pop3s 配置	• 是	• 是	—	—	• 是
Imap4s 配置	• 是	• 是	—	—	• 是
SMTPS 配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何设置 IP 地址为 10.1.1.7 的默认 POP3S 邮件服务器：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# server 10.1.1.7
```

server (ssh pubkey-chain)

要在自注册安全复制 (SCP) 客户端的 ASA 数据库中手动添加或删除服务器及其密钥，请在 ssh pubkey-chain 配置模式下使用 **server** 命令。要删除服务器及其主机密钥，请使用此命令的 **no** 形式。

server *ip_address*

no server *ip_address*

语法说明

ip_address	指定 SSH 服务器 IP 地址。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Ssh pubkey-chain 配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.1(5)	我们引入了此命令。

使用指南

可以使用自注册 SCP 客户端将文件复制到 ASA 或者从其中复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如有需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器，可以指定 SSH 主机的 **key-string**（公共密钥）或 **key-hash**（哈希值）。

示例

以下示例为 10.86.94.170 上的服务器添加经过哈希处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

相关命令

命令	说明
copy	将文件复制到 ASA 或者从其中复制文件。
key-hash	输入哈希 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
ssh pubkey-chain	在 ASA 数据库中手动添加或删除服务器及其密钥。
ssh stricthostkeycheck	为自注册安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

server authenticate-client

要让 ASA 在 TLS 握手时对 TLS 客户端进行身份验证，请在 TLS 代理配置模式下使用 **server authenticate-client** 命令。

要绕过客户端身份验证，请使用此命令的 **no** 形式。

server authenticate-client

no server authenticate-client

语法说明

此命令有参数或关键字。

默认值

此命令默认启用，这意味着 TLS 客户端在与 ASA 握手时需要提供证书。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TLS 代理配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

使用 **server authenticate-client** 命令控制在 TLS 代理握手时是否需要客户端身份验证。启用时（默认情况下），安全设备会将证书请求 TLS 握手消息发送到 TLS 客户端，而 TLS 客户端需要提供其证书。

使用此命令的 **no** 形式则会禁用客户端身份验证。当 ASA 必须与网络浏览器等无法发送客户端证书的 CUMA 客户端互操作时，适合禁用 TLS 客户端身份验证。

示例

以下示例配置禁用了客户端身份验证的 TLS 代理实例：

```
ciscoasa(config)# tls-proxy mmp_tls
ciscoasa(config-tlsp)# no server authenticate-client
ciscoasa(config-tlsp)# server trust-point cuma_server_proxy
```

相关命令

命令	说明
tls-proxy	配置 TLS 代理实例。

server backup

要配置备用 云网络安全 代理服务器，请在 scansafe general-options 配置模式下使用 **server backup** 命令。要删除服务器，请使用此命令的 **no** 形式。

server backup {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server backup [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

语法说明

ip *ip_address*	指定服务器 IP 地址。
fqdn *fqdn*	指定服务器的完全限定域名 (FQDN)。
port *port*	（可选）默认情况下，云网络安全 代理服务器对 HTTP 和 HTTPS 流量使用端口 8080；若无明确指示，请勿更改此值。

命令默认

默认端口为 8080。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Scansafe 常规选项配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

当您订用思科云网络安全服务，您将分配主要云网络安全代理服务器和备用代理服务器。请参阅 **server primary** 命令配置主要服务器。系统将定期轮询这些服务器来检查其可用性。如果您的 ASA 无法访问 云网络安全 代理服务器（例如，如果没有来自代理服务器的 SYN/ACK 数据包），则将通过 TCP 三向握手轮询代理服务器，以检查其可用性。如果代理服务器在重试配置的次数（默认值为 5 次）后仍不可用，则将该服务器宣告为不可达，同时激活备用代理服务器。

如果以后的轮询连续两次显示主要服务器已激活，ASA 将自动从备用服务器恢复到主要 云网络安全 代理服务器。使用 **retry-count** 命令可以更改此轮询间隔。

代理服务器不可到达的流量条件	服务器超时计算	连接超时结果
高流量	客户端半开连接超时 + ASA TCP 连接超时	(30 + 30) = 60 秒
单一连接失败	客户端半开连接超时 + ((重试阈值 - 1) x (ASA TCP 连接超时))	(30 + ((5-1) x (30)) = 150 秒
空闲 - 无连接时间超过	15 分钟 + ((重试阈值) x (ASA TCP 连接超时))	900 + (5 x (30) = 1050 秒

示例

以下示例配置主要和备用服务器：

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

server primary

要配置主要 云网络安全 代理服务器，请在 scansafe general-options 配置模式下使用 **server primary** 命令。要删除服务器，请使用此命令的 **no** 形式。

server primary {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server primary [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

语法说明

ip *ip_address*	指定服务器 IP 地址。
fqdn *fqdn*	指定服务器的完全限定域名 (FQDN)。
port *port*	（可选）默认情况下，云网络安全 代理服务器对 HTTP 和 HTTPS 流量使用端口 8080；若无明确指示，请勿更改此值。

命令默认

默认端口为 8080。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Scansafe 常规选项配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

当您订用思科云网络安全服务，您将分配主要云网络安全代理服务器和备用代理服务器。请参阅 **server backup** 命令配置备用服务器。系统将定期轮询这些服务器来检查其可用性。如果您的 ASA 无法访问 云网络安全 代理服务器（例如，如果没有来自代理服务器的 SYN/ACK 数据包），则将通过 TCP 三向握手轮询代理服务器，以检查其可用性。如果代理服务器在重试配置的次数（默认值为 5 次）后仍不可用，则将该服务器宣告为不可达，同时激活备用代理服务器。

如果以后的轮询连续两次显示主要服务器已激活，ASA 将自动从备用服务器恢复到主要 云网络安全 代理服务器。使用 **retry-count** 命令可以更改此轮询间隔。

代理服务器不可到达的流量条件	服务器超时计算	连接超时结果
高流量	客户端半开连接超时 + ASA TCP 连接超时	(30 + 30) = 60 秒
单一连接失败	客户端半开连接超时 + ((重试阈值 - 1) x (ASA TCP 连接超时))	(30 + ((5-1) x (30)) = 150 秒
空闲 - 无连接时间超过	15 分钟 + ((重试阈值) x (ASA TCP 连接超时))	900 + (5 x (30) = 1050 秒

示例

以下示例配置主要和备用服务器：

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

server trust-point

要指定在 TLS 握手时提供的代理信任点证书，请在 TLS 服务器配置模式下使用 **server trust-point** 命令。

server trust-point *proxy_trustpoint*

语法说明

proxy_trustpoint	指定 **crypto ca trustpoint** 命令定义的信任点。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TLS-proxy 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

信任点可以自签、向证书颁发机构注册或来自导入的凭证。**server trust-point** 命令优先于全局 **ssl trust-point** 命令。

server trust-point 命令指定在 TLS 握手时提供的代理信任点证书。该证书必须由 ASA （身份证书）拥有。该证书可以是自签证书，由证书颁发机构注册，或来自导入的凭证。

为可以发起连接的每个实体创建 TLS 代理实例。发起 TLS 连接的实体为 TLS 客户端角色。由于 TLS 代理对客户端代理和服务器代理具有严格的定义，因此如果任一实体都可发起连接，则必须定义两个 TLS 代理实例。

注　在创建与电话代理一起使用的 TLS 代理实例时，服务器信任点是创建 CTL 文件实例的内部电话代理信任点。信任点名称的形式为 *internal_PP_<ctl-file_instance_name>*

示例

以下示例展示使用 **server trust-point** 命令指定在 TLS 握手时要提供的代理信任点证书：

```
ciscoasa(config-tlsp)# server trust-point ent_y_proxy
```

相关命令

命令	说明
client（TLS 代理）	为 TLS 代理实例配置信任点、密钥对和密码套件。
client trust-point	指定在 TLS 握手时要提供的代理信任点证书。
ssl trust-point	指定表示接口的 SSL 证书的证书信任点。
tls-proxy	配置 TLS 代理实例。

server-port

要配置主机的 AAA 服务器端口，请在 aaa 服务器主机模式下使用 **server-port** 命令。要删除指定的服务器端口，请使用此命令的 **no** 形式。

server-port *port-number*

no server-port *port-number*

语法说明

port-number	端口号的范围是 0-65535。

默认值

默认服务器端口如下：

- SDI—5500
- LDAP—389
- Kerberos—88
- NT—139
- TACACS+—49

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Aaa 服务器组	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例配置 SDI AAA 服务器 srvgrp1 使用服务器端口号 8888：

```
ciscoasa(config)# aaa-server srvgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
ciscoasa(config-aaa-server-host)# server-port 8888
```

相关命令

命令	说明
aaa-server host	配置主机特定的 AAA 服务器参数。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

server-separator

要指定作为邮件与 VPN 服务器名称间分隔符的字符，请在适用的邮件代理模式下使用 **server-separator** 命令。要恢复为默认的 “:”，请使用此命令的 no 形式。

server-separator {*symbol*}

no server-separator

语法说明

symbol	分隔邮件与 VPN 服务器名称的字符。选项包括 “@”(at)、“|”（竖线）、“:”（冒号）、“#”（井号）、“,”（逗号）和 “;”（分号）。

默认值

默认为 “@”(at)。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

服务器分隔符必须与名称分隔符不同。

示例

以下示例展示如何将竖线 (|) 作为 IMAP4S 的服务器分隔符：

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# server-separator |
```

相关命令

命令	说明
name-separator	分隔邮件与 VPN 用户名及密码。

server-type

要手动配置 LDAP 服务器型号，请在 aaa 服务器主机配置模式下使用 **server-type** 命令。ASA 支持以下服务器型号：

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server，前称 Sun ONE Directory Server
- 符合 LDAPv3 的通用 LDAP 目录服务器（无密码管理）

要禁用此命令，请使用此命令的 **no** 形式。

server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

no server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

语法说明

auto-detect	指定 ASA 通过自动检测确定 LDAP 服务器类型。
generic	指定 Sun 和 Microsoft LDAP 目录服务器以外的 LDAP v3 标准目录服务器。通用 LDAP 服务器不支持密码管理。
microsoft	指定 LDAP 服务器为 Microsoft Active Directory。
openldap	指定 LDAP 服务器为 OpenLDAP 服务器。
novell	指定 LDAP 服务器为 Novell 服务器。
sun	指定 LDAP 服务器为 Sun Microsystems JAVA System Directory Server。

默认值

默认情况下，自动检测会尝试确定服务器类型。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。
8.0(2)	添加了对 OpenLDAP 和 Novell 服务器类型的支持。

使用指南

ASA 支持 LDAP 版本 3，并且兼容 Sun Microsystems JAVA System Directory Server、Microsoft Active Directory 及其他 LDAPv3 目录服务器。

注

- Sun - 在 ASA 上配置用于访问 Sun 目录服务器的 DN 必须能够访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。也可以将 ACI 放入默认密码策略。
- Microsoft - 必须配置 SSL 上的 LDAP 以对 Microsoft Active Directory 启用密码管理。
- 通用 - 不支持密码管理功能。

默认情况下，ASA 自动检测其是否连接到 Microsoft 目录服务器、Sun LDAP 目录服务器或通用 LDAPv3 服务器。但是，如果自动检测无法确定 LDAP 服务器类型，并且您知道服务器是 Microsoft 或 Sun 服务器，则可使用 **server-type** 类型命令将服务器手动配置为 Microsoft 或 Sun Microsystems LDAP 服务器。

示例

以下示例在 aaa 服务器主机配置模式下输入，为 IP 地址为 10.10.0.1 的 LDAP 服务器 ldapsvr1 配置服务器类型。第一个示例配置 Sun Microsystems LDAP 服务器。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type sun
```

以下示例指定 ASA 使用自动检测确定服务器类型：

```
ciscoasa(config)# aaa-server ldapsvr1 protocol LDAP
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

相关命令

命令	说明
ldap-over-ssl	指定以 SSL 保护 LDAP 客户端 - 服务器连接。
sasl-mechanism	在 LDAP 客户端与服务器之间配置 SASL 身份验证。
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于将用户定义的属性名称映射到思科 LDAP 属性名称。

service

要对拒绝的 TCP 连接启用重置，请在全局配置模式下使用 **service** 命令。要禁用重置，请使用此命令的 **no** 形式。

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

service sw-reset-button

no service sw-reset-button

语法说明

interface *interface_name*	对指定的接口启用或禁用重置。
resetinbound	向所有尝试传输 ASA 但被 ASA 根据访问列表或 AAA 设置拒绝的入站 TCP 会话发送 TCP 重置。对于被访问列表或 AAA 允许、但不属于现有连接而被状态防火墙拒绝的数据包，ASA 也会发送重置。安全级别相同的接口之间的流量也会受影响。此选项未启用时，ASA 以静默方式丢弃被拒绝的数据包。如果不指定接口，此设置将应用于所有接口。
resetoutbound	向所有尝试传输 ASA 但被 ASA 根据访问列表或 AAA 设置拒绝的出站 TCP 会话发送 TCP 重置。对于被访问列表或 AAA 允许、但不属于现有连接而被状态防火墙拒绝的数据包，ASA 也会发送重置。安全级别相同的接口之间的流量也会受影响。此选项未启用时，ASA 以静默方式丢弃被拒绝的数据包。默认情况下，此选项启用。例如，您可能想在流量风暴期间禁用出站重置以减小 CPU 负载。
resetoutside	为终止于最不安全接口并且被 ASA 根据访问列表或 AAA 设置拒绝的 TCP 数据包启用重置。对于被访问列表或 AAA 允许、但不属于现有连接而被状态防火墙拒绝的数据包，ASA 也会发送重置。此选项未启用时，ASA 以静默方式丢弃被拒绝的数据包。建议对接口 PAT 使用 **resetoutside** 关键字。此关键字允许 ASA 终止来自外部 SMTP 或 FTP 服务器的 IDENT。主动重置这些连接可避免 30 秒超时延迟。
sw-reset-button	配置软件重置按钮。

默认值

默认情况下，**service resetoutbound** 对所有接口启用。**service sw-reset-button** 默认启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	添加了 **interface** 关键字和 **resetoutbound** 命令。

使用指南

如果需要重置身份请求 (IDENT) 连接，您可能要明确为入站流量发送重置。向拒绝的主机发送 TCP RST（TCP 报头中的重置标记）时，RST 将停止传入 IDENT 过程，这样您就不必等待 IDENT 超时。等待 IDENT 超时可能会导致流量减慢，因为外部主机在 IDENT 超时之前会继续重新传输 SYN，因此，**service resetinbound** 命令可提高性能。

示例

以下示例对内部接口以外的所有接口禁用出站重置：

```
ciscoasa(config)# no service resetoutbound
ciscoasa(config)# service resetoutbound interface inside
```

以下示例对 DMZ 接口以外的所有接口启用入站重置：

```
ciscoasa(config)# service resetinbound
ciscoasa(config)# no service resetinbound interface dmz
```

以下示例对终止于外部接口上的连接启用重置：

```
ciscoasa(config)# service resetoutside
```

相关命令

命令	说明
show running-config service	显示服务配置。

service (ctl-provider)

要指定证书信任列表提供程序侦听的端口，请在 CTL 提供程序配置模式下使用 **service** 命令。要删除配置，请使用此命令的 **no** 形式。

service port *listening_port*

no service port *listening_port*

语法说明

port *listening_port*	指定要导出到客户端的证书。

默认值

默认端口为 2444。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CTL 提供程序配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 CTL 提供程序配置模式下使用 **service** 命令指定 CTL 提供程序侦听的端口。该端口必须是集群中的 CallManager 服务器（在 CallManager 管理页面中的 Enterprise Parameters（企业参数）下配置）侦听的端口。默认端口为 2444。

示例

以下示例展示如何创建 CTL 提供程序实例：

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

相关命令

命令	说明
client	指定允许连接到 CTL 提供程序的客户端，以及用于客户端身份验证的用户名和密码。
ctl	解析来自 CTL 客户端的 CTL 文件并安装信任点。
ctl-provider	在 CTL 提供程序模式下配置 CTL 提供程序实例。

命令	说明
export	指定要导出至客户端的证书
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

service (object service)

要定义服务对象的协议和可选属性，请在对象服务配置模式下使用 **service** 命令。使用此命令的 **no** 形式可删除定义。

service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

no service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

语法说明

destination *operator number*	（可选）对 **tcp** 和 **udp** 协议，指定目标端口名称或 0 至 65535 的端口号。有关支持的名称列表，请参阅 CLI 帮助。运算符包括： • **eq** - 等于端口号。 • **gt** - 大于端口号。 • **lt** - 小于端口号。 • **neq** - 不等于端口号。 • **range** - 端口范围。指定两个用空格分隔的号码，例如 **range 1024 4500**。
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	指定该服务类型用于 ICMP 或 ICMP 版本 6 连接。您可以选择按名称或号码 (0-255) 指定 ICMP 类型。（有关可用的可选 ICMP 类型名称，请参阅 CLI 帮助。）如果指定类型，可以选择包含 ICMP 代码 (1-255)。
protocol	标识协议名称或号码 (0-255)。有关支持的名称列表，请参阅 CLI 帮助。
source *operator number*	（可选）对 **tcp** 和 **udp** 协议，指定源端口名称或 0 至 65535 的端口号。有关支持的名称列表，请参阅 CLI 帮助。运算符与 **destination** 相同。
tcp	指定该服务类型用于 TCP 连接。
udp	指定 UDP 连接的服务类型。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
对象服务配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。
9.0(1)	添加了对 ICMP 代码的支持。

使用指南

您可以在配置的其他部分按名称使用服务对象，例如 ACL（**access-list** 命令）和 NAT（**nat** 命令）。如果使用不同的协议和端口配置现有服务对象，新配置会将现有协议和端口替换为新协议和端口。

示例

以下示例展示如何为 SSH 流量创建服务对象：

```
ciscoasa(config)# service object SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
```

以下示例显示如何为 EIGRP 流量创建服务对象：

```
ciscoasa(config)# service object EIGRP
ciscoasa(config-service-object)# service eigrp
```

以下示例展示如何为从端口 0-1024 到 HTTPS 的流量创建服务对象：

```
ciscoasa(config)# service object HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
```

相关命令

命令	说明
clear configure object	清除所有已创建对象。
object-group service	配置服务对象。
show running-config object service	显示当前的服务对象配置。

service call-home

要启用 Call Home 服务，请在全局配置模式下使用 **service call-home** 命令。要禁用 Call Home 中继服务，请使用此命令的 **no** 形式。

service call-home

no service call-home

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，禁用 service Call Home 命令。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(2)	引入了此命令。

示例

以下示例展示如何启用 Call Home 服务：

```
ciscoasa(config)# service call-home
```

以下示例展示如何禁用 Call Home 服务：

```
hostname(config)# no service call-home
```

相关命令

命令	说明
call-home (global configuration)	进入 Call Home 配置模式。
call-home test	手动发送 Call Home 测试消息。
show call-home	显示 Call Home 配置信息。

service password-recovery

要启用密码恢复，请在全局配置模式下使用 **service password-recovery** 命令。要禁用密码恢复，请使用此命令的 **no** 形式。密码恢复默认启用，但您可能要将其禁用，以确保未授权的用户无法使用密码恢复机制来威胁 ASA。

service password-recovery

no service password-recovery

语法说明

此命令没有任何参数或关键字。

默认值

密码恢复默认启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在 ASA 5500 系列自适应安全设备上，如果您忘记了密码，可以在启动期间收到提示时按终端键盘上的 **Escape** 键，将 ASA 引导到 ROMMON。然后更改配置寄存器（请参阅 **config-register** 命令），将 ASA 设置为忽略启动配置。例如，如果您的配置寄存器是默认值 0x1，则输入 **confreg 0x41** 命令将该值更改为 0x41。在重新加载 ASA 后，它会加载默认配置，并且您可以使用默认密码进入特权 EXEC 模式。然后将启动配置复制到运行配置以加载它，并且重置密码。最后，将配置寄存器设置为原始设置，以将 ASA 设置为像以前一样启动。例如，在全局配置模式下输入 **config-register 0x1** 命令。

在 PIX 500 系列安全设备上，在启动期间收到提示时按终端键盘上的 **Escape** 键，将 ASA 引导到监控模式。然后将 PIX 密码工具下载到 ASA，这会清除所有密码和 **aaa authentication** 命令。

在 ASA 5500 系列自适应安全设备上，**no service password-recovery** 命令使用户在配置不变时无法进入 ROMMON。当用户进入 ROMMON 时，ASA 会提示清除所有闪存文件系统。用户不先执行此清除将无法进入 ROMMON。如果用户选择不清除闪存文件系统，ASA 将重新加载。因为密码恢复取决于使用 ROMMON 和维护现有配置，所以此清除使您无法恢复密码。但禁用密码恢复可防止未授权的用户查看配置或插入不同密码。在这种情况下，要将系统恢复到操作状态，需加载新的映像和备份配置文件（如果有）。配置文件中出现的 **service password-recovery** 命令仅供参考；当您在 CLI 提示符下输入命令时，设置将保存到 NVRAM 中。更改设置的唯一方法是在 CLI 提示符下输入命令。使用不同形式的命令加载新配置不会更改设置。如果在将 ASA 配置为启动时忽略启动配置（在准备密码恢复时）后禁用密码恢复，则 ASA 会将设置更改为像正常一样引导启动配置。如果使用故障切换，并且备用设备配置为忽略启动配置，则当 **no service password recovery** 命令复制到备用设备时，配置寄存器会发生相同的更改。

在 PIX 500 系列安全设备上，**no service password-recovery** 命令强制 PIX 密码工具提示用户清除所有闪存文件系统。用户不先执行此清除将无法使用 PIX 密码工具。如果用户选择不清除闪存文件系统，ASA 将重新加载。因为密码恢复取决于维护现有配置，所以此清除使您无法恢复密码。但禁用密码恢复可防止未授权的用户查看配置或插入不同密码。在这种情况下，要将系统恢复到操作状态，需加载新的映像和备份配置文件（如果有）。

示例

以下示例对 ASA 5500 系列禁用密码恢复：

```
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images. You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

ASA 5500 系列的以下示例展示在启动时何时进入 ROMMON，以及如何完成密码恢复操作。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
####################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
ciscoasa(config)# enable password NewPassword
ciscoasa(config)# config-register 0x1
```

相关命令

命令	说明
config-register	设置 ASA 在重新加载时忽略启动配置。
enable password	设置启用密码。
password	设置登录密码。

service-object

要将服务或服务对象添加到未预定义为 TCP、UDP 或 TCP-UDP 的服务对象组，请在对象组服务配置模式下使用 **service-object** 命令。要删除服务，请使用此命令的 **no** 形式。

service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*]
[**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

no service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*]
[**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

语法说明

destination *operator number*	（可选）对 **tcp**、**udp** 或 **tcp-udp** 协议，指定目标端口名称或 0 至 65535 的端口号。有关支持的名称列表，请参阅 CLI 帮助。运算符包括： • **eq** - 等于端口号。 • **gt** - 大于端口号。 • **lt** - 小于端口号。 • **neq** - 不等于端口号。 • **range** - 端口范围。指定两个用空格分隔的号码，例如 **range 1024 4500**。
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	指定该服务类型用于 ICMP 或 ICMP 版本 6 连接。您可以选择按名称或号码 (0-255) 指定 ICMP 类型。（有关可用的可选 ICMP 类型名称，请参阅 CLI 帮助。）如果指定类型，可以选择包含 ICMP 代码 (1-255)。
protocol	标识协议名称或号码 (0-255)。有关支持的名称列表，请参阅 CLI 帮助。
source *operator number*	（可选）对 **tcp**、**udp** 或 **tcp-udp** 协议，指定源端口名称或 0 至 65535 的端口号。有关支持的名称列表，请参阅 CLI 帮助。运算符与 **destination** 相同。
tcp	指定该服务类型用于 TCP 连接。
tcp-udp	指定服务类型用于 TCP 或 UDP 连接。
udp	指定 UDP 连接的服务类型。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
对象组服务配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(1)	引入了此命令。
8.3(1)	添加了 **object** 关键字（**object service** 命令）以支持服务对象。
9.0(1)	添加了对 ICMP 代码的支持。

使用指南

如果使用 **object-group service** 命令创建服务对象组，并且您没有为整个组预定义协议类型，则可使用 **service-object** 命令将多个服务和服务对象添加到不同协议组成的组，包括端口。使用 **object-group service** [**tcp** | **udp** | **tcp-udp**] 命令为特定协议类型创建服务对象组时，使用 **port-object** 命令只能标识该对象组的目标端口。

示例

以下示例显示如何将 TCP 和 UDP 服务添加到服务对象组：

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示如何将多个服务对象添加到服务对象组：

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh

hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp

hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https

ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object-group** 命令。
network-object	将网络对象添加到网络对象组。
object service	添加服务对象。
object-group	定义对象组以优化配置。
port-object	将端口对象添加到服务对象组。
show running-config object-group	显示当前对象组。

service sw-reset-button

要在 ASA 5506-X 和 ASA 5508-X 系列安全设备上启用重置按钮，请在全局配置模式下使用 **service sw-reset-button** 命令。要禁用重置按钮，请使用此命令的 **no** 形式。

service sw-reset-button

no service sw-reset-button

语法说明

此命令没有任何参数或关键字。

默认值

默认启用 **service sw-reset-button**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(2)	添加了此命令。

示例

以下示例启用软件重置按钮：

```
ciscoasa(config)# service sw-reset-button
ciscoasa# show sw-reset-button

Software Reset Button is configured.
```

以下示例禁用软件重置按钮：

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is not configured.
```

相关命令

命令	说明
show running-config service	显示服务配置。

service-policy (class)

要应用另一个映射策略下的分层策略映射，请在类配置模式下使用 **service-policy** 命令。要禁用服务策略，请使用此命令的 **no** 形式。分层策略仅当您要在整形流量的子集上执行优先队列时才适用于 QoS 流量整形。

service-policy *policymap_name*

no service-policy *policymap_name*

语法说明

policymap_name	指定您在 **policy-map** 命令中配置的策略映射名称。您只能指定包含 **priority** 命令的第 3/4 层策略映射。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。

使用指南

分层优先级队列用于您启用了流量整形队列的接口。整形流量的子集可得到优先处理。不使用标准优先级队列（**priority-queue** 命令）。

对于分层优先级队列，请使用模块化策略框架执行以下任务：

1. **class-map** - 标识用于执行优先级队列的流量。
2. **policy-map**（用于优先级队列）- 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **priority** - 为类映射启用优先级队列。如果要使用的是分层优先级队列，则您仅可在此策略映射中包括优先级命令。
3. **policy-map**（用于流量整形）- 标识与 **class-default** 类映射关联的操作。
   a. **class class-default** - 标识要在其上执行操作的 **class-default** 类映射。
   b. **shape** - 将流量整形应用于类映射中。
   c. **service-policy** - 调用您在其中配置 **priority** 命令的优先级队列策略映射，便于您可以将优先级队列应用于整形流量的子集中。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

示例

以下示例为外部接口上的所有流量启用流量整形，并且将优先处理 VPN tunnel-grp1 中 DSCP 位设置为 ef 的流量：

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

相关命令

命令	说明
class (policy-map)	标识策略映射的类映射。
clear configure service-policy	清除服务策略配置。
clear service-policy	清除服务策略统计信息。
policy-map	标识要对类映射执行的操作。
priority	启用优先级队列。
service-policy (global)	将策略映射应用到接口。
shape	启用流量整形。
show running-config service-policy	显示在运行配置中配置的服务策略。
show service-policy	显示服务策略统计信息。

service-policy (global)

要在所有接口或目标接口上全局激活策略映射，请在全局配置模式下使用 **service-policy** 命令。要禁用服务策略，请使用此命令的 **no** 形式。使用 **service-policy** 命令可在接口上启用一组策略。

service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

no service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

语法说明

fail-close	为不支持 IPv6 流量的应用检查所丢弃的 IPv6 流量生成系统日志 (767001)。默认情况下不生成系统日志。
global	将策略映射应用到所有接口。
interface *intf*	将策略映射应用到特定接口。
policymap_name	指定您在 **policy-map** 命令中配置的策略映射名称。您只能指定第 3/4 层策略映射，而不能指定检查策略映射 (**policy-map type inspect**)。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	添加了 **fail-close** 关键字。

使用指南

要启用服务策略，请使用模块化策略框架：

1. **class-map** - 标识用于执行优先级队列的流量。
2. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. *所支持功能的命令* - 对于给定的类映射，可以为各个功能配置多种操作，包括 QoS、应用检查、CSC 或 AIP SSM、TCP 和 UDP 连接限制以及超时和 TCP 规范化。有关每种功能可使用的命令的更多详细信息，请参阅 CLI 配置指南。
3. **service-policy** - 向接口分配策略映射或全局分配策略映射。

对于指定的功能，接口服务策略优先于全局服务策略。例如，如果您有使用检查的全局策略和使用 TCP 标准化的接口策略，则检查和 TCP 标准化都会应用到接口。但是，如果您有使用检查的全局策略和使用检查的接口策略，则只有接口策略检查应用到该接口。

默认情况下，配置包括与所有默认应用检查流量匹配的全局策略，并且将检查全局应用到流量。您仅能应用一个全局策略，因此如果想要改变全局策略，则需要编辑默认策略或禁用默认策略并应用新策略。

默认服务策略包括以下命令：

```
service-policy global_policy global
```

示例

以下示例展示如何在外部接口上启用 inbound_policy 策略映射：

```
ciscoasa(config)# service-policy inbound_policy interface outside
```

以下命令禁用默认全局策略，并在所有其他 ASA 接口上启用新策略 new_global_policy：

```
ciscoasa(config)# no service-policy global_policy global
ciscoasa(config)# service-policy new_global_policy global
```

相关命令

命令	说明
clear configure service-policy	清除服务策略配置。
clear service-policy	清除服务策略统计信息。
service-policy (class)	应用另一个策略映射下的分层策略。
show running-config service-policy	显示在运行配置中配置的服务策略。
show service-policy	显示服务策略统计信息。

会话

要建立从 ASA 到模块（例如 IPS SSP 或 CSC SSM）的 Telnet 会话以访问模块 CLI，请在特权 EXEC 模式下使用 **session** 命令。

session *id*

语法说明

id	指定模块 ID： • 物理模块 - **1**（表示插槽编号 1） • 软件模块 ASA FirePOWER- **sfr** • 软件模块 IPS - **ips** • 软件模块 ASA CX - **cxsc**

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.6(1)	添加了 IPS SSP 软件模块的 **ips** 模块 ID。
9.1(1)	添加了对 ASA CX 模块的支持（**cxsc** 关键字）。
9.2(1)	添加了对 ASA FirePOWER 模块的支持（**sfr** 关键字）。

使用指南

此命令仅在模块处于运行状态时才可用。有关状态信息，请参阅 **show module** 命令。

要结束会话，请输入 **exit** 或 **Ctrl-Shift-6**，然后按 **x** 键。

请注意，**session 1** 命令不适用于以下硬件模块：

- ASA CX
- ASA FirePOWER

示例

以下示例是到插槽 1 中模块的会话：

```
ciscoasa# session 1
Opening command session with slot 1.
Connected to slot 1.Escape character sequence is 'CTRL-^X'.
```

相关命令

命令	说明
debug session-command	显示会话的调试消息。

session console

要建立从 ASA 到软件模块（例如 IPS SSP 软件模块）的虚拟控制台会话，请在特权 EXEC 模式下使用 **session console** 命令。如果因控制台关闭而不能使用 **session** 命令建立 Telnet 会话，此命令可能非常有用。

session *id* **console**

语法说明

id	指定模块 ID： • ASA FirePOWER 模块 - **sfr** • IPS 模块 - **ips** • ASA CX 模块 - **cxsc**

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	添加了对 ASA CX 模块的支持（**cxsc** 关键字）。
9.2(1)	添加了对 ASA FirePOWER 模块的支持（**sfr** 关键字）。

使用指南

要结束会话，请输入 **Ctrl-Shift-6**，然后按 **x** 键。

当 **Ctrl-Shift-6, x** 是返回终端服务器提示的逸出序列时，请勿将此命令与该终端服务器一起使用。**Ctrl-Shift-6, x** 也是逸出模块并返回 ASA 提示的序列。因此，如果在这种情况下尝试退出模块控制台，您会一直退出至终端服务器提示。如果将终端服务器重新连接到 ASA，模块控制台会话仍处于活动状态；您无法再退出到 ASA 提示。必须使用直接串行连接将控制台返回到 ASA 提示。

改为使用 **session** 命令。

示例

以下示例创建到 IPS 模块的控制台会话：

```
ciscoasa# session ips console

Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips.Escape character sequence is 'CTRL-SHIFT-6 then x'.
```

```
sensor login: service
Password: test
```

相关命令

命令	说明
session	发起到模块的 Telnet 会话。
show module log console	显示控制台日志信息。

session do

要建立 Telnet 会话并执行从 ASA 到模块的命令，请在特权 EXEC 模式下使用 **session do** 命令。

session *id* **do** *command*

语法说明

id	指定模块 ID： • 物理模块 - **1**（表示插槽编号 1） • 软件模块 ASA FirePOWER- **sfr** • 软件模块 IPS - **ips** • 软件模块 ASA CX - **cxsc**
command	在模块上执行命令。支持的命令包括： • **setup host ip** *ip_address*/*mask*,*gateway_ip* - 设置管理 IP 地址和网关。 • **get-config** - 获取模块配置。 • **password-reset** - 将模块密码重置为默认值。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.1(1)	引入了此命令。
8.6(1)	添加了 IPS SSP 软件模块的 **ips** 模块 ID。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
9.2(1)	添加了对 ASA FirePOWER 模块的支持，包括 **sfr** 关键字。

使用指南

此命令仅在模块处于运行状态时才可用。有关状态信息，请参阅 **show module** 命令。

要结束会话，请输入 **exit** 或 **Ctrl-Shift-6**，然后按 **X** 键。

示例

以下示例将管理 IP 地址设置为 10.1.1.2/24，默认网关为 10.1.1.1：

```
ciscoasa# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

相关命令

命令	说明
debug session-command	显示会话的调试消息。

session ip

要配置模块（例如 IPS SSP 或 CSC SSM）的日志记录 IP 地址，请在特权 EXEC 模式下使用 **session ip** 命令。

session *id* **ip** {**address** *address mask* | **gateway** *address*}

语法说明

id	指定模块 ID： • 物理模块 - **1**（表示插槽编号 1） • 软件模块 IPS - **ips**
address *address*	设置系统日志服务器地址。
gateway *address*	设置系统日志服务器的网关。
mask	设置子网掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.1(1)	引入了此命令。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
8.6(1)	添加了 IPS SSP 软件模块的 **ips** 模块 ID。

使用指南

此命令仅在模块处于运行状态时才可用。有关状态信息，请参阅 **show module** 命令。

要结束会话，请输入 **exit** 或 **Ctrl-Shift-6**，然后按 **X** 键。

示例

以下示例是到插槽 1 中模块的会话：

```
ciscoasa# session 1 ip address
```

相关命令

命令	说明
debug session-command	显示会话的调试消息。

session-limit

设置并行 MDM 代理会话的最大数。用于 config-mdm-proxy 模式。此命令的 no 形式必须指定配置的限制。

session-limit *session-limit*

no session-limit *session-limit*

语法说明

session-limit	设置并行 MDM 会话的最大数。有效范围是 1 到 10000；默认值为 1000。

默认值

默认会话限制为 1000。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
config-mdm-proxy	• 是	—	• 是	—	—

命令历史

版本	修改
9.3(1)	为 MDM 代理服务引入了命令。

示例

以下示例展示会话限制对 MDM 代理服务设置为 5000。

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# session-limit 5000
```

相关命令

命令	说明
mdm-proxy	进入 config-mdm-proxy 模式并配置 MDM 代理服务。
show running-config mdm-proxy	查看当前的 MDM 代理配置。

session-timeout

设置 MDM 代理注册和签入会话的最长持续时间（秒）。用于 config-mdm-proxy 模式。此命令的 no 形式必须指定配置的超时。

session-timeout [enrollment *seconds***] [checkin** *seconds***]**

no session-timeout [enrollment *seconds***] [checkin** *seconds***]**

语法说明

seconds	MDM 注册和签入会话的最长持续时间（秒）。有效范围为 60 到 600。默认值为 300 秒。

默认值

默认会话超时为 300 秒。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
config-mdm-proxy	• 是	—	• 是	—	—

命令历史

版本	修改
9.3(1)	为 MDM 代理服务引入了命令。

示例

以下示例展示会话超时对 MDM 代理签入会话设为 600 秒：

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# session-timeout checkin 600
```

相关命令

命令	说明
mdm-proxy	进入 config-mdm-proxy 模式并配置 MDM 代理服务。
show running-config mdm-proxy	查看当前的 MDM 代理配置。

set as-path

要修改 BGP 路由的自主系统路径，请在路由映射配置模式下使用 **set as-path** 命令。不修改自主系统路径则使用此命令的 **no** 形式。

set as-path {**tag** | **prepend** *as-path-string*}

no set as-path {**tag** | **prepend** *as-path-string*}

语法说明

as-path-string	预置到 AS_PATH 属性之前的自主系统编号。此参数值的范围为 1 到 65535 的任何有效自主系统编号。可以输入多个值；最多可输入 10 个 AS。 有关自主系统编号格式的更多详情，请参阅 **router bgp** 命令。
prepend	将关键字 **prepend** 后的字符串附加到路由映射匹配的路由自主系统路径。适用于入站和出站 BGP 路由映射。
tag	将路由标记转换为自主系统路径。仅在将路由重分布到 BGP 中时适用。

默认值

不修改自主系统路径。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

唯一可影响最佳路径选择的全局 BGP 指标是自主系统路径长度。通过改变自主系统路径的长度，BGP 发言方可通过逐渐远离对等设备来影响最佳路径选择。

此命令的 **set as-path tag** 变种允许您将标记转换为自主系统路径，以修改自主系统长度。**set as-path prepend** 变种可让您将任意自主系统路径字符串 “ 附加 ” 到 BGP 路由。通常，本地自主系统编号会在前面预置多次，以增加自主系统路径长度。

4 字节的自主系统编号思科 /Cisco 实现使用 asplain - 例如 65538- 默认正则表达式匹配和输出显示自主系统编号的格式，但您可以配置 4 字节的自主系统编号 asplain 格式和 asdot 格式，在 RFC 5396 中所述。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后接 **clear bgp *** 命令来执行所有当前 BGP 会话的硬重置。

示例

以下示例将重分布路由的标记转换为自主系统路径：

```
ciscoasa(config)# route-map set-as-path-from-tag
ciscoasa(config-route-map)# set as-path tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute ospf 109 route-map set-as-path-from-tag
```

以下示例将 100 100 100 预置到向 10.108.1.1 通告的所有路由前面：

```
ciscoasa(config)# route-map set-as-path
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set as-path prepend 100 100 100
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 route-map set-as-path out
```

相关命令

命令	说明
clear bgp	使用硬重新配置或软重新配置重置 BGP 连接。
bgp asnotation dot	将边界网关协议 (BGP) 4 字节自主系统编号的默认显示和正则表达式匹配格式从 asplain 格式（十进制值）更改为点记法。

set automatic-tag

要自动计算标记值，请在路由映射配置模式下使用 set automatic-tag 命令。要禁用此功能，请使用此命令的 **no** 形式。

set automatic-tag

no set automatic-tag

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

如果要设置标记，必须有 match 子句（即使它指向 “ 允许所有内容 ”）。

使用 **route-map** 全局配置命令以及 match 和 set **route-map** 配置命令，定义将路由从一个路由协议重分布到另一个协议的条件。每条 **route-map** 命令都有关联的 match 和 set 命令列表。match 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。set 命令指定设置操作 - 在满足 match 命令实施的条件时要执行的特定重分布操作。no **route-map** 命令删除路由映射。

set **route-map** 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布设置操作。当所有匹配条件都满足时，将会执行所有设置操作。

示例

以下示例将思科 ASA 软件配置为自动计算边界网关协议 (BGP) 获知的路由的标记值：

```
ciscoasa(config-route-map)# route-map tag
ciscoasa(config-route-map)# match as-path 10
iscoasa(config-route-map)# set automatic-tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# table-map tag
```

set community

要设置 BGP 社区属性，请使用 **set community** 路由映射配置命令。要删除条目，请使用此命令的 **no** 形式。

set community {*community-number* [**additive**] | [*well-known-community*] [**additive**] | **none**}

no set community

语法说明

additive	（可选）将社区添加到现有社区。
community-number	指定社区编号。有效值为 1 到 4294967200、**no-export** 或 **no-advertise**。
none	（可选）从通过路由映射的前缀中删除社区属性。
well-known-community	（可选）使用以下关键字可指定已知社区： • **internet** • **local-as** • **no-advertise** • **no-export**

默认值

BGP 社区属性不存在。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

如果要设置标记，必须有 match 子句（即使它指向 “ 允许所有内容 ” 列表）。

使用 **route-map** 全局配置命令以及 **match** 和 **set** route map 配置命令可定义在不同路由协议之间重分布路由的条件。每条 **route-map** 命令都有关联的 **match** 和 **set** 命令列表。**match** 命令指定*匹配条件* - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定 *设置操作* - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。no **route-map** 命令删除路由映射。

set route map 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布 *设置操作*。当所有匹配条件都满足时，将会执行所有设置操作。

示例

在以下示例中，通过自主系统路径访问列表 1 的路由的社区设置为 109。通过自主系统路径访问列表 2 的路由的社区设置为 no-export（这些路由不会向任何外部 BGP [eBGP] 对等设备通告）。

```
ciscoasa(config-route-map)# set community 10
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set community 109
ciscoasa(config-route-map)# set community 20
ciscoasa(config-route-map)# match as-path 2
ciscoasa(config-route-map)# set community no-export
```

相关命令

命令	说明
match as-path	匹配由访问列表指定的 BGP 自主系统路径。

set connection

要为策略映射中的流量类指定连接限制，请在类配置模式下使用 **set connection** 命令。要删除这些指定，从而允许无限制连接，请使用此命令的 **no** 形式。

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

语法说明

conn-max *n*	设置允许的并发 TCP 和 UDP 连接最大数（0 至 2000000）。默认值为 0，允许无限制连接。例如，如果两部服务器配置为允许并发 TCP 和 / 或 UDP 连接，则连接限制分别应用到每部配置的服务器。在类下配置时，此参数会限制整个类允许的并发连接最大数。在这种情况下，一台攻击主机可能会占用所有连接，而该类下访问列表中匹配的所有其他主机都没有连接。
embryonic-conn-max *n*	设置允许的并发初期连接最大数（0 至 2000000）。默认值为 0，允许无限制连接。
per-client-embryonic-max *n*	设置每个客户端允许的并发初期连接最大数（0 至 2000000）。客户端定义为通过 ASA 发送初始连接数据包（建立新连接）的主机。如果同时使用 **access-list** 与 **class-map** 来匹配此功能的流量，将应用每个主机的初期限制，而不是与访问列表匹配的所有客户端的初期连接总数。默认值为 0，允许无限制连接。此关键字不适用于管理类映射。
per-client-max *n*	设置每个客户端允许的最大并发连接数（0 至 2000000）。客户端定义为通过 ASA 发送初始连接数据包（建立新连接）的主机。如果同时使用 **access-list** 与 **class-map** 来匹配此功能的流量，将应用每个主机的连接限制，而不是与访问列表匹配的所有客户端的连接总数。默认值为 0，允许无限制连接。此关键字不适用于管理类映射。在类下配置时，此关键字通过类下的访问列表限制匹配的每个主机允许的最大并发连接数。
random-sequence-number {**enable** | **disable**}	启用或禁用 TCP 序列号随机化。此关键字不适用于管理类映射。有关详细信息请参阅 “ 使用指南 ”。

默认值

对于 **conn-max**、**embryonic-conn-max**、**per-client-embryonic-max** 和 **per-client-max** 参数，*n* 的默认值为 0，这表示允许无限的连接。

默认启用序列号随机化。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	添加了 **per-client-embryonic-max** 和 **per-client-max** 关键字。
8.0(2)	此命令现在适用于第 3/4 层管理类映射，用于到 ASA 的管理流量。只有 **conn-max** 和 **embryonic-conn-max** 关键字可用。
9.0(1)	最大连接数从 65535 增加至 2000000。

使用指南

使用模块化策略框架配置此命令。先使用 **class-map** 命令（用于通过流量）或 **class-map type management** 命令（用于管理流量）定义要应用超时的流量。然后输入 **policy-map** 命令以定义策略，输入 **class** 命令以引用类映射。在类配置模式下，可以输入 **set connection** 命令。最后，将政策映射应用到接口使用**服务策略**的命令。有关模块化策略框架工作原理的详细信息，请参阅 CLI 配置指南。

注　根据 ASA 型号中 CPU 核心的数量，由于每个核心管理连接的方式不同，最大并发和初期连接数可能超过配置的数量。在最糟糕的情况下，ASA 最多允许 *n*-1 个额外连接和初期连接，其中 *n* 是核心数。例如，如果您的型号有 4 个核心，而您配置 6 个并发连接和 4 个初期连接，那么每个类型可能有 3 个额外连接。要确定您的型号的核心数，请输入 **show cpu core** 命令。

TCP 拦截概述

限制初期连接数可以保护您免受 DoS 攻击。ASA 使用每客户端限制和初期连接限制来触发 TCP 拦截，这可保护内部系统免受使用 TCP SYN 数据包对接口进行泛洪的 DoS 攻击。初期连接是源与目标之间尚未完成必要握手的连接请求。TCP 拦截使用 SYN cookie 算法防止 TCP SYN 泛洪攻击。SYN 泛洪攻击包括一系列 SYN 数据包，通常来自伪装的 IP 地址。SYN 数据包的持续泛滥将使服务器 SYN 队列始终充满，而无法处理连接请求。超过连接的初期连接阈值时，ASA 将作为服务器的代理，对客户端 SYN 请求生成 SYN-ACK 响应。当 ASA 收到来自客户端的 ACK 后，可以对客户端进行身份验证，并且允许连接到服务器。

TCP 序列随机化

每个 TCP 连接都有两个 ISN：一个由客户端生成，一个由服务器生成。ASA 随机化入站和出站方向的 TCP SYN 的 ISN。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

可根据需要禁用 TCP 初始序列号随机化。例如：

- 如果另一个在线防火墙也随机化初始序列号，则即使此操作不影响流量，两个防火墙也无需执行此操作。
- 如果您通过 ASA 使用 eBGP 多跳，并且 eBGP 对等设备在使用 MD5。随机化会中断 MD5 校验和。
- 您可以使用要求 ASA 不随机化连接序列号的 WAAS 设备。

示例

以下示例使用 **set connection** 命令将最大并发连接数配置为 256，并且禁用 TCP 序列号随机化：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
ciscoasa(config-pmap-c)#
```

您可以输入此命令并加入多个参数，也可以将每个参数输入为单独的命令。ASA 将这些命令组合到运行配置中的一行。例如，如果在类配置模式中输入了以下两个命令：

```
ciscoasa(config-pmap-c)# set connection conn-max 600
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map 命令的输出将在一个组合命令中显示两个命令的结果：

```
set connection conn-max 600 embryonic-conn-max 50
```

相关命令

命令	说明
class	指定用于流量分类的类映射。
clear configure policy-map	删除所有策略映射配置，正用于 service-policy 命令中的策略映射除外。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config policy-map	显示所有当前策略映射配置。
show service-policy	显示服务策略配置。使用 **set connection** 关键字查看包含 **set connection** 命令的策略。

set connection advanced-options

要定制 TCP 标准化，请在类配置模式下使用 **set connection advanced-options** 命令。要删除 TCP 标准化选项，请使用此命令的 **no** 形式。

set connection advanced-options *tcp_mapname*

no set connection advanced-options *tcp_mapname*

语法说明

tcp_mapname	**tcp-map** 命令创建的 TCP 映射的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使用 TCP 映射定制 TCP 标准化，请使用模块化策略框架：

1. **tcp-map** - 标识 TCP 标准化操作。
2. **class-map** - 标识要对其执行 TCP 标准化操作的流量。
3. **policy-map** - 标识与类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced options** - 将 TCP 映射应用到类映射。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

示例

以下示例展示使用 **set connection advanced-options** 命令来指定 TCP 映射 localmap 的使用：

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# tcp-map localmap
ciscoasa(config)# policy-map global_policy global
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
```

```
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection advanced-options localmap
ciscoasa(config-pmap-c)#
```

相关命令

命令	说明
class	指定用于流量分类的类映射。
class-map	在类映射配置模式下，发出最多一个（tunnel-group 和 default-inspection-traffic 除外）match 命令，指定匹配条件，以配置流量类。
clear configure policy-map	删除所有策略映射配置，除非策略映射正在 service-policy 命令中使用，此时无法删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config policy-map	显示所有当前的策略映射配置。
tcp-map	创建 TCP 映射。

set connection advanced-options tcp-state-bypass

要启用 TCP 状态旁路，请在类配置模式下使用 **set connection advanced-options** 命令。类配置模式可从策略映射配置模式访问。要禁用 TCP 状态旁路，请使用此命令的 **no** 形式。

set connection advanced-options tcp-state-bypass

no set connection advanced-options tcp-state-bypass

语法说明

此命令没有任何参数或关键字。

默认值

默认禁用 TCP 状态旁路。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

要启用 TCP 状态旁路，请使用模块化策略框架：

1. **class-map** - 标识要对其执行 TCP 状态旁路的流量。
2. **policy-map** - 标识与类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced options tcp-state-bypass** - 将 TCP 状态旁路应用到类映射。
3. **service-policy** - 向接口分配策略映射或全局分配策略映射。

允许出站和入站流量通过单独的设备

默认情况下，所有经过 ASA 的流量都会使用自适应安全算法检查，并根据安全策略允许通过或予以丢弃。ASA 通过检查每个数据包的状态（这是新连接还是现有连接？）并将其分配到会话管理路径（新连接 SYN 数据包）、快速路径（现有连接）或控制平面路径（高级检查），最大程度地提高防火墙性能。

匹配快速路径中现有连接的 TCP 数据包，不重新检查安全策略的每个方面即可通过 ASA。此功能可最大程度地提高性能。但是，使用 SYN 数据包在快速路径中建立会话的方法，以及在快速路径中进行的检查（例如 TCP 序列号），可能会阻碍非对称路由解决方案：出站和入站连接流必须通过同一 ASA。

例如，新连接接入 ASA 1。SYN 数据包通过会话管理路径，而且连接的条目添加到快速路径表中。如果此连接的后续数据包通过 ASA 1，这些数据包将与快速路径中的条目进行匹配，然后通过。但是，如果后续数据包前往 ASA 2，其中没有经过管理会话路径的 SYN 数据包，快速路径中也没有连接的对应条目，数据包将被丢弃。

如果在上游路由器中配置了非对称路由，且流量在两个 ASA 之间交替，则可以为特定流量配置 TCP 状态旁路。TCP 状态旁路将改变会话在快速路径中建立的方式，并且禁用快速路径检查。此功能处理 TCP 流量与处理 UDP 连接几乎一样：当与指定网络匹配的非 SYN 数据包进入 ASA，并且没有快速路径条目时，这些数据包将通过会话管理路径，在快速路径中建立连接。流量到达快速路径后，将绕过快速路径检查。

不支持的功能

使用 TCP 状态旁路时不支持以下功能：

- 应用检查 - 应用检查需要入站和出站流量通过同一 ASA，因此使用 TCP 状态旁路时不支持应用检查。
- AAA 验证的会话 - 当用户向一个 ASA 进行身份验证时，经由另一个 ASA 返回的流量将被拒绝，因为用户未向该 ASA 做身份验证。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - ASA 不跟踪连接的状态，因此这些功能不适用。
- TCP 标准化 - 禁用 TCP 规范器。
- SSM 功能 - 不能使用 TCP 状态旁路和 SSM 上运行的任何应用，例如 IPS 或 CSC。

NAT 指南

由于转换会话单独为每个 ASA 建立，因此请确保在两个 ASA 上为 TCP 状态旁路流量配置静态 NAT ；如果使用动态 NAT，为 ASA 1 上的会话选择的地址，将不同于为 ASA 2 上的会话中选择的地址。

连接超时指南

如果指定的连接上在 2 分钟内没有流量，则连接超时。您可以使用 **set connection timeout tcp** 命令覆盖此默认值。一般的 TCP 连接超时默认为 60 分钟。

示例

以下是 TCP 状态旁路的示例配置：

```
ciscoasa(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map tcp_bypass
ciscoasa(config-cmap)# description "TCP traffic that bypasses stateful firewall"
ciscoasa(config-cmap)# match access-list tcp_bypass

ciscoasa(config-cmap)# policy-map tcp_bypass_policy
ciscoasa(config-pmap)# class tcp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options tcp-state-bypass

ciscoasa(config-pmap-c)# service-policy tcp_bypass_policy outside
```

相关命令

命令	说明
class	标识策略映射中的类映射。
class-map	创建用于服务策略的类映射。
policy-map	配置用于关联类映射与一项或多项操作的策略映射。
service-policy	将策略映射分配到接口。
set connection timeout	设置连接超时。

set connection decrement-ttl

要减小策略映射中某流量类的生存时间值，请在类配置模式下使用 **set connection decrement-ttl** 命令。若不想减少生存时间，请使用此命令的 **no** 形式。

set connection decrement-ttl

no set connection decrement-ttl

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，ASA 不减少生存时间。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(2)	引入了此命令。

使用指南

需要使用此命令及 **icmp unreachable** 命令，才允许经过 ASA（它将 ASA 显示为其中一个跃点）的跟踪路由。

示例

以下示例用于减少生存时间并设置 ICMP 不可达速率限制：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

相关命令

命令	说明
class	指定要用于流量分类的类映射。
icmp unreachable	控制允许 ICMP 不可达通过 ASA 的速率。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config policy-map	显示所有当前策略映射配置。
show service-policy	显示服务策略配置。

set connection timeout

要为策略映射中的流量类指定连接超时，请在类配置模式下使用 **set connection timeout** 命令。要删除超时，请使用此命令的 **no** 形式。

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

语法说明

dcd	启用中断连接检测 (DCD)。DCD 可检测中断的连接并允许其过期，但不让仍在处理流量的连接过期。如果想不操作但又保持连接有效，可以配置 DCD。在 TCP 连接超时后，ASA 将发送 DCD 探测到终端主机，确定连接的有效性。如果有一端主机在最大重试次数后未响应，ASA 便会释放该连接。如果两端主机响应连接有效，ASA 会将活动超时更新为当前时间，并相应地重新安排空闲超时。
embryonic *hh*:*mm*:*ss*	设置在 TCP 初期（半开）连接关闭之前的超时时间，范围是 0:0:5 到 1193:0:0。默认值为 0:0:30。您也可以将此值设为 0，这表示连接永不超时。三向握手未完成时的 TCP 连接即为初期连接。
half-closed *hh*:*mm*:*ss*	设置在半闭连接关闭之前的空闲超时时间，范围是 0:5:0（适用于 9.1(1) 及更低版本）或 0:0:30（适用于 9.1(2) 及更高版本）到 1193:0:0。默认值为 0:10:0。您也可以将此值设为 0，这表示连接永不超时。半闭连接不受 DCD 影响。此外，ASA 在压倒半闭连接时不发送重置。
idle *hh*:*mm*:*ss*	设置在任何协议的现有连接关闭后的空闲超时时间。有效范围是 0:0:1 到 1193:0:0。
max_retries	设置在宣告连接中断之前 DCD 的连续失败尝试次数。最小值为 1，最大值为 255。默认值为 5。
reset	（仅适用于 TCP 流量）在空闲连接删除后发送 TCP RST 数据到两端系统。
retry_interval	每个 DCD 探测无响应后再发送另一个探测之前等待的时间（*hh*:*mm*:*ss* 格式），范围是 0:0:1 到 24:0:0。默认值为 0:0:15。

默认值

除非使用 timeout 命令全局更改默认值，否则默认值为：

- 默认 **embryonic** 超时为 30 秒。
- 默认 **half-closed** 空闲超时为 10 分钟。
- 默认 **dcd** *max_retries* 值为 5。
- 默认 **dcd** *retry_interval* 值为 15 秒。
- 默认 **idle** 超时为 1 小时。
- 默认 **udp** 空闲超时为 2 分钟。
- 默认 **icmp** 空闲超时为 2 秒。
- 默认 **esp** 和 **ha** 空闲超时为 30 秒。
- 对于所有其他协议，默认空闲超时为 2 分钟。
- 要想永不超时，请输入 0:0:0。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	增加了对 DCD 的支持。
8.2(2)	为支持 **idle** 关键字（控制所有协议的空闲超时），废弃了 **tcp** 关键字。
9.1(2)	**half-closed** 最小值已降至 30 秒 (0:0:30)。

使用指南

使用模块化策略框架配置此命令。先使用 **class-map** 命令定义要应用超时的流量。然后输入 **policy-map** 命令以定义策略，输入 **class** 命令以引用类映射。在类配置模式下，您可以输入 **set connection timeout** 命令。最后，将政策映射应用到接口使用**服务策略**的命令。有关模块化策略框架工作原理的详细信息，请参阅 CLI 配置指南。

show service-policy 命令包含计数器，用以显示 DCD 的活动量。

示例

以下示例设置所有流量的连接超时：

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# policy-map CONNS
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
ciscoasa(config-pmap-c)# service-policy CONNS interface outside
```

您可以输入 **set connection** 命令并加入多个参数，也可以将每个参数输入为单独的命令。ASA 将这些命令组合到运行配置中的一行。例如，如果在类配置模式中输入了以下两个命令：

```
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0
ciscoasa(config-pmap-c)# set connection timeout embryonic 0:40:0
```

show running-config policy-map 命令的输出将在以下一个组合命令中显示两个命令的结果：

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

相关命令

命令	说明
class	指定用于流量分类的类映射。
clear configure policy-map	删除所有策略映射配置，除非策略映射正在 service-policy 命令中使用，此时无法删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
set connection	配置连接值。

命令	说明
show running-config policy-map	显示所有当前的策略映射配置。
show service-policy	显示用于 DCD 及其他服务活动的计数器。

set local-preference

要指定自主系统路径的首选项值，请在路由映射配置模式下合适 set local-preference 命令。要删除条目，请使用此命令的 **no** 形式。

set local-preference *number-value*

no set local-preference *number-value*

语法说明

number-value	首选项值。从 0 到 4294967295 的整数。

默认值

首选项值为 100。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

首选项只发送到本地自主系统中的所有路由器。

使用 **route-map** 全局配置命令以及 match 和 set **route-map** 配置命令，定义将路由从一个路由协议重分布到另一个协议的条件。每条 **route-map** 命令都有关联的 match 和 set 命令列表。match 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。set 命令指定设置操作 - 在满足 match 命令实施的条件时要执行的特定重分布操作。no **route-map** 命令删除路由映射。

set **route-map** 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布设置操作。当所有匹配条件都满足时，将会执行所有设置操作。

您可以使用 **bgp default local-preference** 命令更改默认首选项值。

示例

以下示例将包含在访问列表 1 中所有路由的本地首选项设为 100：

```
ciscoasa(config-route-map)# route-map map-preference
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

set metric

要为路由映射中的 OSPF 及其他动态路由协议设置路由指标值，请在路由映射配置模式下使用 **set metric** 命令。要恢复 OSPF 及其他动态路由协议的默认指标值，请使用此命令的 **no** 形式。

set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

no set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

语法说明

bandwidth	路由的 EIGRP 带宽 (kbps)。有效值范围为 0 到 4294967295。
delay	EIGRP 路由延迟（十微秒）。有效值范围为 0 到 4294967295。
loading	路由的有效 EIGRP 带宽，表示为 0 至 255 的数字。值 255 表示 100% 负载。
metric-value	OSPF 及其他动态路由协议（EIGRP 除外）的路由指标值，表示为数字。有效值范围为 0 到 4294967295。
mtu	用于 EIGRP 的路由的最小 MTU（字节）。有效值范围为 0 到 4294967295。
reliability	EIGRP 的数据包传输成功的可能性，表示为 0 到 255 的数字。255 表示 100% 可靠； 0 表示不可靠。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(5)	添加了 *bandwidth*、*delay*、*reliability*、*loading* 和 *mtu* 参数，以支持路由映射中的 EIGRP。
9.0(1)	支持多情景模式。

使用指南

no set metric 命令可用于恢复 OSPF 及其他动态路由协议的默认指标值。在此情景下，*metric-value* 参数是 0 到 4294967295 的整数。

示例

以下示例展示如何配置 OSPF 路由的路由映射：

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
```

```
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

以下示例展示如何设置路由映射中 EIGRP 的指标值：

```
ciscoasa(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# route-map rmap permit 10
ciscoasa(config-route-map)# set metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。

设置指标（BGP、OSPF、RIP）

要设置路由协议的指标值，请在路由映射配置模式下使用 **set metric** 命令。要恢复默认指标值，请使用此命令的 **no** 形式。

set metric *metric-value*

no set metric

语法说明

metric-value	指标值或带宽（KB/ 秒）； 0 到 4294967295 的整数值。此参数适用于除增强型内部网关路由协议 (EIGRP) 外的所有路由协议。

默认值

动态获知的指标值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

建议在更改默认值之前咨询您的思科技术支持代表。

使用 **route-map** 全局配置命令以及 **match** 和 **set** route-map 配置命令，定义将路由从一个路由协议重分布到另一个协议的条件。每条 **route-map** 命令都有关联的 **match** 和 **set** 命令列表。**match** 命令指定*匹配条件* - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定*设置操作* - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。no **route-map** 命令删除路由映射。

set route-map 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布*设置操作*。当所有匹配条件都满足时，将会执行所有设置操作。

示例

以下示例将路由协议的指标值设置为 100：

```
ciscoasa(config-route-map)# route-map set-metric 100
ciscoasa(config-route-map)# set metric 100
```

set metric-type

要指定 OSPF 指标路由的类型，请在路由映射配置模式下使用 **set metric-type** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

set metric-type{**type-1** | **type-2**}

no set metric-type

语法说明

type-1	指定某指定自主系统外部的 OSPF 指标路由类型。
type-2	指定某指定自主系统外部的 OSPF 指标路由类型。

默认值

默认值为 **type-2**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下示例展示如何配置 OSPF 路由的路由映射：

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# set metric-type type-2
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
ciscoasa(config-route-map)# exit
ciscoasa(config)#
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

set metric-type internal

要将前缀上向外部 BGP (eBGP) 邻居通告的多出口标识符 (MED) 值设置为匹配下一跃点的内部网关协议 (IGP) 指标，请在路由映射配置模式下使用 **set metric-type internal** 命令。要恢复默认值，请使用此命令的 **no** 形式。

set metric-type internal

no set metric-type internal

语法说明

此命令没有任何参数或关键字。

命令默认

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

此命令将导致 BGP 通告与关联路由下一跃点的 IGP 指标对应的 MED 值。此命令适用于生成的内部 BGP (iBGP) 和 eBGP 派生的路由。

如果使用此命令，通用自主系统中的多个 BGP 发言方可以通告特定前缀的不同 MED 值。另请注意，如果 IGP 指标改变，BGP 将每隔 10 分钟重新通告一次路由。

使用 **route-map** 全局配置命令以及 **match** 和 **set** route-map 配置命令，定义将路由从一个路由协议重分布到另一个协议的条件。每条 **route-map** 命令都有关联的 **match** 和 **set** 命令列表。**match** 命令指定*匹配条件* - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定*设置操作* - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。**no route-map** 命令删除路由映射。

set route-map 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布*设置操作*。当所有匹配条件都满足时，将会执行所有设置操作。

注　此命令不支持将路由重分布到边界网关协议 (BGP)。

示例

在以下示例中，所有通告路由到邻居 172.16.2.3 的 MED 值设置为下一跃点的对应 IGP 指标：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 172.16.0.0
ciscoasa(config-router-af)# neighbor 172.16.2.3 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.2.3 route-map setMED out
ciscoasa(config-route-map)# route-map setMED permit 10
ciscoasa(config-route-map)# match as-path as-path-acl
ciscoasa(config-route-map)# set metric-type internal
ciscoasa(config-route-map)# ip as-path access-list as-path-acl permit .*
```

set ip next-hop BGP

要指示在哪里输出为策略路由传递路由映射 match 子句的数据包，请在路由映射配置模式下使用 **set ip next-hop** 命令。要删除条目，请使用此命令的 **no** 形式。

set ip next-hop *ip-address* [*... ip-address*] [**peer-address]**

no set ip next-hop *ip-address* [*... ip-address*] **[peer-address]**

语法说明

ip-address	输出数据包的下一跃点的 IP 地址。它不需要邻接路由器。
peer-address	（可选）设置要成为 BGP 对等地址的下一跃点。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

命令语法中的省略号 (...) 表示命令输入可以包含多个 *ip-address* 参数值。

使用 **ip policy route-map** 接口配置命令、**route-map** 全局配置命令和以及 **match** 和 **set** 路由映射配置命令定义策略路由数据包的条件。**ip policy route-map** 命令按名称标识路由映射。每条 **route-map** 命令都有关联的 **match** 和 **set** 命令列表。**match** 命令指定*匹配条件* - 策略路由发生的条件。**set** 命令指定*设置操作* - 在满足 **match** 命令实施的条件时要执行的特定路由操作。

如果使用 **set next-hop** 命令指定的第一个下一跃点已关闭，则会尝试选择性指定的 IP 地址。

当 **set next-hop** 命令与 **peer-address** 关键字一起用于 BGP 对等设备的入站路由映射中时，收到的匹配路由的下一跃点将设置为邻接对等地址，覆盖任何第三方下一跃点。因此，同一路由映射可应用到多个 BGP 对等设备以覆盖第三方下一跃点。

当 **set next-hop** 命令与 **peer-address** 关键字一起用于 BGP 对等设备的出站路由映射中时，通告的匹配路由的下一跃点将设置为本地路由器的对等地址，从而禁用下一跃点计算。**set next-hop** 命令的粒度超过（每个邻接设备）**neighbor next-hop-self** 命令，因为您可以为某些路由设置下一跃点，而不为另一些路由设置。**neighbor next-hop-self** 命令将设置发送到该邻接设备的所有路由的下一跃点。

set 子句可以互相配合使用。它们按以下顺序接受评估：

1. **set next-hop**
2. **set interface**

3. **set default next-hop**
4. **set default interface**

注　为避免反射路由的常见配置错误，请不要在要应用到 BGP 路由反射器客户端的路由映射中使用 **set next-hop** 命令。

示例

在以下示例中，三台路由器处于同一个 LAN 中（IP 地址分别为 10.1.1.1、10.1.1.2 和 10.1.1.3）。每台路由器都在不同的自主系统中。**set ip next-hop peer-address** 命令指定，从远程自主系统 100 中路由器 (10.1.1.1) 到远程自主系统 300 中路由器 (10.1.1.3)、与路由映射匹配的流量，将通过路由器 bgp 200 发送，而不是通过其与 LAN 的相互连接直接发送到自主系统 100 中的路由器 (10.1.1.1)。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.1.1.3 remote-as 300
ciscoasa(config-router-af)# neighbor 10.1.1.3 route-map set-peer-address out
ciscoasa(config-router-af)# neighbor 10.1.1.1 remote-as 100
ciscoasa(config-route-af)# route-map set-peer-address permit 10
ciscoasa(config-route-map)# set ip next-hop peer-address
```

set origin (BGP)

要设置 BGP 源代码，请在路由映射配置模式下使用 **set origin** 命令。要删除条目，请使用此命令的 **no** 形式。

set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

no set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

语法说明

autonomous-system-number	远程自主系统编号。 此参数值的范围为 1 到 65535 的任何有效自主系统编号。
egp	本地外部网关协议 (EGP) 系统。
igp	远程内部网关协议 (IGP) 系统。
incomplete	传承的未知语法。

默认值

路由的起点基于主要 IP 路由表中路由的路径信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

如果要设置路由的起点，必须有 match 子句（即使它指向 “ 允许所有内容 ” 列表）。使用此命令设置当路由重分布到 BGP 时的具体起点。重分布路由时，起点通常记录为不完整，在 BGP 表中 使用 ? 标识。

使用 **route-map** 全局配置命令以及 **match** 和 **set** route-map 配置命令，定义将路由从一个路由协议重分布到另一个协议的条件。每条 **route-map** 命令都有关联的 **match** 和 **set** 命令列表。**match** 命令指定*匹配条件* - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定*设置操作* - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。**no route-map** 命令删除路由映射。

set route-map 配置命令指定当满足路由映射的所有匹配条件时要执行的重分布*设置操作*。当所有匹配条件都满足时，将会执行所有设置操作。

示例

以下示例将通过路由映射到 IGP 的路由起点：

```
ciscoasa(config-route-map)# route-map set_origin
ciscoasa(config-route-map)# match as-path 10
ciscoasa(config-route-map)# set origin igp
```

set weight

要指定路由表的 BGP 权重，请在路由映射配置模式下使用 **set weight** 命令。要删除条目，请使用此命令的 **no** 形式。

set weight *number*

no set weight *number*

语法说明

number	权重值。可以是从 0 到 65535 的整数。

默认值

权重不因指定的路由映射而更改。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由映射配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

实施的权重基于第一个匹配的自主系统路径。自主系统路径匹配时指定的权重将覆盖全局 **neighbor** 命令分配的权重。也就是说，使用 **set weight** 路由映射配置命令分配的权重将覆盖使用 **neighbor weight** 命令分配的权重。

示例

以下示例将匹配自主系统路径访问列表的路由的 BGP 权重设置为 200：

```
ciscoasa(config-route-map)# route-map set-weight
ciscoasa(config-route-map)# match as-path as_path_acl
iscoasa(config-route-map)# set weight 200
```

setup

要为使用交互式提示的 ASA 配置最低配置，请在全局配置模式下输入 **setup** 命令。

setup

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	在 ASA 5510 和更高版本的路由模式中，配置的接口现在是管理*插槽 / 端口*接口，而不是 “ 内部 ” 接口。对于 ASA 5505，配置的接口是 VLAN 1 接口，也不是 “ 内部 ” 接口。
9.0(1)	更改了默认配置提示，使用 Ctrl+Z 可退出设置过程。

使用指南

如果闪存中没有启动配置，开机时会自动出现设置提示。

setup 命令通过最低配置提示您建立 ASDM 连接。此命令专为没有配置或只有部分配置的设备而设计。如果您的产品型号支持出厂默认配置，我们建议使用出厂默认配置而不使用 **setup** 命令（要恢复默认配置，请使用 **configure factory-default** 命令）。

setup 命令需要称为 “management” 的已命名接口。

当您输入 **setup** 命令时，您需要使用表 1-1 中的信息。如果列出的参数已有配置，将会出现在方括号中，您可以将其作为默认值或输入新值覆盖它。可用的准确提示可能根据型号而有所不同。系统 **setup** 命令包括上面一部分提示。

表 1-1　　设置提示

提示符	说明
`Pre-configure Firewall now through interactive prompts [yes]?`	输入 **yes** 或 **no**。如果输入 **yes**，则设置继续。如果输入 **no**，则设置停止，并且出现全局配置提示 (ciscoasa(config)#)。
`Firewall Mode [Routed]:`	输入 **routed** 或 **transparent**。

表 1-1　设置提示（续）

Enable password:	输入启用密码。（密码必须至少有三个字符。）
Allow password recovery [yes]?	输入 **yes** 或 **no**。
Clock (UTC):	在此字段不可输入任何内容。默认使用 UTC 时间。
Year:	使用四位数输入年份，例如 2005。年范围为 1993 至 2035。
Month:	输入月份名称的前三个字符，例如，**Sep** 表示 9 月。
Day:	输入月日期，从 1 到 31。
Time:	输入 24 小时制的时、分、秒，例如，输入 **20:54:44** 表示晚上 8 时 54 分 44 秒。
Host name:	输入要在命令行提示符中显示的主机名。
Domain name:	输入 ASA 所在网络的域名。
IP address of host running Device Manager:	输入需要访问 ASDM 的主机的 IP 地址。
Use this configuration and save to flash (yes)?	输入 **yes** 或 **no**。如果输入 **yes**，将会启用内部接口，并且将请求的配置写入闪存分区。 如果输入 **no**，设置提示将重复出现，从第一个问题开始： `Pre-configure Firewall now through interactive prompts [yes]?` 输入 **Ctrl + Z** 退出设置，输入 **yes** 则重复提示。

示例

以下示例展示如何完成 **setup** 命令：

```
ciscoasa(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

相关命令

命令	说明
配置出厂默认设置	恢复默认配置。

sfr

要将流量重新定向到 ASA FirePOWER 模块，请在类配置模式下使用 **sfr** 命令。要删除重新定向，请使用此命令的 **no** 形式。

sfr {**fail-close** | **fail-open**} [**monitor-only**]

no sfr {**fail-close** | **fail-open**} [**monitor-only**]

语法说明

fail-close	设置 ASA 在模块不可用时阻止流量。
fail-open	将 ASA 设置为允许流量通过，仅当模块不可用时才应用 ASA 策略。
monitor-only	将流量的只读副本发送到模块，例如被动模式。如果没有包含关键字，流量将以内联模式发送。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

可以先输入 policy-map 命令来访问类配置模式。

在 ASA 上配置 **sfr** 命令前后，使用 FireSIGHT 管理中心 在模块上配置安全策略。

要配置 **sfr** 命令，必须配置 **class-map** 命令、**policy-map** 命令和 **class** 命令。

交通流量

ASA FirePOWER 模块从 ASA 运行独立的应用。但是将其集成到 ASA 流量。当您对 ASA 上的流量类应用 **sfr** 命令时，流量会以下列方式通过 ASA 和模块：

1. 流量进入 ASA。
2. 流入 VPN 流量被解密。
3. 应用防火墙策略。
4. 流量通过背板发送到 ASA FirePOWER 模块。
5. 模块将对流量应用其安全策略并采取适当的措施。
6. 在内联模式下，有效的流量通过背板发送回 ASA；ASA FirePOWER 模块可能会根据其安全策略阻止某些流量，该流量无法通过。在被动模式下不会返回流量，模块也不能阻止流量。

7. 流出 VPN 流量被加密。
8. 流量退出 ASA。

与 ASA 功能的兼容性

ASA 带有诸多高级应用检查功能，其中包括 HTTP 检查。但是，ASA FirePOWER 模块比 ASA 提供了更高级的 HTTP 检查，以及适用于其他应用的其他功能，包括监测和控制应用的使用情况。

要充分利用 ASA FirePOWER 模块的功能，请参阅以下与您发送到 ASA FirePOWER 模块的流量有关的指导原则：

- 请勿对 HTTP 流量配置 ASA 检查。
- 请勿配置云网络安全 (ScanSafe) 检查。如果为同一流量配置了 ASA FirePOWER 检查和云网络安全检查，ASA 只执行 ASA FirePOWER 检查。
- ASA 的其他应用检查（包括默认检查）与 ASA FirePOWER 模块兼容。
- 请勿启用移动用户安全 (MUS) 服务器；此服务器与 ASA FirePOWER 模块不兼容。
- 如果启用故障切换，则当 ASA 进行故障切换时，所有现有 ASA FirePOWER 流将传输到新的 ASA。新 ASA 中的 ASA FirePOWER 从该点开始检查流量；旧检查状态不会传输。

Monitor-Only 模式

仅监控模式下的流量与内联模式下相同。唯一的区别是 ASA FirePOWER 模块不将流量传回 ASA， 而是对流量应用安全策略，如果是在内联模式下操作，还会让您知道已对其执行的操作，例如，在某些事件中流量可能被标记为 “ 已丢弃 ”。您可以使用这些信息来分析流量，帮助您确定内联模式是否合适。

注　在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许一种安全策略。在多情景模式下，对某些情景无法配置仅监控模式，另一些情景则无法配置正常的内联模式。

示例

以下示例将所有 HTTP 流量转移到 ASA FirePOWER 模块，并且在模块因任何原因出现故障时阻止所有 HTTP 流量：

```
ciscoasa(config)# access-list ASASFR permit tcp any any eq port 80
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list ASASFR
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-close
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

以下示例中将去往 10.1.1.0 网络及 10.2.1.0 网络的所有 IP 流量将转移到 ASA FirePOWER 模块，并且在模块因任何原因出现故障时允许所有流量通过。

```
ciscoasa(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list my-sfr-acl
ciscoasa(config)# class-map my-sfr-class2
ciscoasa(config-cmap)# match access-list my-sfr-acl2
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap)# class my-sfr-class2
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)# service-policy my-sfr-policy interface outside
```

相关命令

命令	说明
class	指定要用于流量分类的类映射。
class-map	标识策略映射中使用的流量。
hw-module module reload	重新加载模块。
hw-module module reset	执行重置，然后重新加载模块。
hw-module module shutdown	关闭模块。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show asp table classify domain sfr	显示为将流量发送到 ASA FirePOWER 模块而创建的 NP 规则。
show module	显示模块状态。
show running-config policy-map	显示所有当前策略映射配置。
show service-policy	显示服务策略统计信息。
sw-module module sfr reload	重新加载软件模块。
sw-module module sfr reset	重置软件模块。
sw-module module sfr recover	安装软件模块引导映像。
sw-module module sfr shutdown	关闭软件模块。

shape

要启用 QoS 流量整形，请在类配置模式下使用 **shape** 命令。如果您有高速传输数据包的设备，例如使用快速以太网的 ASA，但它连接到低速设备，例如电缆调制解调器，则电缆调制解调器是导致数据包被频繁丢弃的瓶颈。要管理具有不同线路速率的网络，可将 ASA 配置为以较慢的固定速率传输数据包，这称为*流量整形*。要删除此配置，请使用此命令的 **no** 形式。

注　只有 ASA 5505、5510、5520、5540 和 5550 才支持流量整形。多核模式（例如 ASA 5500-X）不支持整形。

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

语法说明

average *rate*	设置流量在某个固定时间段的平均速率，以位 / 秒为单位，范围是 64000 到 154400000。指定 8000 的倍数值。有关如何计算时间段的详细信息，请参阅 “ 使用指南 ” 部分。
burst_size	设置在某个固定时间段可以传输的平均突发大小，以位为单位，范围是 2048 到 154400000。指定 128 的倍数值。如果不指定 *burst_size*，默认值等于指定平均速率下 4 毫秒的流量。例如，如果平均速率为 1000000 位 / 秒，4 毫秒的流量 = 1000000 * 4/1000 = 4000。

默认值

如果不指定 *burst_size*，默认值等于指定平均速率下 4 毫秒的流量。例如，如果平均速率为 1000000 位 / 秒，4 毫秒的流量 = 1000000 * 4/1000 = 4000。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。

使用指南

要启用流量整形，请使用模块化策略框架：

1. **policy-map** - 标识与 **class-default** 类映射关联的操作。
   a. **class class-default** - 标识要在其上执行操作的 **class-default** 类映射。
   b. **shape** - 将流量整形应用于类映射中。
   c. （可选）**service-policy** - 调用不同的策略，其中您配置了 **priority** 命令，可将优先级队列应用到一部分整形流量。
2. **service-policy** - 向接口分配策略映射或全局分配策略映射。

流量整形概述

流量整形用于匹配设备和链路速度，从而控制可能导致抖动和延迟的数据包丢失、可变延迟及链路饱和。

- 必须将流量整形应用到物理接口（如果是 ASA 5505，则应用到 VLAN）上的所有输出流量。您无法为特定类型的流量配置流量整形。
- 当数据包准备在接口上传输时实施流量整形，因此，速率计算基于要传输的数据包实际大小，包括所有可能的开销，例如 IPsec 报头和 L2 报头。
- 成形的流量包括通过机箱和来自机箱的流量。
- 整形速率计算基于标准令牌桶算法。令牌桶大小是突发大小值的两倍。有关令牌桶的详细信息，请参阅 CLI 配置指南。
- 当突发流量超过指定的整形速率时，数据包将会排队，稍后再发送。以下是关于整形队列的一些特性（有关分层优先级队列的信息，请参阅 **priority** 命令）：
  - 队列大小根据整形速率计算。假设是 1500 字节的数据包，队列可以容纳 200 毫秒的整形速率流量。最小队列大小是 64。
  - 达到队列限制时，后面传入的数据包将被丢弃。
  - 但某些关键的保持数据包（如 OSPF Hello 数据包）永丢弃。
  - 时间间隔使用 *time_interval* = *burst_size* / *average_rate* 计算。时间间隔越大，整形流量的突发大小就可能越大，链路空闲时间也可能越长。通过下面这个夸张的示例很容易理解这种影响：

    平均速率 = 1000000

    突发大小 = 1000000

    在上面的示例中，时间间隔为 1 秒，这意味着，在 100 Mbps FE 链路上，1 秒间隔的前 10 毫秒可能突发 1 Mbps 的流量，而剩余的 990 毫秒处于空闲状态，在下一个时间间隔之前不能发送任何数据包。因此，如果有对延迟敏感的流量（如语音流量），应减小突发流量大小（相比于平均速率），从而缩短时间间隔。

QoS 功能的交互方式

如果 ASA 需要，您可以单独配置每个服务质量功能。但是，您通常可在 ASA 上配置多个服务质量功能，便于设置一些流量的优先级（示例），并阻止其他流量引发带宽问题。

请参阅每个接口的以下支持功能组合：

- 标准优先级队列（用于特定流量）+ 策略（用于其余流量）。

  您无法配置同一流量集的优先级队列和策略。
- 流量整形（用于接口上的所有流量）+ 分层优先级队列（用于流量的子集）。

不可为同一接口配置流量整形和标准优先级队列；只允许分层优先级队列。例如，如果为全局策略配置标准优先队列，然后为特定接口配置流量整形，则后面配置的功能将被拒绝，因为全局策略与接口策略重叠。

通常，如果启用流量整形，则您无需再为同一流量启用策略，不过 ASA 不会限制您进行此配置。

示例

以下示例为外部接口上的所有流量启用流量整形，并且将优先处理 VPN tunnel-grp1 中 DSCP 位设置为 ef 的流量：

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef
```

```
ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

相关命令

命令	说明
class	在策略映射中标识要对其执行操作的类映射。
police	启用 QoS 策略。
policy-map	在服务策略中标识要应用到流量的操作。
priority	启用 QoS 优先级队列。
service-policy (class)	应用分级策略映射。
service-policy (global)	将服务策略应用于接口。
show service-policy	显示 QoS 统计数据。

第 2 章

show aaa kerberos 至 show asdm sessions 命令

show aaa kerberos

要显示 ASA 上缓存的所有 Kerberos 票证，请在 webvpn 配置模式下使用 **show aaa kerberos** 命令。

show aaa kerberos [**username** *user* | **host** *ip* | *hostname*]

语法说明

host	指定您要查看的特定主机。
hostname	指定主机名。
ip	指定主机的 IP 地址。
username	指定您要查看的特定用户。

默认值

此命令不存在默认值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

在 webvpn 配置模式下使用 **show aaa kerberos** 命令可查看 ASA 上缓存的所有 Kerberos 票证。**username** 和 **host** 关键字用于查看特定用户或主机的 Kerberos 票证。

示例

以下示例展示 **show aaa kerberos** 命令的用法：

```
ciscoasa(config)# show aaa kerberos

Default Principal      Valid Starting Expires        Service Principal
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00 asa$/mycompany.com@example.com
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00
http/owa.mycompany.com@example.com
```

相关命令

命令	说明
clear aaa kerberos	清除 ASA 上缓存的所有 Kerberos 票证。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

show aaa local user

要显示当前锁定的用户名列表或显示用户名的详细信息，请在全局配置模式下使用 **show aaa local user** 命令。

show aaa local user [locked]

语法说明

locked	（可选）显示当前锁定的用户名列表。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果忽略可选关键字 **locked**，ASA 将显示所有 AAA 本地用户的失败尝试和锁定状态详细信息。

您可以使用 **username** 选项指定单个用户或使用 **all** 选项指定全部用户。

此命令仅影响被锁定用户的状态。

管理员无法被设备锁定。

示例

以下示例展示使用 **show aaa local user** 命令显示所有用户名的锁定状态：

此示例展示在限制设置为 5 后，如何使用 **show aaa local user** 命令显示所有 AAA 本地用户的失败身份验证尝试次数和锁定状态详细信息：

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
ciscoasa(config)#
```

此示例展示在限制设置为 5 后，如何使用 **show aaa local user** 命令及 **lockout** 关键字只显示已锁定 AAA 本地用户的失败身份验证尝试次数和锁定状态详细信息：

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
ciscoasa(config)#
```

相关命令

命令	说明
aaa local authentication attempts max-fail	配置用户在被锁定之前可以输入错误密码的最大次数。
clear aaa local user fail-attempts	将失败尝试次数重置为 0 而不修改锁定状态。
clear aaa local user lockout	清除指定用户或所有用户的锁定状态，并将其失败的尝试次数计数器设置为 0。

show aaa-server

要显示 AAA 服务器的 AAA 服务器统计信息，请在特权 EXEC 模式下使用 **show aaa-server** 命令。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

语法说明

LOCAL	（可选）显示 LOCAL 用户数据库的统计信息。
groupname	（可选）显示组中服务器的统计信息。
host *hostname*	（可选）显示组中特定服务器的统计信息。
protocol *protocol*	（可选）显示以下指定协议的服务器统计信息： • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

默认值

默认显示所有 AAA 服务器统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	添加了 http 形式的协议。
8.0(2)	服务器状态显示是否使用 **aaa-server active** 命令或 **fail** 命令手动更改了状态。

示例

以下是 **show aaa-server** 命令的输出示例：

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE.Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
```

```
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

下表显示 **show aaa-server** 命令的字段说明：

字段	说明
Server Group	**aaa-server** 命令指定的服务器组名称。
Server Protocol	**aaa-server** 命令指定的服务器组的服务器协议。
Server Address	AAA 服务器的 IP 地址。
Server port	ASA 和 AAA 服务器使用的通信端口。您可以使用 **authentication-port** 命令指定 RADIUS 身份验证端口。您可以使用 **accounting-port** 命令指定 RADIUS 记账端口。对于非 RADIUS 服务器，该端口由 **server-port** 命令设置。
Server status	服务器的状态。将出现以下值之一： • ACTIVE - ASA 将与此 AAA 服务器通信。 • FAILED - ASA 无法与 AAA 服务器通信。根据配置的策略，处于此状态的服务器将保持该状态一段时间，然后重新激活。 如果状态后接 “(admin initiated)”，则表示服务器是使用 **aaa-server active** 命令或 **fail** 命令手动重新激活或设置成失败的。 最后一个事务的日期和时间使用以下形式显示： **Last transaction ({success | failure}) at** *time timezone date* 如果 ASA 从未与服务器通信，该消息显示如下： **Last transaction at Unknown**
Number of pending requests	仍在进行中的请求数。
Average round trip time	完成与服务器的事务所需的平均时间。
Number of authentication requests	ASA 发送的身份验证请求数。此值不包括在超时之后的重新传输。
Number of authorization requests	授权请求数。此值是指源于以下项的授权请求：命令授权、通过机箱流量的授权（对于 TACACS+ 服务器）、为隧道组启用的 WebVPN 和 IPsec 授权功能。此值不包括在超时之后的重新传输。
Number of accounting requests	记账请求数。此值不包括在超时之后的重新传输。
Number of retransmissions	在内部超时后重新传输消息的次数。此值仅适用于 Kerberos 和 RADIUS 服务器 (UDP)。
Number of accepts	成功的身份验证请求数。

字段	说明
Number of rejects	拒绝的请求数。此值包括错误情况以及来自 AAA 服务器的真实凭证拒绝。
Number of challenges	AAA 服务器在收到初始用户名和密码信息后要求提供其他信息的次数。
Number of malformed responses	不适用。已保留供将来使用。
Number of bad authenticators	以下情况出现的次数： • RADIUS 数据包中的 “authenticator” 字符串已损坏（很少发生）。 • ASA 上的共享密钥与 RADIUS 服务器上的不匹配。要解决此问题，请输入正确的服务器密钥。 此值仅适用于 RADIUS。
Number of timeouts	ASA 检测到 AAA 服务器未响应或行为错误并已宣布其离线的次数。
Number of unrecognized responses	ASA 从 AAA 服务器收到它无法标识或支持的响应的次数。例如，来自服务器的 RADIUS 数据包代码是 “access-accept”、“access-reject”、“access-challenge” 或 “accounting-response” 以外的未知类型。通常情况下，这意味着来自服务器的 RADIUS 响应数据包已损坏，但这种情况很少出现。

相关命令

命令	说明
show running-config aaa-server	为指定的服务器组中的所有服务器或特定服务器显示统计信息。
clear aaa-server statistics	清除 AAA 服务器统计信息。

show access-list

要显示访问列表的命中计数器和时间戳值，请在特权 EXEC 模式下使用 **show access-list** 命令。

show access-list *id_1* [*...*[*id_2*]] [**brief**]

语法说明

brief	（可选）显示访问列表标识符、命中计数以及最后规则命中的时间戳，全部采用十六进制格式。
id_1	用于标识现有访问列表的名称或一组字符。
id_2	（可选）用于标识现有访问列表的名称或一组字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了对 **brief** 关键字的支持。
8.3(1)	修改了用于显示 ACL 时间戳的 ACE 显示样式。

使用指南

您可以在一个命令中输入访问列表标识符，一次显示多个访问列表。

您可以指定 **brief** 关键字，以十六进制格式显示访问列表命中数、标识符和时间戳信息。以十六进制格式显示配置标识符分三列显示，与系统日志 106023 和 106100 中使用的标识符相同。

集群指导原则

使用 ASA 集群时，由于集群管理逻辑的作用，如果其中一台设备收到流量，其他设备仍可能显示 ACL 的命中计数。这是预期行为。由于未直接从客户端收到任何数据包的设备可能会收到通过所有者请求的集群控制链路转发的数据包，因此，该设备在将数据包发回接收设备之前，可能会检查 ACL。因此，即使设备未传递流量，ACL 命中计数也会增加。

示例

以下示例以十六进制格式显示指定访问策略的简短信息（命中计数不是零的 ACE）。前两列以十六进制格式显示标识符，第三列显示命中计数，第四列显示时间戳值（也是十六进制格式）。命中计数值代表流量命中规则的次数。时间戳值报告最后一次命中的时间。如果命中计数为零，则不会显示任何信息。

以下是 **show access-list** 命令的输出示例，显示访问列表名称 “test”，该访问列表在外部接口上以 “IN” 方向应用：

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

以下是 **object-group-search** 组未启用时 **show access-list** 命令的输出示例：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

以下是 **object-group-search** 组启用时 **show access-list** 命令的输出示例：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

以下是 Telnet 流量通过时 **show access-list brief** 命令的输出示例：

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
```

以下是 SSH 流量通过时 **show access-list brief** 命令的输出示例：

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158 44ae5901 00000001 4a68aaa9
```

以下是 **show access-list** 命令的输出示例，显示访问列表名称 “test”，该访问列表在外部接口上以 “IN” 方向应用，而且 ACL 优化已启用：

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq ssh
(hitcnt=1) 0x3666f922
```

以下是 Telnet 流量通过时 **show access-list brief** 命令的输出示例：

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

以下是 SSH 流量通过时 **show access-list brief** 命令的输出示例：

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

相关命令

命令	说明
access-list ethertype	配置根据其 EtherType 控制流量的访问列表。
access-list extended	向配置添加访问列表并通过防火墙配置 IP 流量的策略。
clear access-list	清除访问列表计数器。
clear configure access-list	从运行配置中清除访问列表。
show running-config access-list	显示当前正在运行的访问列表配置。

show activation-key

要显示永久许可证、活动的时效性许可证和运行的许可证（永久许可证和活动的时效性许可证组合），请在特权 EXEC 模式下使用 **show activation-key** 命令。对于故障切换设备，此命令还显示“故障切换集群”许可证（主要和辅助设备的组合密钥）。

show activation-key [detail]

语法说明

detail	显示非活动的时效性许可证。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(4)	添加了 **detail** 关键字。
8.2(1)	修改了输出，其中包含额外许可信息。
8.3(1)	输出现在显示某功能使用永久还是时效性密钥，以及时效性密钥的使用时长。它还显示所有已安装的时效性密钥（活动和非活动）。
8.4(1)	支持无负载加密型号。

使用指南

有些永久许可证会在激活后要求您重新加载 ASA。表 2-1 列出了需要重新加载的许可证。

表 2-1　永久许可证重新加载要求

型号	要求重新加载的许可证操作
所有型号	降级加密许可证。
ASAv	降级 vCPU 许可证。

如果需要重新加载，则 **show activation-key** 的输出如下：

```
The flash activation key is DIFFERENT from the running key.

The flash activation key takes effect after the next reload.
```

如果您有无负载加密型号，则在查看许可证时，VPN 和 Unified Communications 许可证不会列出。

示例

示例 2-1　独立设备使用 show activation-key 命令时的输出

以下是独立设备使用 **show activation-key** 命令时的输出，显示运行的许可证（组合永久许可证和时效性许可证）以及每个活动的时效性许可证：

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

示例 2-2　独立设备使用 show activation-key detail 时的输出

以下是独立设备使用 **show activation-key detail** 命令时的输出，显示运行的许可证（组合永久许可证和时效性许可证），以及永久许可证和每个已安装的时效性许可证（活动和非活动）：

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Standby perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Enabled        39 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5505 Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces   : 8              perpetual
VLANs                         : 20             DMZ Unrestricted
Dual ISPs                     : Enabled        perpetual
VLAN Trunk Ports              : 8              perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Standby perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Enabled        39 days
Intercompany Media Engine     : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                   : 25     7 days
```

示例 2-3　故障切换对中主要设备使用 show activation-key detail 时的输出

以下是对主要故障切换设备使用 **show activation-key detail** 命令时的输出示例，显示：

- 主要设备许可证（组合永久许可证和时效性许可证）。
- “故障切换集群”许可证（主要和辅助设备中的组合许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主要和辅助许可证组合的值以粗体显示。
- 主要设备永久许可证。
- 主要设备安装的时效性许可证（活动和非活动）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
```

```
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

示例 2-4　故障切换对中辅助设备使用 show activation-key detail 时的输出

以下是对辅助故障切换设备使用 **show activation-key detail** 命令时的输出示例，显示：

- 辅助设备许可证（组合永久许可证和时效性许可证）。
- “ 故障切换集群 ” 许可证（主要和辅助设备中的组合许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主要和辅助许可证组合的值以粗体显示。
- 辅助设备永久许可证。
- 辅助设备安装的时效性许可证（活动和非活动）。此设备没有任何时效性许可证，因此此输出示例未显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
```

```
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

示例 2-5　没有许可证的 ASAv 独立设备使用 show activation-key 时的输出

部署了 1 个 vCPU 的 ASAv 的以下输出显示空白激活密钥、未许可状态以及一条表示安装 1 个 vCPU 许可证的消息。

注 命令输出显示“This platform has an ASAv VPN Premium license.”。此消息表明，ASAv 可以执行负载加密；它不提及 ASAv 标准与 高级许可证。

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

示例 2-6　有 4 个 vCPU 标准许可证的 ASAv 独立设备使用 show activation-key 时的输出

注 命令输出显示“This platform has an ASAv VPN Premium license.”。此消息表明，ASAv 可以执行负载加密；它不提及 ASAv 标准与 高级许可证。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
```

```
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 2-7　有 4 个 vCPU 高级许可证的 ASAv 独立设备使用 show activation-key 时的输出

注 命令输出显示“This platform has an ASAv VPN Premium license.”。此消息表明，ASAv 可以执行负载加密；它不提及 ASAv 标准与 高级许可证。

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
```

```
This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

示例 2-8　故障切换对中的 ASA 服务模块 主要设备使用 show activation-key 时的输出

以下是对主要故障切换设备使用 **show activation-key** 命令时的输出示例，显示：

- 主要设备许可证（组合永久许可证和时效性许可证）。
- “ 故障切换集群 ” 许可证（主要和辅助设备中的组合许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主要和辅助许可证组合的值以粗体显示。
- 主要设备安装的时效性许可证（活动和非活动）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

示例 2-9　故障切换对中的 ASA 服务模块 辅助设备使用 show activation-key 时的输出

以下是对辅助故障切换设备使用 **show activation-key** 命令时的输出示例，显示：

- 辅助设备许可证（组合永久许可证和时效性许可证）。
- “ 故障切换集群 ” 许可证（主要和辅助设备中的组合许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主要和辅助许可证组合的值以粗体显示。

- 辅助设备安装的时效性许可证（活动和非活动）。此设备没有任何时效性许可证，因此此输出示例未显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 2-10　集群使用 show activation-key 时的输出

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
```

```
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

相关命令 Serial

命令	说明
activation-key	更改激活密钥。

show ad-groups

要显示 Active Directory 服务器上列出的组，请在特权 EXEC 模式下使用 **show ad-groups** 命令：

show ad-groups *name* **[filter** *string***]**

语法说明

name	要查看的 Active Directory 服务器组的名称。
string	引号中指定要搜索的全部或部分组名称的字符串。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC 模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

show ad-groups 命令仅适用于使用 LDAP 协议来检索组的 Active Directory 服务器。使用此命令显示可用于动态访问策略 AAA 选择条件的 AD 组。

当 LDAP 属性类型 = LDAP 时，ASA 等待服务器响应的默认时间为 10 秒。您可以在 aaa 服务器主机配置模式下使用 **group-search-timeout** 命令调整此时间。

注　如果 Active Directory 服务器有大量的组，**show ad-groups** 命令的输出可能会根据服务器可放入响应数据包的数据量限制而截断。为避免此问题，可使用 **filter** 选项减少服务器报告的组数量。

示例

```
ciscoasa# show ad-groups LDAP-AD17
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
```

```
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

下一个示例展示使用 **filter** 选项的相同命令：

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter “Eng”
.
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

相关命令

命令	说明
ldap-group-base-dn	指定服务器在 Active Directory 的层次结构的哪个级别开始搜索动态组策略所使用的组。
group-search-timeout	调整 ASA 为一系列组等待 Active Directory 服务器响应的时间。

show admin-context

要显示当前指定为管理情景的情景名称，请在特权 EXEC 模式下使用 **show admin-context** 命令。

show admin-context

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show admin-context** 命令的输出示例： 以下示例展示名为 “admin” 并且存储在闪存根目录中的管理情景：

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

相关命令

命令	说明
admin-context	设置管理情景。
changeto	在情景或系统执行空间之间切换。
clear configure context	删除所有情景。
mode	将情景模式设置为单个或多个。
show context	显示情景列表（系统执行空间）或有关当前情景的信息。

show arp

要查看 ARP 表，请在特权 EXEC 模式下使用 **show arp** 命令。

show arp

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(8)/7.2(4)/8.0(4)	为显示添加了动态 ARP 时限。

使用指南

显示输出会显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。静态 ARP 条目以短划线 (-) 取代时限，代理 ARP 条目则显示 “ 别名 ”。

示例

以下是 **show arp** 命令的输出示例： 第一个条目是时限为 2 秒的动态条目。第二个条目是静态条目，第三个条目来自代理 ARP。

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config arp	显示 ARP 超时的当前配置。

show arp-inspection

要查看每个接口的 ARP 检查设置，请在特权 EXEC 模式下使用 **show arp-inspection** 命令。

show arp-inspection

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	—	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show arp-inspection** 命令的输出示例：

```
ciscoasa# show arp-inspection
interface               arp-inspection         miss
-----------------------------------------------------
inside1                 enabled                flood
outside                 disabled                -
```

miss 列显示在 ARP 检查启用后要对非匹配数据包采取的默认操作（“ 泛洪 ” 或 “ 无泛洪 ”）。

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config arp	显示 ARP 超时的当前配置。

show arp statistics

要查看 ARP 统计信息，请在特权 EXEC 模式下使用 show arp statistics 命令。

show arp statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show arp statistics** 命令的输出示例：

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 2-2 显示每个字段的说明。

表 2-2　show arp statistics 字段

字段	说明
Number of ARP entries	ARP 表条目的总数。
Dropped blocks in ARP	当 IP 地址解析为其相应的硬件地址时丢弃的块数。
Maximum queued blocks	在等待 IP 地址被解析时曾排入 ARP 模块队列的最大块数。
Queued blocks	当前排入 ARP 模块队列的块数。

表 2-2　show arp statistics 字段（续）

字段	说明
Interface collision ARPs received	所有 ASA 接口上收到的 IP 地址与 ASA 接口 IP 地址相同的 ARP 数据包数量。
ARP-defense gratuitous ARPs sent	由 ASA 作为 ARP 防御机制一部分发送的自然 ARP 数。
Total ARP retries	当地址在对第一个 ARP 请求的响应中未解析时由 ARP 模块发送的 ARP 请求总数。
Unresolved hosts	其 ARP 请求仍由 ARP 模块发出的未解析主机数。
Maximum unresolved hosts	自上次清除或 ASA 启动后曾在 ARP 模块中的未解析主数最大数。

相关命令

命令	说明
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
clear arp statistics	清除 ARP 统计信息，并将值重置为零。
show arp	显示 ARP 表。
show running-config arp	显示 ARP 超时的当前配置。

show asdm history

要显示 ASDM 历史记录缓冲区的内容，请在特权 EXEC 模式下使用 **show asdm history** 命令。

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

语法说明

asdmclient	（可选）显示针对 ASDM 客户端格式化的 ASDM 历史数据。
feature *feature*	（可选）将历史记录显示限制于指定的功能。以下是 *feature* 参数的有效值： • **all** - 显示所有功能的历史记录（默认值）。 • **blocks** - 显示系统缓冲区的历史记录。 • **cpu** - 显示 CPU 使用情况的历史记录。 • **failover** - 显示故障切换的历史记录。 • **ids** - 显示 IDS 的历史记录。 • **interface** *if_name* - 显示指定接口的历史记录。*if_name* 参数是 **nameif** 命令指定的接口名称。 • **memory** - 显示内存使用历史记录。 • **perfmon** - 显示性能历史记录。 • **sas** - 显示安全关联的历史记录。 • **tunnels** - 显示隧道的历史记录。 • **xlates** - 显示转换插槽历史记录。
snapshot	（可选）只显示最后一个 ASDM 历史记录数据点。
view *timeframe*	（可选）将历史记录显示限制于指定的时间段。*timeframe* 参数的有效值包括： • **all** - 历史记录缓冲区中的所有内容（默认值）。 • **12h** - 12 小时 • **5d** - 5 天 • **60m** - 60 分钟 • **10m** - 10 分钟

默认值

如果未指定任何参数或关键字，将显示所有功能的所有历史记录信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	此命令已从 **show pdm history** 改为 **show asdm history**。

使用指南

show asdm history 命令显示 ASDM 历史记录缓冲区的内容。必须先使用 **asdm history enable** 命令启用 ASDM 历史记录跟踪，然后才可查看 ASDM 历史记录信息。

示例

以下是 **show asdm history** 命令的输出示例： 它将输出限制于最近 10 分钟收集的外部接口数据。

```
ciscoasa# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

以下是 **show asdm history** 命令的输出示例：像上一个示例一样，它将输出限制于最近 10 分钟收集的外部接口数据。但在此示例中，输出已针对 ASDM 客户端格式化。

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|6
2469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|6
2553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|6
2636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|6
2723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|2
5026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|2
5102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|2
5169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|2
5381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750
|750|750|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|7
51|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753
|753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|5
5|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|5
5|55|55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|4
381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|5
401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698
|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349
|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|33
49|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|5
|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|7|
6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|3750
10|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|375
395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|37
5794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|3
76200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
```

```
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|1
28|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
ciscoasa#
```

以下是使用 **snapshot** 关键字的 **show asdm history** 命令的输出示例：

```
ciscoasa# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
```

```
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
```

```
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

相关命令

命令	说明
asdm history enable	启用 ASDM 历史记录跟踪。

show asdm image

要显示当前 ASDM 软件映像文件，请在特权 EXEC 模式下使用 show **asdm image** 命令。

show asdm image

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	此命令已从 **show pdm image** 改为 **show asdm image**。

示例

以下是 **show asdm image** 命令的输出示例：

```
ciscoasa# show asdm image

Device Manager image file, flash:/ASDM
```

相关命令

命令	说明
asdm image	指定当前的 ASDM 映像文件。

show asdm log_sessions

要显示活动 ASDM 日志记录会话及其相关会话 ID 的列表，请在特权 EXEC 模式下使用 **show asdm log_sessions** 命令。

show asdm log_sessions

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

每个活动 ASDM 会话有一个或多个关联 ASDM 日志记录会话。ASDM 使用日志记录会话从 ASA 检索系统日志消息。每个 ASDM 日志记录会话都分配有唯一的会话 ID。您可以使用此会话 ID 及 **asdm disconnect log_session** 命令来终止指定的会话。

注　因为每个 ASDM 会话至少有一个 ASDM 日志记录会话，所以 **show asdm sessions** 和 **show asdm log_sessions** 的输出可能相同。

示例

以下是 **show asdm log_sessions** 命令的输出示例：

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

相关命令

命令	说明
asdm disconnect log_session	终止活动的 ASDM 日志记录会话。

show asdm sessions

要显示活动 ASDM 会话及其相关会话 ID 的列表，请在特权 EXEC 模式下使用 **show asdm sessions** 命令。

show asdm sessions

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	此命令已从 **show pdm sessions** 改为 **show asdm sessions**。

使用指南

每个活动 ASDM 会话都分配有唯一的会话 ID。您可以使用此会话 ID 及 **asdm disconnect** 命令来终止指定的会话。

示例

以下是 **show asdm sessions** 命令的输出示例：

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

相关命令

命令	说明
asdm disconnect	终止活动的 ASDM 会话。

show as-path-access-list 至 show auto-update 命令

show as-path-access-list

要显示所有当前自主系统 (AS) 路径访问列表的内容，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show as-path-access-list** 命令

show as-path-access-list [*name*]

语法说明

name	（可选）指定 AS 路径访问列表名称。

默认值

如果没有指定 *name* 参数，命令输出将显示所有 AS 路径访问列表。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show as-path-access-list** 命令的输出示例：

```
ciscoasa# show as-path-access-list
AS path access list as-path-acl-1
    deny RTR$
AS path access list as-path-acl-2
    permit 100$
```

表 3-1 显示每个字段的说明。

表 3-1　show as-path-access-list 字段

字段	说明
AS path access list	表示 AS 路径访问列表名称。
deny	表示由于正则表达式未能匹配 ASCII 字符串形式的路由 AS 路径表示而拒绝的数据包数量。
permit	表示由于正则表达式匹配 ASCII 字符串形式的路由 AS 路径表示而转发的数据包数量。

show asp cluster counter

要在集群环境下调试全局或情景特定信息，请在特权 EXEC 模式下使用 **show asp cluster counter** 命令。

show asp cluster counter

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show asp cluster counter 命令显示全局和情景特定的 DP 计数器，可帮助您对问题进行故障排除。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC，以帮助您使用此命令调试您的系统。

示例

以下是 **show asp cluster counter** 命令的输出示例：

```
ciscoasa# show asp cluster counter

Global dp-counters:


Context specific dp-counters:

MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

相关命令

命令	说明
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp drop

要调试加速安全路径丢弃的数据包或连接，请在特权 EXEC 模式下使用 **show asp drop** 命令。

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

语法说明

flow [*flow_drop_reason*]	（可选）显示丢弃的流量（连接）。通过使用 *flow_drop_reason* 参数，您可以指定特定的原因。“ 使用指南 ” 部分中列出了 *flow_drop_reason* 参数的有效值。
frame [*frame_drop_reason*]	（可选）显示丢弃的数据包。通过使用 *frame_drop_reason* 参数，您可以指定特定的原因。“ 使用指南 ” 部分中列出了 *frame_drop_reason* 参数的有效值。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.0(8)/7.2(4)/8.0(4)	输出包括指示计数器上次清除时间的时间戳（请参阅 **clear asp drop** 命令）。输出还会在说明旁边显示丢弃原因关键字，以便您能够轻松使用 **capture asp-drop** 命令及关联的关键字。

使用指南

show asp drop 命令显示加速安全路径丢弃的数据包或连接，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

以下各部分包含每个丢弃原因名称和说明，包括建议：

- 第 3-4 页上的丢帧原因
- 第 3-64 页上的流量丢弃原因

丢帧原因

```
----------------------------------------------------------------
Name: natt-keepalive
NAT-T keepalive message:
    This counter will increment when the appliance receives an IPsec NAT-T keepalive
message. NAT-T keepalive messages are sent from the IPsec peer to the appliance to keep
NAT/PAT flow information current in network devices between the NAT-T IPsec peer and the
appliance.
```

```
 Recommendation:
    If you have configured IPsec NAT-T on your appliance, this indication is normal and
doesn't indicate a problem. If NAT-T is not configured on your appliance, analyze your
network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsecudp-keepalive
IPSEC/UDP keepalive message:
    This counter will increment when the appliance receives an IPsec over UDP keepalive
message. IPsec over UDP keepalive messages are sent from the IPsec peer to the appliance
to keep NAT/PAT flow information current in network devices between the IPsec over UDP
peer and the appliance. Note - These are not industry standard NAT-T keepalive messages
which are also carried over UDP and addressed to UDP port 4500.
 Recommendation:
    If you have configured IPsec over UDP on your appliance, this indication is normal and
doesn't indicate a problem. If IPsec over UDP is not configured on your appliance, analyze
your network traffic to determine the source of the IPsec over UDP traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-prot
IPsec not AH or ESP:
    This counter will increment when the appliance receives a packet on an IPsec
connection which is not an AH or ESP protocol. This is not a normal condition.

 Recommendation:
    If you are receiving many IPsec not AH or ESP indications on your appliance, analyze
your network traffic to determine the source of the traffic.

 Syslogs:
    402115


----------------------------------------------------------------
Name: ipsec-ipv6
IPsec via IPV6:
    This counter will increment when the appliance receives an IPsec ESP packet, IPsec
NAT-T ESP packet or an IPsec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPsec sessions encapsulated in IP version 6.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-natt
Bad IPsec NATT packet:
    This counter will increment when the appliance receives a packet on an IPsec
connection which has negotiated NAT-T but the packet is not addressed to the NAT-T UDP
destination port of 4500 or had an invalid payload length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.
```

```
 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-udp
Bad IPsec UDP packet:
    This counter will increment when the appliance receives a packet on an IPsec
connection that has negotiated IPsec over UDP, but the packet has an invalid payload
length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: inspect-srtp-encrypt-failed
Inspect SRTP Encryption failed:
    This counter will increment when SRTP encryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP encryption is
failing in the hardware crypto accelerator.

Syslogs:
    337001.


----------------------------------------------------------------
Name: inspect-srtp-decrypt-failed
Inspect SRTP Decryption failed:
    This counter will increment when SRTP decryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP decryption is
failing in the hardware crypto accelerator.

Syslogs:
    337002.


----------------------------------------------------------------
Name: inspect-srtp-validate-authtag-failed
Inspect SRTP Authentication tag validation failed:
    This counter will increment when SRTP authentication tag validation fails.

Recommendation:
    No action is required. If error persists SRTP packets arriving at the firewall are
being tampered with and the administrator has to identify the cause.

Syslogs:
    337003.


----------------------------------------------------------------
Name: inspect-srtp-generate-authtag-failed
Inspect SRTP Authentication tag generation failed:
    This counter will increment when SRTP authentication tag generation fails.
```

```
Recommendation:
    No action is required.

Syslogs:
    337004.


----------------------------------------------------------------
Name: inspect-srtp-no-output-flow
Inspect SRTP failed to find output flow:
    This counter will increment when the flow from the Phone proxy could not be created or
if the flow has been torn down

Recommendation:
    No action is required. The flow creation could have failed because of low memory
conditions.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-setup-srtp-failed
Inspect SRTP setup in CTM failed:
    This counter will increment when SRTP setup in the CTM fails.

Recommendation:
    No action is required. If error persists call TAC to see why the CTM calls are
failing.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-one-part-no-key
Inspect SRTP failed to find keys for both parties:
    This counter will increment when Inspect SRTP finds only one party's keys populated in
the media session.

Recommendation:
    No action is required. This counter could increment in the beginning phase of the call
but eventually when the call signaling exchange completes both parties should know their
respective keys.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-media-session
Inspect SRTP Media session lookup failed:
    This counter will increment when SRTP media session lookup fails.

Recommendation:
    No action is required. The media session is created by Inspect SIP or Skinny when the
IP address is parsed as part of the signaling exchange. Debug the signaling messages to
figure out the cause.

Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: inspect-srtp-no-remote-phone-proxy-ip
Inspect SRTP Remote Phone Proxy IP not populated:
    This counter will increment when remote phone proxy IP is not populated

Recommendation:
    No action is required. The remote phone proxy IP address is populated from the
signaling exchange. If error persists debug the signaling messages to figure out if ASA is
seeing all the signaling messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-client-port-not-present
Inspect SRTP client port wildcarded in media session:
    This counter will increment when client port is not populated in media session

Recommendation:
    No action is required. The client port is populated dynamically when the media stream
comes in from the client. Capture the media packets to see if the client is sending media
packets.

Syslogs:
    None.


----------------------------------------------------------------
Name: ipsec-need-sa
IPsec SA not negotiated yet:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPsec security association. This is generally a normal
condition for LAN-to-LAN IPsec configurations. This indication will cause the appliance to
begin ISAKMP negotiations with the destination peer.

 Recommendation:
    If you have configured IPsec LAN-to-LAN on your appliance, this indication is normal
and doesn't indicate a problem. However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing. Verify that you can communicate with the destination peer and verify your
crypto configuration via the 'show running-config' command.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof
IsSec spoof detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received unencrypted.
This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
```

```
Name: ipsec-clearpkt-notun
IPsec Clear Pkt w/no tunnel:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received unencrypted.
This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-tun-down
IPsec tunnel is down:
    This counter will increment when the appliance receives a packet associated with an
IPsec connection which is in the process of being deleted.

 Recommendation:
    This is a normal condition when the IPsec tunnel is torn down for any reason.

 Syslogs:
    None


----------------------------------------------------------------
Name: mp-svc-delete-in-progress
SVC Module received data while connection was being deleted:
    This counter will increment when the security appliance receives a packet associated
with an SVC connection that is in the process of being deleted.

Recommendation:
    This is a normal condition when the SVC connection is torn down for any reason. If
this error occurs repeatedly or in large numbers, it could indicate that clients are
having network connectivity issues.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-bad-framing
SVC Module received badly framed data:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software that it is unable to decode.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-bad-length
SVC Module received bad data length:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software where the calculated and specified lengths do not match.
```

```
Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-unknown-type
SVC Module received unknown data frame:
    This counter will increment when the security appliance receives a packet from an SVC
where the data type is unknown.

Recommendation:
    Validate that the SVC being used by the client is compatible with the version of
security appliance software.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-addr-renew-response
SVC Module received address renew response data frame:
    This counter will increment when the security appliance receives an Address Renew
Response message from an SVC. The SVC should not be sending this message.

Recommendation:
    This indicates that an SVC software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-prepend
SVC Module does not have enough space to insert header:
    This counter will increment when there is not enough space before the packet data to
prepend a MAC header in order to put the packet onto the network.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-channel
SVC Module does not have a channel for reinjection:
    This counter will increment when the interface that the encrypted data was received
upon cannot be found in order to inject the decrypted data.

Recommendation:
    If an interface is shut down during a connection, this could happen; re-enable/check
the interface. Otherwise, this indicates that a software error should be reported to the
Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
```

```
Name: mp-svc-no-session
SVC Module does not have a session:
    This counter will increment when the security appliance cannot determine the SVC
session that this data should be transmitted over.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-session-lock-failure
SVC Module failed to acquire the session lock:
    This counter will increment when the security appliance cannot grab the lock for the
SVC session that this data should be transmitted over.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.  Contact the Cisco Technical Assistance
Center (TAC) if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-decompres-error
SVC Module decompression error:
    This counter will increment when the security appliance encounters an error during
decompression of data from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-compress-error
SVC Module compression error:
    This counter will increment when the security appliance encounters an error during
compression of data to an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-no-mac
SVC Module unable to find L2 data for frame:
    This counter will increment when the security appliance is unable to find an L2 MAC
header for data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.
```

```
Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac
SVC Module found invalid L2 data in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
header attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac-len
SVC Module found invalid L2 data length in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
length attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-flow-control
SVC Session is in flow control:
    This counter will increment when the security appliance needs to drop data because an
SVC is temporarily not accepting any more data.

Recommendation:
    This indicates that the client is unable to accept more data.The client should reduce
the amount of traffic it is attempting to receive.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-fragment
SVC Module unable to fragment packet:
    This counter is incremented when a packet to be sent to the SVC is not permitted to be
fragmented or when there are not enough data buffers to fragment the packet.

Recommendation:
    Increase the MTU of the SVC to reduce fragmentation.Avoid using applications that do
not permit fragmentation.Decrease the load on the device to increase available data
buffers.

Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-handle-error
VPN Handle Error:
    This counter is incremented when the appliances is unable to create a VPN handle
because the VPN handle already exists.
```

```
 Recommendation:
    It is possible to see this counter increment as part of normal operation However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

 Syslogs:
    None.


----------------------------------------------------------------
Name: ipsec-lock-error
IPsec locking error:
    This counter is incremented when an IPsec operation is attempted but fails due to an
internal locking error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-handle-mismatch
VPN Handle Mismatch:
    This counter is incremented when the appliance wants to forward a block and the flow
referred to by the VPN Handle is different than the flow associated with the block.

 Recommendation:
    This is not a normal occurrence. Please enter the show console-output command and
forward that output to CISCO TAC for further analysis.

 Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-reclassify-failed
VPN Reclassify Failed:
    This counter is incremented when a packet for a VPN flow is dropped due to the flow
failing to be reclassified after a VPN state change.

 Recommendation:
    This counter is incremented when a packet for a VPN flow arrives that requires
reclassification due to VPN CLI or Tunnel state changes. If the flow no longer matches the
existing policies, then the flow is freed and the packet dropped.

 Syslogs:
    No new syslogs accompany this event.


----------------------------------------------------------------
Name: punt-rate-limit
Punt rate limit exceeded:
    This counter will increment when the appliance attempts to forward a layer-2 packet to
a rate-limited control point service routine and the rate limit (per/second) is now being
exceeded. Currently, the only layer-2 packets destined for a control point service routine
which are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second
per interface.
```

```
Recommendation:
    Analyze your network traffic to determine the reason behind the high rate of ARP
packets.

 Syslogs:
    322002, 322003


----------------------------------------------------------------
Name: punt-no-mem
Punt no memory:
    This counter is incremented and the packet is dropped when there is no memory to
create data structure for punting a packet to Control Point.

Recommendation:
    No action needs to be taken if this condition is transient.If this condition persists
due to low memory, then system upgrade might be necessary.

Syslogs:
    None


----------------------------------------------------------------
Name: punt-queue-limit
Punt queue limit exceeded:
    This counter is incremented and the packet is dropped when punt queue limit is
exceeded, an indication that a bottle-neck is forming at Control Point.

Recommendation:
    No action needs to be taken.This is a design limitation.

Syslogs:
    None


----------------------------------------------------------------
Name: flow-being-freed
Flow is being freed:
    This counter is incremented when the flow is being freed and all packets queued for
inspection are dropped.

Recommendation:
    No action needs to be taken.

Syslogs:
    None


----------------------------------------------------------------
Name: invalid-encap
Invalid Encapsulation:
    This counter is incremented when the security appliance receives a frame belonging to
an unsupported link-level protocol or if the L3type specified in the frame is not
supported by the appliance.The packet is dropped.

Recommendation:
    Verify that directly connected hosts have proper link-level protocol settings.

Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: invalid-ip-header
Invalid IP header:
    This counter is incremented and the packet is dropped when the appliance receives an
IP packet whose computed checksum of the IP header does not match the recorded checksum in
the header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line.It may also be
that a peer is sending corrupted packets and an attack is in progress.Please use the
packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: unsupported-ip-version
Unsupported IP version:
    This counter is incremented when the security appliance receives an IP packet that has
an unsupported version in version field of IP header.Specifically, if the packet does not
belong to version 4 or version 6.The packet is dropped.

Recommendation:
    Verify that other devices on connected network are configured to send IP packets
belonging to versions 4 or 6 only.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-length
Invalid IP Length:
    This counter is incremented when the security appliance receives an IPv4 or IPv6
packet in which the header length or total length fields in IP header are not valid or do
not conform to the received packet length.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ethertype
Invalid Ethertype:
    This counter is incremented when the fragmentation module on the security appliance
receives or tries to send a fragmented packet that does not belong IP version 4 or version
6.The packet is dropped.

Recommendation:
    Verify mtu of device and other devices on connected network to determine why the
device is processing such fragments.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-tcp-hdr-length
Invalid TCP Length:
```

```
    This counter is incremented when the security appliance receives a TCP packet whose
size is smaller than minimum-allowed header length or does not conform to the received
packet length.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.
Investigate the traffic from source in the following syslog.

Syslogs:
    500003.


------------------------------------------------------------------
Name: invalid-udp-length
Invalid UDP Length:
    This counter is incremented when the security appliance receives a UDP packet whose
size as calculated from the fields in header is different from the measured size of packet
as received from the network.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.

Syslogs:
    None.


------------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter is incremented when the security appliance has tried to obtain an
adjacency and could not obtain mac-address for next hop.The packet is dropped.

Recommendation:
    Configure a capture for this drop reason and check if a host with specified
destination address exists on connected network or is routable from the device.

Syslogs:
   None.


------------------------------------------------------------------
Name: unexpected-packet
Unexpected packet:
    This counter is incremented when the appliance in transparent mode receives a non-IP
packet, destined to its MAC address, but there is no corresponding service running on the
appliance to process the packet.

Recommendation:
    Verify if the appliance is under attack.If there are no suspicious packets, or the
device is not in transparent mode, this counter is most likely being incremented due to a
software error.Attempt to capture the traffic that is causing the counter to increment and
contact the Cisco TAC.

Syslogs:
    None


------------------------------------------------------------------
Name: no-route
No route to host:
    This counter is incremented when the security appliance tries to send a packet out of
an interface and does not find a route for it in routing table.
```

```
Recommendation:
    Verify that a route exists for the destination address obtained from the generated
syslog.

Syslogs:
   110002, 110003.


----------------------------------------------------------------
Name: rpf-violated
Reverse-path verify failed:
    This counter is incremented when ip-verify is configured on an interface and the
security appliance receives a packet for which the route lookup of source-ip did not yield
the same interface as the one on which the packet was received.

Recommendation:
    Trace the source of traffic based on source-ip printed in syslog below and investigate
why it is sending spoofed traffic.

Syslogs:
    106021.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by configured rule:
    This counter is incremented when a drop rule is hit by the packet and gets
dropped.This rule could be a default rule created when the box comes up, when various
features are turned on or off, when an acl is applied to interface or any other feature
etc. Apart from default rule drops, a packet could be dropped because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface

Recommendation:
    Note if one of ACLs listed below are fired.

Syslogs:
    106023, 106100, 106004


----------------------------------------------------------------
Name: unable-to-create-flow
Flow denied due to resource limitation:
    This counter is incremented and the packet is dropped when flow creation fails due to
a system resource limitation.The resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
    Causes 1 and 2 will occur simultaneously with flow drop reason "No memory to complete
flow".

Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with the command
"show resource usage".

Syslogs:
    None


----------------------------------------------------------------
```

```
Name: unable-to-add-flow
Flow hash full:
    This counter is incremented when a newly created flow is inserted into flow hash table
and the insertion failed because the hash table was full. The flow and the packet are
dropped. This is different from counter that gets incremented when maximum connection
limit is reached.

Recommendation:
    This message signifies lack of resources on the device to support an operation that
should have been successful. Please check if the connections in the 'show conn' output
have exceeded their configured idle timeout values. If so, contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None.


----------------------------------------------------------------
Name: np-sp-invalid-spi
Invalid SPI:
    This counter will increment when the appliance receives an IPsec ESP packet addressed
to the appliance which specifies a SPI (security parameter index) not currently known by
the appliance.

 Recommendation:
    Occasional invalid SPI indications are common, especially during rekey processing.
Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing
a high rate of invalid SPI indications, analyze your network traffic to determine the
source of the ESP traffic.

 Syslogs:
    402114


----------------------------------------------------------------
Name: unsupport-ipv6-hdr
Unsupported IPv6 header:
    This counter is incremented and the packet is dropped if an IPv6 packet is received
with an unsupported IPv6 extension header. The supported IPv6 extension headers are: TCP,
UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment. The IPv6 routing
extension header is not supported, and any extension header not listed above is not
supported.  IPv6 ESP and AH headers are supported only if the packet is through-the-box.
To-the-box IPv6 ESP and AH packets are not supported and will be dropped.

Recommendation:
    This error may be due to a misconfigured host. If this error occurs repeatedly or in
large numbers, it could also indicate spurious or malicious activity such as an attempted
DoS attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: tcp-not-syn
First TCP packet not SYN:
    Received a non SYN packet as the first packet of a non intercepted and non nailed
connection.

Recommendation:
    Under normal conditions, this may be seen when the appliance has already closed a
connection, and the client or server still believe the connection is open, and continue to
transmit data.  Some examples where this may occur is just after a 'clear local-host' or
```

```
'clear xlate' is issued. Also, if connections have not been recently removed, and the
counter is incrementing rapidly, the appliance may be under attack. Capture a sniffer
trace to help isolate the cause.

Syslogs:
    6106015


----------------------------------------------------------------
Name: bad-tcp-cksum
Bad TCP checksum:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line.It may also be
that a TCP endpoint is sending corrupted packets and an attack is in progress.Please use
the packet capture feature to learn more about the origin of the packet.To allow packets
with incorrect TCP checksum disable checksum-verification feature under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: bad-tcp-flags
Bad TCP flags:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with invalid TCP flags in TCP header.Example a packet with SYN and FIN TCP
flags set will be dropped.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line.It may also be
that a TCP endpoint is sending corrupted packets and an attack is in progress.Please use
the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-reserved-set
TCP reserved flags set:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with reserved flags set in TCP header.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line.It may also be
that a TCP endpoint is sending corrupted packets and an attack is in progress.Please use
the packet capture feature to learn more about the origin of the packet.To allow such TCP
packets or clear reserved flags and then pass the packet use reserved-bits configuration
under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-bad-option-list
TCP option list invalid:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with a non-standard TCP header option.
```

```
Recommendations:
    To allow such TCP packets or clear non-standard TCP header options and then allow the
packet, use tcp-options configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-mss-exceeded
TCP data exceeded MSS:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with data length greater than the MSS advertised by peer TCP endpoint.

Recommendations:
    To allow such TCP packets use exceed-mss configuration under tcp-map

Syslogs:
    4419001


----------------------------------------------------------------
Name: tcp-synack-data
TCP SYNACK with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN-ACK packet with data.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line.It may also be
that a TCP endpoint is sending corrupted packets and an attack is in progress.Please use
the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-syn-data
TCP SYN with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet with data.

Recommendations:
    To allow such TCP packets use syn-data configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dual-open
TCP Dual open denied:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet from the server, when an embryonic TCP connection is already open.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
```

```
Name: tcp-data-past-fin
TCP data send after FIN:
    This counter is incremented and the packet is dropped when the appliance receives new
TCP data packet from an endpoint which had sent a FIN to close the connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-3whs-failed
TCP failed 3 way handshake:
    This counter is incremented and the packet is dropped when appliance receives an
invalid TCP packet during three-way-handshake.Example SYN-ACK from client will be dropped
for this reason.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-rstfin-ooo
TCP RST/FIN out of order:
    This counter is incremented and the packet is dropped when appliance receives a RST or
a FIN packet with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-seq-syn-diff
TCP SEQ in SYN/SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a SYN or
SYN-ACK packet during three-way-handshake with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-ack-syn-diff
TCP ACK in SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a
SYN-ACK packet during three-way-handshake with incorrect TCP acknowledgement number.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-syn-ooo
TCP SYN on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-synack-ooo
TCP SYNACK on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN-ACK packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-seq-past-win
TCP packet SEQ past window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
data packet with sequence number beyond the window allowed by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-invalid-ack
TCP invalid ACK:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with acknowledgment number greater than data sent by peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-fo-drop
TCP replicated flow pak drop:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with control flag like SYN, FIN or RST on an established connection just after the
appliance has taken over as active unit.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: tcp-discarded-ooo
TCP ACK in 3 way handshake invalid:
    This counter is incremented and the packet is dropped when appliance receives a TCP
ACK packet from client during three-way-handshake and the sequence number is not next
expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-full
TCP Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when appliance receives an
out-of-order TCP packet on a connection and there is no buffer space to store this
packet.Typically TCP packets are put into order on connections that are inspected by the
appliance or when packets are sent to SSM for inspection.There is a default queue size and
when packets in excess of this default queue size are received they will be dropped.

Recommendations:
    On ASA platforms the queue size could be increased using queue-limit configuration
under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-global-buffer-full
TCP global Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when the security appliance
receives an out-of-order TCP packet on a connection and there are no more global buffers
available.Typically TCP packets are put into order on connections that are inspected by
the security appliance or when packets are sent to the SSM for inspection.When the global
Out-of-Order buffer queue is full, the packet will be dropped and this counter will
increment.

Recommendations:
    This is a temporary condition when all global buffers are used.If this counter is
constantly incrementing, then please check your network for large amounts of Out-of-Order
traffic, which could be caused by traffic of the same flow taking different routes through
the network.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-timeout
TCP Out-of-Order packet buffer timeout:
    This counter is incremented and the packet is dropped when a queued out of order TCP
packet has been held in the buffer for too long.Typically, TCP packets are put into order
on connections that are inspected by the security appliance or when packets are sent to
the SSM for inspection.When the next expected TCP packet does not arrive within a certain
period, the queued out of order packet is dropped.
```

```
Recommendations:
    The next expected TCP packet may not arrive due to congestion in the network which is
normal in a busy network.The TCP retransmission mechanism in the end host will retransmit
the packet and the session will continue.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-rst-syn-in-win
TCP RST/SYN in window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN or TCP RST packet on an established connection with sequence number within window but
not next expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-acked
TCP DUP and has been ACKed:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet and the data has been acknowledged by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dup-in-queue
TCP dup of packet in Out-of-Order queue:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet that is already in our out of order packet queue.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-paws-fail
TCP packet failed PAWS test:
    This counter is incremented and the packet is dropped when TCP packet with timestamp
header option fails the PAWS (Protect Against Wrapped Sequences) test.

Recommendations:
    To allow such connections to proceed, use tcp-options configuration under tcp-map to
clear timestamp option.

Syslogs:
    None


----------------------------------------------------------------
```

```
Name: tcp-conn-limit
TCP connection limit reached:
    This reason is given for dropping a TCP packet during TCP connection establishment
phase when the connection limit has been exceeded.The connection limit is configured via
the 'set connection conn-max' action command.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached.The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: conn-limit
Connection limit reached:
    This reason is given for dropping a packet when the connection limit or host
connection limit has been exceeded.If this is a TCP packet which is dropped during TCP
connection establishment phase due to connection limit, the drop reason 'TCP connection
limit reached' is also reported.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached.The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp_xmit_partial
TCP retransmission partial:
    This counter is incremented and the packet is dropped when check-retransmission
feature is enabled and a partial TCP retransmission was received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This counter is incremented and the packet is dropped when check-retransmission
feature is enabled and a TCP retransmission with different data from the original packet
was received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This counter is incremented and the packet is dropped when window size advertised by
TCP endpoint is drastically changed without accepting that much data.
```

```
Recommendations:
    In order to allow such packet, use the window-variation configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: rate-exceeded
QoS rate exceeded:
    This counter is incremented when rate-limiting (policing) is configured on an
egress/ingress interface and the egress/ingress traffic rate exceeds the burst rate
configured.The counter is incremented for each packet dropped.

Recommendation:
    Investigate and determine why the rate of traffic leaving/entering the interface is
higher than the configured rate.This may be normal, or could be an indication of virus or
attempted attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: queue-removed
Rate-limiter queued packet dropped:
    When QoS config is changed or removed, the existing packets in the output queues
awaiting transmission are dropped and this counter is incremented.

Recommendation:
    Under normal conditions, this may be seen when the QoS configuration has been changed
by the user.If this occurs when no changes to QoS config were performed, please contact
Cisco Technical Assistance Center (TAC).

Syslogs:
   None.


----------------------------------------------------------------
Name: bad-crypto
Bad crypto return in packet:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails.This is not a normal condition and could
indicate possible software or hardware problems with the appliance

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.You
should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors.You can also check the error counter in the global IPsec statistics with
the 'show ipsec stats' CLI command.If the IPsec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: ctm-error
CTM returned error:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails.This is not a normal condition and could
indicate possible software or hardware problems with the appliance.
```

```
 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors. You can also check the error counter in the global IPsec statistics with
the 'show ipsec stats' CLI command. If the IPsec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: send-ctm-error
Send to CTM returned error:
    This counter is obsolete in the appliance and should never increment.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: security-failed
Early security checks failed:
    This counter is incremented and packet is dropped when the security appliance :
    - receives an IPv4 multicast packet when the packets multicast MAC address doesn't
match the packets multicast destination IP address
    - receives an IPv6 or IPv4 teardrop fragment containing either small offset or
fragment overlapping
    - receives an IPv4 packet that matches an IP audit (IPS) signature

Recommendation:
    Contact the remote peer administrator or escalate this issue according to your
security policy
    For detailed description and syslogs for IP audit attack checks please refer the ip
audit signature section of command reference guide

Syslogs:
    106020
    400xx in case of ip audit checks


----------------------------------------------------------------
Name: sp-security-failed
Slowpath security checks failed:
    This counter is incremented and packet is dropped when the security appliance is:
    1) In routed mode receives a through-the-box:
       - L2 broadcast packet
       - IPv4 packet with destination IP address equal to 0.0.0.0
       - IPv4 packet with source IP address equal to 0.0.0.0
    2) In routed or transparent mode and receives a through-the-box IPv4 packet with:
       - first octet of the source IP address equal to zero
       - source IP address equal to the loopback IP address
       - network part of source IP address equal to all 0's
       - network part of the source IP address equal to all 1's
       - source IP address host part equal to all 0's or all 1's
    3) In routed or transparent mode and receives an IPv4 or IPv6 packet with same source
and destination IP addresses
```

```
Recommendation:
    1 and 2) Determine if an external user is trying to compromise the protected
network.Check for misconfigured clients.
    3) If this message counter is incrementing rapidly, an attack may be in progress.Use
the packet capture feature to capture type asp packets, and check the source MAC address
in the packet to see where they are coming from.

Syslogs:
    1 and 2) 106016
    3) 106017


----------------------------------------------------------------
Name: ipv6_sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.

Syslogs:
    For identical source and destination address, syslog 106016, else none.


----------------------------------------------------------------
Name: invalid-ip-option
IP option drop:
    This counter is incremented when any unicast packet with ip options or a multicast
packet with ip-options that have not been configured to be accepted, is received by the
security appliance.The packet is dropped.

Recommendation:
    Investigate why a packet with ip options is being sent by the sender.

Syslogs:
    None.


----------------------------------------------------------------
Name: lu-invalid-pkt
Invalid LU packet:
    Standby unit received a corrupted Logical Update packet.

Recommendation:
    The packet corruption could be caused by a bad cable, interface card, line noise, or
software defect.If the interface appears to be functioning properly, then report the
problem to Cisco TAC.

Syslogs:
    None


----------------------------------------------------------------
Name: fo-standby
Dropped by standby unit:
    If a through-the-box packet arrives at an appliance or context in a Standby state and
a flow is created, the packet is dropped and the flow removed.This counter will increment
each time a packet is dropped in this manner.
```

```
Recommendation:
    This counter should never be incrementing on the Active appliance or context.However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: dst-l2_lookup-fail
Dst MAC L2 Lookup Failed:
    This counter will increment when the appliance is configured for transparent mode and
the appliance does a Layer 2 destination MAC address lookup which fails.Upon the lookup
failure, the appliance will begin the destination MAC discovery process and attempt to
find the location of the host via ARP and/or ICMP messages.

 Recommendation:
    This is a normal condition when the appliance is configured for transparent mode. You
can also execute (show mac-address-table) to list the L2 MAC address locations currently
discovered by the appliance.

 Syslogs:
    None


----------------------------------------------------------------
Name: l2_same-lan-port
L2 Src/Dst same LAN port:
    This counter will increment when the appliance/context is configured for transparent
mode and the appliance determines that the destination interface's L2 MAC address is the
same as its ingress interface.

 Recommendation:
    This is a normal condition when the appliance/context is configured for transparent
mode.  Since the appliance interface is operating in promiscuous mode, the
appliance/context receives all packets on the local LAN seqment.

 Syslogs:
    None


----------------------------------------------------------------
Name: flow-expired
Expired flow:
    This counter is incremented when the security appliance tries to inject a new or
cached packet belonging to a flow that has already expired.It is also incremented when the
appliance attempts to send an rst on a tcp flow that has already expired or when a packet
returns from IDS blade but the flow had already expired.The packet is dropped

Recommendation:
    If valid applications are getting pre-empted, investigate if a longer timeout is
needed.

Syslogs:
   None.


----------------------------------------------------------------
Name: inspect-icmp-out-of-app-id
ICMP Inspect out of App ID:
    This counter will increment when the ICMP inspection engine fails to allocate an 'App
ID' data structure.The structure is used to store the sequence number of the ICMP packet.
```

```
Recommendation:
    Check the system memory usage.This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmp-bad-code
ICMP Inspect bad icmp code:
    This counter will increment when the ICMP code in the ICMP echo request or reply
message is non-zero.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313009.


----------------------------------------------------------------
Name: inspect-icmp-seq-num-not-matched
ICMP Inspect seq num not matched:
    This counter will increment when the sequence number in the ICMP echo reply message
does not match any ICMP echo message that passed across the appliance earlier on the same
connection.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004


----------------------------------------------------------------
Name: inspect-icmp-error-no-existing-conn
ICMP Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMP error message.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-nat64-error
ICMP NAT64 Error Inspect XLATE Error:
    This counter will increment when the appliance is unable to translate ICMP error
messages between IPv6 and IPv4.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005
```

```
----------------------------------------------------------------
Name: inspect-icmp-nat64-frag
ICMP NAT64 Inspect Fragmentation Error:
    This counter will increment when the appliance is unable to translate ICMP messages
between IPv6 and IPv4 due to fragmentation.Per RFC-6145, ICMP packet fragments will not be
translated.

Recommendation:
    No action required.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-different-embedded-conn
ICMP Error Inspect different embedded conn:
    This counter will increment when the frame embedded in the ICMP error message does not
match the established connection that has been identified when the ICMP connection is
created.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmpv6-error-invalid-pak
ICMPv6 Error Inspect invalid packet:
    This counter will increment when the appliance detects an invalid frame embedded in
the ICMPv6 packet.This check is the same as that on IPv6 packets.Examples: Incomplete IPv6
header; malformed IPv6 Next Header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmpv6-error-no-existing-conn
ICMPv6 Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMPv6 error message.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-dns-invalid-pak
DNS Inspect invalid packet:
    This counter will increment when the appliance detects an invalid DNS packet.Examples:
A DNS packet with no DNS header; the number of DNS resource records not matching the
counter in the header; etc.
```

```
Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-invalid-domain-label
DNS Inspect invalid domain label:
    This counter will increment when the appliance detects an invalid DNS domain name or
label.DNS domain name and label is checked per RFC 1035.

Recommendation:
    No action required.If the domain name and label check is not desired, disable the
protocol-enforcement parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-pak-too-long
DNS Inspect packet too long:
    This counter is incremented when the length of the DNS message exceeds the configured
maximum allowed value.

Recommendation:
    No action required.If DNS message length checking is not desired, enable DNS
inspection without the 'maximum-length' option, or disable the 'message-length maximum'
parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    410001


----------------------------------------------------------------
Name: inspect-dns-out-of-app-id
DNS Inspect out of App ID:
    This counter will increment when the DNS inspection engine fails to allocate a data
structure to store the identification of the DNS message.
Recommendation:
    Check the system memory usage.This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-id-not-matched
DNS Inspect ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: dns-guard-out-of-app-id
DNS Guard out of App ID:
    This counter will increment when the DNS Guard function fails to allocate a data
structure to store the identification of the DNS message.

Recommendation:
    Check the system memory usage.This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: dns-guard-id-not-matched
DNS Guard ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same
connection.This counter will increment by the DNS Guard function.

Recommendation:
    No action required if it is an intermittent event.If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-length
Invalid RTP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTP header.

Recommendation:
    No action required.A capture can be used to figure out which RTP source is sending the
incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-version
Invalid RTP Version field:
    This counter will increment when the RTP version field contains a version other than 2.

Recommendation:
    The RTP source in your network does not seem to be sending RTP packets conformant with
the RFC 1889.The reason for this has to be identified and you can deny the host using ACLs
if required.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-invalid-payload-type
Invalid RTP Payload type field:
    This counter will increment when the RTP payload type field does not contain an audio
payload type when the signalling channel negotiated an audio media type for this RTP
secondary connection.The counter increments similarly for the video payload type.
```

```
Recommendation:
    The RTP source in your network is using the audio RTP secondary connection to send
video  or vice versa.If you wish to prevent this you can deny the host using ACLs.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-ssrc-mismatch
Invalid RTP Synchronization Source field:
    This counter will increment when the RTP SSRC field in the packet does not match the
SSRC which the inspect has been seeing from this RTP source in all the RTP packets.

Recommendation:
    This could be because the RTP source in your network is rebooting and hence changing
the SSRC or it could be because of another host on your network trying to use the opened
secondary RTP connections on the firewall to send RTP packets.This should be investigated
further to confirm if there is a problem.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-sequence-num-outofrange
RTP Sequence number out of range:
    This counter will increment when the RTP sequence number in the packet is not in the
range expected by the inspect.

Recommendation:
    No action is required because the inspect tries to recover and start tracking from a
new sequence number after a lapse in the sequence numbers from the RTP source.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-max-outofseq-paks-probation
RTP out of sequence packets in probation period:
    This counter will increment when the out of sequence packets when the RTP source is
being validated exceeds 20.During the probation period, the inspect looks for 5
in-sequence packets to consider the source validated.

Recommendation:
    Check the RTP source to see why the first few packets do not come in sequence and
correct it.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-length
Invalid RTCP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTCP header.

Recommendation:
    No action required.A capture can be used to figure out which RTP source is sending the
incorrect packets and you can deny the host using the ACLs.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-version
Invalid RTCP Version field:
    This counter will increment when the RTCP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTCP packets conformant
with the RFC 1889.The reason for this has to be identified and you can deny the host using
ACLs if required.

Syslogs:
    431002.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-payload-type
Invalid RTCP Payload type field:
    This counter will increment when the RTCP payload type field does not contain the
values 200 to 204.

Recommendation:
    The RTP source should be validated to see why it is sending payload types outside of
the range recommended by the RFC 1889.

Syslogs:
    431002.


----------------------------------------------------------------
Name: cxsc-request
Flow terminated by CXSC:
This reason is given for terminating a flow as requested by CXSC module.Recommendations:
Check syslogs and alerts on CXSC module.
Syslogs: 429002


----------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when CXSC configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for CXSC.

Syslogs:
   None


----------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
    Check and bring up CXSC card.
```

```
Syslogs:
    429001


----------------------------------------------------------------
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet has bad TLV's.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, like
right after ASA HA state change.If the counter is constantly increasing however, then it
can be because CXSC and ASA are out of sync.If that happens, contact Cisco TAC for
assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with
invalid messsage header, and the packet is dropped.

Recommendation:
    This should not happen.Contact Cisco TAC for assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet is malformed.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-request
IPS Module requested drop:
    This counter is incremented and the packet is dropped as requested by IPS module when
the packet matches a signature on the IPS engine.
```

```
Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: ips-fail-close
IPS card is down:
    This counter is incremented and the packet is dropped when IPS card is down and
fail-close option was used in IPS inspection.

Recommendations:
    Check and bring up the IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: ips-fail
IPS config removed for connection:
    This counter is incremented and the packet is dropped when IPS configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for IPS.

Syslogs:
   None


----------------------------------------------------------------
Name: ips-no-ipv6
Executing IPS software does not support IPv6:
    This counter is incremented when an IPv6 packet, configured to be directed toward IPS
SSM, is discarded since the software executing on IPS SSM card does not support IPv6.

Recommendations:
   Upgrade the IPS software to version 6.2 or later.

Syslogs:
   None


----------------------------------------------------------------
Name: l2_acl
FP L2 rule drop:
    This counter will increment when the appliance denies a packet due to a layer-2 ACL.By
default, in routed mode the appliance will PERMIT:
    1) IPv4 packets
    2) IPv6 packets
    3) ARP packets
    4) L2 Destination MAC of FFFF:FFFF:FFFF (broadcast)
    5) IPv4 MCAST packet with destination L2 of 0100:5E00:0000-0100:5EFE:FFFF
    6) IPv6 MCAST packet with destination L2 of 3333:0000:0000-3333:FFFF:FFFF

    By default, in Transparent mode permits the routed mode ACL and PERMITS:

    1) BPDU packets with destination L2 of 0100:0CCC:CCCD
    2) Appletalk packets with destination L2 of 0900:0700:0000-0900:07FF:FFFF
```

```
    The user can also configure ethertype ACL(s) and apply them to an interface to permit
other types of L2 traffic.

    The default L2 ACL can be seen in routed and transparent mode with the show asp table
classify domain permit command.

    Note - Packets permitted by L2 ACLs may still be dropped by L3-L4 ACLs.

 Recommendation:
    If your running the appliance/context in transparent mode and your non-IP packets are
dropped by the appliance, you can configure an ethertype ACL and apply the ACL to an
access group. Note - the appliance ethertype CLI only supports protocol types and not L2
destination MAC addresses.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: intercept-unexpected
Intercept unexpected packet:
    Either received data from client while waiting for SYNACK from server or received a
packet which cannot be handled in a particular state of TCP intercept.

Recommendation:
    If this drop is causing the connection to fail, please have a sniffer trace of the
client and server side of the connection while reporting the issue.The box could be under
attack and the sniffer traces or capture would help narrowing down the culprit.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-mcast-entry
FP no mcast entry:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    A multicast entry change has been detected after a packet was punted to the CP, and
the NP can no longer forward the packet since no entry is present.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: no-mcast-intrf
FP no mcast output intrf:
    All output interfaces have been removed from the multicast entry.
    - OR -
    The multicast packet could not be forwarded.

Recommendation:
    Verify that there are no longer any receivers for this group.
    - OR -
    Verify that a flow exists for this packet.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: fragment-reassembly-failed
Fragment reassembly failed:
    This counter is incremented when the appliance fails to reassemble a chain of
fragmented packets into a single packet.All the fragment packets in the chain are
dropped.This is most probably because of failure while allocating memory for the
reassembled packet.

Recommendation:
    Use the show blocks command to monitor the current block memory.

Syslogs:
    None


----------------------------------------------------------------
Name: ifc-classify
Virtual firewall classification failed:
    A packet arrived on a shared interface, but failed to classify to any specific context
interface.

Recommendation:
    For software versions without customizable mac-address support, use the "global" or
"static" command to specify the IPv4 addresses that belong to each context interface.For
software versions with customizable mac-address support, enable "mac-address auto" in
system context.Alternatively, configure unique MAC addresses for each context interfaces
residing over a shared interface with "mac-address" command under each context interface
submode.

Syslogs:
    None.


----------------------------------------------------------------
Name: connection-lock
Connection locking failed:
    While the packet was waiting for processing, the flow that would be usedwas destroyed.

Recommendation:
    The message could occur from user interface command to remove connection in an device
that is actively processing packet.Otherwise, investigate flow drop counter.This message
may occur if the flow are forced dropped from error.

Syslogs:
    None.


----------------------------------------------------------------
Name: interface-down
Interface is down:
    This counter will increment for each packet received on an interface that is shutdown
via the 'shutdown' interface sub-mode command.For ingress traffic, the packet is dropped
after security context classification and if the interface associated with the context is
shut down.For egress traffic, the packet is dropped when the egress interface is shut
down.

Recommendation:
    No action required.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-app-length
Invalid App length:
    This counter will increment when the appliance detects an invalid length of the Layer
7 payload in the packet.Currently, it counts the drops by the DNS Guard function
only.Example: Incomplete DNS header.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-buffer-full
Loopback buffer full:
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface and there is no
buffer space in loopback queue.

Recommendations:
    Check system CPU to make sure it is not overloaded.

Syslogs:
    None


----------------------------------------------------------------
Name: non-ip-pkt-in-routed-mode
Non-IP packet received in routed mode:
    This counter will increment when the appliance receives a packet which is not IPv4,
IPv6 or ARP and the appliance/context is configured for routed mode.In normal operation
such packets should be dropped by the default L2 ACL configuration.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: host-move-pkt
FP host move packet:
    This counter will increment when the appliance/context is configured for transparent
and source interface of a known L2 MAC address is detected on a different interface.

 Recommendation:
    This indicates that a host has been moved from one interface (i.e. LAN segment) to
another. This condition is normal while in transparent mode if the host has in fact been
moved. However, if the host move toggles back and forth between interfaces, a network loop
may be present.

 Syslogs:
    412001, 412002, 322001


----------------------------------------------------------------
```

```
Name: tfw-no-mgmt-ip-config
No management IP address configured for TFW:
    This counter is incremented when the security appliance receives an IP packet in
transparent mode and has no management IP address defined.The packet is dropped.

Recommendation:
    Configure the device with management IP address and mask values.

Syslogs:
    322004


----------------------------------------------------------------
Name: shunned
Packet shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: rm-conn-limit
RM connection limit reached:
    This counter is incremented when the maximum number of connections for a context or
the system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-conn-rate-limit
RM connection rate limit reached:
    This counter is incremented when the maximum connection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: np-socket-closed
Dropped pending packets in a closed socket:
    If a socket is abruptly closed, by the user or software, then any pending packets in
the pipeline for that socket are also dropped.This counter is incremented for each packet
in the pipeline that is dropped.
```

```
Recommendation:
    It is common to see this counter increment as part of normal operation.However, if the
counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect.Contact the Cisco TAC to
investigate the issue further.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-pf-queue-full
Port Forwarding Queue Is Full:
       This counter is incremented when the Port Forwarding application's internal queue
is full and it receives another packet  for transmission.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-dpp-invalid
Invalid packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when the security appliance receives a packet from the internal data plane
interface but could not find the proper driver to parse it.

Recommendation:
    The data plane driver is dynamically registered depending on the type of SSM installed
in the system.So this could happen if data plane packets arrive before the security
appliance is fully initialized.This counter is usually 0.You should not be concerned if
there are a few drops.However, if this counter keeps rising when system is up and running,
it may indicate a problem.Please contact Cisco Technical Assistance Center (TAC) if you
suspect it affects the normal operation of your the security appliance.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-asdp-invalid
Invalid ASDP packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when the security appliance receives an ASA SSM Dataplane Protocol (ASDP)
packet from the internal data plane interface, but the driver encountered a problem when
parsing the packet.ASDP is a protocol used by the security appliance to communicate with
certain types of SSMs, like the CSC-SSM.This could happen for various reasons, for example
ASDP protocol version is not compatible between the security appliance and SSM, in which
case the card manager process in the control plane issues system messages and CLI warnings
to inform you of the proper version of images that need to be installed; the ASDP packet
belongs to a connection that has already been terminated on the security appliance; the
security appliance has switched to the standby state (if failover is enable) in which case
it can no longer pass traffic; or any unexpected value when parsing the ASDP header and
payload.

Recommendation:
    The counter is usually 0 or a very small number.But user should not be concerned if
the counter slowly increases over the time, especially when there has been a failover, or
you have manually cleared connections on the security appliance via CLI.If the counter
increases drastically during normal operation, please contact Cisco Technical Assistance
Center (TAC).
```

```
Syslogs:
    421003
    421004


------------------------------------------------------------------
Name: ssm-app-request
Service module requested drop:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when the application running on the SSM requests the security appliance to
drop a packet.

Recommendation:
    More information could be obtained by querying the incident report or system messages
generated by the SSM itself.Please consult the documentation that comes with your SSM for
instructions.

Syslogs:
    None.


------------------------------------------------------------------
Name: ssm-app-fail
Service module is down:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when a packet to be inspected by the SSM is dropped because the SSM has become
unavailable.Some examples of this are: software or hardware failure, software or signature
upgrade, or the module being shut down.

Recommendation:
    The card manager process running in the security appliance control plane would have
issued system messages and CLI warning to inform you of the failure.Please consult the
documentation that comes with the SSM to trouble shoot the SSM failure.Contact Cisco
Technical Assistance Center (TAC) if needed.

Syslog:
    None.


------------------------------------------------------------------
Name: wccp-return-no-route
No route to host for WCCP returned packet:
    This counter is incremented when a packet is returned from the Cache Engine and the
security appliance does not find a route for the original source of the packet.

Recommendation:
    Verify that a route exists for the source ip address of the packet returned from Cache
Engine.

Syslogs:
    None.


------------------------------------------------------------------
Name: wccp-redirect-no-route
No route to Cache Engine:
    This counter is incremented when the security appliance tries to redirect a packet and
does not find a route to the Cache Engine.

Recommendation:
    Verify that a route exists for Cache Engine.
```

```
Syslogs:
   None.


-----------------------------------------------------------------
Name: telnet-not-permitted
Telnet not permitted on least secure interface:
    This counter is incremented and packet is dropped when the appliance receives a TCP
SYN packet attempting to establish a TELNET session to the appliance and that packet was
received on the least secure interface.

 Recommendation:
    To establish a Telnet session to the appliance via the least secure interface, first
establish an IPsec tunnel to that interface and then connect the Telnet session over that
tunnel.

 Syslogs:
    402117


-----------------------------------------------------------------
Name: ipv6-sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.
Syslogs:
    For identical source and destination address, syslog 106016, else none.


-----------------------------------------------------------------
Name: ipv6-eh-inspect-failed
IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet but extension header could not be inspected due to memory allocation failed.

 Recommendation:
Also check 'show memory' output to make sure appliance has enough memory to operate.

 Syslogs:
    None


-----------------------------------------------------------------
Name: ipv6-bad-eh
Bad IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with bad extension header.

 Recommendation:
Check 'verify-header type' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header type' if the header conformance can be skipped.

 Syslogs:
    325005
```

```
----------------------------------------------------------------
Name: ipv6-bad-eh-order
IPv6 extension headers not in proper order is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with extension headers not in proper order.

 Recommendation:
Check 'verify-header order' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header order' if the header order can be arbitrary.

 Syslogs:
    325005


----------------------------------------------------------------
Name: ipv6-mobility-denied
IPv6 mobility extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-mobility-type-denied
IPv6 mobility type extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility type' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-fragment-denied
IPv6 fragmentation extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-address-denied
IPv6 routing extension header exceeding configured maximum routing addresses is denied:
routing count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with too many routing addresses in routing extension header whichis denied by the
user configuration rule.
```

```
 Recommendation:
    Check action of 'match header routing-address count' in 'policy-map type ipv6'. Remove
action 'drop' or increase <count> if <count> routing addresses should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-type-denied
routing type is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with routing type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header routing-type' in 'policy-map type ipv6'. Remove action
'drop' if routing-type should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-eh-count-denied
IPv6 extension headers exceeding configured maximum extension headers is denied:
extension header count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-dest-option-denied
destination-option is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with destination-option extension header which is denied by the user configuration
rule.

 Recommendation:
    Check action of 'match header destination-option' in 'policy-map type ipv6'. Remove
action 'drop' if destination-option should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-hop-by-hop-denied
IPv6 hop-by-hp extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with hop-by-hop extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header hop-by-hop' in 'policy-map type ipv6'. Remove action
'drop' if hop-by-hop should be allowed.

 Syslogs:
    325004
```

```
----------------------------------------------------------------
Name: ipv6-esp-denied
ESP is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with ESP extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header esp' in 'policy-map type ipv6'. Remove action 'drop' if
ESP should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-ah-denied
AH is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with AH extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header ah' in 'policy-map type ipv6'. Remove action 'drop' if
AH should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: channel-closed
Data path channel closed:
    This counter is incremented when the data path channel has been closed before the
packet attempts to be sent out through this channel.

Recommendation:
    It is normal in multi-processor system when one processor closes the channel (e.g.,
via CLI), and another processor tries to send a packet through the channel.

 Syslogs:
    None


----------------------------------------------------------------
Name: dispatch-decode-err
Diapatch decode error:
    This counter is incremented when the packet dispatch module finds an error when
decoding the frame.An example is an unsupported packet frame.
Recommendation:
    Verify the packet format with a capture tool.

 Syslogs:
    None


----------------------------------------------------------------
Name: cp-event-queue-error
CP event queue error:
    This counter is incremented when a CP event queue enqueue attempt has failed due to
queue length exceeded.This queue is used by the data-path to punt packets to the
control-point for additional processing.This condition is only possible in a
multi-processor enviroment.The module that attempted to enqueue the packet may issue its
own packet specific drop in response to this error.
```

```
Recommendation:
    While this error does indicate a failure to completely process a packet, it may not
adversely affect the connection.If the condition persists or connections are adversely
affected contact the Cisco Technical Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: host-limit
Host limit exceeded:
    This counter is incremented when the licensed host limit is exceeded.

Recommendation:
    None.

Syslogs:
    450001


----------------------------------------------------------------
Name: cp-syslog-event-queue-error
CP syslog event queue error:
    This counter is incremented when a CP syslog event queue enqueue attempt has failed
due to queue length exceeded.This queue is used by the data-path to punt logging events to
the control-point when logging destinations other than to a UDP server are configured.This
condition is only possible in a multi-processor environment.

Recommendation:
    While this error does indicate a failure to completely process a logging event,
logging to UDP servers should not be affected.If the condition persists consider lowering
the logging level and/or removing logging destinations or contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: dispatch-block-alloc
Dispatch block unavailable:
     This counter is incremented and the packet is dropped when the appliance could not
allocate a core local block to process the packet that was received by the interface
driver.

Recommendation:
    This may be due to packets being queued for later processing or a block leak.Core
local blocks may also not be available if they are not replenished on time by the free
resource rebalancing logic.Please use "show blocks core" to further diagnose the problem.

Syslogs:
    None


----------------------------------------------------------------
Name: async-lock-queue-limit
Async lock queue limit exceeded:
    Each async lock working queue has a limit of 1000.When more SIP packets are attempted
to be dispatch to the work queue, packet will be dropped.
```

```
Recommendation:
    Only SIP traffic may be dropped.When SIP packets have the same parent lock and they
can be queued into the same async lock queue, thus may result into blocks depletion,
becasue only single core is handling all the media.If a SIP packet attempts to be queued
when the size of the async lock queue exceeds the limit, the packet will be dropped.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-lock-failed
Loopback lock failed
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared intrface and the loopback
queue has failed to acquire a lock.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance.Contact the Cisco Techncial Assistance Center (TAC) if
this error occurs.

Syslogs:
    None

----------------------------------------------------------------
Name: loopback-ifc-not-found
Loopback output interface not found
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface, and the output
interface is not found by the loopback queue.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance.Contact the Cisco Techncial Assistance Center (TAC) if
this error occurs.

Syslogs:
    None


----------------------------------------------------------------
Name: loopback-count-exceeded
Loopback count exceeded
    This counter is incremented and the packet is dropped when a packet is sent from one
context of the appliance to another context through a shared interface, but this packet
has exceeded the number of times it is allowed to queue to the loopback queue.

Recommendations:
    Check the context configuration for each context.The packet is entering a loop in the
context configurations so that it is stuck between contexts, and is repeatedly put into
the loopback queue.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-license-disabled-fail-close
IPS module license disabled
    The IPS module license has been disabled and when the fail-close mode is configured,
all traffic destined for the IPS module will be dropped.The status of the license can be
checked using the "show activation-key" command.
```

```
Recommendation:
    Please apply an activation key using the "activation-key" command that has the IPS
license enabled.

Syslogs:
    420008


------------------------------------------------------------------
Name: backplane-channel-null
Backplane channel null:
The card backplane channel was NULL.This may happen because the channel
was not initialized correctly and had to be closed.ASA will drop the packet.
Recommendation:
    This should not happen.Contact Cisco TAC for assistance.

Syslogs:
    None.


------------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of IPv6 traffic to IPv4 or
vice-versa.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.
```

```
Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if the director/backup unit no longer
receives periodic updates from the owner, which is supposed to happen at fixed intervals
when the flow is alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected.The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.

Recommendations:
    This counter is informational and the behavior expected.The packet is processed by
master.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow.The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or  backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-public_key_not_configured
Scansafe public key not configured:
    This counter is incremented when the scansafe public key is not configured.The packet
is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe public key is configured on the security appliance.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-license-key-not-configured
Scansafe license key not configured:
    This counter is incremented when the scansafe licnese key is not configured.The packet
is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe license key is configured on the security appliance.

Syslogs:
    775002.
```

```
----------------------------------------------------------------
Name: inspect-scansafe-encoding-failed
Inspect  scansafe header encoding failed :
    This counter is incremented when the base64 encoding of user and group name is
failed.The packet is dropped and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-hdr-encryption-failed
Inspect  scansafe header encryption failed:
    This counter is incremented when the encryption of scansafe header is failed.The
packet is dropped and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-max-conn-reached
Inspect  scansafe max allowed connections reached:
    This counter is incremented when we get a new connection and the maximum allowed
concurrent scansafe connection for the platform is already reached.The packet is dropped
and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-duplicate-conn
Inspect scansafe duplicate connection:
     This counter is incremented when duplicate connection with the same source ip address
and port.This packet will be dropped and connection will be closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync becase cluster master has
changed.

Recommendation:
    This counter is informational and the behavior expected.
```

```
Syslogs:
    302014


------------------------------------------------------------------
Name: np-socket-lock-failure
Dropped pending packets due to a failed attempt to get an internal socket lock:
    This error occurs if an attempt to grab an internal socket lock fails.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.Contact the Cisco     Technical Assistance
Center (TAC) if this error occurs.

Syslogs:
    None.


------------------------------------------------------------------
Name: mp-service-inject-failed
SERVICE Module failed to inject a packet:
    This error occurs if an attempt to inject a packet via the SERVICE     Module fails.

Recommendation:
    None.

Syslogs:
    None.


------------------------------------------------------------------
Name: nat-64-or-46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of     IPv6 traffic to IPv4
or vice-versa.

Recommendation:
    Verify if the NAT64 or NAT46 policies are configured properly.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-not-owner
Cluster not owner:
    A Cluster data packet was received without a flow.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-ccl-cfull-sent
CLU FULL sent:
    A Cluster data packet was received over CCL and full flow is built on a new owner.This
packet is no longer needed.
Recommendation:
    None.
Syslogs:
    None.
```

```
-------------------------------------------------------------
Name: cluster-ccl-backup
Cluster CCL backup:
    A Cluster data packet was received over CCL on a backup unit, when it should have been
received on the owner+director unit.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-ccl-unknown-stub
Cluster CCL unknown stub:
    A Cluster data packet was received over CCL and a matching stub flow found, but unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-stub-to-full
Cluster stub to full flow:
    A Cluster packet was received on director, stub flow was converted to full flow.Drop
this packet and wait for retransmission.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-ccl-unknown
Cluster CCL unknown role:
    A Cluster data packet was received over CCL and no matching flow is found, and unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-owner-update
Cluster owner update:
    A Cluster data packet was received updating the flow owner.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-invalid-pkt
Cluster rcvd invalid packet:
    An invalid cluster packet was received.
Recommendation:
    None.
Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-no-msgp
Cluster unit is out of message descriptor:
    Cluster unit is out of message descriptor.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-slave-ignored
Flow matched a cluster drop-on-slave classify rule:
    A multicast routing packet was received on a L3 cluster     interface when the unit
was a slave.Only a master unit     is permitted to process these packets.
Recommendation:
    This counter is informational and the behavior expected.The packet is    processed by
master.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-non-owner-ignored
Flow matched a cluster drop-on-non-owner classify rule:
    A multicast data packet was received on a L3 cluster     interface when the unit was
not an elected owner unit.     Only an elected owner unit is permitted to process
these packets.
Recommendation:
    This counter is informational and the behavior expected.The packet is    processed by
one elected owner unit.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-xlate-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.For dynamic NAT, ensure that
each "nat" command is paired with at least one "global" command.Use "show nat" and "debug
pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


----------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host.Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005
```

```
----------------------------------------------------------------
Name: nat-cluster-input
NAT invalid input:
    An input value for clustering communication contains an unexpected or invalid value.
Recommendation:
    This could be an internal software error.Contact Cisco Systems.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-no-xlate-to-pat-pool
NAT no xlate to pat pool:
    No pre-existing xlate found for a connection with a destination matching a mapped
address in a PAT pool.
Recommendation:
    Configure static PAT is access is desired.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat--xlate-create-failed
NAT xlate creation failed:
    Creation of a PAT xlate failed.
Recommendation:
    Check system memory.Configure at least one backup PAT address.Configure a NAT address
to translate non-overload IP address.Only TCP, UDP, ICMP echo, and PPTP GRE overloadable.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-peer-mcast-ignored
Flow matched a cluster peer mcast data traffic classify rule:
    A multicast data packet was received on a L3 cluster interface when it is from a
cluster peer unit corresponding interface.This is a packet flooded back from L3 subnet.
Recommendation:
    This counter is informational and the behavior expected.The packet has been forwarded
out of the cluster and should be ignored by cluster.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dispatch-queue-fail
Cluster failed to enqueue into global dispatch work queue:
    A forwarded data packet failed to enqueue into global dispatch work queue.
Recommendation:
    This could be an internal software error.Contact Cisco Systems.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-flow-create-fail
Cluster director failed to create director flow:
    Director is trying to create a stub flow but failed due to resource     limitation.The
resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
```

```
    Causes 1 and 2 will occur simultaneously with flow drop reason "No     memory to
complete flow".
Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with     the command
"show resource usage".
Syslogs:
    None


----------------------------------------------------------------
Name: cluster-early-sec-chk-fail
Cluster early security check has failed:
    Director applied early security check has failed due to ACL, WCCP     redirect,
TCP-intercept or IP option.
Recommendation:
    This counter is informational and the behavior expected.The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-queued-ccl-unknown
Cluster CCL unknown stub:
    A queued cluster data packet received over ccl was processed but unit has     unknown
role.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-nat-changed
Cluster director NAT action changed:
    Cluster director NAT action has changed due to NAT policy change, update     or
expiration before queued ccl data packet can be processed.Recommendation:
    This counter is informational and the behavior expected.The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-invalid-ifc
Cluster director has packet with invalid ingress/egress interface:
    Cluster director has processed a previously queued packet with invalid     ingress
and/or egress interface.This is a result of interface removal     (through CLI) before the
packet can be processed.
Recommendation:
    This counter is informational and the behavior expected.The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync because the parent flow's owner has left the cluster.
```

```
Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster, and there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: ike-sa-rate-limit
IKE need SA indication per SA rule rate limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the rate
limit (per/second) is now being exceeded.The current rate is one message every two
seconds.

Recommendation:
     This counter is informational and the behavior expected.The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: ike-sa-global-rate-limit
IKE new SA global limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the global
rate limit (per/second) is now being exceeded.The current rate is ten messages per second.

Recommendation:
     This counter is informational and the behavior expected.The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: nat-cluster-invalid-unxlate-redirect
Cluster member dropped an invalid NAT untranslate redirect packet from peer:
    Cluster member received a NAT untranslate packet from peer.However this member does
not own the NAT address pool the packet belongs to.

Recommendation:
    This counter is a temporal condition after a cluster member failure.However, if this
counter is incremented continuously, it could be an internal software error.Contact Cisco
TAC in this case.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: nat-cluster-pool-update-fail
Cluster master failed to send NAT pool update to slave:
    Cluster master has failed to send NAT pool update to slave unit.This drop will
increase if system resources is low.

Recommendation:
    - Observe if free system memory is low.
    - Observe if "SEC_NAT_SEND_NO_BUFFER" counter is increasing.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-forward-error
Cluster member failed to send data packet over CCL:
    Cluster member failed to transmit control packet over the CCL link.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-tp-version-incompatible
The packet contains an incompatible transport protocol:
    The transport protocol of the packet contains a transport protocol that is not
compatible.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ip-version-error
IP version mismatch between layer-2 and layer-3 headers:
    The IP protocol versions in layer-2 and layer-3 headers mismatch.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-tp-sender-myself
DP message over CCL from a unit with same ID as myself:
    The sender information in the transport header indicates that the sender is myself,
which could happen if two clusters (with overlapping IDs) exist on the same network
segment.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ttl-expired
TTL of the packet has expired:
    Maximum TTL value has exceeded for this packet.
Recommendation:
    None.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ttl-invalid
TTL of the packet is invalid:
    The TTL value of the packet is not a valid value.
Recommendation:
    None.
Syslogs:
    None.
----------------------------------------------------------------
Name: cluster-non-ip-pkt
Layer 3 protocol of the packet is not IP:
    The packet is not IPv4, IPv6 or an ARP packet.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-bad-tp-pkt
Failed to fetch the transport layer header of the packet:
    Fetching the transport layer header of the packet failed.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-bad-trailer
Failed to fetch the trailer of the packet:
    Fetching the trailer of the packet failed.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-frag-owner-query-error
Cluster fragment failed to query flow director for flow owner:
    A failure either when forwarding first fragment to flow director or     fragment chain
reinsert failure.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-frag-error
The fragment is not formatted correctly:
    The fragment is not formatted correctly and cannot be processed or     forwarding to
the Fragment Owner failed.
Recommendation:
    None.
Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-bad-ifc-goid-in-trailer
Failed to find ifc from goid in the trailer:
    The goid extracted from the trailer does not yield a     valid real ifc.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: platform-unlicensed
ASAv platform is unlicensed:
    The ASAv is not licensed.All data traffic traversing the appliance will be     dropped
until the ASAv is licensed.
Recommendation:
    Check the platform license state with "show activation-key" and install the
appropriate ASAv platform license.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-bad-tlv-received
Received a packet from SFR without a Policy ID TLV:
    The ASA received a packet from SFR without a Policy ID TLV.This TLV must be present in
non-control packets if it does not have the Standby/Active bit set in the actions field.
Recommendation:
    None
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-request
Frame was requested to be dropped by SFR:
    The frame was requested to be dropped by SFR due a policy on SFR whereby SFR would set
the actions to Deny Source, Deny Destination, or Deny Pkt.
Recommendation:
    Review SFR policies for any such rule denying the flow.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-fail-close
Packet was dropped:
    The packet was dropped because the card is not up and the policy configured was
'fail-close' (rather than 'fail-open,' which allows packets through even if the card was
down).
Recommendation:
    Check card status and attempt to restart services or reboot it.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-fail
SFR configuration was removed for an existing flow:
    The SFR configuration was removed for an existing flow and we are not able to process
it through SFR, so it will be dropped.This is very unlikely to occur.
Recommendation:
    Review SFR policies for any such rule denying the flow.
```

```
Syslogs:
    None.


-------------------------------------------------------------
Name: sfr-malformed-packet
Packet from SFR contains an invalid header:
    The packet from SFR contains an invalid header.For instance, the header length may not
be correct.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: sfr-ha-request
Security appliance received a SFR HA request packet:
    This counter is incremented when the security appliance received a SFR HA request
packet, but could not process it and the packet is dropped.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: sfr-invalid-encap
Security appliance received a SFR packet with invalid message header:
    This counter is incremented when the security appliance received a SFR packet with
invalid message header and the packet is dropped.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: sfr-bad-handle-received
Received Bad flow handle in a packet from SFR Module:
    Received Bad flow handle in a packet from SFR Module, thus dropping flow.This counter
is incremented; flow and packet are dropped on ASA as the handle for SFR flow has changed
in flow duration.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: sfr-rx-monitor-only
Security appliance received a SFR packet when in monitor-only mode:
    This counter is incremented when the security appliance receives a SFR packet when in
monitor-only mode, and the packet is dropped.
Recommendation:
    Remove “monitor-only” keyword in class configuration if not intentional.
Syslogs:
    None.


-------------------------------------------------------------
```

流量丢弃原因

Name: tunnel-torn-down
Tunnel has been torn down:
    This counter will increment when the appliance receives a packet associated with an established flow whose IPsec security association is in the process of being deleted.

Recommendation:
    This is a normal condition when the IPsec tunnel is torn down for any reason.
Syslogs:
    None

Name: no-ipv6-ipsec
IPsec over IPv6 unsupported:
    This counter will increment when the appliance receives an IPsec ESP packet, IPsec NAT-T ESP packet or an IPsec over UDP ESP packet encapsulated in an IP version 6 header.The appliance does not currently support any IPsec sessions encapsulated in IP version 6.

Recommendation:
    None

Syslogs:
    None

Name: tunnel-pending
Tunnel being brought up or torn down:
    This counter will increment when the appliance receives a packet matching an entry in the security policy database (i.e. crypto map) but the security association is in the process of being negotiated; it’s not complete yet.

    This counter will also increment when the appliance receives a packet matching an entry in the security policy database but the security association has been or is in the process of being deleted.The difference between this indication and the 'Tunnel has been torn down' indication is that the 'Tunnel has been torn down' indication is for established flows.

Recommendation:
    This is a normal condition when the IPsec tunnel is in the process of being negotiated or deleted.

Syslogs:
    None

Name: need-ike
Need to start IKE negotiation:
    This counter will increment when the appliance receives a packet which requires encryption but has no established IPsec security association.This is generally a normal condition for LAN-to-LAN IPsec configurations.This indication will cause the appliance to begin ISAKMP negotiations with the destination peer.

Recommendation:
    If you have configured IPsec LAN-to-LAN on your appliance, this indication is normal and does not indicate a problem.However, if this counter increments rapidly it may indicate a crypto configuration error or network error preventing the ISAKMP negotiation from completing.

```
    Verify that you can communicate with the destination peer and verify your crypto
configuration via the 'show running-config' command.

Syslogs:
    None


----------------------------------------------------------------
Name: vpn-handle-error
VPN handle error:
    This counter is incremented when the appliance is unable to create a VPN handle
because the VPN handle already exists.

Recommendation:
    It is possible to see this counter increment as part of normal operation.However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect.Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-error
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


----------------------------------------------------------------
Name: vpn-handle-not-found
VPN handle not found:
    This counter is incremented when a datagram hits an encrypt or decrypt rule, and no
VPN handle is found for the flow the datagram is on.

Recommendation:
    It is possible to see this counter increment as part of normal operation.However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect.Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-not-found
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof-detect
IPsec spoof packet detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received
unencrypted.This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

Syslogs:
    402117
```

```
----------------------------------------------------------------
Name: svc-spoof-detect
SVC spoof packet detected:
    This counter will increment when the security appliance receives a packet which should
have been encrypted but was not.The packet matched the inner header security policy check
of a configured and established SVC connection on the security appliance but was received
unencrypted.This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed SVC traffic.

Syslogs:
    None


----------------------------------------------------------------
Name: svc-failover
An SVC socket connection is being disconnected on the standby unit:
    This counter is incremented for each new SVC socket connection that is disconnected
when the active unit is transitioning into standby state as part of a failover transition.

Recommendation:
    None.This is part of a normal cleanup of a SVC connection when the current device is
transitioning from active to standby.Existing SVC connections on the device are no longer
valid and need to be removed.

Syslogs:
    None.


----------------------------------------------------------------
Name: svc-replacement-conn
SVC replacement connection established:
    This counter is incremented when an SVC connection is replaced by a new connection.

Recommendation:
    None.This may indicate that users are having difficulty maintaining connections to the
ASA.Users should evaluate the quality of their home network and Internet connection.

Syslog:
    722032


----------------------------------------------------------------
Name: ipsec-selector-failure
IPsec VPN inner policy selector mismatch detected:
    This counter is incremented when an IPsec packet is received with an inner IP header
that does not match the configured policy for the tunnel.

 Recommendation:
    Verify that the crypto ACLs for the tunnel are correct and that all acceptable packets
are included in the tunnel identity. Verify that the box is not under attack if this
message is repeatedly seen.

 Syslogs:
    402116


----------------------------------------------------------------
Name: vpn-context-expired
Expired VPN context:
    This counter will increment when the security appliance receives a packet that
requires encryption or decryption, and the ASP VPN context required to perform the
operation is no longer valid.
```

```
 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    None


----------------------------------------------------------------
Name: vpn-lock-error
IPsec locking error:
  This counter is incremented when VPN flow cannot be created due to an internal locking
error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: out-of-memory
No memory to complete flow:
    This counter is incremented when the appliance is unable to create a flow because of
insufficient memory.

Recommendation:
    Verify that the box is not under attack by checking the current connections.Also
verify if the configured timeout values are too large resulting in idle flows residing in
memory longer.Check the free memory available by issuing 'show memory'.If free memory is
low, issue the command 'show processes memory' to determine which processes are utilizing
most of the memory.

Syslogs:
    None


----------------------------------------------------------------
Name: parent-closed
Parent flow is closed:
    When the parent flow of a subordinating flow is closed, the subordinating flow is also
closed.For example, an FTP data flow (subordinating flow) will be closed with this
specific reason when its control flow (parent flow) is terminated.This reason is also
given when a secondary flow (pin-hole) is closed by its controlling application.For
example, when the BYE messaged is received, the SIP inspection engine (controlling
application) will close the corresponding SIP RTP flows (secondary flow).

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: closed-by-inspection
Flow closed by inspection:
    This reason is given for closing a flow due to an error detected during application
inspection.For example, if an error is detected during inspecting an H323 message, the
corresponding H323 flow is closed with this reason.
```

```
Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: fo-primary-closed
Failover primary closed:
    Standby unit received a flow delete message from the active unit and terminated the
flow.

Recommendation:
    If the appliance is running stateful failover, then this counter should increment for
every replicated connection that is torn down on the standby appliance.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo-standby
Flow closed by failover standby:
    If a through-the-box packet arrives at an appliance or context is in a Standby state,
and a flow is created, the packet is dropped and the flow removed.This counter will
increment each time a flow is removed in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context.However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo_rep_err
Standby flow replication error:
    Standby unit failed to replicate a flow.

Recommendation:
    If appliance is processing VPN traffic, then this counter could be constantly
increasing on the standby unit because of the flow could be replicated before the IKE SA
info.No action is required in this case.If the appliance is not processing VPN traffic,
then this indicate a software detect, turn on the debug: "debug fover fail" on the standby
unit, collect the debug output, and report the problem to Cisco TAC.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: loopback
Flow is a loopback:
    This reason is given for closing a flow due to the following conditions: 1) when
U-turn traffic is present on the flow, and, 2) 'same-security-traffic permit
intra-interface' is not configured.

Recommendation:
    To allow U-turn traffic on an interface, configure the interface with
'same-security-traffic permit intra-interface'.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by access rule:
     This counter is incremented when a drop rule is hit by the packet and flow creation
is denied.This rule could be a default rule created when the box comes up, when various
features are turned on or off, when an acl is applied to interface or any other feature
etc. Apart from default rule drops, a flow could be denied because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface
     5) Implicity deny 'ip any any' at the end of an ACL

Recommendation:
    Observe if one of syslogs related to packet drop are fired.Flow drop results in the
corresponding packet-drop that would fire requisite syslog.

Syslogs:
    None.


----------------------------------------------------------------
Name: pinhole-timeout
Pinhole timeout:
    This counter is incremented to report that the appliance opened a secondary flow, but
no packets passed through this flow within the timeout interval, and hence it was
removed.An example of a secondary flow is the FTP data channel that is created after
successful  negotiation on the FTP control channel.

Recommendation:
    No action required.

Syslogs:
    302014, 302016


----------------------------------------------------------------
Name: host-removed
Host is removed:
    Flow removed in response to "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


----------------------------------------------------------------
Name: xlate-removed
Xlate Clear:
    Flow removed in response to "clear xlate" or "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002
```

```
----------------------------------------------------------------
Name: connection-timeout
Connection timeout:
    This counter is incremented when a flow is closed because of the expiration of it's
inactivity timer.

Recommendation:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021


----------------------------------------------------------------
Name: conn-limit-exceeded
Connection limit exceeded:
    This reason is given for closing a flow when the connection limit has been
exceeded.The connection limit is configured via the 'set connection conn-max' action
command.

Recommendation:
    None.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp-fins
TCP FINs:
    This reason is given for closing a TCP flow when TCP FIN packets are received.

Recommendations:
    This counter will increment for each TCP connection that is terminated normally with
FINs.

Syslogs:
    302014


----------------------------------------------------------------
Name: syn-timeout
SYN Timeout:
    This reason is given for closing a TCP flow due to expiry of embryonic timer.

Recommendations:
    If these are valid session which take longer to establish a connection increase the
embryonic timeout.

Syslogs:
    302014


----------------------------------------------------------------
Name: fin-timeout
FIN Timeout:
    This reason is given for closing a TCP flow due to expiry of half-closed timer.

Recommendations:
    If these are valid session which take longer to close a TCP flow, increase the
half-closed timeout.
```

```
Syslogs:
    302014


----------------------------------------------------------------
Name: reset-in
TCP Reset-I:
    This reason is given for closing an outbound flow (from a low-security interface to a
same- or high-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-out
TCP Reset-O:
    This reason is given for closing an inbound flow (from a high-security interface to
low-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-appliance
TCP Reset-APPLIANCE:
    This reason is given for closing a flow when a TCP reset is generated by appliance.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: recurse
Close recursive flow:
    A flow was recursively freed.This reason applies to pair flows, multicast slave flows,
and syslog flows to prevent syslogs being issued for each of these subordinate flows.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intecept-no-response
TCP intercept, no response from server:
    SYN retransmission timeout after trying three times, once every second.Server
unreachable, tearing down connection.

Recommendation:
    Check if the server is reachable from the ASA.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-unexpected
TCP intercept unexpected state:
    Logic error in TCP intercept module, this should never happen.

Recommendation:
    Indicates memory corruption or some other logic error in the TCP intercept module.

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This reason is given for closing a TCP flow when check-retransmission feature is
enabled and the TCP endpoint sent a retransmission with different data from the original
packet.

Recommendations:
    The TCP endpoint maybe attacking by sending different data in TCP retransmits.Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This reason is given for closing a TCP flow when window size advertised by TCP
endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow this connection, use the window-variation configuration under
tcp-map.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-invalid-syn
TCP invalid SYN:
    This reason is given for closing a TCP flow when the SYN packet is invalid.

Recommendations:
    SYN packet could be invalid for number of reasons, like invalid checksum, invalid TCP
header.Please use the packet capture feature to understand why the SYN packet is
invalid.If you would like to allow these connection use tcp-map configurations to bypass
checks.

Syslogs:
    302014


----------------------------------------------------------------
Name: mcast-intrf-removed
Multicast interface removed:
    An output interface has been removed from the multicast entry.
```

```
    - OR -
    All output interfaces have been removed from the multicast entry.

Recommendation:
    No action required.
    - OR -
    Verify that there are no longer any receivers for this group.

Syslogs:
    None


----------------------------------------------------------------
Name: mcast-entry-removed
Multicast entry removed:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    The multicast entry has been deleted so the flow is being cleaned up, but the packet
will be reinjected into the data path.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-kill
Flow terminated by TCP Intercept:
    TCP intercept would tear down a connection if this is the first SYN, a connection is
created for the SYN, and TCP intercept replied with a SYN cookie, or after seeing a valid
ACK from client, when TCP intercept sends a SYN to server, server replies with a RST.

Recommendation:
    TCP intercept normally does not create a connection for first SYN, except when there
are nailed rules or the packet comes over a VPN tunnel or the next hop gateway address to
reach the client is not resolved.So for the first SYN this indicates that a connection got
created.When TCP intercept receives a RST from server, its likely the corresponding port
is closed on the server.

Syslogs:
    None


----------------------------------------------------------------
Name: audit-failure
Audit failure:
    A flow was freed after matching an "ip audit" signature that had reset as the
associated action.

Recommendation:
    If removing the flow is not the desired outcome of matching this signature, then
remove the reset action from the "ip audit" command.

Syslogs:
    None


----------------------------------------------------------------
```

```
Name: cxsc-request
Flow terminated by CXSC:
    This reason is given for terminating a flow as requested by CXSC module.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    429002


----------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
    Check and bring up CXSC card.

Syslogs:
    429001


----------------------------------------------------------------
Name: reset-by-cx
Flow reset by CXSC:
    This reason is given for terminating a TCP flow as requested by the CXSC module.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    429003


----------------------------------------------------------------
Name: ips-request
Flow terminated by IPS:
    This reason is given for terminating a flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: cxsc-request
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet matches a signature on the CXSC engine.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    429002


----------------------------------------------------------------
```

```
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet has bad TLVs.

Recommendations:
    Check syslogs and alerts on the CXSC module.
Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet is malformed.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when the CXSC configuration is
not found for a particular connection.

Recommendations:
    Check if any configuration changes have been made for CXSC.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, such
as right after an ASA HA state change.If the counter is constantly increasing however, it
may be because CXSC and ASA are out of sync.If that happens, contact Cisco TAC for
assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with an
invalid messsage header, and the packet is dropped.

Recommendation: This should not happen.Contact Cisco TAC for assistance.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: ips-fail-close
IPS fail-close:
    This reason is given for terminating a flow since IPS card is down and fail-close
option was used with IPS inspection.

Recommendations:
    Check and bring up IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: reinject-punt
Flow terminated by punt action:
    This counter is incremented when a packet is punted to the exception-path for
processing by one of the enhanced services such as inspect, aaa etc and the servicing
routine, having detected a violation in the traffic flowing on the flow, requests that the
flow be dropped.The flow is immediately dropped.

Recommendation:
    Please watch for syslogs fired by servicing routine for more information.Flow drop
terminates the corresponding connection.

Syslogs:
    None.


----------------------------------------------------------------
Name: shunned
Flow shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.When a shun command is applied, it will be
incremented for each existing flow that matches the shun command.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: host-limit
host-limit

----------------------------------------------------------------
Name: nat-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.For dynamic NAT, ensure that
each "nat" command is paired with at least one "global" command.Use "show nat" and "debug
pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


----------------------------------------------------------------
```

```
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host.Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005


----------------------------------------------------------------
Name: inspect-fail
Inspection failure:
    This counter will increment when the appliance fails to enable protocol inspection
carried out by the NP for the connection.The cause could be memory allocation failure, or
for ICMP error message, the appliance not being able to find any established connection
related to the frame embedded in the ICMP error message.

Recommendation:
    Check system memory usage.For ICMP error message, if the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004 for ICMP error.


----------------------------------------------------------------
Name: no-inspect
Failed to allocate inspection:
    This counter will increment when the security appliance fails to allocate a run-time
inspection data structure upon connection creation.The connection will be dropped.

Recommendation:
    This error condition is caused when the security appliance runs out of system memory.
Please check the current available free memory by executing the "show memory" command.

Syslogs:
    None


----------------------------------------------------------------
Name: reset-by-ips
Flow reset by IPS:
    This reason is given for terminating a TCP flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420003


----------------------------------------------------------------
Name: flow-reclaimed
Non-tcp/udp flow reclaimed for new request:
    This counter is incremented when a reclaimable flow is removed to make room for a new
flow.This occurs only when the number of flows through the appliance equals the maximum
number permitted by the software imposed limit, and a new flow request is received.When
```

```
this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels
permitted by the appliance, then the oldest reclaimable flow is removed to make room for
the new flow.All flows except the following are deemed to be reclaimable:
    1. TCP, UDP, GRE and Failover flows
    2. ICMP flows if ICMP stateful inspection is enabled
    3. ESP flows to the appliance

Recommendation:
    No action is required if this counter is incrementing slowly.If this counter is
incrementing rapidly, it could mean that the appliance is under attack and the appliance
is spending more time reclaiming and rebuilding flows.

Syslogs
    302021


------------------------------------------------------------------
Name: non_tcp_syn
non-syn TCP:
    This reason is given for terminating a TCP flow when the first packet is not a SYN
packet.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: rm-xlate-limit
RM xlate limit reached:
    This counter is incremented when the maximum number of xlates for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


------------------------------------------------------------------
Name: rm-host-limit
RM host limit reached:
    This counter is incremented when the maximum number of hosts for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


------------------------------------------------------------------
Name: rm-inspect-rate-limit
RM inspect rate limit reached:
    This counter is incremented when the maximum inspection rate for a context or the
system has been reached and a new connection is attempted.
```

```
 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


------------------------------------------------------------------
Name: tcpmod-connect-clash
A TCP connect socket clashes with an existing listen connection.This is an internal system
error.Contact TAC.

------------------------------------------------------------------
Name: ssm-app-request
Flow terminated by service module:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when the application running on the SSM requests the security appliance to
terminate a connection.

Recommendation:
    You can obtain more information by querying the incident report or system messages
generated by the SSM itself.Please consult the documentation that comes with comes with
the SSM for instructions.

Syslogs:
    None.


------------------------------------------------------------------
Name: ssm-app-fail
Service module failed:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when a connection that is being inspected by the SSM is terminated because the
SSM has failed.

Recommendation:
    The card manager process running in the security appliance control plane issued system
messages and CLI warning to inform you of the failure.Please consult the documentation
that comes with the SSM to trouble shoot the SSM failure.Contact Cisco Technical
Assistance Center (TAC) if needed.

Syslog:
    421001.


------------------------------------------------------------------
Name: ssm-app-incompetent
Service module incompetent:
    This counter only applies to the ASA 5500 series adaptive security appliance.It is
incremented when a connection is supposed to be inspected by the SSM, but the SSM is not
able to inspect it.This counter is reserved for future use.It should always be 0 in the
current release.

Recommendation:
    None.

Syslog:
    None.


------------------------------------------------------------------
```

```
Name: ssl-bad-record-detect
SSL bad record detected:
    This counter is incremented for each unknown SSL record type received from the remote
peer.Any unknown record type received from the peer is treated as a fatal error and the
SSL connections that encounter this error must be terminated.

Recommendation:
    It is not normal to see this counter increment at any time.If this counter is
incremented, it usually means that the SSL protocol state is out of sync with the client
software.The most likely cause of this problem is a software defect in the client
software.Contact the Cisco TAC with the client software or web browser version and provide
a network trace of the SSL data exchange to troubleshoot this problem.

Syslogs:
    None.


-------------------------------------------------------------------
Name: ssl-handshake-failed
SSL handshake failed:
    This counter is incremented when the TCP connection is dropped because the SSL
handshake failed.

Recommendation:
    This is to indicate that the TCP connection is dropped because the SSL handshake
failed.If the problem cannot be resolved based on the syslog information generated by the
handshake failure condition, please include the related syslog information when contacting
the Cisco TAC.

Syslogs:
    725006.
    725014.


-------------------------------------------------------------------
Name: ssl-malloc-error
SSL malloc error:
    This counter is incremented for each malloc failure that occurs in the SSL lib.This is
to indicate that SSL encountered a low memory condition where it can't allocate a memory
buffer or packet block.

Recommendation:
    Check the security appliance memory and packet block condition and contact Cisco the
TAC with this memory information.

Syslogs:
    None.


-------------------------------------------------------------------
Name: ctm-crypto-request-error
CTM crypto request error:
    This counter is incremented each time CTM cannot accept our crypto request.This
usually means the crypto hardware request queue is full.

Recommendation:
    Issue the show crypto protocol statistics ssl command and contact the Cisco TAC with
this information.

Syslogs:
    None.


-------------------------------------------------------------------
```

```
Name: ssl-record-decrypt-error
SSL record decryption failed:
    This counter is incremented when a decryption error occurs during SSL data
receive.This usually means that there is a bug in the SSL code of the ASA or peer, or an
attacker may be modifying the data stream.The SSL connection has been closed.

Recommendation:
    Investigate the SSL data streams to and from your ASA.If there is no attacker, then
this indicates a software error that should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: np-socket-conn-not-accepted
A new socket connection was not accepted:
    This counter is incremented for each new socket connection that is not accepted by the
security appliance.

Recommendation:
    It is possible to see this counter increment as part of normal operation.However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect.Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-failure
NP socket failure:
    This is a general counter for critical socket processing errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-relay-failure
NP socket relay failure:
    This is a general counter for socket relay processing errors.

Recommendation:
    It is possible to see this counter increment as part of normal operation.However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect.Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-data-move-failure
NP socket data movement failure:
    This counter is incremented for socket data movement errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.
```

```
Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-new-conn-failure
NP socket new connection failure:
    This counter is incremented for new socket connection failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-transport-closed
NP socket transport closed:
    This counter is incremented when the transport attached to the socket is abruptly
closed.

Recommendation:
    It is possible to see this counter increment as part of normal operation.However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect.Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-block-conv-failure
NP socket block conversion failure:
    This counter is incremented for socket block conversion failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: ssl-received-close-alert
SSL received close alert:
    This counter is incremented each time the security appliance receives a close alert
from the remote client.This indicates that the client has notified us they are going to
drop the connection.It is part of the normal disconnect process.

Recommendation:
    None.

Syslog:
    725007.


----------------------------------------------------------------
Name: children-limit
Max per-flow children limit exceeded:
    The number of children flows associated with one parent flow exceeds the internal
limit of 200.
```

```
Recommendation:
    This message indicates either a misbehaving application or an active attempt to
exhaust the firewall memory.Use "set connection per-client-max" command to further fine
tune the limit.For FTP, additionally enable the "strict" option in "inspect ftp".

Syslogs:
    210005


----------------------------------------------------------------
Name: tracer-flow
packet-tracer traced flow drop:
    This counter is internally used by packet-tracer for flow freed once tracing is
complete.

Recommendation:
    None.

Syslog:
    None.


----------------------------------------------------------------
Name: sp-looping-address
looping-address:
    This counter is incremented when the source and destination addresses in a flow are
the same.SIP flows where address privacy is enabled are excluded, as it is normal for
those flows to have the same source and destination address.

 Recommendation:
    There are two possible conditions when this counter will increment. One is when the
appliance receives a packet with the source address equal to the destination. This
represents a type of DoS attack. The second is when the NAT configuration of the appliance
NATs a source address to equal that of the destination. One should examine syslog message
106017 to determine what IP address is causing the counter to increment, then enable
packet captures to capture the offending packet, and perform additional analysis.

 Syslogs:
    106017


----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter will increment when the security appliance receives a packet on an
existing flow that no longer has a valid output adjacency.This can occur if the nexthop is
no longer reachable or if a routing change has occurred typically in a dynamic routing
environment.

 Recommendation:
    No action required.

 Syslogs:
    None


----------------------------------------------------------------
Name: np-midpath-service-failure
NP midpath service failure:
    This is a general counter for critical midpath service errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.
```

```
Syslog:
    None.


----------------------------------------------------------------
Name: np-midpath-cp-event-failure
NP midpath CP event failure:
    This is counter for critical midpath events that could not be sent to the CP.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-context-removed
NP virtual context removed:
    This counter is incremented when the virtual context with which the flow is going to
be associated has been removed.This could happen in multi-core environment when one CPU
core is in the process of destroying the virtual context, and another CPU core tries to
create a flow in the context.

Recommendation:
    No action is required.

Syslog:
    None.


----------------------------------------------------------------
Name: fover-idle-timeout
Flow removed from standby unit due to idle timeout:
    A flow is considered idle if standby unit no longer receives periodical update from
active which is supposed to happen to at fixed internal when flow is alive.This counter is
incremented when such flow is removed from standby unit.

Recommendation:
    This counter is informational.

Syslogs:
    None.


----------------------------------------------------------------
Name: dynamic-filter
Flow matched dynamic-filter blacklist:
    A flow matched a dynamic-filter blacklist or greylist entry with a threat-level higher
than the threat-level threshold configured to drop traffic.

Recommendation:
    Use the internal IP address to trace the infected host.Take remediation steps to
remove the infection.

Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: route-change
Flow terminated due to route change:
    When the system adds a lower cost (better metric) route, incoming packets that match
the new route will cause their existing connection to be torn down after the user
configured timeout (floating-conn) value.Subsequent packets will rebuild the connection
out the interface with the better metric.

Recommendation:
    To prevent the addition of lower cost routes from affecting active flows, the
'floating-conn' configuration timeout value can be set to 0:0:0.

Syslogs:
    None.


----------------------------------------------------------------
Name: svc-selector-failure
SVC VPN inner policy selector mismatch detected:
    This counter is incremented when an SVC packet is received with an inner IP header
that does not match the policy for the tunnel.

 Recommendation:
    None. This packet will be discarded automatically.

 Syslogs:
    None.


----------------------------------------------------------------
Name: dtls-hello-close
DTLS hello processed and closed:
     This counter is incremented when the UDP connection is dropped after the DTLS client
hello message processing is finished.This does not indicate an error.

Recommendation:
None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.
```

```
 Syslogs:
    None.


----------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in conversion of IPv6 traffic to IPv4 or
vice-versa.

 Recommendation:
    None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if director/backup unit no longer receives
periodical update from owner which is supposed to happen at fixed interval when flow is
alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected.The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.
```

```
Recommendations:
    This counter is informational and the behavior expected.The packet is processed by
master.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow.The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync because cluster master has
changed.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync becasue the parent flow's owner has left the cluster.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster.And there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: vpn-overlap-conflict

VPN Network Overlap Conflict:
When a packet is decrypted, the inner packet is examined against the crypto map
configuration.If the packet matches a different crypto map entry than the one it was
received on, it will be dropped and this counter will increment.A common cause for this is
two crypto map entries containing similar/overlapping address spaces.

Recommendation:
    Check your VPN configuration for overlapping networks.Verify the
    order of your crypto maps and use of deny rules in ACLs.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: invalid-vxlan-segment-id
Invalid VXLAN segment-id:
    This counter is incremented when the security appliance sees an invalid VXLAN
segment-id attached to a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-valid-nve-ifc
No valid NVE interface:
    This counter is incremented when the security appliance fails to identify the NVE
interface of a VNI interface for a flow.

Recommendation:
    Verify that the nve is configured for all interfaces.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-peer-nve
Invalid peer NVE:
    This counter is incremented when the security appliance fails to get IP and MAC
address of a peer NVE for a flow.

Recommendation:
    Verify that peer nve is configured or learned for the nve.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-encap-error
Fail to encap with VXLAN:
    This counter is incremented when the security appliance fails to encapsulate a packet
with VXLAN for a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-request
SFR requested to terminate the flow:
    The SFR requested to terminate the flow.The actions bit 0 is set.
Recommendation:
    Review SFR policies for any such rule denying the flow.
```

```
Syslogs:
    None.


-----------------------------------------------------------------
Name: reset-by-sfr
SFR requested to terminate and reset the flow:
    The SFR requested to terminate and reset the flow.The actions bit 1 is set.
Recommendation:
    Review SFR policies for any such rule denying the flow.

Syslogs:
    None.


-----------------------------------------------------------------
Name: sfr-fail-close
Flow was terminated:
    The flow was terminated because the card is down and the configured policy was
'fail-close'.
Recommendation:
    Check card status and attempt to restart services or reboot it.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cmd-invalid-encap
The security appliance received an invalid CMD packet.
     An invalid CMD packet is one which does not conform to the standard CMD header
values.This counter checks if the packet conforms to the correct metadata, version,
length, option and sgt range.
Recommendation:
     None.

Syslogs:
     None.


-----------------------------------------------------------------
Name: ifc-not-cmd-enabled
The security appliance receives a CMD packet on an interface not configured to receive
one.
     The packet is dropped.
Recommendation:
     None.

Syslogs:
     None.


-----------------------------------------------------------------
Name: ifc-zn-chg
Interface experienced a zone change
     The parent interface has been joined or left a zone.
Recommendation:
     None.

Syslogs:
     302014, 302016, 302018, 302021, 302304


-----------------------------------------------------------------
```

示例

以下是 **show asp drop** 命令的输出示例，带有指示计数器上次清除时间的时间戳：

```
ciscoasa# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                              3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                          4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                             760
  Expired flow (flow-expired)                                               1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                                 24
  NAT failed (nat-failed)                                               28739
  NAT reverse path failed (nat-rpf-failed)                              22266
  Inspection failure (inspect-fail)                                     19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

相关命令

命令	说明
capture	捕获数据包，包括基于 ASP 丢弃代码捕获数据包的选项。
clear asp drop	清除加速安全路径的丢弃统计信息。
show conn	显示关于连接的信息。

show asp event dp-cp

要调试数据路径或控制路径事件队列，请在特权 EXEC 模式下使用 **show asp event dp-cp** 命令。

show asp event dp-cp [**cxsc msg**]

语法说明

cxsc msg	（可选）标识发送到 CXSC 事件队列的 CXSC 事件消息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.0(1)	引入了此命令。
9.1(3)	添加了路由事件队列条目。

使用指南

show asp event dp-cp 命令显示数据路径和控制路径的内容，可帮助您对问题进行故障排除。有关数据路径和控制路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp event dp-cp** 命令的输出示例：

```
ciscoasa# show asp event dp-cp

DP-CP EVENT QUEUE                 QUEUE-LEN  HIGH-WATER
Punt Event Queue                          0        2048
Routing Event Queue                       0           1
Identity-Traffic Event Queue              0          17
General Event Queue                       0           0
Syslog Event Queue                        0        3192
Non-Blocking Event Queue                  0           4
Midpath High Event Queue                  0           0
Midpath Norm Event Queue                  0           0
SRTP Event Queue                          0           0
HA Event Queue                            0           3
Threat-Detection Event Queue              0           3
ARP Event Queue                           0           3
IDFW Event Queue                          0           0
CXSC Event Queue                          0           0
```

```
EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920        4372
  inspect-sunrp   4005920          0   935295  3070625  4005920        4372
routing              77          0       77        0       77           0
arp-in              618          0      618        0      618           0
identity-traffic   1519          0     1519        0     1519           0
syslog             5501          0     5501        0     5501           0
threat-detection     12          0       12        0       12           0
ips-cplane         1047          0     1047        0     1047           0
ha-msg              520          0      520        0      520           0
cxsc-msg            127          0      127        0      127           0
```

show asp load-balance

要显示负载平衡器队列大小的直方图，请在特权 EXEC 模式下使用 **show asp load-balance** 命令。

show asp load-balance [detail]

语法说明

detail	（可选）显示关于哈希桶的详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.1(1)	引入了此命令。

使用指南

show asp load-balance 命令可帮助您对问题进行故障排除。通常，数据包将由从接口接收环拉入的同一核心进行处理。但是，如果另一个核心已经处理与刚接收的数据包相同的连接，则该数据包将排队至该核心。这种排队可能会导致负载平衡器队列增长，而其他核心处于空闲状态。有关详细信息，请参阅 **asp load-balance per-packet** 命令。

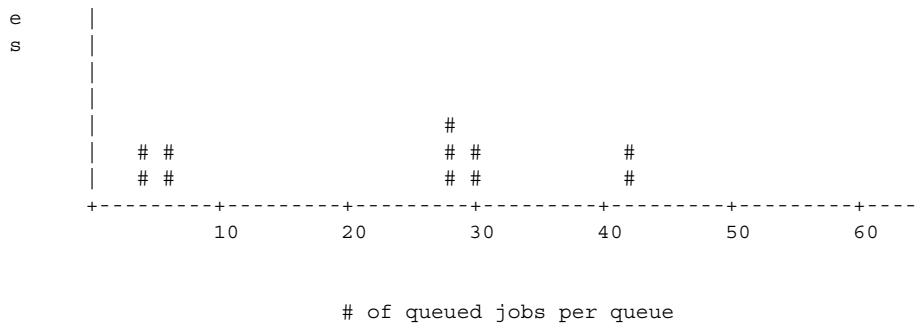
示例

以下是 **show asp load-balance** 命令的输出示例。X 轴表示在不同队列中排队的数据包数量。Y 轴表示有数据包排队的负载平衡器哈希桶数量，请不要与直方图标题中的桶（指直方图桶）混淆。要了解拥有队列的哈希桶的确切数量，请使用 **detail** 关键字。

```
ciscoasa# show asp load-balance

Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes

  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
```



以下是 **show asp load-balance detail** 命令的输出示例。

```
ciscoasa# show asp load-balance detail

<Same histogram output as before with the addition of the following values for the
histogram>

Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

相关命令

命令	说明
asp load-balance per-packet	更改多核心 ASA 型号的核心负载平衡方法。

show asp load-balance per-packet

要显示每个数据包 ASP 负载平衡的特定统计信息，请在特权 EXEC 模式下使用 **show asp load-balance per-packet** 命令。

show asp load-balance per-packet [**history**]

语法说明

history	（可选）显示配置状态（已启用、已禁用或自动）、当前状态（已启用或已禁用）、高低水印、全局阈值、自动切换发生次数，自动切换启用后的最短和最长等待时间、每个数据包的 ASP 负载平衡历史及时间戳及其打开和关闭的原因。

默认值

如果您没有指定任何选项，此命令将显示基本状态、相关值以及每个数据包的 ASP 负载平衡统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

show asp load-balance per-packet 命令显示配置状态（已启用、已禁用或自动）、当前状态（已启用或已禁用）、高低水印、全局阈值、自动切换发生次数，自动切换启用后的最短和最长等待时间（针对每个数据包的 ASP 负载平衡）。

该信息将显示为以下格式：

```
Config mode    : [ enabled | disabled | auto ]
Current status : [ enabled | disabled ]

RX ring Blocks low/high watermark      : [RX ring Blocks low watermark in percentage] /
[RX ring Blocks high watermark in percentage]
System RX ring count low threshold     : [System RX ring count low threshold] / [Total
number of RX rings in the system]
System RX ring count high threshold    : [System RX ring count high threshold] / [Total
number of RX rings in the system]
```

自动模式

```
Current RX ring count threshold status : [Number of RX rings crossed watermark] / [Total
number of RX rings in the system]
```

```
Number of times auto switched          : [Number of times ASP load-balance per-packet has
been switched]
Min/max wait time with auto enabled    : [Minimal wait time with auto enabled] / [Maximal
wait time with auto enabled] (ms)
```

手动模式

```
Current RX ring count threshold status : N/A
```

只有 ASA 5585-X 和 ASASM 支持使用此命令。

示例

以下是 **show asp load-balance per-packet** 命令的输出示例：

```
ciscoasa# show asp load-balance per-packet

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)
```

以下是 **show asp load-balance per-packet history** 命令的输出示例：

```
ciscoasa# show asp load-balance per-packet history

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)

==========================================================================================
From State          To State            Reason
==========================================================================================
15:07:13 UTC Dec 17 2013
Manually Disabled   Manually Disabled   Disabled at startup

15:09:14 UTC Dec 17 2013
Manually Disabled   Manually Enabled    Config

15:09:15 UTC Dec 17 2013
Manually Enabled    Auto Disabled       0/33 of the ring(s) crossed the watermark

15:10:16 UTC Dec 17 2013
Auto Disabled       Auto Enabled        1/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[04] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[05] crossed above high watermark
```

```
15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] dropped below low watermark

15:10:17 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] crossed above high watermark

(---More---)

15:14:01 UTC Dec 17 2013
Auto Enabled        Auto Disabled       8/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] crossed above high watermark

15:14:01 UTC Dec 17 2013
Auto Disabled       Auto Enabled        7/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] dropped below low watermark

(---More---)

15:20:11 UTC Dec 17 2013
Auto Enabled        Auto Disabled       0/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] dropped below low watermark
(---More---)
```

相关命令

命令	说明
asp load-balance per-packet auto	在每个接口接收环或流量组上自动打开和关闭每个数据包的 ASP 负载平衡。
clear asp load-balance history	清除每个数据包的 ASP 负载平衡历史并重置自动切换发生的次数。

show asp table arp

要调试加速安全路径 ARP 表，请在特权 EXEC 模式下使用 **show asp table arp** 命令。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

语法说明

address *ip_address*	（可选）标识您要查看 ARP 表条目的 IP 地址。
interface *interface_name*	（可选）标识您要查看 ARP 表的特定接口。
netmask *mask*	（可选）设置 IP 地址的子网掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show arp 命令显示控制层面的内容，而 **show asp table arp** 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table arp** 命令的输出示例：

```
ciscoasa# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

相关命令

命令	说明
show arp	显示 ARP 表。
show arp statistics	显示 ARP 统计信息。

show asp table classify

要调试加速安全路径分类器表，请在特权 EXEC 模式下使用 **show asp table classify** 命令。

show asp table classify [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

语法说明

crypto	（可选）仅显示加密、解密和 ipsec 隧道流域。
domain *domain_name*	（可选）显示特定分类器域的条目。有关域列表，请参阅 “ 使用指南 ” 部分。
hits	（可选）显示具有非零命中值的分类器条目。
interface *interface_name*	（可选）标识您要查看分类器表的特定接口。
match *regexp*	（可选）显示匹配正则表达式的分类器条目。正则表达式包含空格时请使用引号。
user-statistics	（可选）指定用户和组信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(4)	添加了 **hits** 选项和时间戳，用于指示 ASP 表计数器上次清除时间。
8.0(2)	添加了新计数器，用于显示匹配汇编中止的次数。此计数器仅当该值大于 0 时显示。
8.2(2)	添加了 **match** *regexp* 选项。
8.4(4.1)	为 ASA CX 模块添加了 **csxc** 和 **cxsc-auth-proxy** 域。
9.0(1)	添加了 **user-statistics** 关键字。输出已更新为添加安全组名称以及源和目标标记。
9.2(1)	为 ASA FirePOWER 模块添加了 sfr 域。
9.3(1)	安全组标记 (SGT) 值在输出中已修改。标记值 “tag=0” 表示确切匹配 0x0，即 “ 未知 ” 的保留 SGT 值。SGT 值 “tag=any” 表示该规则中您无需考虑的值。

使用指南

show asp table classify 命令显示加速安全路径的分类器内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。分类器检查传入数据包的属性（例如协议）以及源和目标地址，从而将每个数据包匹配适当的分类规则。每个规则均使用确定执行何种类型操作（例如丢弃数据包还是允许其通过）的分类域进行标记。所示信息仅用于调试目的，输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

分类器域包括以下内容：

```
aaa-acct
aaa-auth
aaa-user
accounting
app-redirect
arp
autorp
backup interface CLI (Apply backup interface rule)
capture
cluster-drop-mcast-from-peer
cluster-drop-on-non-owner
cluster-drop-on-slave
cluster-mark-mcast-from-peer
cluster-redirect
conn-nailed
conn-set
ctcp
cxsc
cxsc-auth-proxy
debug-icmp-trace
decrypt
dhcp
dynamic-filter
eigrp
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
flow-export
host
host-limit
hqf
ids
inspect-ctiqbe
inspect-dcerpc
inspect-dns-cp
inspect-dns-ids
inspect-dns-np
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-im
inspect-ip-options
inspect-ipsec-pass-thru
inspect-ipv6
inspect-mgcp
inspect-mmp
inspect-netbios
```

```
inspect-phone-proxy
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-scansafe
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-srtp
inspect-sunrpc
inspect-tftp
inspect-waas
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipv6
l2tp
l2tp-ppp
limits
lu
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-per-session
nat-reverse
no forward CLI (Apply no forward interface rule)
null
ospf
permit
permit-ip-option
permit-ip-option-explicit
pim
ppp
priority-q
punt
punt-root (soft NP)
qos
qos-per-class (soft NP)
qos-per-dest  (soft NP)
qos-per-flow  (soft NP)
qos-per-source (soft NP)
rip
sal-relay
sfr
shun
soft-np-tcp-module
soft-np-udp-module
splitdns
ssm
ssm-app-capacity
ssm-isvw
ssm-isvw-capable
svc-ib-tunnel-flow
svc-ob-tunnel-flow
tcp-intercept
tcp-ping
udp-unidirectional
user-statistics
vpn-user
wccp
```

示例

以下是 **show asp table classify** 命令的输出示例：

```
ciscoasa# show asp table classify

Interface test:
No.of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

以下是 **show asp table classify hits** 命令的输出示例，带有上次清除命中计数器的记录：

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

以下是 **show asp table classify hits** 命令的输出示例，其中包括第 2 层信息：

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any

.
.
.
```

```
Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

以下是访问列表中未指定安全组时 **show asp table classify** 命令的输出示例：

```
ciscoasa# show asp table classify
in  id=0x7ffedb54cfe0, priority=500, domain=permit, deny=true
        hits=0, user_data=0x6, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=224.0.0.0, mask=240.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any
```

相关命令

命令	说明
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp table cluster chash-table

要调试加速安全路径 cHash 表用于集群，请在特权 EXEC 模式下使用 **show asp table cluster chash-table** 命令。

show asp table cluster chash-table

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show asp table cluster chash-table 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table cluster chash-table** 命令的输出示例：

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
33111111
11000112
22332000
00231121
```

```
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

相关命令

命令	说明
show asp cluster counter	显示集群数据路径计数器信息。

show asp table cts sgt-map

要显示 Cisco TrustSec 数据路径内维护的 IP 地址安全组表数据库中的 IP 地址安全组表映射，请在特权 EXEC 模式下使用 **show asp table cts sgt-map** 命令。

show asp table cts sgt-map [**address** *ipv4* | **address** *ipv6* | **ipv4** | **ipv6** | **sgt** *sgt*]

语法说明

address *ipv4*	（可选）显示指定 IPv4 地址的 IP 地址安全组表映射。
address *ipv6*	（可选）显示指定 IPv6 地址的 IP 地址安全组表映射。
ipv4	（可选）显示 IPv4 地址的所有 IP 地址安全组表映射。
ipv6	（可选）显示 IPv6 地址的所有 IP 地址安全组表映射。
sgt *sgt*	（可选）显示指定安全组表的 IP 地址安全组表映射。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

如果没有指定地址，则数据路径内 IP 地址安全组表数据库中的所有条目都将显示。地址可以是具体的地址，也可以是基于子网的地址。此外，安全组名称将在可用时显示。

示例

以下是 **show asp table cts sgt-map** 命令的输出示例：

```
ciscoasa# show asp table cts sgt-map

IP Address                              SGT
================================================
10.10.10.5                              1234:Marketing
55.67.89.12                             5:Engineering
56.34.0.0                               338:HR
192.4.4.4                               345:Finance

Total number of entries shown = 4
```

以下是 **show asp table cts sgt-map address** 命令的输出示例：

```
ciscoasa# show asp table cts sgt-map address 10.10.10.5

IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing

Total number of entries shown = 1
```

以下是 **show asp table cts sgt-map ipv6** 命令的输出示例：

```
ciscoasa# show asp table cts sgt-map ipv6

IP Address                                SGT
============================================================
FE80::A8BB:CCFF:FE00:110                  17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                  18:Eng-Servers

Total number of entries shown = 2
```

以下是 **show asp table cts sgt-map sgt** 命令的输出示例：

```
ciscoasa# show asp table cts sgt-map sgt 17

IP Address                                SGT
============================================
FE80::A8BB:CCFF:FE00:110                  17

Total number of entries shown = 1
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts environment	显示环境数据刷新操作的运行状况和状态。

show asp table dynamic-filter

要调试加速安全路径僵尸网络流量过滤器表，请在特权 EXEC 模式下使用 **show asp table dynamic-filter** 命令。

show asp table dynamic-filter [**hits**]

语法说明

hits	（可选）显示具有非零命中值的分类器条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

show asp table dynamic-filter 命令显示加速安全路径中的僵尸网络流量过滤器规则，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table dynamic-filter** 命令的输出示例：

```
ciscoasa# show asp table dynamic-filter

Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
 Address 10.64.147.16 mask 255.255.255.255 name:
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show asp table filter

要调试加速安全路径过滤器表，请在特权 EXEC 模式下使用 **show asp table filter** 命令。

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

语法说明

acl-name	（可选）指定用于指定访问列表的已安装过滤器。
hits	（可选）指定具有非零命中值的过滤器规则。
match *regexp*	（可选）显示匹配正则表达式的分类器条目。正则表达式包含空格时请使用引号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

当过滤器应用到 VPN 隧道后，过滤器规则将安装到过滤器表。如果隧道已指定过滤器，则加密前和解密后检查过滤器表，以确定应允许还是拒绝内部数据包。

示例

以下是 user1 连接前 **show asp table filter** 命令的输出示例。IPv4 和 IPv6 在入站和出站方向均只安装了隐含的拒绝规则。

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
```

以下是 user1 连接后 **show asp table filter** 命令的输出示例。VPN 过滤器 ACL 基于入站方向定义 - 源表示对等设备，而目标表示内部资源。出站规则通过交换入站规则的源和目标得出。

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
         hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
         hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
         src ip=95.1.224.100, mask=255.255.255.255, port=21
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
         src ip=95.1.224.100, mask=255.255.255.255, port=5001
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
         src ip=95.1.224.100, mask=255.255.255.255, port=5002
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
         src ip=95.1.224.100, mask=255.255.255.255, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
         hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f298, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

相关命令

命令	说明
show asp drop	显示已丢弃数据包的加速安全路径计数器。
show asp table classifier	显示加速安全路径的分类器内容。

show asp table interfaces

要调试加速安全路径接口表，请在特权 EXEC 模式下使用 **show asp table interfaces** 命令。

show asp table interfaces

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show asp table interfaces 命令显示加速安全路径的接口表内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table interfaces** 命令的输出示例：

```
ciscoasa# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
```

```
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。

show asp table routing

要调试加速安全路径路由表，请在特权 EXEC 模式下使用 **show asp table routing** 命令。此命令支持 IPv4 和 IPv6 地址。

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

语法说明

address *ip_address*	设置您要查看路由条目的 IP 地址。对于 IPv6 地址，您可以包含子网掩码，形式为斜线 (/) 后跟前缀（0 至 128）。例如，输入以下内容： `fe80::2e0:b6ff:fe01:3b7a/128`
input	显示输入路由表的条目。
interface *interface_name*	（可选）标识您要查看路由表的特定接口。
netmask *mask*	对于 IPv4 地址，指定子网掩码。
output	显示输出路由表的条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(2)	我们添加了每个区域信息的路由。

使用指南

show asp table routing 命令显示加速安全路径的路由表内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

注　ASA 5505 的 show asp table routing 命令输出中可能会显示无效的条目。

示例

以下是 **show asp table routing** 命令的输出示例：

```
ciscoasa# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

注　ASA 5505 平台的 **show asp table routing** 命令输出中可能会显示无效的条目。忽略这些条目；它们没有任何影响。

相关命令

命令	说明
show route	在控制层面中显示路由表。

show asp table socket

为帮助调试加速安全路径套接字信息，请在特权 EXEC 模式下使用 **show asp table socket** 命令。

show asp table socket [**socket handle**] [**stats**]

语法说明

socket handle	指定套接字的长度。
stats	显示加速安全路径套接字表的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

show asp table socket 命令显示加速安全路径套接字信息，可在对加速安全路径套接字问题进行故障排除时提供帮助。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table socket** 命令的输出示例：

```
TCP Statistics:
  Rcvd:
     total14794
     checksum errors0
     no port0
  Sent:
     total0

UDP Statistics:
  Rcvd:
     total0
     checksum errors0
  Sent:
     total0
     copied0

NP SSL System Stats:
  Handshake Started:33
```

```
Handshake Complete:33
SSL Open:4
SSL Close:117
SSL Server:58
SSL Server Verify:0
SSL Client:0
```

TCP/UDP 统计信息是数据包计数器，表示指向 ASA 上运行或侦听的服务（例如 Telnet、SSH 或 HTTPS）的发送或接收数据包数量。校验和错误是由于计算的数据包校验和不匹配数据包中存储的校验和值（也就是说，数据包已损坏）而丢弃的数据包数量。NP SSL 统计信息指示收到的每种类型的消息数量。大多数消息均指示开始和结束到 SSL 服务器或 SSL 客户端的新 SSL 连接。

相关命令

命令	说明
show asp table vpn-context	显示加速安全路径 VPN 情景表。

show asp table vpn-context

要调试加速安全路径 VPN 情景表，请在特权 EXEC 模式下使用 **show asp table vpn-context** 命令。

show asp table vpn-context [**detail**]

语法说明

detail	（可选）显示 VPN 情景表的更多详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(4)	添加了 +PRESERVE 标记，用于隧道丢弃后保持状态流量的每个情景。
9.0(1)	增加了多情景模式支持。

使用指南

show asp table vpn-context 命令显示加速安全路径的 VPN 情景内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table vpn-context** 命令的输出示例：

```
ciscoasa# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

以下是启用永久 IPsec 隧道流功能后（如 PRESERVE 标记所示）**show asp table vpn-context** 命令的输出示例：

```
ciscoasa(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

以下是 **show asp table vpn-context detail** 命令的输出示例：

```
ciscoasa# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

以下是启用永久 IPsec 隧道流功能后（如 PRESERVE 标记所示）**show asp table vpn-context detail** 命令的输出示例：

```
ciscoasa(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
ciscoasa(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

相关命令

命令	说明
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp table zone

要调试加速安全路径区域表，请在特权 EXEC 模式下使用 **show asp table zone** 命令。

show asp table zone [*zone_name*]

语法说明

zone_name	（可选）标识区域名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

show asp table zone 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。有关加速安全路径的详细信息，请参阅 CLI 配置指南。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table zone** 命令的输出示例：

```
ciscoasa# show asp table zone

Zone: outside-zone id: 2
 Context: test-ctx
  Zone Member(s) : 2
   outside1       GigabitEthernet0/0
   outside2       GigabitEthernet0/1
```

相关命令

命令	说明
show asp table routing	显示用于调试的加速安全路径表，并显示与每个路由关联的区域。
show zone	显示区域 ID、情景、安全级别和成员。

show auto-update

要查看自动更新服务器状态，请在特权 EXEC 模式下使用 **show auto-update** 命令。

show auto-update

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	我们引入了此命令。

使用指南

使用此命令可查看自动更新服务器状态。

示例

以下是 **show auto-update** 命令的输出示例：

```
ciscoasa(config)# show auto-update
Poll period: 720 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: host name [ciscoasa]
```

相关命令

auto-update device-id	设置 ASA 设备 ID 用于自动更新服务器。
auto-update poll-period	设置 ASA 从自动更新服务器检查更新的频率。
auto-update server	标识自动更新服务器。
auto-update timeout	如果未在超时时间内连接到自动更新服务器，则阻止流量通过 ASA。
clear configure auto-update	清除自动更新服务器配置。
show running-config auto-update	显示自动更新服务器配置。

show bgp 至 show cpu 命令

show bgp

要显示边界网关协议 (BGP) 路由表中的条目，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp** 命令。

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*]]

语法说明

ip-address	（可选）指定 AS 路径访问列表名称。
mask	（可选）用于过滤作为指定网络的一部分的主机或与它们匹配的掩码。
longer-prefixes	（可选）显示指定的路由和所有更具体的路由。
injected	（可选）显示向 BGP 路由表中注入的更具体的前缀。
shorter-prefixes	（可选）显示指定的路由和所有不太具体的路由。
length	（可选）前缀长度。此参数的值是一个介于 0 到 32 之间的数字。
bestpath	（可选）显示此前缀的最佳路径。
multipaths	（可选）显示此前缀的多个路径。
subnets	（可选）显示指定前缀的子网路由。
all	（可选）显示 BGP 路由表中的所有地址系列信息。
prefix-list *name*	（可选）过滤基于指定的前缀列表的输出。
pending-prefixes	（可选）显示有待从 BGP 路由表中删除的前缀。
route-map *name*	（可选）过滤基于指定的路由映射的输出。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

show bgp 命令用于显示 BGP 路由表的内容。可以过滤输出以显示特定前缀、前缀长度和通过前缀列表、路由映射或条件通告注入的前缀的条目。

在思科 IOS 版本 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、思科 IOS XE 版本 2.4 及更高版本中，思科实施 4 字节自主系统编号时使用 asplain（例如 65538）作为自主系统编号的默认正则表达式匹配和输出显示格式，但您可以 RFC 5396 中所述的 asplain 格式和 asdot 格式配置 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后接 **clear bgp *** 命令来执行所有当前 BGP 会话的硬重置。

示例

以下输出示例展示 BGP 路由表：

```
Router# show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

表 4-1 显示每个字段的说明。

表 4-1　show bgp 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： • s - 表条目被抑制。 • d - 表条目被阻尼。 • h - 表条目历史记录。 • * - 表条目有效。 • > - 表条目是用于该网络的最佳条目。 • i - 通过内部 BGP (iBGP) 会话获知表条目。 • r - 表条目为 RIB 故障。 • S - 表条目过时。 • m - 表条目具有用于该网络的多个路径。 • b - 表条目具有用于该网络的备用路径。 • x - 表条目具有用于该网络的最佳外部路由。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： • i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 • e - 从外部网关协议 (EGP) 发起的条目。 • ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。

字段	说明
Network	网络实体的 IP 地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示路由器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。
(stale)	表示在平滑重启过程中将指定的自主系统的以下路径标记为“stale”。

show bgp（4 字节自主系统编号）：示例

以下输出示例展示具有 4 字节自主系统编号（65536 和 65550，显示在路径字段下）的 BGP 路由表。此示例需要思科 IOS 版本 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、思科 IOS XE 版本 2.4 或更高版本。

```
RouterB# show bgp

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show bgp IP 地址：示例

以下输出示例展示 BGP 路由表中的 192.168.1.0 条目的有关信息：

```
Router# show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

以下输出示例展示 BGP 路由表中的 10.3.3.3 255.255.255.255 条目的有关信息：

```
Router# show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
```

```
    Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

表 4-2 显示每个字段的说明。

表 4-2　show bgp (4 byte autonomous system numbers) 字段

字段	说明
BGP routing table entry fo	路由表条目的 IP 地址或网络号。
version	表的内部版本号。每当表更改时，此数字就会增加。
Paths	可用路径的数量和安装的最佳路径的数量。当最佳路径安装在 IP 路由表中时，此行显示 “Default-IP-Routing-Table”。
Multipath	启用多路径负载共享时，显示此字段。此字段表示多个路径是 iBGP，还是 eBGP。
Advertised to update-groups	为每个更新组处理通告的数量。
Origin	条目的来源。来源可以是 IGP、EGP 或不完整的协议。此行显示配置的指标（0，如果未配置任何指标）、本地首选项值（100 为默认值）和路由（内部、外部、多路径、最佳）的状态和类型。
Extended Community	如果路由具有扩展的社区属性，则显示此字段。属性代码显示在此行上。在后面的一行上显示有关扩展的社区的信息。

show bgp all：示例

以下是使用 **all** 关键字输入的 **show bgp** 命令的输出示例。显示有关所有配置的地址系列的信息。

```
Router# show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
```

```
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

show bgp longer-prefixes：示例

以下是使用 **longer-prefixes** 关键字输入的 **show bgp** 命令的输出示例：

```
Router# show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

show bgp shorter-prefixes：示例

以下是使用 **shorter-prefixes** 关键字输入的 **show bgp** 命令的输出示例。指定 8 位前缀长度。

```
Router# show bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                 0             0 200 ?
```

show bgp prefix-list：示例

以下是使用 **prefix-list** 关键字输入的 **show bgp** 命令的输出示例：

```
Router# show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?

*                   10.0.0.2                 0             0 200 ?
```

show bgp route-map：示例

以下是使用 **route-map** 关键字输入的 **show bgp** 命令的输出示例：

```
Router# show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

show bgp all community

要显示属于特定边界网关协议 (BGP) 社区的所有地址系列的路由，请在用户 EXEC 或特权 EXEC 配置模式下使用 **show bgp all community** 命令。

show bgp all community [*community-number...*[*community-number*]] **[local-as] [no-advertise] [no-export] [exact-match]**

语法说明

community-number.	（可选）显示与指定的社区编号相关的路由。 您可以指定多个社区编号。范围为从 1 到 4294967295 或 AA:NN（自主系统：社区编号，即一个 2 字节数字）。
local-as	（可选）仅显示未在本地自主系统（已知社区）的外部发送的路由。
no-advertise	（可选）仅显示不向任何对等设备（已知社区）通告的路由。
no-export	（可选）仅显示未在本地自主系统（已知社区）的外部导出的路由。
exact-match	（可选）仅显示与指定的 BGP 社区列表完全匹配的路由。 **注**　命令中关键字的可用性取决于命令模式。**exact-match** 关键字在用户 EXEC 模式下不可用。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

用户可以任何顺序输入 **local-as**、**no-advertise** 和 **no-export** 关键字。使用 **bgp all community** 命令时，请确保在已知社区前输入数字社区。

例如，以下字符串无效：

```
ciscoasa# show bgp all community local-as 111:12345
```

使用以下字符串代替：

```
ciscoasa# show bgp all community 111:12345 local-as
```

示例

以下是 **show bgp all community** 命令的输出示例，指定 1, 2345 和 6789012 的社区：

```
ciscoasa# show bgp all community 1 2345 6789012 no-advertise local-as no-export
exact-match

For address family: IPv4 Unicast

BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network  Next Hop            Metric LocPrf Weight Path
*> 10.0.3.0/24       10.0.0.4                               0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                 0             0 4 ?
*> 10.12.34.0/24     10.0.0.6                 0             0 6 ?
```

表 4-3 显示每个字段的说明。

表 4-3　show bgp all community 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	设置为显示 BGP 社区的路由器的路由器 ID。一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 d - 表条目被阻尼。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP 会话获知表条目。
Origin codes	表示条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用网络路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由。
Network	网络实体的网络地址和网络掩码。地址类型取决于地址系列。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。地址类型取决于地址系列。
Metric	自主系统间指标的值。未频繁使用此字段。
LocPrf	使用 **set local-preference** 命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。

show bgp all neighbors

要显示到所有地址系列的邻居的边界网关协议 (BGP) 连接的有关信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp all neighbors** 命令。

show bgp all neighbors [*ip-address*] [**advertised-routes | paths [***reg-exp***] | policy [detail] | received prefix-filter | received-routes | routes]**

语法说明

ip-address	（可选）邻居的 IP 地址。如果省略此参数，则显示有关所有邻居的信息。
advertised-routes	（可选）显示已向邻居通告的所有路由。
paths *reg-exp*	（可选）显示从指定的邻居获知的自主系统路径。可选正则表达式用于过滤输出。
policy	（可选）显示每个地址系列应用于邻居的策略。
detail	（可选）显示详细的策略信息，例如路由映射、前缀列表、社区列表、访问控制列表 (ACL) 和自主系统路径过滤器列表。
received prefix-filter	（可选）显示从指定邻居（出站路由过滤器 [ORF]）发送的前缀列表。
received-routes	（可选）显示从指定邻居收到的所有路由（接受和拒绝的路由）。
routes	（可选）显示收到并接受的所有路由。输入此关键字时显示的输出是 **received-routes** 关键字显示的输出的子集。

默认值

此命令的输出展示所有邻居的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **show bgp all neighbors** 命令显示特定于地址系列（例如 IPv4）的邻居会话的 BGP 和 TCP 连接信息。

示例

以下示例展示 **show bgp all neighbors** 命令的输出：

```
ciscoasa# show bgp all neighbors

For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
```

```
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0


Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent:4445 (retransmit: 5), with data: 4445, total data bytes; 244128
```

表 4-4 显示每个字段的说明。

表 4-4　　show bgp all neighbor 字段

字段	说明
For address family	以下字段引用的地址系列。
BGP neighbor	BGP 邻居的 IP 地址及其自主系统编号。
remote AS	邻居的自主系统编号。
external link	外部边界网关协议 (eBGP) peerP。
BGP version	正在用于与远程路由器通信的 BGP 版本。
remote router ID	邻居的 IP 地址。
BGP state	此 BGP 连接的状态。

表 4-4　show bgp all neighbor 字段（续）

字段	说明
up for	基本 TCP 连接已存在的时间（采用 hh:mm:ss 格式）。
Last read	BGP 最后收到此邻居的消息后的时间（采用 hh:mm:ss 格式）。
hold time	BGP 将保持与此邻居的会话（没有收到消息）的时间（以秒为单位）。
keepalive interval	向此邻居传输保持连接消息的时间间隔（以秒为单位）。
Message statistics	按消息类型组织的统计信息。
InQ depth is	输入队列中的消息的数量。
OutQ depth is	输出队列中的消息的数量。
Sent	传输的消息的总数。
Rcvd	收到的消息的总数。
Opens	发送和收到的 OPEN 消息的数量。
Notifications	发送和收到的通知（错误）消息的数量。
Updates	发送和收到的更新消息的数量。
Keepalives	发送和收到的保持连接消息的数量。
Route Refresh	发送和收到的路由刷新请求消息的数量。
Total	发送和收到的消息的总数。
Default minimum time between...	通告传输之间的时间（以秒为单位）。
Connections established	已成功建立 TCP 和 BGP 连接的次数。
dropped	有效会话失败或被关闭的次数。
Last reset	最后重置此对等会话后的时间（采用 hh:mm:ss 格式）。重置的原因显示在此行上。
External BGP neighbor may be...	表示启用 BGP 生存时间 (TTL) 安全检查。可分离本地和远程对等设备的跃点的最大数量显示在此行上。
Connection state	BGP 对等设备的连接状态。
Local host, Local	本地 BGP 发言者的 IP 地址和端口号。
Foreign host, Foreign port	邻居地址和 BGP 目标端口号。
Enqueued packets for retransmit:	排队进行 TCP 重新传输的数据包。
Event Timers	TCP 事件计时器。用于启动和唤醒的计数器（到期的计时器）。
Retrans	已重新传输数据包的次数。
TimeWait	等待重新传输计时器到期的时间。
AckHold	确认保持计时器。
SendWnd	传输（发送）窗口。
KeepAlive	保持连接数据包的数量。
GiveUp	因不确认而丢弃数据包的次数。
PmtuAger	路径 MTU 发现计时器。

表 4-4　show bgp all neighbor 字段（续）

字段	说明
DeadWait	失效段的到期计时器。
iss:	初始数据包传输序列号。
snduna:	未确认的最后一个传输序列号。
sndnxt:	要传输的下一个数据包序列号。
sndwnd:	远程主机的 TCP 窗口大小。
irs:	初始数据包接收序列号。
rcvnxt:	本地确认的最后一个接收序列号。
rcvwnd:	本地主机的 TCP 窗口大小。
delrcvwnd:	延迟的接收窗口 - 本地主机从连接中读取，但未从主机向远程主机通告的接收窗口中减去的数据。此字段中的值逐渐增加，直到它大于全尺寸数据包为止，届时将该值应用于 rcvwnd 字段。
SRTT:	计算的平滑的往返超时。
RTTO:	往返超时。
RTV:	往返时间的差异。
KRTT:	新的往返超时（使用 Karn 算法）。此字段分别跟踪重新发送的数据包的往返时间。
minRTT:	记录的最小往返超时（用于计算的硬接线值）。
maxRTT:	记录的最大往返超时。
ACK hold	本地主机将延迟确认以携带（背载）附加数据的时间长度。
IP Precedence value	BGP 数据包的 IP 优先级。
Datagrams	从邻居收到的更新数据包的数量。
Rcvd:	收到的数据包的数量。
with data	与数据一起发送的更新数据包的数量。
total data bytes	收到的数据的总量（以字节为单位）。
Sent	发送的更新数据包的数量。
with data	与数据一起收到的更新数据包的数量。
total data bytes	发送的数据的总量（以字节为单位）。

show bgp cidr-only

要使用无类域间路由 (CIDR) 显示路由，请在 EXEC 模式下使用 **show bgp cidr-only** 命令。

show bgp cidr-only

语法说明

此命令没有任何参数或关键字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp cidr-only** 命令的输出示例：

```
ciscoasa# show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

表 4-5 显示每个字段的说明。

表 4-5　show bgp cidr-only 字段

字段	说明
BGP table version is 220	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。

表 4-5　show bgp cidr-only 字段（续）

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp community

要显示属于指定的 BGP 社区的路由，请在 EXEC 模式下使用 **show bgp community** 命令。

show bgp community *community-number* **[exact]**

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp community** 命令在特权 EXEC 模式下的输出示例：

```
ciscoasa# show bgp community 111:12345 local-as

 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ?- incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2            0             0 222 ?
 *> 10.0.0.0         10.43.222.2            0             0 222 ?
 *> 10.43.0.0        10.43.222.2            0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2            0             0 222 ?
 *  10.43.222.0/24   10.43.222.2            0             0 222 i
 *> 172.17.240.0/21  10.43.222.2            0             0 222 ?
 *> 192.168.212.0    10.43.222.2            0             0 222 i
 *> 172.31.1.0       10.43.222.2            0             0 222 ?
```

表 4-6 显示每个字段的说明。

表 4-6　show bgp community 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。

表 4-6　show bgp community 字段（续）

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp community-list

要显示边界网关协议 (BGP) 社区列表允许的路由，请在用户或特权 EXEC 模式下使用 **show bgp community-list** 命令。

show bgp community-list {*community-list-number* | *community-list-name* [**exact-match**]}

语法说明

community-list-number	标准或扩展的社区列表编号，范围为从 1 到 500。
community-list-name	社区列表名称。社区列表名称可以是标准名称或扩展的名称。
exact-match	（可选）仅显示具有完全匹配项的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令需要您指定使用时的参数。**exact-match** 关键字是可选的。

示例

以下是 **show bgp community-list** 命令在特权 EXEC 模式下的输出示例：

```
ciscoasa# show bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1              0    100      0 1800 1239 ?
*>i                 10.0.16.1              0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1              0    100      0 1800 690 568 ?
*>i                 10.0.16.1              0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1              0    100      0 1800 701 35 ?
*>i                 10.0.16.1              0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1              0    100      0 1800 690 560 ?
*>i                 10.0.16.1              0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1              0    100      0 1800 690 200 ?
*>i                 10.0.16.1              0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1              0    100      0 1800 174 ?
*>i                 10.0.16.1              0    100      0 1800 174 ?
```

```
* i10.16.0.0         10.0.22.1               0    100      0 1800 701 i
*>i                  10.0.16.1               0    100      0 1800 701 i
*                    10.92.72.24                           0 1878 704 701 i
```

表 4-7 显示每个字段的说明。

表 4-7　show bgp community-list 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp filter-list

要显示符合指定的过滤器列表的路由，请在 EXEC 模式下使用 **show bgp filter-list** 命令。

show bgp filter-list *access-list-name*

语法说明

access-list-name	自主系统路径访问列表的名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp filter-list** 命令在特权 EXEC 模式下的输出示例：

```
ciscoasa# show bgp filter-list filter-list-acl

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

表 4-8 显示每个字段的说明。

表 4-8　show bgp filter-list 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp injected-paths

要显示边界网关协议 (BGP) 路由表中的所有注入的路径，请在用户或特权 EXEC 模式下使用 **show bgp injected-paths** 命令。

show bgp injected-paths

语法说明

此命令没有任何参数或关键字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp injected-paths** 命令在 EXEC 模式下的输出示例：

```
ciscoasa# show bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

表 4-9 显示每个字段的说明。

表 4-9　show bgp injected-path 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。

表 4-9　show bgp injected-path 字段（续）

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv4

要显示 IP 版本 4 (IPv4) 边界网关协议 (BGP) 路由表中的条目，请在特权 EXEC 模式下使用 **show bgp ipv4** 命令。

show bgp ipv4

语法说明

此命令没有任何参数或关键字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp ipv4 unicast** 命令的输出示例：

```
ciscoasa# show bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

以下是 **show bgp ipv4 multicast** 命令的输出示例：

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

表 4-10 显示每个字段的说明。

表 4-10　show bgp ipv4 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6

要显示 IPv6 边界网关协议 (BGP) 路由表中的条目，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp ipv6** 命令。

show bgp ipv6 unicast [*ipv6-prefix*/*prefix-length*] **[longer-prefixes]** [**labels**]

语法说明

unicast	指定 IPv6 单播地址前缀。
ipv6-prefix	（可选）IPv6 网络号，输入该网络号以显示 IPv6 BGP 路由表中的特定网络。 此参数必须是 RFC 2373 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
/prefix-length	（可选）IPv6 前缀的长度。十进制值，表示地址的多少个高位连续位构成前缀（地址的网络部分）。十进制值前面必须有斜线标记。
longer-prefixes	（可选）显示路由和更具体的路由。
labels	（可选）显示每个地址系列应用于此邻居的策略。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

以下是 **show bgp ipv6** 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast

BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete


Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0             0  300 i
*> 10.10.20.0/24   172.16.10.1             0             0  300 i
*  10.20.10.0/24   172.16.10.1             0             0  300 i
```

以下是 **show bgp ipv4 multicast** 命令的输出示例：

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
```

```
Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                       0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                          0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1            0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                          0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                          0 3320 1275 559 i
*                   3FFE:C00:E:9::2                       0 1251 1930 559 i
*                   3FFE:3600::A                          0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                          0 293 1275 559 i
*                   3FFE:C00:E:4::2          1            0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                       0 237 3748 1275 559 i
```

表 4-11 显示每个字段的说明。

表 4-11　show bgp ipv6 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

以下是 **show bgp ipv6** 命令的输出示例，其中显示前缀 3FFE:500::/24 的信息：

```
ciscoasa# show bgp ipv6 unicast 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external

ciscoasa# show bgp ipv6 unicast

BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv6 community

要显示 IPv6 边界网关协议 (BGP) 路由表中的条目，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp ipv6community** 命令。

show bgp ipv6 unicast community [*community-number***] [exact-match] [local-as | no-advertise | no-export]**

语法说明

unicast	指定 IPv6 单播地址前缀。
community-number	（可选）有效值为一个从 1 到 4294967295 或 AA:NN 的范围内的社区编号（自主系统：社区编号，即一个 2 字节数字）。
exact-match	（可选）仅显示具有完全匹配项的路由。
local-as	（可选）仅显示未在本地自主系统（已知社区）的外部发送的路由。
no-advertise	（可选）仅显示不向任何对等设备（已知社区）通告的路由。
no-export	（可选）仅显示未在本地自主系统（已知社区）的外部导出的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 community 命令提供类似于 **show ip bgp community** 命令的输出，但该命令是特定于 IPv6 的。

使用 **set community** 路由映射配置命令设置社区。您必须在已知社区前输入数字社区。例如，以下字符串无效：

```
ciscoasa# show ipv6 bgp unicast community local-as 111:12345
```

使用以下字符串代替：

```
ciscoasa# show ipv6 bgp unicast community 111:12345 local-as
```

示例

以下是 **show bgp ipv6 community** 命令的输出示例：

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ?- incomplete

      Network               Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                   0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                   0 32768 ?
```

```
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                         0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                         0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                         0 2 ?
*>                        ::                                  0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                         0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                    0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                         0 2 3 i
*> 2010::/64                 ::                                    0 32768 ?
*> 2020::/64                 ::                                    0 32768 ?
*> 2030::/64                 ::                                    0 32768 ?
*> 2040::/64                 ::                                    0 32768 ?
*> 2050::/64                 ::                                    0 32768 ?
```

表 4-12　show bgp ipv6 community 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 community-list

要显示 IPv6 边界网关协议 (BGP) 社区列表允许的路由，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 community-list 命令。

show bgp ipv6 unicast community-list {*number* | *name*} **[exact-match]**

语法说明

unicast	指定 IPv6 单播地址前缀。
number	社区列表编号，范围为从 1 到 199。
name	社区列表名称。
exact-match	（可选）仅显示具有完全匹配项的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast community-list 命令提供类似于 **show ip bgp community-list** 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是用于社区列表编号 3 的 **show bgp ipv6 community-list** 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast community-list 3

BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ?- incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64     2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64              2001:0DB8:0:3::1                         0 1 ?
```

```
*> 2030::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                        0 1 ?
```

下表描述屏幕上展示的重要字段。

表 4-13　show bgp ipv6 community-list 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 filter-list

要显示符合指定的 IPv6 过滤器列表的路由，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp ipv6 filter-list** 命令。

show bgp ipv6 unicast filter-list *access-list-number*

语法说明

unicast	指定 IPv6 单播地址前缀。
access-list-number	IPv6 自主系统路径访问列表的编号。它可以是一个介于 1 到 199 之间的数字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 filter-list 命令提供类似于 **show ip bgp filter-list** 命令的输出，但该命令是特定于 IPv6 的。

示例：

以下是用于 IPv6 自主系统路径访问列表编号 1 的 **show bgp ipv6 filter-list** 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast filter-list 1

BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ?- incomplete

    Network              Next Hop                          Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                         32768  i
*> 2030::/64                 2001:0DB8:0:4::2                         0 1
*> 2040::/64                 2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                 2001:0DB8:0:4::2                         0 2 1 ?
```

下表描述屏幕上展示的重要字段。

表 4-14　show bgp ipv6 community-list 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 inconsistent-as

要显示具有不一致源自主系统的 IPv6 边界网关协议 (BGP) 路由，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 inconsistent-as 命令。

show bgp ipv6 unicast inconsistent-as

语法说明

unicast	指定 IPv6 单播地址前缀。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast inconsistent-as 命令提供类似于 **show ip bgp inconsistent-as** 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是 **show bgp ipv6 inconsistent-as** 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                       0 1251 4270 10318 ?
*                   3FFE:3600::A                          0 3462 6175 ?
*                   3FFE:700:20:1::11                     0 293 6175 ?
```

下表描述屏幕上展示的重要字段。

表 4-15　show bgp ipv6 community-list 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。

表 4-15　show bgp ipv6 community-list 字段（续）

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 neighbors

要显示关于到邻居的 IPv6 边界网关协议 (BGP) 连接的信息，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 neighbors 命令。

show bgp ipv6 unicast neighbors [*ipv6-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regular-expression* **]**

语法说明

unicast	指定 IPv6 单播地址前缀。
ipv6-address	（可选）IPv6 BGP 发言邻居的地址。如果省略此参数，则显示所有 IPv6 邻居。 此参数必须采用 RFC 2373 中记录的形式，其中在冒号之间使用 16 位值来以十六进制指定该地址。
received-routes	（可选）显示从指定邻居收到的所有路由（接受和拒绝的路由）。
routes	（可选）显示收到并接受的所有路由。这是 received-routes 关键字的输出的子集。
advertised-routes	（可选）显示向邻居通告的网络设备的所有路由。
paths *regular-expression*	（可选）用于与收到的路径匹配的正则表达式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast neighbors 提供类似于 show ip bgp neighbors 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是 show bgp ipv6 neighbors 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
```

```
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

下表描述屏幕上展示的重要字段。

表 4-16　show bgp ipv6 community-list 字段

字段	说明
BGP neighbor	BGP 邻居的 IP 地址及其自主系统编号。如果邻居位于与路由器相同的自主系统中，则它们之间的链路是内部链路；否则，将该链路视为外部链路。
remote AS	邻居的自主系统。
internal link	表示此对等设备为内部边界网关协议 (iBGP) 对等设备。
BGP version	正在用于与远程路由器通信的 BGP 版本；还指定邻居的路由器 ID（IP 地址）。
remote router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
BGP state	此 BGP 连接的内部状态。
up for	基本 TCP 连接已存在的时间量。
Last read	BGP 最后从此邻居读取消息的时间。
hold time	对等设备的消息之间可消耗的最大时间量。

表 4-16　show bgp ipv6 community-list 字段（续）

字段	说明
keepalive interval	发送保持连接数据包之间的时间段，这有助于确保 TCP 连接正常运行。
Neighbor capabilities	从此邻居通告并收到的 BGP 功能。
Route refresh	表示邻居使用路由刷新功能支持动态软重置。
Address family IPv6 Unicast	表示 BGP 对等设备正在交换 IPv6 可达性信息。
Received	从此对等设备收到的 BGP 消息（包括保持连接消息）的总数。
notifications	从对等设备收到的错误消息的数量。
Sent	已发送给此对等设备的 BGP 消息（包括保持连接消息）的总数。
notifications	路由器已发送给此对等设备的错误消息的数量。
advertisement runs	最小通告间隔的值。
For address family	以下字段引用的地址系列。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
neighbor version	编号，软件使用它跟踪已发送和必须发送给此邻居的前缀。
Route refresh request	从此邻居发送和收到的路由刷新请求的数量。
Community attribute（不在输出示例中展示）	如果为此邻居配置邻居 send-community 命令，则出现该字段。
Inbound path policy（不在输出示例中展示）	表示是配置入站过滤器列表，还是配置路由映射。
Outbound path policy（不在输出示例中展示）	表示是配置出站过滤器列表、路由映射，还是配置未抑制映射。
bgp-in（不在输出示例中展示）	用于 IPv6 单播地址系列的入站更新前缀过滤器列表的名称。
aggregate（不在输出示例中展示）	用于 IPv6 单播地址系列的出站更新前缀过滤器列表的名称。
uni-out（不在输出示例中展示）	用于 IPv6 单播地址系列的出站路由映射的名称。
accepted prefixes	接受的前缀的数量。
Prefix advertised	通告的前缀的数量。
suppressed	抑制的前缀的数量。
withdrawn	撤消的前缀的数量。
history paths（不在输出示例中展示）	保存以记录历史的路径条目的数量。

表 4-16　show bgp ipv6 community-list 字段（续）

字段	说明
Connections established	路由器已建立 TCP 连接的次数，且两个对等设备已同意彼此使用 BGP 发言。
dropped	正常的连接失败或被关闭的次数。
Last reset	最后重置此对等会话后消耗的时间（采用小时：分钟：秒钟格式）。
Connection state	BGP 对等设备的状态
unread input bytes	仍然要处理的数据包的字节数。
Local host, Local port	本地路由器的对等地址和端口。
Foreign host, Foreign port	邻居的对等地址。
Event Timers	显示每个计时器的启动和唤醒数量的表。
snduna	最后发送本地主机发送但未收到确认的序列号。
sndnxt	本地主机接下来将发送的序列号。
sndwnd	远程主机的 TCP 窗口大小。
irs	最初接收序列号。
rcvnxt	最后接收本地主机已确认的序列号。
rcvwnd	本地主机的 TCP 窗口大小。
delrecvwnd	延迟的接收窗口 - 本地主机从连接中读取，但未从主机向远程主机通告的接收窗口中减去的数据。此字段中的值逐渐增加，直到它大于全尺寸数据包为止，届时将该值应用于 rcvwnd 字段。
SRTT	计算的平滑的往返超时（以毫秒为单位）。
RTTO	往返超时（以毫秒为单位）。
RTV	往返时间的差异（以毫秒为单位）。
KRTT	新的往返超时（以毫秒为单位），使用 Karn 算法。此字段分别跟踪重新发送的数据包的往返时间。
minRTT	记录的最小往返超时（以毫秒为单位），具有用于计算的硬接线值。
maxRTT	记录的最大往返超时（以毫秒为单位）。
ACK hold	本地主机将延迟确认以在其上 “ 背载 ” 数据的时间（以毫秒为单位）。
Flags	BGP 数据包的 IP 优先级。
Datagrams: Rcvd	从邻居收到的更新数据包的数量。
with data	与数据一起收到的更新数据包的数量。
total data bytes	数据的总字节数。
Sent	发送的更新数据包的数量。
with data	具有发送的数据的更新数据包的数量。
total data bytes	数据的总字节数。

以下是具有 advertised-routes 关键字的 show bgp ipv6 neighbors 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

以下是具有 routes 关键字的 show bgp ipv6 neighbors 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
```

下表描述屏幕上展示的重要字段。

表 4-17　show bgp ipv6 neighbors advertised-routes and routes 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。

表 4-17　show bgp ipv6 neighbors advertised-routes and routes 字段（续）

字段	说明
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

以下是具有 paths 关键字的 show bgp ipv6 neighbors 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

下表描述屏幕上展示的重要字段。

show bgp ipv6 neighbors paths 字段

字段	说明
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（此用于 BGP 版本 2 和 3 的指标的名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp ipv6 neighbors 命令的以下输出示例展示 IPv6 地址 2000:0:0:4::2 收到的路由：

```
ciscoasa# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ?- incomplete
```

```
Network                Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                         0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                         0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                         0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                         0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                         0 2 ?
```

show bgp ipv6 paths

要显示数据库中的所有 IPv6 边界网关协议 (BGP) 路径，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 paths 命令。

show bgp ipv6 unicast paths *regular-expression*

语法说明

unicast	指定 IPv6 单播地址前缀。
regular-expression	用于与数据库中的收到的路径匹配的正则表达式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast paths 命令提供类似于 show ip bgp paths 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是 show bgp ipv6 paths 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

下表描述屏幕上展示的重要字段。

字段	说明
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（此用于 BGP 版本 2 和 3 的指标的名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp ipv6 prefix-list

要显示与前缀列表匹配的路由，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 prefix-list 命令。

show bgp ipv6 unicast prefix-list *name*

语法说明

unicast	指定 IPv6 单播地址前缀。
name	指定的前缀列表

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

指定的前缀列表必须是 IPv6 前缀列表，它在格式上类似于 IPv4 前缀列表。

示例

以下是 show bgp ipv6 prefix-list 命令的输出示例：

```
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

下表描述屏幕上展示的重要字段。

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 quote-regexp

要将与自主系统路径正则表达式匹配的 IPv6 边界网关协议 (BGP) 路由显示为一个引用的字符的字符串，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 quote-regexp 命令。

show bgp ipv6 unicast quote-regexp *regular expression*

语法说明

unicast	指定 IPv6 单播地址前缀。
regular expression	用于与 BGP 自主系统路径匹配的正则表达式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast quote-regexp 命令提供类似于 **show** ip bgp quote-regexp 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是展示从 33 开始或包含 293 的路径的 show bgp ipv6 quote-regexp 命令的输出示例：

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*  3FFE:C00:E:F::2                       0 6389 1849 293 1275
```

下表描述屏幕上展示的重要字段。

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 regexp

要显示与自主系统路径正则表达式匹配的 IPv6 边界网关协议 (BGP) 路由，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 regexp 命令。

show bgp ipv6 unicast regexp *regular-expression*

语法说明

unicast	指定 IPv6 单播地址前缀。
regular-expression	用于与 BGP 自主系统路径匹配的正则表达式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast regexp 命令提供类似于 show ip bgp regexp 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是展示从 33 开始或包含 293 的路径的 show bgp ipv6 regexp 命令的输出示例：

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                          0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

下表描述屏幕上展示的重要字段。

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 route-map

要显示未能安装在路由表中的 IPv6 边界网关协议 (BGP) 路由，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 route-map 命令。

show bgp ipv6 unicast route-map *name*

语法说明

unicast	指定 IPv6 单播地址前缀。
name	要匹配的指定路由映射。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

以下是用于名为 rmap 的路由映射的 show bgp ipv6 route-map 命令的输出示例：

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
             r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1             0    100     50 ?
*>i543::/64         2001:0DB8:101::1             0    100     50 ?
```

下表描述了屏幕上显示的重要字段。

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	一个 32 位数字，写为以句点分隔的 4 八位字节（点分十进制格式）。

字段	说明
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 h - 表条目是历史记录。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp ipv6 summary

要显示所有 IPv6 边界网关协议 (BGP) 连接的状态，请在用户 EXEC 或特权 EXEC 模式下使用 show bgp ipv6 summary 命令。

show bgp ipv6 unicast summary

语法说明

unicast	指定 IPv6 单播地址前缀。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

show bgp ipv6 unicast summary 命令提供类似于 show ip bgp summary 命令的输出，但该命令是特定于 IPv6 的。

示例

以下是 show bgp ipv6 summary 命令的输出示例：

```
ciscoasa# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor           V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

下表描述屏幕上展示的重要字段。

字段	说明
BGP device identifier	网络设备的 IP 地址。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
main routing table version	注入主路由表中的 BGP 数据库的上一版本。
Neighbor	邻居的 IPv6 地址。
V	向该邻居传达的 BGP 版本号。
AS	自主系统

字段	说明
MsgRcvd	从该邻居收到的 BGP 消息。
MsgSent	发送给该邻居的 BGP 消息。
TblVer	发送给该邻居的 BGP 数据库的上一版本。
InQ	来自该等待处理的邻居的消息的数量。
OutQ	等待发送给该邻居的消息的数量。
Up/Down	BGP 会话处于 “ 已建立 ” 状态或当前状态（如果它不处于 “ 已建立 ” 状态）的时间长度。
State/PfxRcd	BGP 会话的当前状态 / 设备已从邻居收到的前缀的数量。达到（如 neighbor maximum-prefix 命令所设置）最大数量时，条目中显示字符串 “PfxRcd”，邻居会关闭，且连接处于 “ 空闲 ” 状态。 具有空闲状态的 (Admin) 条目表示使用 neighbor shutdown 命令已关闭连接。

show bgp neighbors

要显示边界网关协议 (BGP) 和到邻居的 TCP 连接的有关信息，请在用户或特权 EXEC 模式下使用 **show bgp neighbors** 命令。

show bgp neighbors [slow | *ip-address* [**advertised-routes** | | **paths** [*reg-exp*] |**policy [detail]** | **received prefix-filter** | **received-routes** | **routes]]**

语法说明

slow	（可选）显示动态配置的缓慢对等设备的有关信息。
ip-address	（可选）显示有关 IPv4 邻居的信息。如果省略此参数，则显示有关所有邻居的信息。
advertised-routes	（可选）显示已向邻居通告的所有路由。
paths *reg-exp*	（可选）显示从指定的邻居获知的自主系统路径。可选正则表达式用于过滤输出。
policy	（可选）显示每个地址系列应用于此邻居的策略。
detail	（可选）显示详细的策略信息，例如路由映射、前缀列表、社区列表、访问控制列表 (ACL) 和自主系统路径过滤器列表。
received prefix-filter	（可选）显示从指定邻居（出站路由过滤器 [ORF]）发送的前缀列表。
received-routes	（可选）显示从指定邻居收到的所有路由（接受和拒绝的路由）。
routes	（可选）显示收到并接受的所有路由。输入此关键字时显示的输出是 **received-routes** 关键字显示的输出的子集。

命令默认

此命令的输出展示所有邻居的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **show bgp neighbors** 命令显示邻居会话的 BGP 和 TCP 连接信息。对于 BGP，这包括详细的邻居属性、功能、路径和前缀信息。对于 TCP，这包括与 BGP 邻居会话建立和维护相关的统计信息。

根据通告和撤消的前缀的数量显示前缀活动。策略拒绝显示已通告但随后基于输出中显示的功能或属性忽略的路由的数量。

4 字节的自主系统编号思科 /Cisco 实现使用 asplain - 例如 65538- 默认正则表达式匹配和输出显示自主系统编号的格式，但您可以配置 4 字节的自主系统编号 asplain 格式和 asdot 格式，在 RFC 5396 中所述。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后跟 **clear bgp *** 命令执行所有当前 BGP 会话的硬重置。

示例

show bgp neighbors 命令可用的各种关键字的输出示例是不同的。使用各种关键字的示例显示在以下部分中：

show bgp neighbors：示例

以下示例展示位于 10.108.50.2 的 BGP 邻居的输出。此邻居是内部 BGP (iBGP) 对等设备。此邻居支持路由刷新和平滑重启功能。

```
ciscoasa# show bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 0:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0

                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
```

```
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

下表描述屏幕上展示的重要字段。仅当计数器具有非零值时，才显示星号字符 (*) 后的字段。

表 4-18 显示每个字段的说明。

表 4-18　show bgp ipv4 字段

字段	说明
BGP neighbor	BGP 邻居的 IP 地址及其自主系统编号。
remote AS	邻居的自主系统编号。
local AS 300 no-prepend（不在屏幕中展示）	验证未将本地自主系统编号预置到收到的外部路由。迁移自主系统时，此输出支持隐藏本地自主系统。
internal link	为 iBGP 邻居显示 “internal link”。为外部 BGP (eBGP) 邻居显示 “external link”。
BGP version	正在用于与远程路由器通信的 BGP 版本。
remote router ID	邻居的 IP 地址。
BGP state	会话协商的有限状态机 (FSM) 阶段。
up for	基本 TCP 连接已存在的时间（采用 hh:mm:ss 格式）。
Last read	BGP 最后收到此邻居的消息后的时间（采用 hh:mm:ss 格式）。
last write	BGP 最后向此邻居发送消息后的时间（采用 hh:mm:ss 格式）。
hold time	BGP 将保持与此邻居的会话（没有收到消息）的时间（以秒为单位）。
keepalive interval	向此邻居传输保持连接消息的时间间隔（以秒为单位）。

表 4-18　show bgp ipv4 字段（续）

字段	说明
Neighbor capabilities	从此邻居通告并收到的 BGP 功能。在两个路由器之间成功交换功能时显示“advertised and received”。
Route Refresh	路由刷新功能的状态。
Graceful Restart Capability	平滑重启功能的状态。
Address family IPv4 Unicast	此邻居的特定于 IP 版本 4 单播的属性。
Message statistics	按消息类型组织的统计信息。
InQ depth is	输入队列中的消息的数量。
OutQ depth is	输出队列中的消息的数量。
Sent	传输的消息的总数。
Received	收到的消息的总数。
Opens	发送和收到的 OPEN 消息的数量。
notifications	发送和收到的通知（错误）消息的数量。
Updates	发送和收到的更新消息的数量。
Keepalives	发送和收到的保持连接消息的数量。
Route Refresh	发送和收到的路由刷新请求消息的数量。
Total	发送和收到的消息的总数。
Default minimum time between...	通告传输之间的时间（以秒为单位）。
For address family:	以下字段引用的地址系列。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
neighbor version	编号，软件使用它跟踪已发送和需要发送的前缀。
update-group	此地址系列的更新组成员的编号。
Prefix activity	此地址系列的前缀统计信息。
Prefixes current	为此地址系列接受的前缀的数量。
Prefixes total	收到的前缀的总数。
Implicit Withdraw	已撤消和重新通告前缀的次数。
Explicit Withdraw	因不再可行而撤消前缀的次数。
Used as bestpath	收到的作为最佳路径安装的前缀的数量。
Used as multipath	收到的作为多个路径安装的前缀的数量。
* Saved（软重新配置）	通过支持软重新配置的邻居执行的软重置的数量。仅当计数器具有非零值时，才显示此字段。
* History paths	仅当计数器具有非零值时，才显示此字段。
* Invalid paths	无效路径的数量。仅当计数器具有非零值时，才显示此字段。
Local Policy Denied Prefixes	因本地策略配置而拒绝的前缀。为入站和出站策略拒绝更新计数器。仅当计数器具有非零值时，才显示此标题下的字段。
* route-map	显示入站和出站路由映射策略拒绝。

表 4-18　show bgp ipv4 字段（续）

字段	说明
* filter-list	显示入站和出站过滤器列表策略拒绝。
* prefix-list	显示入站和出站前缀列表策略拒绝。
* AS_PATH too long	显示出站 AS 路径长度策略拒绝。
* AS_PATH loop	显示出站 AS 路径环路策略拒绝。
* AS_PATH confed info	显示出站联盟策略拒绝。
* AS_PATH contains AS 0	显示自主系统 (AS) 0 的出站拒绝。
* NEXT_HOP Martian	显示出站 martian 拒绝。
* NEXT_HOP non-local	显示出站非本地下一跃点拒绝。
* NEXT_HOP is us	显示出站下一跃点自拒绝。
* CLUSTER_LIST loop	显示出站集群列表环路拒绝。
* ORIGINATOR loop	显示本地发起的路由的出站拒绝。
* unsuppress-map	显示因未抑制映射而引起的入站拒绝。
* advertise-map	显示因通告映射而引起的入站拒绝。
* Well-known Community	显示已知社区的入站拒绝。
* SOO loop	显示因源站点而引起的入站拒绝。
* Bestpath from this peer	显示因最佳路径来自本地路由器而引起的入站拒绝。
* Suppressed due to dampening	显示因邻居或链路处于阻尼状态而引起的入站拒绝。
* Bestpath from iBGP peer	部署因最佳路径来自 iBGP 邻居而引起的入站拒绝。
* Incorrect RIB for CE	部署因 CE 路由器的 RIB 错误而引起的入站拒绝。
* BGP distribute-list	显示因分发列表而引起的入站拒绝。
Number of NLRIs...	更新中的网络层可达性属性的数量。
Connections established	已成功建立 TCP 和 BGP 连接的次数。
dropped	有效会话失败或被关闭的次数。
Last reset	最后重置此对等会话后的时间。重置的原因显示在此行上。
外部 BGP 邻居可能是 ……（不在屏幕中展示）	表示启用 BGP TTL 安全检查。可分离本地和远程对等设备的跃点的最大数量显示在此行上。

表 4-18　show bgp ipv4 字段（续）

字段	说明
Connection state	BGP 对等设备的连接状态。
Connection is ECN Disabled	显式堵塞通知状态（启用或禁用）。
Local host: 10.108.50.1, Local port: 179	本地 BGP 发言者的 IP 地址。BGP 端口号 179。
Foreign host: 10.108.50.2, Foreign port: 42698	邻居地址和 BGP 目标端口号。
Enqueued packets for retransmit:	排队进行 TCP 重新传输的数据包。
Event Timers	TCP 事件计时器。用于启动和唤醒的计数器（到期的计时器）。
Retrans	已重新传输数据包的次数。
TimeWait	等待重新传输计时器到期的时间。
AckHold	确认保持计时器。
SendWnd	传输（发送）窗口。
KeepAlive	保持连接数据包的数量。
GiveUp	因不确认而丢弃数据包的次数。
PmtuAger	路径 MTU 发现计时器。
DeadWait	失效段的到期计时器。
iss:	初始数据包传输序列号。
snduna	未确认的最后一个传输序列号。
sndnxt:	要传输的下一个数据包序列号。
sndwnd:	远程邻居的 TCP 窗口大小。
irs:	初始数据包接收序列号。
rcvnxt:	本地确认的最后一个接收序列号。
rcvwnd:	本地主机的 TCP 窗口大小。
delrcvwnd:	延迟的接收窗口 - 本地主机从连接中读取，但未从主机向远程主机通告的接收窗口中减去的数据。此字段中的值逐渐增加，直到它大于全尺寸数据包为止，届时将该值应用于 rcvwnd 字段。
SRTT:	计算的平滑的往返超时。
RTTO:	往返超时。
RTV:	往返时间的差异。
KRTT:	新的往返超时（使用 Karn 算法）。此字段分别跟踪重新发送的数据包的往返时间。
minRTT:	记录的最小往返超时（用于计算的硬接线值）。
maxRTT:	记录的最大往返超时。
ACK hold:	本地主机将延迟确认以携带（背载）附加数据的时间长度。
IP Precedence value:	BGP 数据包的 IP 优先级。

表 4-18　show bgp ipv4 字段（续）

字段	说明
Datagrams	从邻居收到的更新数据包的数量。
Rcvd:	收到的数据包的数量。
with data	与数据一起发送的更新数据包的数量。
total data bytes	收到的数据的总量（以字节为单位）。
Sent	发送的更新数据包的数量。
Second Congestion	因堵塞而发送的第二次重新传输的数量。
Datagrams: Rcvd	从邻居收到的更新数据包的数量。
out of order:	在序列外收到的数据包的数量。
with data	与数据一起收到的更新数据包的数量。
Last reset	最后重置此对等会话后消耗的时间。
unread input bytes	仍然要处理的数据包的字节数。
retransmit	重新传输的数据包的数量。
fastretransmit	在重新传输计时器到期前为无序段重新传输的重复确认的数量。
partialack	部分确认的重新传输的数量（在后续确认前或无后续确认时传输）。

show bgp neighbors advertised-routes：示例

以下示例展示仅为 172.16.232.178 邻居通告的路由：

```
ciscoasa# show bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

表 4-19 显示每个字段的说明。

表 4-19　show bgp neighbors advertised routes 字段

字段	说明
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： s - 表条目被抑制。 * - 表条目有效。 > - 表条目是用于该网络的最佳条目。 i - 通过内部 BGP (iBGP) 会话获知表条目。

表 4-19　show bgp neighbors advertised routes 字段（续）

字段	说明
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： i - 从内部网关协议 (IGP) 发起的条目，且使用 **network** 路由器配置命令通告该条目。 e - 从外部网关协议 (EGP) 发起的条目。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	条目描述的网络的互联网地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示接入服务器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	使用 **set local-preference** 路由映射配置命令设置的本地首选项值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。路径的源代码位于该路径的终点： i - 使用 IGP 发起条目并使用 **network** 路由器配置命令通告该条目。 e - 使用 EGP 发起的路由。 ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路径。

show bgp neighbors paths：示例

以下是使用 **paths** 关键字输入的 **show bgp neighbors** 命令的输出示例：

```
ciscoasa# show bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

表 4-20 显示每个字段的说明。

表 4-20　show bgp neighbors paths 字段

字段	说明
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（用于 BGP 版本 2 和 3 的此指标名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp neighbors received prefix-filter：示例

以下示例展示已从 192.168.20.72 邻居收到过滤 10.0.0.0 网络中的所有路由的前缀列表：

```
ciscoasa# show bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

表 4-21 显示每个字段的说明。

表 4-21　show bgp neighbors received prefix filter 字段

字段	说明
Address family	收到前缀过滤器所在的地址系列模式。
ip prefix-list	从指定邻居发送的前缀列表。

show bgp neighbors policy：示例

以下输出示例展示应用于位于 192.168.1.2 的邻居的策略。输出展示邻居设备上配置的策略。

```
ciscoasa# show bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

show bgp neighbors：示例

以下是 **show bgp neighbors** 命令的输出示例，该命令验证是否为位于 172.16.1.2 的 BGP 邻居启用 BGP TCP 路径最大传输单元 (MTU) 发现：

```
ciscoasa# show bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

以下是 **show bgp neighbors** 命令的部分输出，该命令验证位于 192.168.3.2 的外部 BGP 对等设备的 BGP 平滑重启功能的状态。平滑重启展示为已为此 BGP 对等设备禁用。

```
ciscoasa# show bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 0:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

show bgp paths

要显示数据库中的所有 BGP 路径，请在 EXEC 模式下使用 **show bgp paths** 命令。

show bgp paths

Cisco 10000 Series Router

show bgp paths *regexp*

语法说明

regexp	与 BGP 自主系统路径匹配的正则表达式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp paths** 命令在特权 EXEC 模式下的输出示例：

```
ciscoasa# show bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

表 4-22 显示每个字段的说明。

表 4-22　show bgp paths 字段

字段	说明
Address	存储路径的内部地址。
Hash	存储路径的哈希桶。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（此用于 BGP 版本 2 和 3 的指标的名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp policy-list

要显示配置的策略列表和策略列表条目的有关信息，请在用户 EXEC 模式下使用 **show bgp policy-list** 命令。

show bgp policy-list [*policy-list-name***]**

语法说明

policy-list-name	（可选）显示具有此参数的指定策略列表的有关信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp policy-list** 命令的输出示例。此命令的输出会展示策略列表名称和配置的 match 子句。以下输出示例类似于会展示的输出示例：

```
ciscoasa# show bgp policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show bgp prefix-list

要显示有关前缀列表或前缀列表条目的信息，请在用户或特权 EXEC 模式下使用 **show bgp prefix-list** 命令。

show bgp prefix-list [detail | summary][*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer**| **first-match**]]]

语法说明

detail | **summary**	（可选）显示有关所有前缀列表的详细信息或摘要信息。
first-match	（可选） 显示与给定 *network/length* 匹配的指定前缀列表的第一个条目。
longer	（可选）显示与给定 *network/length* 匹配或比其更具体的指定前缀列表的所有条目。
network/length	（可选）显示使用此网络地址和网络掩码长度（以位为单位）的指定前缀列表中的所有条目。
prefix-list-name	（可选）显示特定前缀列表中的条目。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下示例展示 **show bgp prefix-list** 命令的输出，其中具有有关名为 test 的前缀列表的详细信息：

```
ciscoasa# show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

要显示与自主系统路径正则表达式匹配的路由，请在 EXEC 模式下使用 **show bgp regexp** 命令。

show bgp regexp *regexp*

语法说明

regexp	与 BGP 自主系统路径匹配的正则表达式。 有关自主系统编号格式的更多详细信息，请参阅 **router bgp** 命令。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

思科实施 4 字节自主系统编号，使用 asplain（例如 65538）作为自主系统编号的默认正则表达式匹配和输出显示格式，但您可以如 RFC 5396 中所述配置 asplain 格式和 asdot 格式的 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后接 **clear bgp *** 命令来执行所有当前 BGP 会话的硬重置。

为确保顺利过渡，我们建议将使用 4 字节自主系统编号标识自主系统内的所有 BGP 发言者升级为支持 4 字节自主系统编号。

示例

以下是 **show bgp regexp** 命令在特权 EXEC 模式下的输出示例：

```
Router# show bgp regexp 108$

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

配置 **bgp asnotation dot** 命令后，4 字节自主系统路径的正则表达式匹配格式更改为 asdot 记数法格式。尽管可在正则表达式中使用 asplain 或 asdot 格式配置 4 字节自主系统编号，但仅与使用当前默认格式配置的 4 字节自主系统编号匹配。在第一个示例中，**show bgp regexp** 命令采用 asplain 格式的 4 字节自主系统编号进行配置。匹配失败是因为默认格式当前为 asdot 格式且没有输出。在使用 asdot 格式的第二个示例中，匹配通过并且关于 4 字节自主系统路径的信息使用 asdot 表示法展示。

注 asdot 记数法使用句点，它是思科正则表达式中的一个特殊字符。要删除特殊意义，请在句点前使用反斜线。

```
Router# show bgp regexp ^65536$

Router# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

以下是输入 **bgp asnotation dot** 命令以显示 4 字节自主系统编号后 **show bgp regexp** 命令的输出示例。

注 asdot 记数法使用句点，它是思科正则表达式中的一个特殊字符。要删除特殊意义，请在句点前使用反斜线。

```
Router# show bgp regexp ^1\.14$

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

show bgp replication

要显示边界网关协议 (BGP) 更新组的更新复制统计信息，请在 EXEC 模式下使用 **show bgp replication** 命令。

show bgp replication [*index-group* | *ip-address*]

语法说明

index-group	（可选）显示具有相应索引编号的更新组的更新复制统计信息。更新组索引编号的范围为从 1 到 4294967295。
ip-address	（可选）显示此邻居的更新复制统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令的输出展示 BGP 更新组复制统计信息。

发生出站策略更改时，路由器自动重新计算更新组成员，并在 3 分钟计时器到期后通过触发出站软重置应用更改。如果产生错误，则此行为设计为为网络操作员提供更改配置的时间。您可以通过输入 **clearbgp** *ip-address* ***soft out*** 命令，在计时器到期前手动启用出站软重置。

示例

show bgp replication 命令的以下输出示例展示所有邻居的更新组复制信息：

```
ciscoasa# show bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
```

show bgp replication 命令的以下输出示例展示 10.4.9.5 邻居的更新组统计信息：

```
Router# show bgp replication 10.4.9.5

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2       10.4.9.5        0        0      0      0
```

表 4-23 显示每个字段的说明。

表 4-23　show bgp replication 字段

字段	说明
Index	更新组的索引编号。
Type	对等设备（内部或外部）的类型。
Members	动态更新对等设备组中的成员的数量。
Leader	动态更新对等设备组的第一个成员。

show bgp rib-failure

要显示未能安装在路由信息库 (RIB) 表中的边界网关协议 (BGP) 路由，请在特权 EXEC 模式下使用 **show bgp rib-failure** 命令。

show bgp rib-failure

语法说明

此命令没有关键字或参数。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show bgp rib-failure** 命令的输出示例：

```
ciscoasa# show bgp rib-failure

Network          Next Hop                  RIB-failure   RIB-NH Matches
10.1.15.0/24     10.1.35.5          Higher admin distance             n/a
10.1.16.0/24     10.1.15.1          Higher admin distance             n/a
```

表 4-24 显示每个字段的说明。

表 4-24　show bgp rib-failure 字段

字段	说明
Network	网络实体的 IP 地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示路由器具有一些到此网络的非 BGP 路由。
RIB-failure	RIB 故障的原因。更高的管理距离意味着具有更好（较低）管理距离的路由（例如静态路由）已存在于 IP 路由表中。
RIB-NH Matches	仅当更高管理距离出现在 RIB 故障列中，且为正在使用的地址系列配置 **bgp suppress-inactive** 时才应用的路由状态。有三种选择： • 是 - 意味着 RIB 中的路由具有与 BGP 路由相同的下一跃点，或下一跃点下行递归到与 BGP 下一跃点相同的邻接。 • 否 - 意味着 RIB 中的下一跃点下行递归到与 BGP 路由不同的下一跃点。 • N/A - 意味着不为正在使用的地址系列配置 **bgp suppress-inactive**。

show bgp summary

要显示所有边界网关协议 (BGP) 连接的状态，请在用户 EXEC 或特权 EXEC 模式下使用 **show bgp summary** 命令。

show bgp summary

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

show bgp summary 命令用于显示到 BGP 邻居的所有连接的 BGP 路径、前缀和属性信息。

前缀是 IP 地址和网络掩码。它可表示整个网络、网络的子集或单个主机路由。路径是到给定目标的路由。默认情况下，BGP 仅会为每个目标安装一个路径。如果配置多路径路由，则 BGP 会为每个多路径路由安装一个路径条目，且仅会将一个多路径路由标记为最佳路径。

分别显示 BGP 属性和缓存条目，以组合形式显示会影响最佳路径选择过程。当配置相关 BGP 功能或收到属性时，显示此输出的字段。以字节为单位显示内存使用率。

思科实施 4 字节自主系统编号时使用 asplain（例如 65538）作为自主系统编号的默认正则表达式匹配和输出显示格式，但您可以 RFC 5396 中所述的 asplain 格式和 asdot 格式配置 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后接 **clear bgp *** 命令来执行所有当前 BGP 会话的硬重置。

示例

以下是 **show bgp summary** 命令在特权 EXEC 模式下的输出示例：

```
Router# show bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled.4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

表 4-25 显示每个字段的说明。

表 4-25　show bgp summary 字段

字段	说明
BGP router identifier	按照优先级和可用性、**bgp router-id** 命令指定的路由器标识符、环回地址或最高 IP 地址的顺序。
BGP table version	BGP 数据库的内部版本号。
main routing table version	注入主路由表中的 BGP 数据库的上一版本。
...network entries	BGP 数据库中的单一前缀条目的数量。
...using ... bytes of memory	为同一行上显示的路径、前缀或属性条目所消耗的内存量（以字节为单位）。
...path entries using	BGP 数据库中的路径条目的数量。仅会为给定目标安装一个路径条目。如果配置多路径路由，则会为每个多路径路由安装一个路径条目。
...multipath network entries using	为给定目标安装的多路径条目的数量。
* ...BGP path/bestpath attribute entries using	单一 BGP 属性组合的数量，其中选择这些组合的路径为最佳路径。
* ...BGP rrinfo entries using	单一 ORIGINATOR 和 CLUSTER_LIST 属性组合的数量。
...BGP AS-PATH entries using	单一 AS_PATH 条目的数量。
...BGP community entries using	单一 BGP 社区属性组合的数量。
*...BGP extended community entries using	单一扩展的社区属性组合的数量。
BGP route-map cache entries using	BGP 路由映射 match 和 set 子句组合的数量。0 值表示路由缓存为空。
...BGP filter-list cache entries using	与 AS 路径访问列表 permit 或 deny 语句匹配的过滤器列表条目的数量。0 值表示过滤器列表缓存为空。
BGP advertise-bit cache entries using	（仅限于思科 IOS 版本 12.4(11)T 及更高版本）通告的位域条目的数量和关联的内存使用率。位域条目表示向对等设备通告前缀时生成的一部分信息（一个位）。在需要时动态构建通告的位缓存。

表 4-25　show bgp summary 字段（续）

字段	说明
...received paths for inbound soft reconfiguration	为入站软重新配置收到和存储的路径的数量。
BGP using...	BGP 进程使用的内存总量（以字节为单位）。
Dampening enabled...	表示启用 BGP 阻尼。携带累积处罚规则的路径的数量和阻尼的路径的数量显示在此行上。
BGP activity...	显示已为路径或前缀分配或释放内存的次数。
Neighbor	邻居的 IP 地址。
V	向该邻居传达的 BGP 版本号。
AS	自主系统编号。
MsgRcvd	从邻居收到的消息的数量。
MsgSent	发送给邻居的消息的数量。
TblVer	发送给邻居的 BGP 数据库的上一版本。
InQ	要从邻居排队处理的消息的数量。
OutQ	要排队发送给邻居的消息的数量。
Up/Down	BGP 会话处于 “ 已建立 ” 状态或当前状态（如果它不处于 “ 已建立 ” 状态）的时间长度。
State/PfxRcd	BGP 会话的当前状态和已从邻居或对等设备组收到的前缀的数量。达到（如 **neighbor maximum-prefix** 命令所设置）最大数量时，条目中显示字符串 “PfxRcd”，邻居会关闭，且连接处于 “ 空闲 ” 状态。 具有空闲状态的 (Admin) 条目表示使用 **neighbor shutdown** 命令已关闭连接。

show bgp summary 命令的以下输出展示动态创建 BGP 邻居 192.168.3.2，且它是侦听范围组 group192 的成员。输出还展示为名为 group192 的侦听范围组定义 192.168.0.0/16 的 IP 前缀范围。在思科 IOS 版本 12.2(33)SXH 及更高版本中，BGP 动态邻居功能引入了使用与对等设备组（侦听范围组）关联的子网范围支持动态创建 BGP 邻居对等设备的能力。

```
ciscoasa# show bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
192.168.0.0/16
```

show bgp summary 命令的以下输出展示两个采用不同 4 字节自主系统编号（65536 和 65550）的 BGP 邻居（192.168.1.2 和 192.168.3.2）。本地自主系统 65538 也是一个 4 字节自主系统编号，且编号以默认 asplain 格式显示。

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
```

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 0:00:15        0
```

show bgp summary 命令的以下输出展示相同的两个 BGP 邻居，但以 asdot 记数法格式显示 4 字节自主系统编号。要更改显示格式，必须在路由器配置模式下配置 **bgp asnotation dot** 命令。

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13       0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24       0
```

以下示例展示 **show bgp summary slow** 命令的输出示例：

```
ciscoasa> show bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

show bgp system-config

要在用户情景中显示用于系统情景的 bgp 的运行配置，请在用户或特权 EXEC 模式下使用 **show bgp system-config** 命令。

show bgp system-config

语法说明

此命令没有任何参数或关键字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC、用户 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令仅可在用户情景中使用，无需使用任何参数或关键字。 此命令可用于检查系统情景在用户情景上实施的运行配置。

示例

以下输出示例类似于在用户 EXEC 模式下输入 **show bgp system-config** 命令时会展示的输出示例：

```
ciscoasa/c1(config)# show bgp system-config
router bgp 1
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 no bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
 address-family ipv4 unicast
  bgp scan-time 0
  bgp nexthop trigger enable
  bgp nexthop trigger delay 5
 exit-address-family
```

show blocks

要显示数据包缓冲区利用率，请在特权 EXEC 模式下使用 **show blocks** 命令。

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** | [**exhaustion snapshot** | **history** [**list**] [*1-MAX_NUM_SNAPSHOT* | *index*] [**detail**]]

语法说明

address *hex*	（可选）显示与此地址对应的块（以十六进制形式）。
all	（可选）显示所有块。
assigned	（可选）显示分配的且应用正在使用的块。
detail	（可选）显示每个单一队列类型的第一个块的一部分（128 个字节）。
dump	（可选）显示整个块内容，包括报头和数据包信息。转储与数据包之间的差异在于转储包括报头和数据包之间的附加信息。
diagnostics	（可选）显示块诊断。
exhaustion snapshot	（可选）打印拍取的最后 x 个（x 当前为 10）快照和最后一个快照的时间戳。拍取快照后，如果已过不到 5 分钟，则不拍取另一个快照。
free	（可选）显示可用的块。
header	（可选）显示块的报头。
history *1-MAX_NUM_SNAPSHOT* **history** *index* **history list**	**history** 选项显示历史记录中的最近所有快照。 **history list** 选项显示历史记录中的快照的摘要。 **history** *index* 选项显示历史记录中的快照的索引。 **history** *1-MAX_NUM_SNAPSHOT* 选项仅显示历史记录中的一个快照。
old	（可选）显示超过一分钟前分配的块。
packet	（可选）显示块的报头和数据包内容。
pool *size*	（可选）显示特定大小的块。
queue history	（可选）显示当 ASA 耗尽块时分配块的位置。有时，从池中分配块，但从不将块分配给队列。在这种情况下，位置是分配块的代码地址。
summary	（可选）显示按应用（在此类中分配块）的程序地址、在此类中释放块的应用的程序地址和此类中的有效块所属的队列排序的块使用率的有关详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	添加了 **pool summary** 选项。
8.0(2)	现在，dupb 块使用 0 长度块，而非 4 字节块。为 0 字节块添加了一个附加行。
9.1(5)	添加了 **exhaustion snapshot**、**history list**、**history** *index* 和 **history** *1-MAX_NUM_SNAPSHOT* 选项。

使用指南

show blocks 命令可帮助您确定 ASA 是否过载。此命令列出预分配的系统缓冲区利用率。只要流量通过 ASA 移动，内存已满就不是问题。您可以使用 **show conn** 命令查看流量是否移动。如果流量不移动且内存已满，则可能存在问题。

您也可以使用 SNMP 查看此信息。

在安全情景中展示的信息包括整个系统的信息，以及正在使用的块和块使用率的上限的有关情景特定信息。

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show blocks** 命令在单模式下的输出示例：

```
ciscoasa# show blocks
  SIZE     MAX     LOW     CNT
     0     100      99     100
     4    1600    1598    1599
    80     400     398     399
   256    3600    3540    3542
  1550    4716    3177    3184
 16384      10      10      10
  2048    1000    1000    1000
```

表 4-26 显示每个字段的说明。

表 4-26　show blocks 字段

字段	说明
SIZE	块池的大小（以字节为单位）。每个大小表示一个特定类型。
0	为 dupb 块使用。
4	复制应用（例如 DNS、ISAKMP、URL 过滤、uauth、TFTP 和 TCP 模块）中的现有块。此外，代码通常可使用这种大小的块将数据包发送给驱动程序等。
80	用于在 TCP 拦截中为故障切换问候消息生成确认数据包。

表 4-26　show blocks 字段（续）

字段	说明
256	用于状态化故障切换更新、系统日志记录和其他 TCP 功能。 这些块主要用于状态化故障切换消息。主用 ASA 生成并发送数据包到备用 ASA 以更新转换和连接表。在突发流量中，创建或断开高速率连接时，可用块的数量可能降至 0。此情况表示未将一个或多个连接更新到备用 ASA。状态化故障切换协议会在下次捕获缺少的转换或连接。如果 256 字节块的 CNT 列在扩展的时间段内保持为或接近于 0，则 ASA 会因 ASA 每秒处理的连接的数量而难以保持转换和连接表同步。 从 ASA 发出的系统日志消息也使用 256 字节块，但通常不会如此大量地释放它们，以免导致 256 字节块池耗尽。如果 CNT 列显示 256 字节块的数量接近于 0，请确保您不会在调试级别（第 7 级）登录到系统日志服务器。这通过 ASA 配置中的 logging trap 行表示。我们建议您在通知级别（第 5 级）或更低级别设置日志记录，除非您需要附加信息来进行调试。
1550	用于存储通过 ASA 处理的以太网数据包。 当数据包进入 ASA 接口时，它被置于输入接口队列中，传递到操作系统上，然后置于块中。ASA 确定是应根据安全策略允许数据包，还是予以拒绝，然后在出站接口上处理到达输出队列的数据包。如果 ASA 难以承载流量负载，则可用块的数量会在 0（正如命令输出的 CNT 列中所示）附近浮动。当 CNT 列是零时，ASA 尝试分配更多块。如果发出此命令，则 1550 字节块的最大数量可大于 8192。如果无更多可用块，则 ASA 丢弃数据包。
16384	仅用于 64 位 66 MHz 千兆以太网卡 (i82543)。 请参阅 1550 的说明，了解有关以太网数据包的更多信息。
2048	用于控制更新的控制或引导的帧。
MAX	指定字节块池的可用块的最大数量。在启动时从内存中划分块的最大数量。通常，块的最大数量不会更改。但 256 字节和 1550 字节块的最大数量是例外，其中 ASA 可在需要时动态创建更多块。如果发出此命令，则 1550 字节块的最大数量可大于 8192。
LOW	下限。此数字表示自 ASA 通电或最后清除块（使用 **clear blocks** 命令）后这种大小的可用块的最小数量。LOW 列中的零表示上一个事件，其中内存已满。
CNT	该特定大小块池的可用块的当前数量。CNT 列中的零意味着内存现在已满。

以下是 **show blocks all** 命令的输出示例：

```
ciscoasa# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 4-27 显示每个字段的说明。

表 4-27　show blocks all 字段

字段	说明
Block	块地址。
allocd_by	最后使用块的应用的程序地址（如果未使用，则为 0）。
freed_by	最后释放块的应用的程序地址。
data size	块内的应用缓冲区 / 数据包数据的大小。
alloccnt	自块存在后已使用此块的次数。
dup_cnt	对此块（如果使用）的引用的当前数量：0 表示 1 个引用，1 表示 2 个引用。
oper	最后在块上执行的四个操作之一：分配、获得、放置或释放。
location	使用块的应用，或最后分配块的应用的程序地址（与 allocd_by 字段相同）。

以下是 **show blocks** 命令在情景中的输出示例：

```
ciscoasa/contexta# show blocks
  SIZE     MAX     LOW     CNT  INUSE   HIGH
     4    1600    1599    1599      0      0
    80     400     400     400      0      0
   256    3600    3538    3540      0      1
  1550    4616    3077    3085      0      0
```

以下是 **show blocks queue history** 命令的输出示例：

```
ciscoasa# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

以下是 **show blocks queue history detail** 命令的输出示例：

```
ciscoasa# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

以下是 **show blocks pool summary** 命令的输出示例：

```
ciscoasa# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
```

```
0x9a0326         00000053         00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2         00000005         00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18         00000256         00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b         00001275         00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

以下是 **show blocks exhaustion history list** 命令的输出示例：

```
ciscoasa# show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

表 4-28 显示每个字段的说明。

表 4-28　show blocks pool summary 字段

字段	说明
total_count	给定类的块的数量。
miss_count	因技术原因而未在指定类别中报告的块的数量。
Freed_pc	在此类中释放块的应用的程序地址。
Alloc_pc	在此类中分配块的应用的程序地址。
Queue	此类中的有效块所属的队列。
valid_cnt	当前分配的块的数量。
invalid_cnt	当前未分配的块的数量。
Invalid Bad qtype	已释放此队列且内容无效，或从未初始化此队列。
Valid tcp_usr_conn_inp	队列有效。

相关命令

命令	说明
blocks	增加分配给块诊断的内存。
clear blocks	清除系统缓冲区统计信息。
show conn	显示活动连接。

show boot device (IOS)

要查看默认引导分区，请使用 **show boot device** 命令。

show boot device [*mod_num*]

语法说明

mod_num	（可选）指定模块编号。使用 **show module** 命令查看已安装的模块及其号码。

默认值

默认引导分区是 cf:4。

命令模式

特权 EXEC 模式。

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show boot device** 命令的输出示例，该命令展示安装在思科 IOS 软件上的每个 ASA 的引导分区：

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

相关命令

命令	说明
boot device (IOS)	设置默认引导分区。
show module (IOS)	显示所有已安装的模块。

show bootvar

要显示引导文件和配置属性，请在特权 EXEC 模式下使用 **show bootvar** 命令。

show bootvar

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

BOOT 变量指定各种设备上的可引导映像的列表。CONFIG_FILE 变量指定在系统初始化期间使用的配置文件。分别使用 **boot system** 命令和 **boot config** 命令设置这些变量。

示例

BOOT 变量包含 disk0:/f1_image，它是系统重新加载时引导的映像。BOOT 的当前值为 disk0:/f1_image; disk0:/f1_backupimage。此值意味着已使用 **boot system** 命令修改 BOOT 变量，但尚未使用 **write memory** 命令保存运行配置。保存运行配置时，BOOT 变量和当前 BOOT 变量都会是 disk0:/f1_image; disk0:/f1_backupimage。假设保存了运行配置，则引导加载程序会尝试从 disk0:/f1image 开始加载 BOOT 变量的内容，但如果该变量不存在或无效，则引导加载程序会尝试引导 disk0:1/f1_backupimage。

CONFIG_FILE 变量指向系统启动配置。在此示例中未设置该变量，因此启动配置文件是使用 **boot config** 命令指定的默认值。使用 **boot config** 命令可修改当前 CONFIG_FILE 变量且使用 **write memory** 命令可保存该变量。

以下是 **show bootvar** 命令的输出示例：

```
ciscoasa# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
```

相关命令

命令	说明
boot	指定配置文件或启动时使用的映像文件。

show bridge-group

要显示网桥组信息（例如分配的接口、MAC 地址和 IP 地址），请在特权 EXEC 模式下使用 **show bridge-group** 命令。

show bridge-group *bridge-group-number*

语法说明

bridge-group-number	将网桥组编号指定为一个介于 1 和 100 之间的整数。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	—	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(1)	我们引入了此命令。

示例

以下是具有 IPv4 地址的 **show bridge-group** 命令的输出示例：

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

以下是具有 IPv4 和 IPv6 地址的 **show bridge-group** 命令的输出示例：

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
    2000:101::1, subnet is 2000:101::/64
    2000:102::1, subnet is 2000:102::/64
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

相关命令

命令	说明
bridge-group	将透明防火墙接口组合在一个桥组。
clear configure interface bvi	清除网桥组接口配置。
interface	配置一个接口。
interface bvi	创建网桥虚拟接口。
ip address	设置一个桥组的管理 IP 地址。
show running-config interface bvi	显示该桥组接口配置。

show call-home

要显示配置的 Call Home 信息，请在特权 EXEC 模式下使用 **show call-home** 命令。

[cluster exec] show call-home [alert-group | detail | events | mail-server status | profile {*profile _name* | **all**} | **statistics]**

语法说明

alert-group	（可选）显示可用警报组。
cluster exec	（可选）在一个集群环境中，使您能够在一个设备中发出 **show call-home** 命令，并同时在所有其他设备中运行该命令。
detail	（可选）显示 Call Home 配置的详细信息。
events	（可选）显示当前检测的事件。
mail-server status	（可选）显示 Call Home 邮件服务器状态信息。
profile *profile _name* **all**	（可选）显示所有现有配置文件的配置信息。
statistics	（可选）显示 Call Home 统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(2)	引入了此命令。
9.1(3)	添加了 Smart Call Home 消息的新类型以包括 **show cluster history** 命令和 **show cluster info** 命令的输出。

示例

以下是 **show call-home** 命令的输出示例并展示配置的 Call Home 设置：

```
ciscoasa# show call-home
Current Smart Call-Home settings:
Smart Call-Home feature : enable
Smart Call-Home message's from address: from@example.com
Smart Call-Home message's reply-to address: reply-to@example.com
contact person's email address: example@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: ExampleCorp
contract ID: X123456789
site ID: SantaClara
```

```
Mail-server[1]: Address: smtp.example.com Priority: 1
Mail-server[2]: Address: 192.168.0.1 Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword                  State
------------------------ -------
Syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile Name: prof1
Profile Name: prof2
```

以下是 **show call-home detail** 命令的输出示例并展示详细的 Call Home 配置信息：

```
ciscoasa# show call-home detail
Description: Show smart call-home configuration in detail.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Current Smart Call-Home settings:
Smart Call-Home feature: enable
Smart Call-Home message's from address: from@example.example.com
Smart Call-Home message's reply-to address: reply-to@example.example.com
contact person's email address: abc@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: 111111
contract ID: 123123
site ID: SantaClara
Mail-server[1]: Address: example.example.com Priority: 1
Mail-server[2]: Address: example.example.com Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
```

```
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

以下是 **show call-home events** 命令的输出示例并展示可用 Call Home 事件：

```
ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

以下是 **show call-home mail-server status** 命令的输出示例并展示可用 Call Home 邮件服务器状态：

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: example.example.com Priority: 1 [Available]
Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

以下是 **show call-home alert-group** 命令的输出示例并展示可用警报组：

```
ciscoasa# show call-home alert-group
Description: Show smart call-home alert-group states.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
```

以下是 **show call-home profile profile-name | all** 命令的输出示例并展示所有预定义的配置文件和用户定义的配置文件的信息：

```
ciscoasa# show call-home profile {profile-name | all}
Description: Show smart call-home profile configuration.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Profiles:
```

```
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

以下是 **show call-home statistics** 命令的输出示例并展示 Call Home 统计信息：

```
ciscoasa# show call-home statistics
Description: Show smart call-home statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Message Types Total Email HTTP
-------------------- ---------------- ---------------- ----------------
Total Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1
Tx Failed 5 4 1
inventory 3 2 1
configuration 2 2 0
Event Types Total
-------------------- ----------------
Total Detected 2
inventory 1
configuration 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

以下是 **show call-home status** 命令的输出示例并展示 Call Home 状态：

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: kafan-lnx-01.cisco.com Priority: 1 [Available]
Mail-server[2]: Address: kafan-lnx-02.cisco.com Priority: 10 [Not Available]
```

```
37.ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

以下是 **cluster exec show call-home statistics** 命令的输出示例并展示集群的 Call Home 统计信息：

```
ciscoasa(config)# cluster exec show call-home statistics
A(LOCAL):**********************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 3                3                0
                test                 3                3                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0

Total Dropped                       8                8                0
           Tx Failed                8                8                0
       configuration                2                2                0
                test                6                6                0


Event Types             Total
--------------------   ----------------
      Total Detected               10
       configuration                1
                test                9

 Total In-Processing                0

      Total In-Queue                0

Total Dropped                       0

Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00

B:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 1                1                0
                test                 1                1                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0

Total Dropped                       2                2                0
           Tx Failed                2                2                0
       configuration                2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                2
       configuration                1
                test                1

 Total In-Processing                0
```

```
      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00

C:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  0                0                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
          Tx Failed                   2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  1
       configuration                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: n/a

D:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
          Tx Failed                   2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00

ciscoasa(config)#
```

相关命令

命令	说明
call-home	进入 call home 配置模式。
call-home send alert-group	发送特定警报组消息。
service call-home	启用或禁用 Call Home。

show call-home registered-module status

要显示注册的模块状态，请在特权 EXEC 模式下使用 **show call-home registered-module status** 命令。

show call-home registered-module status [all]

注　**[all]** 选项仅在系统情景模式下有效。

语法说明

all	显示基于设备而非每个情景的模块状态。在多情景模式下，如果在至少一个情景中启用模块，则它显示为启用（如果包括“**all**”选项）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(2)	引入了此命令。

示例

以下示例展示 **show call-home registered-module status all** 输出：

```
Output:
Module Name Status
---------------------------------------- --------------------
Smart Call-Home enabled
Failover Standby/Active
```

相关命令

命令	说明
call-home	进入 Call Home 配置模式。
call-home send alert-group	发送特定警报组消息。
service call-home	启用或禁用 Call Home。

show capture

要在未指定任何选项时显示捕获配置，请在特权 EXEC 模式下使用 **show capture** 命令。

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

语法说明

access-list *access_list_name*	（可选）显示基于用于标识特定访问列表的 IP 或较高字段的数据包的信息。
capture_name	（可选）指定数据包捕获的名称。
cluster exec	（可选）在一个集群环境中，使您能够在一个设备中发出 **show capture** 命令，并同时在所有其他设备中运行该命令。
count *number*	（可选）显示数据包指定的数据的数量。
decode	当类型 ISAKMP 的捕获应用于接口时，此选项非常有用。在解密后会捕获流过该接口的所有 ISAKMP 数据并在解码字段后展示更多信息。
detail	（可选）显示每个数据包的附加协议信息。
dump	（可选）显示通过数据链路传输的数据包的十六进制转储。
packet-number *number*	以指定的数据包编号开始显示。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(2)	在 IDS 的输出中添加了详细信息。
9.0(1)	增加了 **cluster exec** 选项。
9.2(1)	**vpn-user** 域名更改为输出中的 **filter-aaa**。
9.3(1)	添加了 SGT 的输出和以太网标记。

使用指南

如果指定 *capture_name*，则显示该捕获的捕获缓冲区内容。

dump 关键字不显示十六进制转储中的 MAC 信息。

数据包的解码输出取决于数据包的协议。在表 4-29 中，指定 **detail** 关键字时，显示加括号的输出。

表 4-29　　数据包捕获输出格式

数据包类型	捕获输出格式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

如果 ASA 收到具有格式不正确的 TCP 报头的数据包并因 ASP 丢弃原因 *invalid-tcp-hdr-length* 而丢弃它们，则在收到这些数据包的接口上的 **show capture** 命令输出中不显示这些数据包。

示例

此示例展示如何显示捕获配置：

```
ciscoasa(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

此示例展示如何显示 ARP 捕获捕获的数据包：

```
ciscoasa(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

以下示例展示如何显示在一个集群环境中的单个设备上捕获的数据包：

```
ciscoasa(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

以下示例展示如何显示在一个集群环境中的所有设备上捕获的数据包：

```
ciscoasa(config)# cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------------

capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:--------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

以下示例展示在输入以下命令后，在一个集群环境中的集群控制链路上捕获的数据包：

```
ciscoasa (config)# capture a interface cluster
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet 0/0

ciscoasa(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

以下示例展示已在接口上启用 SGT 和以太网标记时捕获的数据包：

```
ciscoasa(config)# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

已在接口上启用 SGT 和以太网标记时，该接口仍可收到标记或取消标记的数据包。展示的示例用于标记的数据包，该数据包在输出中具有 INLINE-TAG 36。当同一接口收到取消标记的数据包时，输出保持不变（即输出中不包括任何 “INLINE-TAG 36” 条目）。

相关命令

命令	说明
capture	为数据包嗅探和网络故障隔离启用数据包捕获功能。
clear capture	清除捕获缓冲区。
copy capture	将捕获文件复制到服务器。

show chardrop

要显示从串行控制台丢弃的字符计数，请在特权 EXEC 模式下使用 **show chardrop** 命令。

show chardrop

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下是 **show chardrop** 命令的输出示例：

```
ciscoasa# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

相关命令

命令	说明
show running-config	显示当前运行的配置。

show checkheaps

要显示检查堆统计信息，请在特权 EXEC 模式下使用 **show checkheaps** 命令。Checkheaps 是验证堆内存缓冲区健全性（动态内存分配自系统堆内存区域）和代码区域完整性的定期过程。

show checkheaps

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show checkheaps** 命令的输出示例：

```
ciscoasa# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

相关命令

命令	说明
checkheaps	设置检查堆验证间隔。

show checksum

要显示配置校验和，请在特权 EXEC 模式下使用 **show checksum** 命令。

show checksum

语法说明

此命令没有任何参数或关键字。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	我们引入了此命令。

使用指南

show checksum 命令允许您显示充当配置内容的数字摘要的四组十六进制数。仅当您在闪存中存储配置时，才计算此校验和。

如果点（“.”）出现在 **show config** 或 **show checksum** 命令输出中的校验和之前，则输出表示常规配置负载或写入模式指示器（当从 ASA 闪存分区加载或写入该分区时）。“.” 显示操作预占 ASA 但其并非 “ 挂起 ”。此消息类似于 “system processing, please wait（系统正在处理，请稍等）” 消息。

示例

此示例展示如何显示配置或校验和：

```
ciscoasa(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

要显示数据块统计信息，请在特权 EXEC 模式下使用 **show chunkstat** 命令。

show chunkstat

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

此示例展示如何显示数据块统计信息：

```
ciscoasa# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

相关命令

命令	说明
show counters	显示协议堆栈计数器。
show cpu	显示 CPU 利用率信息。

show class

要显示分配给类的情景，请在特权 EXEC 模式下使用 **show class** 命令。

show class *name*

语法说明

name	指定字符串形式的名称，最长 20 个字符。要显示默认类，请为该名称输入 **default**。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下是 **show class default** 命令的输出示例：

```
ciscoasa# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

相关命令

命令	说明
class	配置资源类。
clear configure class	清除类配置。
context	配置安全情景。
limit-resource	设置类的资源限制。
member	为资源类分配情景。

show clock

要在 ASA 上查看时间，请在用户 EXEC 模式下使用 **show clock** 命令。

show clock [detail]

语法说明

detail	（可选）表示时钟源（NTP 或用户配置）和当前夏令时设置（如果有）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show clock** 命令的输出示例：

```
ciscoasa# show clock
12:35:45.205 EDT Tue Jul 27 2004
```

以下是 **show clock detail** 命令的输出示例：

```
ciscoasa# show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

相关命令

命令	说明
clock set	在 ASA 上手动设置时钟。
clock summer-time	设置显示夏令时的日期范围。
clock timezone	设置时区。
ntp server	标识 NTP 服务器。
show ntp status	显示 NTP 关联的状态。

show cluster

要查看整个集群的聚合数据或其他信息，请在特权 EXEC 模式下使用 **show cluster** 命令。

show cluster {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **traffic** | **xlate count**}

语法说明

access-list [*acl_name*]	显示访问策略的计数器。要查看用于特定 ACL 的计数器，请输入 *acl_name*。
conn [**count**]	显示所有设备上正在使用的连接的聚合计数。如果输入 **count** 关键字，则仅显示连接计数。
cpu [**usage**]	显示 CPU 使用率信息。
history	显示集群交换历史记录。
interface-mode	显示集群接口模式，即跨区模式或单个模式。
memory	显示系统内存利用率和其他信息。
resource usage	显示系统资源和使用率。
traffic	显示流量统计信息。
xlate count	显示当前转换信息。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

请同时参阅 **show cluster info** 和 **show cluster user-identity** 命令。

示例

以下是 **show cluster access-list** 命令的输出示例：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
```

```
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0,
0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有设备上正在使用的连接的聚合计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:************************************************************************
  100 in use, 100 most used
```

相关命令

命令	说明
show cluster info	显示集群信息。
show cluster user-identity	显示集群用户身份信息和统计信息。

show cluster info

要查看集群信息，请在特权 EXEC 模式下使用 **show cluster info** 命令。

show cluster info [**clients** | **conn-distribution** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport {asp** | **cp}**]

语法说明

clients	（可选）显示注册客户端的版本。
conn-distribution	（可选）显示集群中的连接分布。
goid [*options*]	（可选）显示全局对象 ID 数据库。选项包括： • **classmap** • **conn-set** • **hwidb** • **idfw-domain** • **idfw-group** • **interface** • **policymap** • **virtual-context**
health	（可选）显示运行状况监控信息。
incompatible-config	（可选）显示与当前运行配置中的集群不兼容的命令。此命令在启用集群前有用。
loadbalance	（可选）显示负载平衡信息。
old-members	（可选）显示集群的前成员。
packet-distribution	（可选）显示集群中的数据包分布。
trace [***options***]	（可选）显示集群控制模块事件跟踪。选项包括： • **latest** [*number*] - 显示最新 *number* 事件，其中该数字介于 1 和 2147483647 之间。默认值为全部显示。 • **level** *level* - 按照级别过滤事件，其中 *level* 为以下项之一：**all**、**critical**、**debug**、**informational** 或 **warning**。 • **module** *module* - 按照模块过滤事件，其中 *module* 为以下项之一：**ccp**、**datapath**、**fsm**、**general**、**hc**、**license**、**rpc** 或 **transport**。 • **time** {[*month day*] [*hh*:*mm*:*ss*]} - 在指定时间或日期前显示事件。
transport {asp | **cp}**	（可选）显示与以下项的统计信息相关的传输： • **asp** - 数据平面传输统计信息。 • **cp** - 控制平面传输统计信息。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。
9.3(1)	我们在 **show cluster info health** 命令中增加了对模块的改进支持。

使用指南

如果您不指定任何选项，则 **show cluster info** 命令显示通用集群信息，其中包括集群名称和状态、集群成员、成员状态等。

使用 **clear cluster info** 命令清除统计信息。

请同时参阅 **show cluster** 和 **show cluster user-identity** 命令。

示例

以下是 **show cluster info** 命令的输出示例：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Version   : 100.8(0.52)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Version   : 100.8(0.52)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Version   : 100.8(0.52)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

以下是 **show cluster info incompatible-config** 命令的输出示例：

```
ciscoasa(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's
confirmation upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close

INFO: No manually-correctable incompatible configuration is found.
```

以下是 **show cluster info trace** 命令的输出示例：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

以下是 **show cluster info health** 命令在 ASA 5500-X 上的输出示例：

```
ciscoasa# show cluster info health
Member ID to name mapping:
0 - A   1 - B(myself)

                         0        1
GigabitEthernet0/0       up       up
Management0/0            up       up

ips (policy off)         up       None
sfr (policy off)         None     up
Unit overall             healthy   healthy
Cluster overall          healthy
```

以上输出列出 ASA IPS (ips) 和 ASA FirePOWER (sfr) 模块，且对于每个模块，ASA 都显示“policy on（策略开启）” 或 “policy off（策略关闭）” 来表明您是否在服务策略中配置了该模块。例如：

```
class-map sfr-class
    match sfr-traffic
policy-map sfr-policy
    class sfr-class
        sfr inline fail-close
service-policy sfr interface inside
```

通过上述配置，ASA FirePOWER 模块（“sfr”）会显示为 “policy on（策略开启）”。如果一个集群成员将模块作为 “up”，另一个成员将该模块作为 “down” 或 “None”，则具有 down 模块的成员将被踢出集群。但是，如果未配置服务策略，则集群成员不会被踢出集群；仅当模块正在运行时才会关联模块状态。

以下是 **show cluster info health** 命令在 ASA 5585-X 上的输出示例：

```
ciscoasa# show cluster info health
spyker-13# sh clu info heal
Member ID to name mapping:
0 - A(myself) 1 - B

                       0 1
GigabitEthernet0/0       upup
```

```
SSM Card (policy off)    upup
Unit overall             healthyhealth
Cluster overall         healthyhealth
```

如果您在服务策略中配置模块，则输出展示“policy on（策略开启）”。如果不配置服务策略，则输出展示“policy off（策略关闭）”，即使模块存在于机箱中。

相关命令

命令	说明
show cluster	显示整个集群的聚合数据。
show cluster user-identity	显示集群用户身份信息和统计信息。

show cluster user-identity

要查看整个集群的用户身份信息和统计信息，请在特权 EXEC 模式下使用 **show cluster user-identity** 命令。

show cluster user-identity {**statistics** [**user** *name* | **user-group** *group_name*] | **user** [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** {**domain** *name* | **user-group** *group_name*] [**list** [*detail*]]}

语法说明

active	显示具有活动 IP 用户映射的用户。
all	显示用户数据库中的所有用户。
domain ***name***	显示域的用户信息。
inactive	显示具有非活动 IP 用户映射的用户。
list [***detail***]	显示用户的列表。
statistics	显示集群用户身份统计信息。
user	显示用户数据库。
user ***name***	显示特定用户的信息。
user-group ***group_name***	显示特定组的每个用户的信息。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	**修改**
9.0(1)	我们引入了此命令。

使用指南

请同时参阅 **show cluster info** 和 **show cluster** 命令。

相关命令

命令	**说明**
show cluster	显示整个集群的聚合数据。
show cluster info	显示集群信息。

show compression svc

要查看 ASA 上的 SVC 连接的压缩统计信息，请在特权 EXEC 模式下使用 **show compression svc** 命令。

show compression svc

默认值

没无默认情况下的，此命令。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是		—

命令历史

版本	修改
7.1(1)	引入了此命令。

示例

以下示例展示 **show compression svc** 命令的输出：

```
ciscoasa# show compression svc
Compression SVC Sessions                    1
Compressed Frames                      249756
Compressed Data In (bytes)            0048042
Compressed Data Out (bytes)           4859704
Expanded Frames                             1
Compression Errors                          0
Compression Resets                          0
Compression Output Buf Too Small            0
Compression Ratio                        2.06
Decompressed Frames                    876687
Decompressed Data In                279300233
```

相关命令

命令	说明
compression	对所有 SVC 和 WebVPN 连接启用压缩。
svc compression	为特定组或用户启用通过 SVC 连接的 http 数据的压缩。

show configuration

要显示保存在 ASA 上的闪存中的配置，请在特权 EXEC 模式下使用 **show configuration** 命令。

show configuration

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	此命令已修改。

使用指南

show configuration 命令显示保存在 ASA 上的闪存中的配置。与 **show running-config** 命令不同，**show configuration** 命令不使用许多 CPU 资源运行。

要显示 ASA 上的内存中的活动配置（包括保存的配置更改），请使用 **show running-config** 命令。

示例

以下是 **show configuration** 命令的输出示例：

```
ciscoasa# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
```

```
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

相关命令

命令	说明
configure	从终端配置 ASA。

show configuration session

要显示当前配置会话和会话中的更改，请在特权 EXEC 模式下使用 **show configuration session** 命令。

show configuration session [*session_name*]

语法说明

session_name	现有配置会话的名称。如果省略此参数，则显示所有现有会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

可将此命令与 **configure session** 命令配合使用；后者为编辑 ACL 及其对象创建独立会话。此命令显示会话的名称和已在会话中做出的所有配置更改。

如果会话显示为已提交，则您可以打开会话，并恢复更改（如果您确定它们并未按预期运行）。

示例

以下示例展示所有可用会话：

```
ciscoasa# show configuration session
config-session abc (un-committed)
 access-list abc permit ip any any
 access-list abc permit tcp any any

config-session abc2 (un-committed)
 object network test
 host 1.1.1.1
 object network test2
 host 2.2.2.2

ciscoasa#
```

相关命令

命令	说明
clear configuration session	删除配置会话及其内容。
clear session	清除配置会话的内容或重置配置会话的访问标志。
configure session	创建或打开会话。

show conn

要显示指定连接类型的连接状态，请在特权 EXEC 模式下使用 **show conn** 命令。此命令支持 IPv4 和 IPv6 地址。

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}] [**scansafe**] [**address** *src_ip*[*-src_ip*] [**netmask** *mask*]] [**port** *src_port*[*-src_port*]] [**address** *dest_ip*[*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[*-dest_port*]] [**user-identity** | **user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **security-group**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

语法说明

address	（可选）显示具有指定源或目标 IP 地址的连接。
all	（可选）除通过流量连接外还显示到达设备或从设备发起的连接。
count	（可选）显示活动连接的数量。
dest_ip	（可选）指定目标 IP 地址（IPv4 或 IPv6）。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如： `10.1.1.1-10.1.1.5`
dest_port	（可选）指定目标端口号。要指定范围，请使用破折号 (-) 分隔各个端口号。例如： `1000-2000`
detail	（可选）显示连接的详细信息，包括转换类型和接口信息。
long	（可选）以长格式显示连接。
netmask *mask*	（可选）指定要与给定 IP 地址配合使用的子网掩码。
port	（可选）显示具有指定源或目标端口的连接。
protocol {**tcp** | **udp**}	（可选）指定连接协议，它可以是 **tcp** 或 **udp**。
scansafe	（可选）显示正在转发到云网络安全服务器的连接。
security-group	（可选）指定显示的所有连接属于指定安全组。
src_ip	（可选）指定源 IP 地址（IPv4 或 IPv6）。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如： `10.1.1.1-10.1.1.5`
src_port	（可选）指定源端口号。要指定范围，请使用破折号 (-) 分隔各个端口号。例如： `1000-2000`
state *state_type*	（可选）指定连接状态类型。请参阅表 4-30，了解连接状态类型的可用关键字的列表。
user [*domain_nickname*\] *user_name*	（可选）指定显示的所有连接属于指定用户。不包括 *domain_nickname* 参数时，ASA 显示默认域中的用户的信息。
user-group [*domain_nickname*\\] *user_group_name*	（可选）指定显示的所有连接属于指定用户组。不包括 *domain_nickname* 参数时，ASA 显示默认域中的用户组的信息。

user-identity	（可选）指定 ASA 显示身份防火墙功能的所有连接。显示连接时，ASA 在标识匹配的用户时显示用户名和 IP 地址。同样，ASA 在标识匹配的主机时显示主机名和 IP 地址。
zone [*zone_name*]	（可选）显示区域的连接。**long** 和 **detail** 关键字展示用于构建连接的主要接口和用于转发流量的当前接口。

默认值

默认情况下显示所有通过连接。您还需要使用 **all** 关键字查看到设备的管理连接。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(8)/7.2(4)/8.0(4)	语法简化为使用源和目标概念而非 “ 本地 ” 和 “ 外部 ”。在新的语法中，源地址是输入的第一个地址，目标地址是第二个地址。旧语法使用诸如 **foreign** 和 **fport** 之类的关键字来确定目标地址和端口。
7.2(5)/8.0(5)/8.1(2)/8.2(4)/8.3(2)	添加了 **tcp_embryonic** 状态类型。此类型显示具有 i 标志的所有 TCP 连接（不完整的连接）；不显示用于 UDP 的 i 标志连接。
8.2(1)	为 TCP 状态旁路添加了 b 标志。
8.4(2)	添加了 **user-identity**、**user** 和 **user-group** 关键字以支持身份防火墙。
9.0(1)	增加了对集群的支持。我们添加了 **scansafe** 和 **security-group** 关键字。
9.3(2)	添加了 **zone** 关键字。

使用指南

show conn 命令显示活动 TCP 和 UDP 连接的数量，并提供各种类型的连接的有关信息。使用 **show conn all** 命令查看整个连接表。

注　在 ASA 创建针孔以允许辅助连接时，**show conn** 命令将此显示为不完整的连接。要清除此不完整的连接，请使用 **clear conn** 命令。

在表 4-30 中定义您可以使用 **show conn state** 命令指定的连接类型。指定多个连接类型时，请使用逗号，不用空格分隔关键字。

表 4-30　连接状态类型

关键字	显示的连接类型
up	处于打开状态的连接。
conn_inbound	入站连接。
ctiqbe	CTIQBE 连接

表 4-30　连接状态类型（续）

关键字	显示的连接类型
data_in	入站数据连接。
data_out	出站数据连接。
finin	FIN 入站连接。
finout	FIN 出站连接。
h225	H.225 连接。
h323	H.323 连接。
http_get	HTTP 获得连接。
mgcp	MGCP 连接。
nojava	拒绝访问 Java 小应用的连接。
rpc	RPC 连接。
service_module	SSM 正在扫描的连接。
sip	SIP 连接。
skinny	SCCP 连接。
smtp_data	SMTP 邮件数据连接。
sqlnet_fixup_data	SQL*Net 数据检查引擎连接。
tcp_embryonic	TCP 初期连接。
vpn_orphan	孤立的 VPN 隧道流。

使用 **detail** 选项时，系统使用表 4-31 中定义的连接标志显示有关转换类型的信息和接口信息。

表 4-31　连接标志

标记	说明
a	在外部等待对 SYN 的 ACK
A	在内部等待对 SYN 的 ACK
b	TCP 状态旁路
B	从外部发起的 SYN
C	计算机电话接口快速缓冲编码 (CTIQBE) 媒体连接
d	dump
D	DNS
E	外部回连接。这是必须从内部主机发起的辅助数据连接。例如，使用 FTP 时，内部客户端发出 PASV 命令且外部服务器接受该命令后，ASA 预分配具有此标志集的外部回连接。如果内部客户端尝试回连接到服务器，则 ASA 拒绝此连接尝试。仅外部服务器可以使用预分配的辅助连接。
f	内部 FIN
F	外部 FIN
g.	媒体网关控制协议 (MGCP) 连接
G	连接是组的一部分[1]

表 4-31　连接标志（续）

标记	说明
h	H.225
H	H.323
i	不完整的 TCP 或 UDP 连接
I	入站数据
k	瘦客户端控制协议 (SCCP) 媒体连接
K	GTP t3-response
m	SIP 媒体连接
M	SMTP 数据
O	出站数据
p	已复制（未使用的）
P	内部回连接。这是必须从内部主机发起的辅助数据连接。例如，使用 FTP 时，内部客户端发出 PORT 命令且外部服务器接受该命令后，ASA 预分配具有此标志集的内部回连接。如果外部服务器尝试回连接到客户端，则 ASA 拒绝此连接尝试。仅内部客户端可以使用预分配的辅助连接。
q	SQL*Net 数据
r	在确认的 FIN 内部
R	在用于 TCP 连接的确认的 FIN 外部。
R	UDP RPC[2]
s	等待外部 SYN
S	等待内部 SYN
t	SIP 临时连接[3]
T	SIP 连接[4]
U	up
V	VPN 孤立
W	WAAS
X	由服务模块（例如 CSC SSM）检查。
y	对于集群，标识备用所有者流。
Y	对于集群，标识控制器流。
z	对于集群，标识转发器流。
Z	云网络安全

1. G 标志表示连接是组的一部分。它由 GRE 和 FTP Strict 修复设置，用以指定控制连接及其所有关联的辅助连接。如果控制连接终止，则也会终止所有关联的辅助连接。
2. 由于 **show conn** 命令输出的每行表示一个连接（TCP 或 UDP），因此每行将只有一个 R 标志。
3. 对于 UDP 连接，值 t 表示该连接将在一分钟后超时。
4. 对于 UDP 连接，值 T 表示该连接将根据使用 **timeout sip** 命令指定的值超时。

注　对于使用 DNS 服务器的连接，**show conn** 命令输出中的 *IP address of DNS server* 可替换连接的源端口。

只要多个 DNS 会话在相同的两个主机之间，且会话具有相同的 5 元组（源 / 目标 IP 地址、源 / 目标端口和协议），就为这些会话创建一个连接。*app_id* 跟踪 DNS 标识，且每个 app_id 的空闲计时器分别运行。

由于 app_id 分别到期，合法的 DNS 响应只能在有限时间段内通过 ASA，且不存在任何资源累积。但是，输入 **show conn** 命令时，您会看到新的 DNS 会话正在重置的 DNS 连接的空闲计时器。这由共享 DNS 连接的性质和设计用意决定。

注　当在 **timeout conn** 命令定义的非活动时间（默认情况下为 1:00:00）内不存在任何 TCP 流量时，连接会关闭，且不再显示相应的连接标志条目。

如果局域网至局域网 / 网络扩展模式隧道丢弃且不会复原，则可能会存在许多孤立的隧道流。这些流不因下行的隧道而中断，但所有尝试流过它们的数据都会丢弃。**show conn** 命令输出展示这些具有 **V** 标志的孤立的流。

当以下 TCP 连接方向性标志应用于相同安全接口之间的连接时（请参阅 **same-security permit** 命令），标志中的方向是不相关的，因为对于相同的安全接口，不存在 “ 内部 ” 或 “ 外部 ” 之分。由于 ASA 必须将这些标志用于相同的安全连接，ASA 可根据其他连接特征选择一个标志而非另一个标志（例如，选择 f 而非 F），但您应忽略选择的方向性。

- B - 从外部的初次 SYN
- a - 等待外部 ACK 以进行 SYN
- A - 等待内部 ACK 以进行 SYN
- f - 内部 FIN
- F - 外部 FIN
- s - 等待外部 SYN
- S - 等待内部 SYN

要显示特定连接的信息，请包括 **security-group** 关键字并为连接的源和目标指定安全组表值或安全组名称。ASA 显示与特定安全组表值或安全组名称匹配的连接。

指定 **security-group** 关键字，而不指定源和目标安全组表值或源和目标安全组名称时，ASA 显示所有 SXP 连接的数据。

当安全组名称未知时，ASA 以 *security_group_name* (*SGT_value*) 格式显示连接数据或仅显示为 *SGT_value*。

注　由于末节连接不通过慢路径，安全组数据对于末节连接不可用。末节连接仅保留将数据包转发给连接的所有者的必要信息。

您可以指定一个安全组名称以显示集群中的所有连接；例如，以下示例展示与集群中的所有设备的安全组 mktg 匹配的连接：

```
ciscoasa# show cluster conn security-group name mktg
```

示例

指定多个连接类型时，请使用逗号，不用空格分隔关键字。以下示例展示处于 “ 打开 ” 状态的 RPC、H.323 和 SIP 连接的有关信息：

```
ciscoasa# show conn state up,rpc,h323,sip
```

以下是 **show conn count** 命令的输出示例：

```
ciscoasa# show conn count
54 in use, 123 most used
```

以下是 **show conn** 命令的输出示例。此示例展示一个从内部主机 10.1.1.15 到位于 10.10.49.10 的外部 Telnet 服务器的 TCP 会话连接。由于不存在 B 标志，连接从内部发起。“U”、“I” 和 “O” 标志表示连接处于活动状态并已收到入站和出站数据。

```
ciscoasa# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

以下是 **show conn** 命令的输出示例，其中包括 “X” 标志以表示 SSM 正在扫描连接。

```
ciscoasa# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

以下是 **show conn detail** 命令的输出示例。此示例展示一个从外部主机 10.10.49.10 到内部主机 10.1.1.15 的 UDP 连接。D 标志表示这是 DNS 连接。数字 1028 是通过连接的 DNS ID。

```
ciscoasa# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

```
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

以下是 **show conn** 命令在孤立流存在时（正如 **V** 标志所表示）的输出示例：

```
ciscoasa# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

要限制对那些具有孤立流的连接的报告，请将 **vpn_orphan** 选项添加到 **show conn state** 命令（如以下示例所示）：

```
ciscoasa# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

对于集群，要排除连接流故障，请首先通过在主设备上输入 **cluster exec show conn** 命令来查看所有设备上的连接。寻找具有以下标志的流：控制器 (Y)、备用 (y) 和转发器 (z)。以下示例展示一个从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接（在全部三个 ASA 上）； ASA 1 具有 z 标志，表明它是连接的转发器，ASA3 具有 Y 标志，表明它是连接的控制器，而 ASA2 不具有任何特殊标志，表明它是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并退出外部接口。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路向 ASA2 转发，然后退出 ASA2 上的内部接口。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):*******************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:*************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
```

```
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
Y
```

ASA2 上的 **show conn detail** 命令的输出展示最近的转发器为 ASA1：

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS, Z - Scansafe redirection,
       X - inspected by service module
       Y - director stub flow
       y - backup stub flow
       z - forwarder stub flow
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

以下示例展示如何显示身份防火墙功能的连接：

```
ciscoasa# show conn user-identity ?
exec mode commands/options:
  all       Enter this keyword to show conns including to-the-box and from-the-box
  detail    Enter this keyword to show conn in detail
  long      Enter this keyword to show conn in long format
  port      Enter this keyword to specify port
  protocol  Enter this keyword to specify conn protocol
  state     Enter this keyword to specify conn state
  |         Output modifiers

ciscoasa# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00,
bytes 10, flags –
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags –
…
ciscoasa# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags –
```

请参阅 **show conn long zone** 命令的以下输出：

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

相关命令

命令	说明
clear conn	清除连接。
inspect ctiqbe	启用 CTIQBE 应用检查。
inspect h323	启用 H.323 应用检查。
inspect mgcp	启用 MGCP 应用检查。
inspect sip	从 HTTP 流量中删除 Java 小应用。
inspect skinny	启用 SCCP 应用检查。

show console-output

要显示当前捕获的控制台输出，请在特权 EXEC 模式下使用 **show console-output** 命令。

show console-output

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show console-output** 命令的输出示例，该命令在不存在任何控制台输出时展示以下消息：

```
ciscoasa# show console-output
Sorry, there are no messages to display
```

相关命令

命令	说明
clear configure console	恢复默认控制台连接设置。
clear configure timeout	恢复配置中的默认空闲持续时间。
console timeout	设置与 ASA 之间的控制台连接的空闲超时。
show running-config console timeout	显示与 ASA 之间的控制台连接的空闲超时。

show context

要显示包括分配的接口和配置文件 URL、配置的情景的数量，或来自系统执行空间的情景信息、所有情景的列表，请在特权 EXEC 模式下使用 **show context** 命令。

show context [*name* | **detail** | **count**]

语法说明

count	（可选）显示配置的情景的数量。
detail	（可选）显示有关情景的附加详细信息，包括运行状态和供内部使用的信息。
name	（可选）设置情景名称。如果不指定名称，则 ASA 显示所有情景。在情景中，您只能输入当前情景名称。

默认值

在系统执行空间中，如果不指定名称，则 ASA 显示所有情景。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	添加了分配的 IPS 虚拟传感器的有关信息。

使用指南

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show context** 命令的输出示例。以下示例展示三个情景：

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 4-32 显示每个字段的说明。

表 4-32　show context 字段

字段	说明
Context Name	列出所有情景名称。带有星号 (*) 的情景名称是管理情景。
Interfaces	分配给情景的接口。
URL	ASA 从中加载情景配置的 URL。

以下是 **show context detail** 命令在系统执行空间中的输出示例：

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 4-33 显示每个字段的说明。

表 4-33　情景状态

字段	说明
Context	情景名称。空的情景信息仅供内部使用。系统情景表示系统执行空间。
State Message:	情景状态。请参阅以下可能的消息。
Has been created, but initial ACL rules not complete	ASA 解析配置，但尚未下载默认 ACL 以建立默认安全策略。默认安全策略最初适用于所有情景，并包括禁止从较低安全级别到较高安全级别的流量、启用应用检查和其他参数。此安全策略确保在解析配置后，但在编译配置 ACL 前无流量可以通过 ASA。由于编译配置 ACL 的速度非常快，您不太可能看到此状态。

表 4-33　情景状态（续）

字段	说明
Has been created, but not initialized	输入了 **context** *name* 命令，但尚未输入 **config-url** 命令。
Has been created, but the config hasn't been parsed	默认 ACL 已下载，但 ASA 尚未解析配置。此状态可能存在，因为配置下载可能会因网络连接问题而失败，或者您尚未输入 **config-url** 命令。要从情景中重新加载配置，请输入 **copy startup-config running-config**。从系统中重新输入 **config-url** 命令。或者，您可以开始配置空的运行配置。
Is a system resource	此状态仅适用于系统执行空间和空的情景。系统使用空的情景，且该信息仅供内部使用。
Is a zombie	使用 **no context** 或 **clear context** 命令删除了情景，但情景信息仍然存在于内存中，直到 ASA 重新使用新情景的情景 ID 或重启为止。
Is active	此情景当前正在运行且可以根据情景配置安全策略传递流量。
Is ADMIN and active	此情景是管理情景且当前正在运行。
Was a former ADMIN, but is now a zombie	使用 **clear configure context** 命令删除了管理情景，但情景信息仍然存在于内存中，直到 ASA 重新使用新情景的情景 ID 或重启为止。
Real Interfaces	分配给情景的接口。如果在 **allocate-interface** 命令中映射了接口 ID，则此屏幕展示接口的真正名称。
Mapped Interfaces	如果在 **allocate-interface** 命令中映射了接口 ID，则此屏幕展示映射的名称。如果未映射接口，则屏幕再次列出真正名称。
Real IPS Sensors	分配给情景的 IPS 虚拟传感器（如果已安装 AIP SSM）。如果在 **allocate-ips** 命令中映射了传感器名称，则此屏幕展示传感器的真正名称。
Mapped IPS Sensors	如果在 **allocate-ips** 命令中映射了传感器名称，则此屏幕展示映射的名称。如果未映射传感器名称，则屏幕再次列出真正名称。
Flag	仅供内部使用。
ID	此情景的内部 ID。

以下是 **show context count** 命令的输出示例：

```
ciscoasa# show context count
Total active contexts: 2
```

相关命令

命令	说明
admin-context	设置管理情景。
allocate-interface	将接口分配到情景。
changeto	在情景或系统执行空间之间切换。
config-url	指定情景配置的位置。
context	在系统配置中创建安全情景并进入情景配置模式。

show controller

要查看当前所有接口的控制器特定信息，请在特权 EXEC 模式下使用 **show controller** 命令。

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

语法说明

bridge	（可选）显示 ASA 5585-X 的 PCI 网桥特定信息。
bridge-id	（可选）显示 ASA 5585-X 的每个单一 PCI 网桥标识符。
detail	（可选）显示有关控制器的附加详细信息。
pci	（可选）显示 PCI 设备的摘要及其 ASA 5585-X 的 PCI 配置空间的前 256 个字节。
physical_interface	（可选）标识接口 ID。
port-num	（可选）显示 ASA 5585-X 自适应 ASA 的每个 PCI 网桥中的单一端口号。
slot	（可选）仅显示 ASA 5580 的 PCI-e 总线和插槽信息。

默认值

如果您不标识接口，则此命令展示所有接口的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	现在，此命令适用于所有平台，而非仅适用于 ASA 5505。添加了 **detail** 关键字。
8.1(1)	为 ASA 5580 添加了 **slot** 关键字。
8.2(5)	为安装 IPS SSP 的 ASA 5585-X 添加了 **pci**、**bridge**、*bridge-id* 和 *port-num* 选项。此外，为所有 ASA 型号增加了对发送暂停帧的支持，以在 1 千兆以太网接口上启用流控制。
8.6(1)	对于通过 ASA 5555-X Internal-Control0/0 接口（用于控制 ASA 与软件模块之间的流量）的 ASA 5512-X，增加了对 **detail** 关键词的支持和对用于到达 ASA 和软件模块的数据流量的 Internal-Data0/1 接口的支持。

使用指南

此命令有助于思科 TAC 在调查内部发现的缺陷和客户发现的缺陷时，收集有关控制器的有用调试信息。实际输出取决于型号和以太网控制器。该命令还展示与安装 IPS SSP 的 ASA 5585-X 相关的所有 PCI 网桥的有关信息。对于 ASA 服务模块，**show controller** 命令输出不展示任何 PCI-e 插槽信息。

示例

以下是 **show controller** 命令的输出示例：

```
ciscoasa# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482

--------------------------------------------------------------------
Number of VLANs: 1
--------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
--------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
--------------------------------------------------------------------

....

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
```

```
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC.ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC.CONFIG  = 0x00

...

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:

....
```

以下是 **show controller detail** 命令的输出示例：

```
ciscoasa# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
         RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
         RX Descriptor 0 Length:     0xf8262808 = 0x00001000
         RX Descriptor 0 Head:       0xf8262810 = 0x00000000
         RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
         RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
         RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
         RX Descriptor 1 Length:     0xf8260140 = 0x00000000
         RX Descriptor 1 Head:       0xf8260148 = 0x00000000
         RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

     TX Descriptor Registers:
         TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
         TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
```

```
        TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
        TX Descriptor 0 Length:     0xf8263808 = 0x00001000
        TX Descriptor 0 Head:       0xf8263810 = 0x00000000
        TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

    RX Address Array:
        Ethernet Address 0:         0012.d948.ef58
        Ethernet Address 1:         Not Valid!
        Ethernet Address 2:         Not Valid!
        Ethernet Address 3:         Not Valid!
        Ethernet Address 4:         Not Valid!
        Ethernet Address 5:         Not Valid!
        Ethernet Address 6:         Not Valid!
        Ethernet Address 7:         Not Valid!
        Ethernet Address 8:         Not Valid!
        Ethernet Address 9:         Not Valid!
        Ethernet Address a:         Not Valid!
        Ethernet Address b:         Not Valid!
        Ethernet Address c:         Not Valid!
        Ethernet Address d:         Not Valid!
        Ethernet Address e:         Not Valid!
        Ethernet Address f:         Not Valid!

    PHY Registers:
        Phy Control:                0x1140
        Phy Status:                 0x7969
        Phy ID 1:                   0x0141
        Phy ID 2:                   0x0c25
        Phy Autoneg Advertise:      0x01e1
        Phy Link Partner Ability:   0x41e1
        Phy Autoneg Expansion:      0x0007
        Phy Next Page TX:           0x2801
        Phy Link Partnr Next Page:  0x0000
        Phy 1000T Control:          0x0200
        Phy 1000T Status:           0x4000
        Phy Extended Status:        0x3000

    Detailed Output - RX Descriptor Ring:

    rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
    rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

   ........
```

以下是 **show controller detail** 命令的输出示例，该命令用于通过 ASA 5555-X 的 ASA 5512-X 上的内部接口：

```
ciscoasa# show controller detail

Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
```

```
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0

Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap2
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
     Transmit Ring [0]:
         tx_pkts_in_queue      : 0
         tx_pkts               : 176
         tx_bytes              : 9664
     Receive Ring [0]:
         rx_pkts_in_queue      : 0
         rx_pkts               : 0
         rx_bytes              : 0
         rx_drops              : 0
```

以下是 **show controller slot** 命令的输出示例：

```
Slot  Card Description                                PCI-e Bandwidth Cap.
----  ----------------                                ----------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x4, Card: x8

4.    ASA 5580 4 port GE Copper Interface Card        Bus: x4, Card: x4

5.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x8, Card: x8

6.    ASA 5580 4 port GE Fiber Interface Card         Bus: x4, Card: x4

7.    empty                                           Bus: x8

8.    empty                                           Bus: x8
```

以下是 **show controller pci** 命令的输出示例：

```
ciscoasa# show controller pci

PCI Evaluation Log:
-------------------------------------------------------------------------------
    Empty

  PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
  -----------------------------------------------------------------------------

    PCI Configuration Space (hex):
    0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
    0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
    0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
```

```
0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Link Capabilities: x4, Gen1
Link Status: x4, Gen1
```

相关命令

命令	说明
show interface	显示接口统计信息。
show tech-support	显示信息，以便思科 TAC 可诊断问题。

show coredump filesystem

要显示核心转储文件系统的内容，请输入 **show coredump filesystem** 命令。

show coredump filesystem

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，核心转储未启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

此命令显示核心转储文件系统的内容。

示例

要显示最近生成的任何核心转储的内容，请输入 **show coredump filesystem** 命令。

```
ciscoasa(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

相关命令

命令	说明
coredump enable	启用核心转储功能。
clear configure coredump	删除当前存储在核心转储文件系统的所有核心转储并清除核心转储日志。不接触核心转储文件系统本身且不更改或影响核心转储配置。
clear coredump	删除当前存储在核心转储文件系统的所有核心转储并清除核心转储日志。不接触核心转储文件系统本身且不更改 / 影响核心转储配置。
show coredump log	显示核心转储日志。

show coredump log

要显示核心转储日志的内容（首先显示最新日志），请输入 **show coredump log** 命令。要显示核心转储日志的内容（首先显示最早日志），请输入 **show coredump log reverse** 命令。

show coredump log

show coredump log [**reverse**]

语法说明

reverse	显示最早的核心转储日志。

默认值

默认情况下，核心转储未启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

此命令展示核心转储日志的内容。日志应反映当前磁盘上的内容。

示例

以下示例展示这些命令的输出：

```
ciscoasa(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

注　删除较早的核心转储文件，为新的核心转储留出空间。当核心转储文件系统填满，且当前核心转储需要空间时，ASA 会自动完成这一操作。这就是必须尽快存档核心转储以确保它们不会在出现故障时被覆盖的原因。

```
ciscoasa(config)# show coredump log reverse
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

相关命令

命令	说明
coredump enable	启用核心转储功能。
clear configure coredump	删除当前存储在核心转储文件系统的所有核心转储并清除核心转储日志。不接触核心转储文件系统本身且不更改 / 影响核心转储配置。
clear coredump	删除当前存储在核心转储文件系统的所有核心转储并清除核心转储日志。不接触核心转储文件系统本身且不更改或影响核心转储配置。
show coredump filesystem	显示核心转储文件系统的内容。

show counters

要显示协议堆栈计数器，请在特权 EXEC 模式下使用 **show counters** 命令。

show counters [all | context *context-name* | **summary | top** *N* **] [detail] [protocol** *protocol_name* **[:***counter_name***]] [threshold** *N***]**

语法说明

all	显示过滤器详细信息。
context *context-name*	指定情景名称。
:*counter_name*	按名称指定计数器。
detail	显示附加计数器信息。
protocol *protocol_name*	显示指定协议的计数器。
summary	显示计数器摘要。
threshold *N*	仅显示那些等于或高于指定阈值的计数器。范围为 1 到 4294967295。
top *N*	显示等于或高于指定阈值的计数器。范围为 1 到 4294967295。

默认值

显示计数器摘要详细阈值 1

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。
9.2(1)	添加了事件管理器的计数器。

示例

以下示例展示如何显示所有计数器：

```
ciscoasa# show counters all
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   single_vf
IOS_IPC       OUT_PKTS              2   single_vf

ciscoasa# show counters
Protocol      Counter           Value   Context
NPCP          IN_PKTS            7195   Summary
NPCP          OUT_PKTS           7603   Summary
IOS_IPC       IN_PKTS             869   Summary
IOS_IPC       OUT_PKTS            865   Summary
IP            IN_PKTS             380   Summary
IP            OUT_PKTS            411   Summary
```

```
IP            TO_ARP               105   Summary
IP            TO_UDP                 9   Summary
UDP           IN_PKTS                9   Summary
UDP           DROP_NO_APP            9   Summary
FIXUP         IN_PKTS              202   Summary
UAUTH         IPV6_UNSUPPORTED      27   Summary
IDFW          HIT_USER_LIMIT         2   Summary
```

以下示例展示如何显示计数器的摘要：

```
ciscoasa# show counters summary
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   Summary
IOS_IPC       OUT_PKTS              2   Summary
```

以下示例展示如何显示情景的计数器：

```
ciscoasa# show counters context single_vf
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               4   single_vf
IOS_IPC       OUT_PKTS              4   single_vf
```

以下示例展示如何显示事件管理器的计数器：

```
ciscoasa# show counters protocol eem
Protocol      Counter           Value   Context
EEM           SYSLOG            22      Summary
EEM           COMMANDS          6       Summary
EEM           FILES             3       Summary
```

相关命令

命令	说明
clear counters	清除协议堆栈计数器。

show cpu

要显示 CPU 利用率信息，请在特权 EXEC 模式下使用 **show cpu** 命令。

[**cluster exec**] **show cpu** [**usage** *core-id* | **profile** | **dump** | **detailed**]

从多情景模式下的系统配置中：

[**cluster exec**] **show cpu** [**usage**] [**context** {**all** | *context_name*}]

语法说明

all	指定屏幕展示所有情景。
cluster exec	（可选）在一个集群环境中，使您能够在一个设备中发出 **show cpu** 命令，并同时在所有其他设备中运行该命令。
context	指定屏幕展示一个情景。
context_name	指定要展示的情景的名称。
core-id	指定处理器内核的编号。
detailed	（可选）显示 CPU 使用内部详细信息。
dump	（可选）显示到 TTY 的转储分析数据。
profile	（可选）显示 CPU 分析数据。
usage	（可选）显示 CPU 使用率。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.6(1)	添加了 *core-id* 选项以支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X。
9.1(2)	为 **show cpu profile** 和 **show cpu profile dump** 命令更新了输出。
9.2(1)	虚拟平台 CPU 使用率已添加到 ASAv 的输出中。

使用指南

每五秒使用负载近似值和通过进一步将此近似值输入以下两个移动平均数来计算 CPU 使用率。

您可以使用 **show cpu** 命令找到与进程相关的负载（即代表 **show process** 命令在单模下和从多情景模式下的系统配置中的输出列出的项目的活动）。

此外，您可以在多情景模式下请求通过更改至每个情景并输入 **show cpu** 命令，或通过输入 **show cpu context** 命令，来将与进程相关的负载细分为任何配置的情景的 CPU 使用率。

在将与进程相关的负载四舍五入到最接近的整数时，与情景相关的负载包括一个附加的高精度十进制数。例如，从系统情景中输入 **show cpu** 命令与输入 **show cpu context system** 命令生成的数字不同。前者是 **show cpu context all** 命令中显示的所有项的近似摘要，而后者仅是该摘要的一部分。

您可以将 **show cpu profile dump** 命令与 **cpu profile activate** 命令结合使用，来收集 TAC 用于排除 CPU 问题的信息。**show cpu profile dump** 命令输出是十六进制格式。

如果 CPU 分析器等待启动条件发生，**show cpu profile** 命令会显示以下输出：

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

对于 ASAv，请注意以下许可准则：

- 允许的 vCPU 的数量由安装的 vCPU 平台许可确定。
  - 如果许可的 vCPU 的数量与调配的 vCPU 的数量匹配，则状态为 “ 兼容 ”。
  - 如果许可的 vCPU 的数量少于调配的 vCPU 的数量，则状态为 “ 不兼容：超额调配 ”。
  - 如果许可的 vCPU 的数量多于调配的 vCPU 的数量，则状态为 “ 兼容：调配不足 ”。
- 内存限制由调配的 vCPU 的数量确定。
  - 如果调配的内存位于允许的限制内，则状态为 “ 兼容 ”。
  - 如果调配的内存高于允许的限制，则状态为 “ 不兼容：超额调配 ”。
  - 如果调配的内存低于允许的限制，则状态为 “ 兼容：调配不足 ”。
- 频率预留限制由调配的 vCPU 的数量确定。
  - 如果频率预留内存等于或高于需要的最小值 (1000 MHz)，则状态为 “ 兼容 ”。
  - 如果频率预留内存低于需要的最小值 (1000 MHz)，则状态为 “ 兼容：调配不足 ”。

例如，以下输出展示尚未应用任何许可。允许的 vCPU 的数量是指许可的数量，且 “ 不兼容：超额调配 ” 表示产品正在使用比已许可的资源多的资源运行。

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

示例

以下示例展示如何显示 CPU 利用率：

```
ciscoasa# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

以下示例展示如何显示详细的 CPU 利用率信息：

```
ciscoasa# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
```

```
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%

CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

注　“Current control point elapsed versus the maximum control point elapsed for” 语句意味着在定义的时间段内将当前控制点负载与看到的最大负载进行比较。这是一个比率而非绝对数。数字 99% 与 5 秒间隔对应意味着当前控制点负载为在此 5 秒间隔内可见的最大负载的 99%。如果负载一直继续增加，则它会始终保持在 100%。但是，由于尚未定义最大绝对值，实际 CPU 可能仍然具有许多可用容量。

以下示例展示如何显示多个模式下的系统情景的 CPU 利用率：

```
ciscoasa# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

以下示例展示如何显示所有情景的 CPU 利用率：

```
ciscoasa# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

以下示例展示如何显示名为 “one” 的情景的 CPU 利用率：

```
ciscoasa/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

以下示例激活分析器并指示其存储 1000 份采样。

```
ciscoasa# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

以下示例展示分析的状态（正在进行中和已完成）：

```
ciscoasa# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

ciscoasa# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
----------------------------
…
----------------------------
```

```
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

以下示例展示 ASAv 的 CPU 使用率：

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     2
Number of allowed vCPUs      :     2
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  4000 MHz
Maximum allowed              :  56000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :   136 MHz
```

以下示例展示 ASAv 的 CPU 使用的详细信息：

```
Break down of per-core data path versus control point cpu usage:
Core         5 sec             1 min             5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.2 (0.2 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.1 (0.0 + 0.1)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


CPU utilization of external processes for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


Total CPU utilization for:
     5 seconds = 0.1%; 1 minute: 0.1%; 5 minutes: 0.1%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     4
Number of allowed vCPUs      :     4
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  20000 MHz
Maximum allowed              :  20000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :    99 MHz
```

复制此信息并将其提供给 TAC 进行解码。

相关命令

命令	说明
show counters	显示协议堆栈计数器。
cpu profile activate	激活 CPU 分析。

第 5 章

show crashinfo 至 show curpriv 命令

show crashinfo

要显示闪存中存储的崩溃文件内容，请在特权 EXEC 模式下输入 **show crashinfo** 命令。

show crashinfo [**save**]

语法说明

save	（可选）显示 ASA 是否配置为将崩溃信息保存到闪存。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.1(5)	输出在 **show process** 命令中显示线程 ID (TID)。

使用指南

如果崩溃文件来自测试崩溃（从 **crashinfo test** 命令生成），则崩溃文件的第一个字符串为“**: Saved_Test_Crash**”而最后一个字符串为“**: End_Test_Crash**”。如果崩溃文件来自真实崩溃，则崩溃文件的第一个字符串为“**: Saved_Crash**”而最后一个字符串为“**: End_Crash**”。（这包括使用 **crashinfo force page-fault** 或 **crashinfo force watchdog** 命令导致的崩溃。）

如果崩溃数据未保存在闪存中，或崩溃数据通过输入 **clear crashinfo** 命令已清除，则 **show crashinfo** 命令将显示错误消息。

示例

以下示例展示如何显示当前崩溃信息配置：

```
ciscoasa# show crashinfo save
crashinfo save enable
```

以下示例展示崩溃文件测试的输出。（不过，此测试不会使 ASA 实际崩溃。它提供一个模拟的示例文件。）

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
```

```
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
F-flags  : 0x2
F-flags2 : 0x0
F-flags3 : 0x10000
F-flags4 : 0x0
F-bytes  : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
```

```
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
```

```
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
```

```
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004
```

```
------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show vpn-sessiondb summary ------------------

Active Session Summary

Sessions:
                          Active : Cumulative : Peak Concurrent : Inactive
  SSL VPN               :       2 :          2 :               2
    Clientless only     :       0 :          0 :               0
    With client         :       2 :          2 :               2 :        0
  Email Proxy           :       0 :          0 :               0
  IPsec LAN-to-LAN      :       1 :          1 :               1
  IPsec Remote Access   :       0 :          0 :               0
  VPN Load Balancing    :       0 :          0 :               0
  Totals                :       3 :          3

License Information:
Shared VPN License Information:
    SSL VPN                    :     1500
      Allocated to this device :       50
      Allocated in network     :       50
      Device limit             :      750

  IPsec   :    750    Configured :    750    Active :      1    Load :   0%
  SSL VPN :     52    Configured :     52    Active :      2    Load :   4%
                           Active : Cumulative : Peak Concurrent
  IPsec                 :          1 :          1 :               1
  SSL VPN               :          2 :         10 :               2
    AnyConnect Mobile   :          0 :          0 :               0
    Linksys Phone       :          0 :          0 :               0
  Totals                :          3 :         11

Tunnels:
                     Active : Cumulative : Peak Concurrent
  IKE          :          1 :          1 :               1
  IPsec        :          1 :          1 :               1
  Clientless   :          2 :          2 :               2
  SSL-Tunnel   :          2 :          2 :               2
  DTLS-Tunnel  :          2 :          2 :               2
  Totals       :          8 :          8
------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927
```

```
------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------

PC  SP       STATE    Runtime  SBASE Stack              Process   TID
Hsi 001e3329 00763e7c 0053e5c8 0     00762ef4 3784/4096 arp_timer 0x000000000000000a
Lsi 001e80e9 00807074 0053e5c8 0     008060fc 3792/4096 FragDBGC  0x000000000000006b
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPsec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
```

```
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
PERFMON STATS:     Current       Average
Xlates                0/s           0/s
Connections           0/s           0/s
TCP Conns             0/s           0/s
UDP Conns             0/s           0/s
URL Access            0/s           0/s
URL Server Req        0/s           0/s
TCP Fixup             0/s           0/s
TCPIntercept          0/s           0/s
HTTP Fixup            0/s           0/s
FTP Fixup             0/s           0/s
AAA Authen            0/s           0/s
AAA Author            0/s           0/s
AAA Account           0/s           0/s
: End_Test_Crash
```

相关命令

命令	说明
clear crashinfo	删除崩溃文件的内容。
crashinfo force	强制 ASA 出现故障。
crashinfo save disable	禁止故障信息写入到闪存。
crashinfo test	测试 ASA 将故障信息保存到闪存中文件的能力。

show crashinfo console

要显示 **crashinfo console** 命令的配置设置，请输入 **show crashinfo console** 命令。

show crashinfo console

语法说明

此命令没有任何参数或关键字。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

FIPS 140-2 的合规性禁止在加密边界（机箱）以外分布关键安全参数（密钥、密码等）。设备由于维护或检查堆故障崩溃时，堆栈或内存区域可能会转储到包含敏感数据的控制台。此输出在 FIPS 模式下必须抑制。

示例

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

相关命令

命令	说明
clear configure fips	清除 NVRAM 中存储的系统或模块 FIPS 配置信息。
crashinfo console disable	禁止对闪存读取、写入和配置故障写入信息。
fips enable	启用或禁用策略检查以在系统或模块上实现 FIPS 合规性。
show running-config fips	显示在 ASA 上运行的 FIPS 配置。

show crypto accelerator statistics

要显示硬件加密加速器 MIB 的全局和加速器特定统计信息，请在全局配置或特权 EXEC 模式下使用 **show crypto accelerator statistics** 命令。

show crypto accelerator statistics

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

输出统计信息定义如下：

加速器 0 显示基于软件的加密引擎的统计信息。

加速器 1 显示基于硬件的加密引擎的统计信息。

RSA 统计信息显示 2048 位密钥的 RSA 操作，该操作默认情况下在软件中执行。这意味着当您拥有 2048 位密钥时，IKE/SSL VPN 在 IPsec/SSL 协商阶段在软件中执行 RSA 操作。实际的 IPsec/SSL 流量仍使用硬件处理。如果有许多同时开始的并发会话，这可能会导致高 CPU，从而可能导致多个 RSA 密钥操作和高 CPU。如果由于此原因进入高 CPU 情况，则应使用 1024 位密钥在硬件中处理 RSA 密钥操作。为此，您必须重新注册身份证书。在版本 8.3(2) 或更高版本中，您还可以在 5510-5550 平台上使用 crypto engine large-mod-accel 命令，以在硬件中执行这些操作。

如果使用 2048 位 RSA 密钥并在软件中执行 RSA 处理，您可以使用 CPU 评测来确定哪些功能导致高 CPU 使用率。通常，bn_* 和 BN_* 函数是用于 RSA 的大型数据集的数学运算，对在软件中执行 RSA 操作期间检查 CPU 使用率最有用。例如：

```
@@@@@@@@@@@@@@@@@@@@.............................36.50% : _bn_mul_add_words
@@@@@@@@@@.......................................19.75% : _bn_sqr_comba8
```

Diffie-Hellman 统计信息显示在软件中执行模数大小大于 1024 的任何加密操作（例如，DH5 (Diffie-Hellman 组 5) 使用 1536）。如果是这样，则 2048 位密钥证书将在软件中进行处理，因此在运行许多会话时可导致高 CPU 使用率。

注　ASA 5505（采用 Cavium CN505 处理器）仅支持 Diffie-Hellman 组 1 和 2 生成硬件加速的 768 位和 1024 位密钥。Diffie-Hellman 组 5（1536 位密钥生成）在软件中执行。

自适应安全设备中的单一加密引擎执行 IPsec 和 SSL 操作。要显示引导时载入硬件加密加速器中的加密 (Cavium) 微代码版本，请输入 **show version** 命令。例如：

```
ciscoasa(config) show version

Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 统计信息在两个阶段显示密钥生成。第一个阶段是选择算法参数，该参数可在系统的不同用户之间共享。第二个阶段计算单一用户的专用密钥和公共密钥。

SSL 统计信息显示到硬件加密加速器的 SSL 事务中涉及的处理器密集公共密钥加密算法记录。

RNG 统计信息显示发送方和接收方的记录，这些记录可自动生成一组相同的随机数用作密钥。

示例

以下示例在全局配置模式下输入，显示全局加密加速器统计信息：

```
ciscoasa # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
```

```
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
```

```
    Verifications: 0
    Encrypted packets: 0
    Encrypted bytes: 0
    Decrypted packets: 0
    Decrypted bytes: 0
 [DSA statistics]
    Keys generated: 0
    Signatures: 0
    Verifications: 0
 [SSL statistics]
    Outbound records: 0
    Inbound records: 0
 [RNG statistics]
    Random number requests: 1
    Random number request failures: 0
```

下表说明了输出条目指示的内容。

输出	说明
Capacity	此部分涉及 ASA 能够支持的加密加速。
Supports hardware crypto	(True/False) ASA 可以支持硬件加密加速。
Supports modular hardware crypto	(True/False) 任何支持的硬件加密加速器均可作为单独的插件卡或模块插入。
Max accelerators	ASA 支持的最大硬件加密加速器数。
Mac crypto throughput	ASA 的最大额定 VPN 吞吐量。
Max crypto connections	ASA 的最大支持 VPN 隧道数。
Global Statistics	此部分涉及 ASA 中的组合硬件加密加速器。
Number of active accelerators	活动硬件加速器数。活动硬件加速器已初始化并可用于处理加密命令。
Number of non-operational accelerators	非活动硬件加速器数。已检测到非活动硬件加速器，但尚未完成初始化，或已失效且不再可用。
Input packets	所有硬件加密加速器处理的入站数据包数。
Input bytes	已处理入站数据包中数据的字节数。
Output packets	所有硬件加密加速器处理的出站数据包数。
Output error packets	其中检测到错误的所有硬件加密加速器处理的出站数据包数。
Output bytes	已处理出站数据包中数据的字节数。
Accelerator 0	每个部分均涉及加密加速器。第一个（加速器 0）始终为软件加密引擎。尽管并非硬件加速器，但 ASA 使用它来执行特定加密任务，并且其统计信息在此处显示。加速器 1 及更高编号始终均为硬件加密加速器。
Status	加速器的状态，指示加速器是已初始化、活动还是已失效。
Software crypto engine	加速器类型和固件版本（如果适用）。
Slot	加速器的插槽编号（如果适用）。
Active time	加速器处于活动状态的时长。
Total crypto transforms	加速器执行的加密命令总数。
Total dropped packets	加速器由于错误而丢弃的数据包总数。

输出（续）	说明（续）
Input statistics	本部分涉及加速器处理的输入流量。输入流量被视为必须进行解密和 / 或验证的密文。
Input packets	加速器已处理的输入数据包数。
Input bytes	加速器已处理的输入字节数。
Input hashed packets	加速器已执行哈希操作的数据包数。
Input hashed bytes	加速器已执行哈希操作的字节数。
Decrypted packets	加速器已执行对称解密操作的数据包数。
Decrypted bytes	加速器已执行对称解密操作的字节数。
Output statistics	本部分涉及加速器已处理的输出流量。输出流量被视为必须进行加密和 / 或哈希的明文。
Output packets	加速器已处理的输出数据包数。
Output bad packets	其中检测到错误的加速器已处理的输出数据包数。
Output bytes	加速器已处理的输出字节数。
Output hashed packets	加速器已执行出站哈希操作的数据包数。
Output hashed bytes	加速器已执行出站哈希操作的字节数。
Encyrpted packets	加速器已执行对称加密操作的数据包数。
Encyrpted bytes	加速器已执行对称加密操作的字节数。
Diffie-Hellman statistics	本部分涉及 Diffie-Hellman 密钥交换操作。
Keys generated	加速器已生成的 Diffie-Hellman 密钥集数。
Secret keys derived	加速器已衍生的 Diffie-Hellman 共享密钥数。
RSA statistics	本部分涉及 RSA 加密操作。
Keys generated	加速器已生成的 RSA 密钥集数。
Signatures	加速器已执行的 RSA 签名操作数。
Verifications	加速器已执行的 RSA 签名验证数。
Encrypted packets	加速器已执行 RSA 加密操作的数据包数。
Decrypted packets	加速器已执行 RSA 解密操作的数据包数。
Decrypted bytes	加速器已执行 RSA 解密操作的数据字节数。
DSA statistics	本部分涉及 DSA 操作。请注意，自版本 8.2 起不再支持 DSA，因此不再显示这些统计信息。
Keys generated	加速器生成的 DSA 密钥集的数量。
Signatures	加速器已执行的 DSA 签名操作的数量。
Verifications	加速器已执行的 DSA 签名验证的数量。
SSL statistics	本部分涉及 SSL 记录处理操作。
Outbound records	加速器已加密和已验证的 SSL 记录数。
Inbound records	加速器已解密和已验证的 SSL 记录数。
RNG statistics	本部分涉及随机数生成。
Random number requests	加速器的随机数请求数。
Random number request failures	对未成功的加速器的随机数请求数。

相关命令

命令	说明
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

show crypto ca certificates

要显示与特定信任点关联的证书或显示系统中安装的所有证书，请在全局配置或特权 EXEC 模式下使用 **show crypto ca certificates** 命令。

show crypto ca certificates [*trustpointname*]

语法说明

trustpointname	（可选）信任点的名称。如果您没有指定名称，此命令将显示 ASA 上安装的所有证书。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show crypto ca certificates** 命令的输出示例：

```
ciscoasa(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
```

```
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca authenticate	获取指定信任点的 CA 证书。
crypto ca crl request	基于指定信任点的配置参数请求 CRL。
crypto ca enroll	启动 CA 的注册流程。
crypto ca import	将证书导入到指定的信任点。
crypto ca trustpoint	进入指定信任点的信任点配置模式。

show crypto ca crl

要显示所有缓存的 CRL 或显示为指定信任点缓存的所有 CRL，请在全局配置或特权 EXEC 模式下使用 **show crypto ca crl** 命令。

show crypto ca crl [trustpool | trustpoint <*trustpointname*>]

语法说明

trustpoint *trustpointname*	（可选）信任点的名称。如果您没有指定名称，此命令将显示 ASA 上缓存的所有 CRL。
trustpool	信任池的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show crypto ca crl** 命令的输出示例：

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca authenticate	获取指定信任点的 CA 证书。
crypto ca crl request	基于指定信任点的配置参数请求 CRL。
crypto ca enroll	启动 CA 的注册流程。
crypto ca import	将证书导入到指定的信任点。
crypto ca trustpoint	进入指定信任点的信任点配置模式。

show crypto ca server

要显示 ASA 中本地 CA 配置的状态，请在 ca 服务器配置、全局配置或特权 EXEC 模式下使用 **show crypto ca server** 命令。

show crypto ca server

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下是 **show crypto ca server** 命令的输出示例：

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
    CRL not present.
    Current primary storage dir: nvram:
ciscoasa#
```

相关命令

命令	说明
crypto ca server	提供 ca 服务器配置模式 CLI 命令集的访问权限，从而允许您配置和管理本地 CA。
debug crypto ca server	显示您配置本地 CA 服务器时的调试消息。
show crypto ca server certificate	以 base64 格式显示本地 CA 的证书。
show crypto ca server crl	显示本地 CA CRL 的生命期。

show crypto ca server cert-db

要显示全部或部分本地 CA 服务器证书（包括颁发给特定用户的证书），请在 ca 服务器配置、全局配置或特权 EXEC 模式下使用 **show crypto ca server cert-db** 命令。

show crypto ca server cert-db [**username** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]

语法说明

allowed	指定显示允许注册的用户，无论其证书状态如何。
enrolled	指定显示具有有效证书的用户。
expired	指定显示持有过期证书的用户。
on-hold	指定显示尚未注册的用户。
serial *certificate-serial-number*	指定显示的特定证书的序列号。序列号必须为十六进制格式。
username *username*	指定证书所有者。username 可以是用户名或邮件地址。对于邮件地址，这是用于联系最终用户以及向其提供一次性密码 (OTP) 的邮件地址。启用最终用户的邮件通知需要邮件地址。

默认值

默认情况下，如果没有指定用户名或证书序列号，则显示颁发证书的整个数据库。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

show crypto ca server cert-db 命令显示本地 CA 服务器颁发的用户证书列表。通过指定特定用户名及一个或多个可选的证书类型关键字，和 / 或可选的证书序列号，您可以显示证书数据库的子集。

如果指定用户名而不带关键字或序列号，则显示为该用户颁发的所有证书。对于每位用户，输出将显示用户名、邮件地址、域名、允许注册的时间段以及通过注册邀请已通知用户的次数。

此外，输出中将显示以下信息：

- 需要 NOTIFIED（已通知）字段以支持多个提醒。需要通知用户注册的 OTP 和提醒通知尝试时，该字段将跟踪。该字段最初设置为 0。用户条目标记为允许注册时该字段增加为 1。此时，初始 OTP 通知已生成。

- 每次发送提醒时 NOTIFY（通知）字段都将递增。OTP 到期之前会发送三次通知。允许用户注册时、有效期中点时以及过期时间经过 ¾ 时会发送通知。此字段仅用于管理员发起的注册。对于自动证书续订，将使用证书数据库中的 NOTIFY（通知）字段。

注　此命令中的通知计数器用于跟踪过期前通知用户续订证书的次数，而 show crypto ca server user-db 中的通知计数器用于跟踪通知用户注册证书的次数。续订通知在 cert-db 下进行跟踪，未包含在 user-db 中。

每个证书都显示证书序列号、颁发和过期日期以及证书状态（已吊销 / 未吊销）。

示例

以下示例请求显示 CA 服务器为 asa 颁发的所有证书：

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

以下示例请求本地 CA 服务器颁发的、序列号为 0x2 的所有证书：

```
ciscoasa# show crypto ca server cert-db serial 2

Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

以下示例请求显示本地 CA 服务器颁发的所有证书：

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

相关命令

命令	说明
crypto ca server	提供 ca 服务器配置模式 CLI 命令集的访问权限，从而允许您配置和管理本地 CA。
crypto ca server revoke	在证书数据库和 CRL 中将本地 CA 服务器颁发的证书标记为已吊销。
lifetime crl	指定 CRL 的生命周期。

show crypto ca server certificate

要以 base64 格式显示本地 CA 服务器的证书，请在 ca 服务器配置、全局配置或特权 EXEC 模式下使用 **show crypto ca server certificate** 命令。

show crypto ca server certificate

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

show crypto ca server certificate 命令以 base64 格式显示本地 CA 服务器证书。此显示在将证书导出到需要信任本地 CA 服务器的其他设备时允许剪切并粘贴证书。

示例

以下是 **show crypto ca server certificate** 命令的输出示例：

```
ciscoasa# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

ciscoasa#
```

相关命令

命令	说明
crypto ca server	提供 ca 服务器配置模式 CLI 命令集的访问权限，从而允许您配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
keysize	指定在用户证书注册时生成的公共密钥和专用密钥的大小。
lifetime	指定 CA 证书和已签发证书的生命期。
show crypto ca server	以 ASCII 文本格式显示本地 CA 配置。

show crypto ca server crl

要显示本地 CA 的当前 CRL，请在 ca 服务器配置、全局配置或特权 EXEC 模式下使用 **show crypto ca server crl** 命令。

show crypto ca server crl

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下是 **show crypto ca server crl** 命令的输出示例：

```
ciscoasa# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
ciscoasa#
```

相关命令

命令	说明
cdp-url	指定要在 CA 颁发的证书中包含的 CRL 分发点 (CDP)。
crypto ca server	提供 ca 服务器配置模式 CLI 命令集的访问权限，从而允许您配置和管理本地 CA。
crypto ca server revoke	将本地 CA 服务器颁发的证书标记为在证书数据库和 CRL 中撤销。
lifetime crl	指定 CRL 的生命周期。
show crypto ca server	显示 CA 配置的状态。

show crypto ca server user-db

要显示本地 CA 服务器用户数据库中包含的用户，请在 ca 服务器配置、全局配置或特权 EXEC 模式下使用 **show crypto ca server user-db** 命令。

show crypto ca server user-db [expired | allowed | on-hold | enrolled]

语法说明

allowed	（可选）指定显示允许注册的用户，无论其证书状态如何。
enrolled	（可选）指定显示具有有效证书的用户。
expired	（可选）指定显示持有过期证书的用户。
on-hold	（可选）指定显示尚未注册的用户。

默认值

如果没有输入关键字，默认情况下显示数据库中的所有用户。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例展示当前注册的用户：

```
ciscoasa# show crypto ca server user-db enrolled
Username    DN                 Certificate issued     Certificate expiration
exampleusercn=Example User,o=...5/31/2009             5/31/2010

ciscoasa#
```

使用指南

此命令中的通知计数器用于跟踪通知用户注册证书的次数，而 show crypto ca server cert-db 中的通知计数器用于跟踪过期前通知用户续订证书的次数。续订通知在 cert-db 下进行跟踪，未包含在 user-db 中。

相关命令

命令	说明
crypto ca server user-db add	将用户添加到 CA 服务器用户数据库。
crypto ca server user-db allow	允许 CA 服务器数据库中特定的用户或用户子集向本地 CA 注册。
crypto ca server user-db remove	从 CA 服务器用户数据库删除用户。
crypto ca server user-db write	将本地 CA 数据库中配置的用户信息写入到存储。
show crypto ca server cert-db	显示本地 CA 颁发的所有证书。

show crypto ca trustpool

要显示构成信任池的证书，请在特权 EXEC 模式下使用 **show crypto ca trustpool** 命令。

show crypto ca trustpool [detail]

语法说明

此命令没有任何参数或关键字。

默认值

此命令显示所有信任池证书的缩略显示。指定 “detail” 选项后，将包含详细信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show crypto ca trustpool 命令的输出包括每个证书的指纹值。删除操作需要这些值。

示例

```
ciscoasa# show crypto ca trustpool

CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024

CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
```

```
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

相关命令

命令	说明
clear crypto ca trustpool	从信任池删除所有证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。
crypto ca trustpool remove	从信任池中删除一个指定的证书。

show crypto ca trustpool policy

要显示配置的信任池策略并处理任何应用的证书映射以展示其如何影响该策略，请在特权 EXEC 模式下使用 **show crypto ca trustpool policy** 命令。

show crypto ca trustpool policy

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#

ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
ciscoasa(config)#

ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
```

```
action:skip revocation-check

map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates

ciscoasa(config)#
```

相关命令

命令	说明
crypto ca trustpool policy	进入子模式，可提供定义 trustpool 策略的命令。

show crypto debug-condition

要显示 IPsec 和 ISAKMP 调试消息的当前配置过滤器、不匹配状态和错误状态，请在全局配置模式下使用 **show crypto debug-condition** 命令。

show crypto debug-condition

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例展示过滤条件：

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON

IKE peer IP address filters:
1.1.1.0/24   2.2.2.2

IKE user name filters:
my_user
```

相关命令

命令	说明
debug crypto condition	设置 IPsec 和 ISAKMP 调试消息的过滤条件。
debug crypto condition error	显示调试消息是否已经指定过滤条件。
debug crypto condition unmatched	显示 IPsec 和 ISAKMP 的调试消息（未包含足够的情景信息用于过滤）。

show crypto ikev1 sa

要显示 IKEv1 运行时 SA 数据库，请在全局配置模式或特权 EXEC 模式下使用 **show crypto ikev1 sa** 命令。

show crypto ikev1 sa [**detail**]

语法说明

detail	显示关于 SA 数据库的详细输出。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	• 是	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令的输出包括以下字段：

详细信息未指定。

IKE 对等设备	Type	Dir	Rky	状态
209.165.200.225	L2L	初始	否	MM_Active

详细信息已指定。

IKE 对等设备	Type	Dir	Rky	状态	加密	Hash	Auth	使用时间
209.165.200.225	L2L	初始	否	MM_Active	3des	md5	preshrd	86400

示例

以下示例在全局配置模式下输入，显示关于 SA 数据库的详细信息：

```
ciscoasa(config)# show crypto ikev1 sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

```
IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

相关命令

命令	说明
show crypto ikev2 sa	显示 IKEv2 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto ikev2 sa

要显示 IKEv2 运行时 SA 数据库，请在全局配置模式或特权 EXEC 模式下使用 **show crypto ikev2 sa** 命令。

show crypto ikev2 sa [**detail**]

语法说明

detail	显示关于 SA 数据库的详细输出。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	• 是	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令的输出包括以下字段：

详细信息未指定。

IKE 对等设备	Type	Dir	Rky	状态
209.165.200.225	L2L	初始	否	MM_Active

详细信息已指定。

IKE 对等设备	Type	Dir	Rky	状态	加密	Hash	Auth	使用时间
209.165.200.225	L2L	初始	否	MM_Active	3des	md5	preshrd	86400

示例

以下示例在全局配置模式下输入，显示关于 SA 数据库的详细信息：

```
ciscoasa(config)# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id                Local                Remote     Status         Role
671069399                10.0.0.0/500 10.255.255.255/500      READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

相关命令

命令	说明
show crypto ikev1 sa	显示 IKEv1 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto ipsec df-bit

要显示指定接口 IPsec 数据包的 IPsec DF 位策略，请在全局配置模式和特权 EXEC 模式下使用 **show crypto ipsec df-bit** 命令。

show crypto ipsec df-bit *interface*

语法说明

interface	指定接口名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示名为 inside 的接口的 IPsec DF 位策略：

```
ciscoasa(config)# show crypto ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

相关命令

命令	说明
crypto ipsec df-bit	配置 IPsec 数据包的 IPsec DF 位策略。
crypto ipsec fragmentation	配置 IPsec 数据包的分段策略。
show crypto ipsec fragmentation	显示 IPsec 数据包的分段策略。

show crypto ipsec fragmentation

要显示 IPsec 数据包的碎片整理策略，请在全局配置或特权 EXEC 模式下使用 **show crypto ipsec fragmentation** 命令。

show crypto ipsec fragmentation *interface*

语法说明

interface	指定接口名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，显示名为 inside 的接口的 IPsec 碎片整理策略：

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

相关命令

命令	说明
crypto ipsec fragmentation	配置 IPsec 数据包的分段策略。
crypto ipsec df-bit	配置 IPsec 数据包的 DF 位策略。
show crypto ipsec df-bit	显示指定接口的 DF 位策略。

show crypto ipsec policy

要显示 OSPFv3 提供的 IPsec 安全套接字 API (SS API) 安全策略信息，请在全局配置或特权 EXEC 模式下使用 **show crypto ipsec policy** 命令。您还可以使用此命令的替代形式：**show ipsec policy**。

show crypto ipsec policy [name]

语法说明

name	指定策略名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，显示名为 CSSU-UTF 的策略的加密安全套接字 API 安装策略信息：

```
ciscoasa(config)# show crypto ipsec policy
Crypto IPsec client security policy data

       Policy name:      CSSU-UTF
       Policy refcount:  0
       Inbound  ESP SPI:         1031 (0x407)
       Outbound ESP SPI:         1031 (0x407)
       Inbound  ESP Auth Key:    0123456789abcdef
       Outbound ESP Auth Key:    0123456789abcdef
       Inbound  ESP Cipher Key:
       Outbound ESP Cipher Key:
       Transform set:    esp-sha-hmac
```

相关命令

命令	说明
show crypto ipsec fragmentation	显示 IPsec 数据包的分段策略。
show crypto ipsec sa	显示 IPsec SA 列表。
show crypto ipsec df-bit	显示指定接口的 DF 位策略。
show crypto sockets	显示加密安全套接字和套接字状态。

show crypto ipsec sa

要显示 IPsec SA 列表，请在全局配置模式或特权 EXEC 模式下使用 **show crypto ipsec sa** 命令。您还可以使用此命令的替代形式：**show ipsec sa**。

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

语法说明

detail	（可选）显示有关所显示内容的详细错误信息。
entry	（可选）显示按对等设备地址排序的 IPsec SA
identity	（可选）显示按身份排序的 IPsec SA，不包括 ESP。这是简洁形式。
map *map-name*	（可选）显示指定加密映射的 IPsec SA。
peer *peer-addr*	（可选）显示指定对等设备 IP 地址的 IPsec SA。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	在转换和 IV 大小部分以及 ESPV3 IPsec 输出中添加了对 OSPFv3、多情景模式、Suite B 算法的支持。

示例

以下示例在全局配置模式下输入，显示包含标识为 OSPFv3 的隧道的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

注　如果 IPsec SA 策略表明在 IPsec 处理前进行碎片整理，则碎片整理统计信息为碎片整理前统计信息。如果 SA 策略表明在 IPsec 处理后进行碎片整理，则显示碎片整理后统计信息。

以下示例在全局配置模式下输入，显示名为 def 的加密映射的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
```

```
            transform: esp-3des esp-md5-hmac
            in use settings ={RA, Tunnel, }
            slot: 0, conn_id: 3, crypto-map: def
            sa timing: remaining key lifetime (sec): 480
            IV size: 8 bytes
            replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例在全局配置模式下输入，显示关键字 **entry** 的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例在全局配置模式下输入，显示采用关键字 **entry detail** 的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
```

```
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
```

```
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 104
          IV size: 8 bytes
          replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例展示采用关键字 **identity** 的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例展示采用关键字 **identity** 和 **detail** 的 IPsec SA。

```
ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
```

```
  dynamic allocated peer ip: 90.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
  current_peer: 10.135.1.8
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
  #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: 3B6F6A35
```

相关命令

命令	说明
clear configure isakmp	清除所有 ISAKMP 配置。
clear configure isakmp policy	清除所有 ISAKMP 策略配置。
clear isakmp sa	清除 IKE 运行时 SA 数据库。
isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show crypto ipsec stats

要显示 IPsec 统计信息列表，请在全局配置模式或特权 EXEC 模式下使用 **show crypto ipsec stats** 命令。

show crypto ipsec stats

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，显示 IPsec 统计信息：

```
ciscoasa(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
```

```
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear ipsec sa	基于指定的参数清除 IPsec SA 或计数器。
crypto ipsec transform-set	定义转换集。
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec sa summary	显示 IPsec SA 摘要。

示例

以下示例在全局配置模式下发出命令，显示 ISAKMP 统计信息：

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
crypto isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto isakmp sa

要显示 IKE 运行时 SA 数据库，请在全局配置模式或特权 EXEC 模式下使用 **show crypto isakmp sa** 命令。

show crypto isakmp sa [detail]

语法说明

detail	显示关于 SA 数据库的详细输出。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了 **show isakmp sa** 命令。
7.2(1)	此命令已弃用。**show crypto isakmp sa** 命令取代了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令的输出包括以下字段：

详细信息未指定。

IKE 对等设备	Type	Dir	Rky	状态
209.165.200.225	L2L	初始	否	MM_Active

详细信息已指定。

IKE 对等设备	Type	Dir	Rky	状态	加密	Hash	Auth	使用时间
209.165.200.225	L2L	初始	否	MM_Active	3des	md5	preshrd	86400

示例

以下示例在全局配置模式下输入，显示关于 SA 数据库的详细信息：

```
ciscoasa(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
```

```
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
crypto isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto isakmp stats

要显示运行时统计信息，请在全局配置模式或特权 EXEC 模式下使用 **show crypto isakmp stats** 命令。

show crypto isakmp stats

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了 **show isakmp stats** 命令。
7.2(1)	**show isakmp stats** 命令已弃用。**show crypto isakmp stats** 命令取代了此命令。

使用指南

此命令的输出包括以下字段：

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

示例

以下示例在全局配置模式下发出命令，显示 ISAKMP 统计信息：

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
crypto isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto key mypubkey

要显示 ECDSA 密钥的密钥名称、用法和椭圆曲线尺寸，请在全局配置模式或特权 EXEC 模式下使用 **show crypto key mypubkey** 命令。

show crypto key mypubkey dsa | rsa

语法说明

dsa	指定密钥名称。
rsa	指定密钥名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了 **show crypto key mypubkey** 命令。

show crypto protocol statistics

要显示加密加速器 MIB 中的协议特定统计信息，请在全局配置或特权 EXEC 模式下使用 **show crypto protocol statistics** 命令。

show crypto protocol statistics *protocol*

语法说明

protocol	指定要显示统计信息的协议名称。协议选项如下所示： **ikev1** - 互联网密钥交换版本 1。 **ipsec** - IP 安全阶段 2 协议。 **ssl** - 安全套接字层。 **other** - 保留以用于新协议。 **all**- 当前支持的所有协议。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，显示指定协议的加密加速器统计信息：

```
ciscoasa # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0
```

```
ciscoasa # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

ciscoasa # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
```

```
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa #
```

相关命令

命令	说明
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto accelerator statistics	显示来自加密加速器 MIB 的全局统计信息和加速器特定统计信息。

show crypto sockets

要显示加密安全套接字信息，请在全局配置模式或特权 EXEC 模式下使用 **show crypto sockets** 命令。

show crypto sockets

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	—
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，显示加密安全套接字信息：

```
ciscoasa(config)# show crypto sockets

Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

下表说明了 **show crypto sockets** 命令输出中的字段。

字段	说明
Number of Crypto Socket connections	系统中的加密套接字数量。
Socket State	此状态可以是 Open（开放），这意味着存在活动的 IPsec 安全关联 (SA)；也可以是 Closed（关闭），这意味着不存在活动的 IPsec SA。

字段	说明
Client	应用名称及其状态。
Flags	如果该字段表明 “ 共享 ”，则套接字与多个隧道接口共享。
Crypto Sockets in Listen state	加密 IPsec 配置文件的名称。

相关命令

命令	说明
show crypto ipsec policy	显示加密安全套接字 API 安装策略信息。

show csc node-count

要显示 CSC SSM 扫描流量的节点数，请在特权 EXEC 模式下使用 **show csc node-count** 命令：

show csc node-count [**yesterday**]

语法说明

yesterday	（可选）显示之前 24 小时时段内（从午夜到午夜）CSC SSM 扫描流量的节点数。

默认值

默认情况下，显示的节点计数是自午夜起扫描的节点数。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

节点是受 ASA 保护的网络上任何不同的源 IP 地址或设备地址。ASA 记录每日节点计数并与 CSC SSM 沟通此情况以进行用户许可证执行。

示例

以下是 **show csc node-count** 命令的输出示例，显示 CSC SSM 自午夜起扫描流量的节点数：

```
ciscoasa# show csc node-count
Current node count is 1
```

以下是 **show csc node-count** 命令的输出示例，显示 CSC SSM 在之前 24 小时时段内（从午夜到午夜）扫描流量的节点数：

```
ciscoasa(config)# show csc node-count yesterday
Yesterday's node count is 2
```

相关命令

命令	说明
csc	将网络流量发送到 CSC SSM 用于 FTP、HTTP、POP3 和 SMTP 的扫描，如 CSC SSM 中所配置。
show running-config class-map	显示当前类映射配置。

命令	说明
show running-config policy-map	显示当前策略映射配置。
show running-config service-policy	显示当前服务策略配置。

show ctiqbe

要显示关于在 ASA 范围内建立的 CTIQBE 会话的信息，请在特权 EXEC 模式下使用 **show ctiqbe** 命令。

show ctiqbe

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show ctiqbe 命令显示在 ASA 范围内建立的 CTIQBE 会话的信息。此命令与 **debug ctiqbe** 和 **show local-host** 一起用于对 CTIQBE 检查引擎问题进行故障排除。

注　我们建议您在使用 **show ctiqbe** 命令之前配置 **pager** 命令。如果有许多 CTIQBE 会话且 **pager** 命令未配置，则 **show ctiqbe** 命令输出可能需要一些时间才能结束。

示例

以下是 **show ctiqbe** 命令在以下情况时的输出示例。只有一个在 ASA 范围内设置的活动 CTIQBE 会话。该会话在位于本地地址 10.0.0.99 的内部 CTI 设备（例如，思科 IP 软电话）与位于 172.29.1.77 的外部 Cisco Call Manager（其中 TCP 端口 2748 为 Cisco CallManager）之间建立。该会话的心跳间隔为 120 秒。

```
ciscoasa# show ctiqbe

Total: 1
  LOCAL  FOREIGN  STATE  HEARTBEAT
-----------------------------------------------------------------
1  10.0.0.99/1117   172.29.1.77/2748  1  120
   RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 1029)
   MEDIA: Device ID 27  Call ID 0
   Foreign 172.29.1.99  (1028 1029)
   Local  172.29.1.88  (26822 26823)
   ------------------------------------------------
```

CTI 设备已注册 CallManager。设备内部地址和 RTP 侦听端口 PAT 为 172.29.1.99 UDP 端口 1028。其 RTCP 侦听端口 PAT 为 UDP 1029。

以 `RTP/RTCP: PAT xlates:` 开头的行仅当内部 CTI 设备注册外部 CallManager 且 CTI 设备地址和端口 PAT 为该外部接口时显示。如果 CallManager 位于内部接口上，或如果内部 CTI 设备地址和端口 NAT 为 CallManager 所使用的相同外部接口，则该行不会显示。

输出指示此 CTI 设备与位于 172.29.1.88 的另一部电话之间的呼叫已建立。另一部电话的 RTP 和 RTCP 侦听端口为 UDP 26822 和 26823。由于 ASA 不会保持 CTIQBE 会话记录关联第二部电话和 CallManager，因此另一部电话位于与 CallManager 相同的接口上。CTI 设备端的活动呼叫分支可通过设备 ID 27 和呼叫 ID 0 进行标识。

以下是这些 CTIBQE 连接的 xlate 信息：

```
ciscoasa# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
ciscoasa#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
inspect ctiqbe	启用 CTIQBE 应用检查。
service-policy	将策略映射应用于一个或多个接口。
show conn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。

show ctl-file

要显示电话代理使用的 CTL 文件的内容，请在全局配置模式下使用 **show ctl-file** 命令。

show ctl-file *filename* [**parsed**]

语法说明

filename	显示数据库中存储的支持安全模式的电话。
parsed	（可选）显示指定的 CTL 文件的详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

指定闪存中存储的 CTL 文件的文件名时，请指定磁盘编号、文件名和扩展名；例如：`disk0:/testctl.tlv`。使用 **show ctl-file** 命令在配置电话代理实例调试时非常有用。

示例

以下示例展示如何使用 **show ctl-file** 命令显示关于 CTL 文件的一般信息：

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv
Total Number of Records: 1
CTL Record Number 1
  Subject Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
     cucm
  IP Address:
     192.168.52.102
  Associated Trustpoint:
     cucm_primary
```

以下示例展示如何使用 **show ctl-file** 命令显示关于 CTL 文件的详细信息：

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
```

```
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
    521debcf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267ce1a7 202b2c8b 2ac980d3
    9608f64d e7cd82df e205e5bf 74a1d9c4 fae20f90 f3d2746a e90f439e ef93fca7
    d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eecb ce37e4d1
    866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

 ### CTL RECORD No.1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
    30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
    af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
    50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
    f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
    040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
    308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
    0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
    4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
    375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
    58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
    b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
    7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
    c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
    15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
    0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
    a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
    9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
    ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
    ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

相关命令

命令	说明
ctl-file (global)	指定要为电话代理创建的 CTL 实例，或解析闪存中存储的 CTL 文件。
ctl-file (phone-proxy)	指定配置电话代理时要使用的 CTL 实例。
phone proxy	配置电话代理实例。

show cts environment-data

要显示 Cisco TrustSec 的 ASA 上环境数据刷新操作的运行状况和状态，请在特权 EXEC 模式下使用 **show cts environment-data** 命令。

show cts environment-data

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令在故障切换配置的备用设备中不受支持。如果您在备用设备上输入此命令，将显示以下错误消息：

```
ERROR: This command is only permitted on the active device.
```

此命令仅在集群配置的主控设备上受支持。如果您在从属设备上输入此命令，将显示以下错误消息：

```
This command is only permitted on the master device.
```

示例

以下是 **show cts environment-data** 命令的输出示例

```
ciscoasa# show cts environment-data

CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 1200 secs
Last update time:          18:12:07 EST Feb 27 2012
Env-data expires in:       0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in:     0:00:02:24 (dd:hr:mm:sec)
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts pac	显示 PAC 上的组件。

show cts environment-data sg-table

要显示 Cisco TrustSec 的 ASA 上驻留的安全组表，请在特权 EXEC 模式下使用 **show cts environment-data sg-table** 命令。

show cts environment-data sg-table

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令在故障切换配置的备用设备中不受支持。如果您在备用设备上输入此命令，将显示以下错误消息：

```
ERROR: This command is only permitted on the active device.
```

此命令仅在集群配置的主控设备上受支持。如果您在从属设备上输入此命令，将显示以下错误消息：

```
This command is only permitted on the master device.
```

示例

以下是 **show cts environment-data sg-table** 命令的输出示例

```
ciscoasa# show cts environment-data sg-table

Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries

SG Name                         SG Tag     Type
-------                         ------     -------------
ANY                              65535     unicast
ExampleSG1                           2     unicast
ExampleSG13                         14     unicast
ExampleSG14                         15     unicast
ExampleSG15                         16     unicast
```

```
ExampleSG16                          17     unicast
ExampleSG17                          18     unicast
ExampleSG18                          19     unicast
Unknown                               0     unicast
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts pac	显示 PAC 上的组件。

show cts pac

要显示 Cisco TrustSec 的 ASA 上 Protected Access Credential (PAC) 的组件，请在特权 EXEC 模式下使用 **show cts pac** 命令。

show cts pac

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show cts pac 命令显示 PAC 信息，包括过期时间。过期时间非常重要，因为 ASA 在 PAC 生命期过后无法检索安全组表更新。管理员必须在旧 PAC 过期之前请求并安装新 PAC，以保持与身份服务引擎上的安全组表同步。

此命令在故障切换配置的备用设备中不受支持。如果您在备用设备上输入此命令，将显示以下错误消息：

```
ERROR: This command is only permitted on the active device.
```

此命令仅在集群配置的主控设备上受支持。如果您在从属设备上输入此命令，将显示以下错误消息：

```
This command is only permitted on the master device.
```

示例

以下是 **show cts pac** 命令的输出示例

```
ciscoasa# show cts pac
PAC-Info:
    Valid until: Jul 28 2012 08:03:23
    AID:         6499578bc0240a3d8bd6591127ab270c
    I-ID:        BrianASA36
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
```

```
PAC-Opaque:
  000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
  00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
  7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
  8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
  00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
  09100e1758
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts environment	显示环境数据刷新操作的运行状况和状态。

show cts sgt-map

要显示控制路径中的 IP 地址安全组表管理器条目，请在特权 EXEC 模式下使用 **show cts sgt-map** 命令。

show cts sgt-map [**sgt** *sgt*] [**address** *ipv4* | **address** *ipv6* [*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**]

语法说明

address i*pv4*/*ipv6* */prefix*	仅显示特定 IPv4 或 IPv6 地址或子网的 IP 地址安全组表映射。
brief	显示 IP 地址安全组表映射摘要。
detail	显示 IP 地址安全组表映射。
ipv4	显示 IPv4 地址安全组表映射。默认情况下，仅显示 IPv4 地址安全组表映射。
ipv6	显示 IPv6 地址安全组表映射。
name	显示具有匹配安全组名称的 IP 地址安全组表映射。
sgt *sgt*	仅显示具有匹配安全组表的 IP 地址安全组表映射。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。
9.3(1)	输出更新为包含来自 “CLI-HI” 来源的 IP-SGT 绑定信息，该信息通过 **cts role-based sgt-map** 命令填充。

使用指南

此命令显示控制路径中的 IP 地址安全组表管理器条目。

示例

以下是 **show cts sgt-map** 命令的输出示例：

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
<IP address> <SGT value> <Source type>
```

```
IP-SGT Active Bindings Summary
============================================
Total number of <Source type> bindings = <Total number of the entries from a source type>
Total number of active CONFIG bindings = <Total number of mapping entries>

ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
1.1.1.1       7 CLI-HI
10.10.10.1    7 CLI-HI
10.10.10.10   3 LOCAL
10.10.100.1   7 CLI-HI
198.26.208.31 7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

以下是 **show cts sgt-map ipv6** 命令的输出示例：

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information

IP Address                                SGT     Source
============================================================
3330::1                                   17      SXP
FE80::A8BB:CCFF:FE00:110                  17      SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

以下是 **show cts sgt-map ipv6 detail** 命令的输出示例：

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information

IP Address                 Security Group                          Source
============================================================================
3330::1                     2345                                    SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP

IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

以下是 **show cts sgt-map ipv6 brief** 命令的输出示例：

```
ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information

IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

以下是 **show cts sgt-map address** 命令的输出示例：

```
ciscoasa# show cts sgt-map address 10.10.10.5 mask 255.255.255.255

Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================================
10.10.10.5              1234    SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts environment	显示环境数据刷新操作的运行状况和状态。

show cts sxp connections

要显示 ASA 上的安全交换协议 (SXP) 连接，请在特权 EXEC 模式下使用 **show cts sxp connections** 命令。

show cts sxp connections [**peer** *peer addr*] [**local** *local addr*] [**ipv4 | ipv6**] [**status** {**on | off | delete-hold-down | pending-on**}] [**mode** {**speaker | listener**}] [**brief**]

语法说明

brief	（可选）显示 SXP 连接摘要。
delete-hold-down	（可选）TCP 连接在处于 ON（打开）状态时将其终止（TCP 关闭）。只有侦听程序模式下配置的 ASA 可处于此状态。
ipv4	（可选）显示具有 IPv4 地址的 SXP 连接。
ipv6	（可选）显示具有 IPv6 地址的 SXP 连接。
监听程序	（可选）显示侦听程序模式下配置的 ASA。
local *local addr*	（可选）显示具有匹配本地 IP 地址的 SXP 连接。
mode	（可选）显示具有匹配模式的 SXP 连接。
off	（可选）TCP 连接未启动。ASA 仅在处于此状态时重试 TCP 连接。
on	（可选）SXP OPEN 或 SXP OPEN RESP 消息已接收。SXP 连接已成功建立。ASA 仅在处于此状态时交换 SXP 消息。
peer *peer addr*	（可选）显示具有匹配对等设备本地 IP 地址的 SXP 连接。
pending-on	（可选）SXP OPEN 消息已发送到对等设备；等待来自对等设备的响应。
speaker	（可选）显示扬声器模式下配置的 ASA。
status	（可选）显示具有匹配状态的 SXP 连接。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

SXP 状态在以下情况时更改：

- 如果 SXP 侦听程序由于其对等设备未配置 SXP 或禁用 SXP 而丢弃其 SXP 连接，则 SXP 侦听程序转为 OFF（关闭）状态。

- 如果 SXP 侦听程序由于其对等设备崩溃或接口关闭而丢弃其 SXP 连接，则 SXP 侦听程序转为 DELETE_HOLD_DOWN 状态。
- 出现前两个条件的任意一个时，SXP 扬声器将转为 OFF（关闭）状态。

此命令在故障切换配置的备用设备中不受支持。如果您在备用设备上输入此命令，将显示以下错误消息：

```
ERROR: This command is only permitted on the active device.
```

此命令仅在集群配置的主控设备上受支持。如果您在从属设备上输入此命令，将显示以下错误消息：

```
This command is only permitted on the master device.
```

示例

以下是 **show cts sxp connections** 命令的输出示例：

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Reconcile period   : 120 secs
Retry open period  : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
----------------------------------------------
Peer IP            : 2.2.2.1
Local IP           : 2.2.2.2
Conn status        : On
Local mode         : Listener
Ins number         : 1
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 3.3.3.1
Local IP           : 3.3.3.2
Conn status        : On
Local mode         : Listener
Ins number         : 2
TCP conn password : None
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 4.4.4.1
Local IP           : 4.4.4.2
Conn status        : On
Local mode         : Speaker
Ins number         : 1
TCP conn password : Set
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts environment	显示环境数据刷新操作的运行状况和状态。

show cts sxp sgt-map

要显示 Cisco TrustSec 的 ASA 上安全交换协议 (SXP) 模块中的当前 IP 地址安全组表映射数据库条目，请在特权 EXEC 模式下使用 **show cts sxp sgt-map** 命令。

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *sgt*] [**address** *ipv4* | **address** *ipv6* [*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**] [**status**]

语法说明

address i*pv4*/*ipv6* */prefix*	仅显示特定 IPv4 或 IPv6 地址或子网的 IP 地址安全组表映射。
brief	显示 IP 地址安全组表映射摘要。
detail	显示安全组表信息。如果安全组名称不可用，则仅显示安全组表值而不带括号。
ipv4	显示具有 IPv4 地址的 IP 地址安全组表映射。默认情况下，仅显示具有 IPv4 地址的 IP 地址安全组表映射。
ipv6	显示具有 IPv6 地址的 IP 地址安全组表映射。
name	显示具有匹配安全组名称的 IP 地址安全组表映射。
peer *peer addr*	仅显示具有匹配对等设备 IP 地址的 IP 地址安全组表映射。
sgt *sgt*	仅显示具有匹配安全组表的 IP 地址安全组表映射。
status	显示活动或非活动映射条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令显示从 SXP 整合的活动 IP 地址安全组表映射条目。

此命令在故障切换配置的备用设备中不受支持。如果您在备用设备上输入此命令，将显示以下错误消息：

```
ERROR: This command is only permitted on the active device.
```

此命令仅在集群配置的主控设备上受支持。如果您在从属设备上输入此命令，将显示以下错误消息：

```
This command is only permitted on the master device.
```

示例

以下是 **show cts sxp sgt-map** 命令的输出示例：

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3

SGT        : 7
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1

SGT        : 7
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1

SGT        : 7
IPv6       : FE80::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
```

以下是 **show cts sxp sgt-map detail** 命令的输出示例：

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3

SGT        : STBU(7)
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active

SGT        : STBU(7)
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
Status     : Inactive

SGT        : 6
IPv6       : 1234::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
```

以下是 **show cts sxp sgt-map brief** 命令的输出示例：

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.1
SGT, IPv4: 7, 3.3.3.0
SGT, IPv6: 7, FE80::A8BB:CCFF:FE00:110
```

相关命令

命令	说明
show running-config cts	显示运行配置的 SXP 连接。
show cts environment	显示环境数据刷新操作的运行状况和状态。

show curpriv

要显示当前用户特权，请使用 **show curpriv** 命令：

show curpriv

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	—	—	• 是
特权 EXEC	• 是	• 是	—	—	• 是
用户 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	已根据 CLI 指南进行修改。

使用指南

show curpriv 命令显示当前特权级别。 较低特权级别编号表示较低特权级别。

示例

以下示例展示名为 enable_15 的用户处于不同特权级别时 **show curpriv** 命令的输出。用户名表示用户登录时输入的名称。P_PRIV 表示用户已输入 **enable** 命令。P_CONF 表示用户已输入 **config terminal** 命令。

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit

ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit

ciscoasa(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

以下示例展示已知行为。如果您处于启用模式，然后进入禁用模式，则初始登录用户名替换为 enable_1：

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit

Logoff

Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

相关命令

命令	说明
clear configure privilege	从配置中删除特权命令语句。
show running-config privilege	显示命令的特权级别。

show ddns update interface 至 show environmentevent manager 命令

show ddns update interface

要显示分配给 ASA 接口的 DDNS 方法，请在特权 EXEC 模式下使用 **show ddns update interface** 命令。

show ddns update interface [*interface-name*]

语法说明

interface-name	（可选）网络接口的名称。

默认值

忽略 *interface-name* 字符串将显示分配给每个接口的 DDNS 方法。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示分配给 inside 接口的 DDNS 方法：

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
ciscoasa#
```

相关命令

命令	说明
ddns（**DDNS 更新方法模式**）	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update（**接口配置模式**）	将 ASA 接口与 DDNS 更新方法或 DDNS 更新主机名关联。
ddns update method（**全局配置模式**）	创建一个用于动态更新 DNS 资源记录的方法。
show ddns update method	显示每种配置的 DDNS 方法的类型和间隔。DHCP 服务器用于执行 DNS 更新。
show running-config ddns	显示运行的配置中所有配置 DDNS 方法的类型和间隔。

show ddns update method

要显示运行的配置中的 DDNS 更新方法，请在特权 EXEC 模式下使用 **show ddns update method** 命令。

show ddns update method [*method-name*]

语法说明

method-name	（可选）配置的 DDNS 更新方法的名称。

默认值

忽略 *method-name* 字符串将显示所有配置的 DDNS 更新方法。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示名为 ddns-2 的 DDNS 方法：

```
ciscoasa(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
ciscoasa(config)#
```

相关命令

命令	说明
ddns（DDNS 更新方法模式）	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update（接口配置模式）	将 ASA 接口与动态 DNS (DDNS) 更新方法或 DDNS 更新主机名关联。
ddns update method（全局配置模式）	创建一个用于动态更新 DNS 资源记录的方法。
show ddns update interface	显示与每种配置的 DDNS 方法关联的接口。
show running-config ddns	显示运行的配置中所有配置 DDNS 方法的类型和间隔。

show debug

要显示当前调试配置，请使用 **show debug** 命令。

show debug [*command* [*keywords*]]

语法说明

command	（可选）指定要查看其当前配置的 **debug** 命令。
keywords	（可选）对于每个 *command*，*command* 后跟的 *keywords* 与关联 **debug** 命令支持的 *keywords* 完全相同。

默认值

此命令没有默认设置。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	**eigrp** 关键字已添加到可能的命令值列表。
8.4(1)	**route** 关键字已添加到可能的命令值列表。
9.2(1)	**event manager** 关键字已添加到可能的命令值列表。

使用指南

对于每个 *command*，*command* 后跟的 *keywords* 与关联 **debug** 命令支持的 *keywords* 完全相同。有关支持的语法信息，请参阅关联的 **debug** 命令。

注　每个 *command* 的可用性取决于支持适用 **debug** 命令的命令模式。

有效的 *command* 值如下：

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**

- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **event manager**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**

- **rip**
- **route**
- **rtsp**
- **sdi**
- **sequence**
- **sfr**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

示例

您可以使用 **show debug** 命令查看所有调试配置、特定功能的调试配置以及部分功能的调试配置。以下命令允许调试身份验证、记账和闪存：

```
ciscoasa# debug aaa authentication
debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

相关命令

命令	说明
debug	显示所有 **debug** 命令。

show debug mmp

要显示 MMP 检查模块的当前调试设置，请在特权 EXEC 模式下使用 **show debug mmp** 命令。

show debug mmp

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。

示例

以下示例展示如何使用 **show debug mmp** 命令显示 MMP 检查模块的当前调试设置：

```
ciscoasa# show debug mmp
debug mmp  enabled at level 1
```

相关命令

命令	说明
debug mmp	显示检查 MMP 事件。
inspect mmp	配置 MMP 检查引擎。

show dhcpd

要查看 DHCP 绑定、状态和统计信息，请在特权 EXEC 或全局配置模式下使用 **show dhcpd** 命令。

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

语法说明

binding	显示指定服务器 IP 地址的绑定信息及其关联客户端硬件地址和租期时长。
IP_address	显示指定 IP 地址的绑定信息。
state	显示 DHCP 服务器的状态，例如在当前情景下是否已启用以及在每个接口上是否已启用。
statistics	显示统计信息，例如地址池、绑定、过期绑定、格式不正确的消息、已发送消息和已接收消息的数量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您在 **show dhcpd binding** 命令中包含了可选的 IP 地址，则仅显示该 IP 地址的绑定。

show dhcpd binding | state | statistics 命令在全局配置模式下也可用。

示例

以下是 **show dhcpd binding** 命令的输出示例：

```
ciscoasa# show dhcpd binding
IP Address Client-id       Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

以下是 **show dhcpd state** 命令的输出示例：

```
ciscoasa# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

以下是 **show dhcpd statistics** 命令的输出示例：

```
ciscoasa# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
clear dhcpd	清除 DHCP 服务器绑定和统计计数器。
dhcpd lease	定义授予客户端的 DHCP 信息的租期时长。
show running-config dhcpd	显示当前 DHCP 服务器配置。

show dhcprelay state

要查看 DHCP 中继代理的状态，请在特权 EXEC 或全局配置模式下使用 **show dhcprelay state** 命令。

show dhcprelay state

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示当前情景和每个接口的 DHCP 中继代理状态信息。

示例

以下是 **show dhcprelay state** 命令的输出示例：

```
ciscoasa# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

相关命令

命令	说明
show dhcpd	显示 DHCP 服务器统计信息和状态信息。
show dhcprelay statistics	显示 DHCP 中继统计信息。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

show dhcprelay statistics

要显示 DHCP 中继统计信息，请在特权 EXEC 模式下使用 **show dhcprelay statistics** 命令。

show dhcprelay statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show dhcprelay statistics 命令的输出将递增，直到您输入 **clear dhcprelay statistics** 命令。

示例

以下内容展示 **show dhcprelay statistics** 命令的输出示例：

```
ciscoasa# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
ciscoasa#
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
clear dhcprelay statistics	清除 DHCP 中继代理统计计数器。
debug dhcprelay	显示 DHCP 中继代理的调试信息。
show dhcprelay state	显示 DHCP 中继代理的状态。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

show disk

要仅显示 ASA 闪存内容，请在特权 EXEC 模式下使用 **show disk** 命令。

show disk[**0** | **1**] [**filesys** | **all**] **controller**

语法说明

0 | 1	指定内部闪存（0，默认值）或外部闪存 (1)。
all	显示闪存内容以及文件系统信息。
controller	指定闪存控制器型号。
filesys	显示关于紧凑型闪存卡的信息。

默认值

默认情况下，此命令显示内部闪存。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show disk** 命令的输出示例：

```
ciscoasa# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 7:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 7:29:18 test9.cfg
 24 1197       Jan 19 2005 8:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 8:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
```

```
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

以下是 **show disk filesys** 命令的输出示例：

```
ciscoasa# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

以下是 **show disk controller** 命令的输出示例：

```
ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA
```

相关命令

命令	说明
dir	系统随即会显示目录的内容。

show dns

要显示所有或指定完全限定域名 (FQDN) 主机的当前解析 DNS 地址，请在特权 EXEC 模式下使用 **show dns** 命令。

show dns [**host** *fqdn_name*]

语法说明

fqdn_name	（可选）指定所选主机的 FQDN。
host	（可选）指示指定主机的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show dns** 命令的输出示例：

```
ciscoasa# show dns
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 0:00:36
  Address: 10.4.1.2                          TTL 0:01:01
Name: www.example2.com
  Address: 10.2.4.1                          TTL 0:25:13
  Address: 10.5.2.1                          TTL 0:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa          TTL 00:00:41
  Address: 10.10.10.2                        TTL 00:25:01
```

注　如果 FQDN 主机尚未激活，则此命令不显示任何输出。

以下是 **show dns host** 命令的输出示例：

```
ciscoasa# show dns host www.example.com
Name:   www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 0:00:36
Address: 10.1.1.2 TTL 0:01:01
```

相关命令

命令	说明
clear dns-hosts	清除 DNS 缓存。
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	配置 DNS 服务器地址。

show dns-hosts

要显示 DNS 缓存，请在特权 EXEC 模式下使用 **show dns-hosts** 命令。DNS 缓存包括从 DNS 服务器动态获知的条目以及手动输入的名称和 IP 地址。

show dns-hosts

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show dns-hosts** 命令的输出示例：

```
ciscoasa# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

相关命令

命令	说明
clear dns-hosts	清除 DNS 缓存。
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	配置 DNS 服务器地址。
dns retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
dns timeout	指定在尝试下一 DNS 服务器之前等待的时间量。

表 6-1 显示每个字段的说明。

表 6-1　show dns-hosts 字段

字段	说明
Host	显示主机名。
Flags	显示条目状态为以下各项的组合： • temp - 由于来自 DNS 服务器，此条目是临时的。ASA 会在 72 小时不活动后删除此条目。 • perm - 由于使用 **name** 命令添加，此条目是永久的。 • OK - 此条目有效。 • ?? - 此条目可疑并需要重新验证。 • EX - 此条目已过期。
Age	显示自此条目上次引用后经过的小时数。
Type	显示 DNS 记录的类型；该值始终为 IP。
Address(es)	IP 地址。

相关命令

命令	说明
clear dns-hosts	清除 DNS 缓存。
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	配置 DNS 服务器地址。
dns retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
dns timeout	指定在尝试下一 DNS 服务器之前等待的时间量。

show dynamic-filter data

要显示关于僵尸网络流量过滤器动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目，请在特权 EXEC 模式下使用 **show dynamic-filter data** 命令。

show dynamic-filter data

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

要查看动态数据库信息，请首先通过 **dynamic-filter use-database** 和 **dynamic-filter updater-client enable** 命令允许使用和下载数据库。

示例

以下是 **show dynamic-filter data** 命令的输出示例：

```
ciscoasa# show dynamic-filter data

Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
cisco.example, cisco.invalid, bad.example.com
bad.example.net, bad.example.org, bad.cisco.example
bad.cisco.ivalid
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 0 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show dynamic-filter dns-snoop

要显示僵尸网络流量过滤器 DNS 监听摘要，或实际的 IP 地址和名称，请在特权 EXEC 模式下使用 **show dynamic-filter dns-snoop** 命令。

show dynamic-filter dns-snoop [**detail**]

语法说明

detail	（可选）显示从 DNS 响应监听的 IP 地址和名称。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

所有检查的 DNS 数据均包含在此输出中，而不仅仅是黑名单中的匹配名称。来自静态条目的 DNS 数据未包括在内。

要清除 DNS 监听数据，请输入 **clear dynamic-filter dns-snoop** 命令。

示例

以下是 **show dynamic-filter dns-snoop** 命令的输出示例：

```
ciscoasa# show dynamic-filter dns-snoop

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

以下是 **show dynamic-filter dns-snoop detail** 命令的输出示例：

```
ciscoasa# show dynamic-filter dns-snoop detail

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
DNS reverse Cache Information:
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
    [www3.example.com] cat=2, ttl=3
    [www.bad.example.com] cat=2, ttl=3
    [www.example.com] cat=2, ttl=3
```

```
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
    [cisco.example] cat=2, ttl=73
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
    [cisco.invalid] cat=2, ttl=2
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show dynamic-filter reports top

要生成按僵尸网络流量过滤器分类的前 10 个恶意站点、端口和受感染主机的报告，请在特权 EXEC 模式下使用 **show dynamic-filter reports top** 命令。

show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]

语法说明

malware-ports	（可选）显示前 10 个恶意端口的报告。
malware-sites	（可选）显示前 10 个恶意站点的报告。
infected-hosts	（可选）显示前 10 个受感染主机的报告。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。
8.2(2)	**botnet-sites** 和 **botnet-ports** 关键字分别更改为 **malware-sites** 和 **malware-ports**。恶意站点报告现在包括丢弃的连接数，以及每个站点的威胁级别和类别。添加了上次清除时间戳。对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

此报告是数据快照，因此可能不匹配自开始收集统计信息后的前 10 个项目。

要清除报告数据，请输入 **clear dynamic-filter reports top** 命令。

示例

以下是 **show dynamic-filter reports top malware-sites** 命令的输出示例：

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                                  Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                    11      0          2      Botnet
bad2.example.com (209.165.200.225)                 8      8          3      Virus
bad1.cisco.example(10.131.36.158)                  6      6          3      Virus
bad2.cisco.example(209.165.201.1)                  2      2          3      Trojan
horrible.example.net(10.232.224.2)                 2      2          3      Botnet
nono.example.org(209.165.202.130)                  1      1          3      Virus

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

以下是 **show dynamic-filter reports top malware-ports** 命令的输出示例：

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                        Connections logged
------------------------------------------------------------------------
tcp 1000                                                 617
tcp 2001                                                 472
tcp 23                                                    22
tcp 1001                                                  19
udp 2000                                                  17
udp 2001                                                  17
tcp 8080                                                   9
tcp 80                                                     3
tcp >8192                                                  2

Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009
```

以下是 **show dynamic-filter reports top infected-hosts** 命令的输出示例：

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                        Connections logged
------------------------------------------------------------------------
10.10.10.51(inside)                                     1190
10.12.10.10(inside)                                       10
10.10.11.10(inside)                                        5

Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。

命令	说明
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show dynamic-filter reports infected-hosts

要生成关于按僵尸网络流量过滤器分类的受感染主机的报告，请在特权 EXEC 模式下使用 **show dynamic-filter reports infected-hosts** 命令。

show dynamic-filter reports infected-hosts {**max-connections** | **latest-active** | **highest-threat** | **subnet** *ip_address netmask* | **all**}

语法说明

all	显示所有缓冲的受感染主机信息。此显示可能包括数千个条目。您可能想要使用 ASDM 而不是使用 CLI 来生成 PDF 文件。
highest-threat	显示连接到具有最高威胁级别的恶意站点的 20 台主机。
latest-active	显示具有最近活动的 20 台主机。对于每台主机，显示将展示关于 5 个已访问恶意站点的详细信息。
max-connections	显示具有最多连接数的 20 台受感染主机。
subnet *ip_address netmask*	最多显示指定子网内的 20 台主机。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

这些报告包含受感染主机的详细历史，展示受感染主机、已访问恶意站点和恶意端口之间的关联。

要清除报告数据，请输入 **clear dynamic-filter reports infected-hosts** 命令。

示例

以下是 **show dynamic-filter reports infected hosts all** 命令的输出示例：

```
ciscoasa# show dynamic-filter reports infected-hosts all

Total 2 infected-hosts in buffer
Host (interface)                        Latest malicious conn time, filter action  Conn logged, dropped
=============================================================================================================
192.168.1.4 (internal)                  15:39:40 UTC Sep 17 2009, dropped                    3      3
Malware-sites connected to (not ordered)
```

```
Site                        Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-----------------------------------------------------------------------------------------------------------
10.73.210.27 (bad.example.com)     80, 15:39:31 UTC Sep 17 2009, dropped      2   2     very-high Malware
10.65.2.119 (bad2.example.com)     0, 15:39:40 UTC Sep 17 2009, dropped       1   1     very-high admin-added
===========================================================================================================
192.168.1.2 (internal)                   15:39:01 UTC Sep 17 2009, dropped                    5      5
Malware-sites connected to (not ordered)
Site                        Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-----------------------------------------------------------------------------------------------------------
10.131.36.158 (bad.example.com)    0, 15:37:46 UTC Sep 17 2009, dropped      1    1    very-high admin-added
10.65.2.119 (bad2.example.com)     0, 15:37:53 UTC Sep 17 2009, dropped      1    1   very-high  admin-added
20.73.210.27 (bad3.example.com)   80, 15:39:01 UTC Sep 17 2009, dropped      3    3   very-high  Malware
===========================================================================================================

Last clearing of the infected-hosts report: Never
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。

命令	说明
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show dynamic-filter statistics

要显示有多少连接使用僵尸网络流量过滤器分类为白名单、黑名单和灰名单连接，请在特权 EXEC 模式下使用 **show dynamic-filter statistics** 命令。

show dynamic-filter statistics [**interface** *name*] [**detail**]

语法说明

detail	（可选）显示每个威胁级别有多少数据包进行分类或丢弃。
interface *name*	（可选）显示特定接口的统计信息。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。
8.2(2)	添加了 **detail** 关键字以显示每个威胁级别有多少数据包进行分类或丢弃。对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

灰名单包含与多个域名关联的地址，但并非所有这些域名均位于黑名单中。

要清除统计信息，请输入 **clear dynamic-filter statistics** 命令。

示例

以下是 **show dynamic-filter statistics** 命令的输出示例：

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

以下是 **show dynamic-filter statistics interface outside detail** 命令的输出示例：

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
 Total conns classified 2108, ingress 2108, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 1, dropped 1, ingress 0, egress 0
   Threat level 5 classified 1, dropped 1, ingress 0, egress 0
   Threat level 4 classified 0, dropped 0, ingress 0, egress 0
   ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
   Threat level 5 classified 6, dropped 6, ingress 4, egress 2
   Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。

命令	说明
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show dynamic-filter updater-client

要显示关于僵尸网络流量过滤器更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本，请在特权 EXEC 模式下使用 **show dynamic-filter updater-client** 命令。

show dynamic-filter updater-client

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下是 **show dynamic-filter updater-client** 命令的输出示例：

```
ciscoasa# show dynamic-filter updater-client

Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。

命令	说明
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

show eigrp events

要显示 EIGRP 事件日志，请在特权 EXEC 模式下使用 **show eigrp events** 命令。

show eigrp [*as-number*] **events** [{*start end*} | **type**]

语法说明

as-number	（可选）指定您查看事件日志的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此您无需指定自主系统编号。
end	（可选）限制以 *start* 索引号开头并以 *end* 索引号结尾的条目的输出。
start	（可选）指定日志条目索引号的数字。指定起始编号将导致输出以指定的事件开头并以通过 *end* 参数指定的事件结尾。有效值为从 1 到 4294967295。
type	（可选）显示所记录的事件。

默认值

如果没有指定 *start* 和 *end*，则显示所有日志条目。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

show eigrp events 输出显示最多 500 个事件。达到最大事件数后，新事件将添加到输出底部，并且旧事件将从输出顶部删除。

您可以使用 **clear eigrp events** 命令清除 EIGRP 事件日志。

show eigrp events type 命令显示 EIGRP 事件的日志记录状态。默认情况下，将记录邻居变更、邻居警告和 DUAL FSM 消息。您可以使用 **no eigrp log-neighbor-changes** 命令禁用邻居变更事件日志记录。您可以使用 **no eigrp log-neighbor-warnings** 命令禁用邻居警告事件日志记录。您无法禁用 DUAL FSM 事件的日志记录。

示例

以下是 **show eigrp events** 命令的输出示例：

```
ciscoasa# show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
```

```
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

以下是定义了起始和停止编号的 **show eigrp events** 命令的输出示例：

```
ciscoasa# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

以下是 EIGRP 事件日志中没有条目时 **show eigrp events** 命令的输出示例：

```
ciscoasa# show eigrp events

Event information for AS 100:  Event log is empty.
```

以下是 **show eigrp events type** 命令的输出示例：

```
ciscoasa# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

相关命令

命令	说明
clear eigrp events	清除 EIGRP 事件日志记录缓冲区。
eigrp log-neighbor-changes	允许记录邻居变更事件。
eigrp log-neighbor-warnings	允许记录邻居警告事件。

show eigrp interfaces

要显示参与 EIGRP 路由的接口，请在特权 EXEC 模式下使用 **show eigrp interfaces** 命令。

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

语法说明

as-number	（可选）指定您显示活动接口的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此您无需指定自主系统编号。
detail	（可选）显示详细信息。
if-name	（可选）通过 **nameif** 命令指定的接口的名称。指定限制指定接口显示的接口名称。

默认值

如果没有指定接口名称，则显示所有 EIGRP 接口的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

使用 **show eigrp interfaces** 命令确定哪些接口上 EIGRP 处于活动状态，并了解关于与这些接口相关 EIGRP 的信息。

如果指定了接口，则仅显示该接口。否则，将显示正在运行 EIGRP 的所有接口。

如果指定了自主系统，则仅显示该指定自主系统的路由进程。否则，将显示所有 EIGRP 进程。

示例

以下是 **show eigrp interfaces** 命令的输出示例：

```
ciscoasa# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt          0         0/0          0      11/434          0          0
outside       1         0/0        337       0/10           0          0
inside        1         0/0         10       1/63         103          0
```

表 6-2 说明了显示中所示的重要字段。

表 6-2　show eigrp interfaces 字段说明

字段	说明
process	EIGRP 路由进程的自主系统编号。
Peers	直连对等设备的数量。
Xmit Queue Un/Reliable	不可靠和可靠传输队列中的剩余数据包数。
Mean SRTT	平均顺利往返时间间隔（以秒为单位）。
Pacing Time Un/Reliable	用于确定 EIGRP 数据包应何时发出接口（不可靠和可靠数据包）的定步计时（以秒为单位）。
Multicast Flow Timer	ASA 将发送组播 EIGRP 数据包的最大秒数。
Pending Routes	传输队列中等待发送的数据包中的路由数。

相关命令

命令	说明
network	定义参与 EIGRP 路由进程的网络和接口。

show eigrp neighbors

要显示 EIGRP 邻居表，请在特权 EXEC 模式下使用 **show eigrp neighbors** 命令。

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

语法说明

as-number	（可选）指定要删除邻居条目的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此您无需指定自主系统编号。
detail	（可选）显示详细邻居信息。
if-name	（可选）通过 **nameif** 命令指定的接口的名称。指定接口名称将显示通过该接口获知的所有邻居表条目。
static	（可选）显示使用 **neighbor** 命令静态定义的 EIGRP 邻居。

默认值

如果没有指定接口名称，则显示通过所有接口获知的邻居。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

您可以使用 **clear eigrp neighbors** 命令清除从 EIGRP 邻居表动态获知的邻居。

除非您使用 **static** 关键字，否则静态邻居不包含在输出中。

示例

以下是 **show eigrp neighbors** 命令的输出示例：

```
ciscoasa# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface       Holdtime Uptime   Q      Seq  SRTT  RTO
                                        (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1       13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0       14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0       12       0:02:02  0      4    5     20
```

表 6-3 说明了显示中所示的重要字段。

表 6-3　show eigrp neighbors 字段说明

字段	说明
process	EIGRP 路由进程的自主系统编号。
Address	EIGRP 邻居的 IP 地址。
Interface	ASA 在其上接收来自邻居的问候数据包的接口。
Holdtime	ASA 在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。 如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认保持时间，则显示非默认保持时间。 如果该值达到 0，则 ASA 认为邻居不可访问。
Uptime	自 ASA 初次从邻居收到消息后经过的时间（小时：分钟：秒钟格式）。
Q Count	ASA 等待发送的 EIGRP 数据包（更新、查询和回复）数。
Seq Num	从邻居接收的上一更新、查询或回复数据包的序列号。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 ASA 接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 ASA 将数据包从重新传输队列重新发送到邻居之前等待的时间量。

以下是 **show eigrp neighbors static** 命令的输出示例：

```
ciscoasa# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                  Interface
192.168.1.5                     management
```

表 6-4 说明了显示中所示的重要字段。

表 6-4　show ip eigrp neighbors static 字段说明

字段	说明
process	EIGRP 路由进程的自主系统编号。
Static Address	EIGRP 邻居的 IP 地址。
Interface	ASA 在其上接收来自邻居的问候数据包的接口。

以下是 **show eigrp neighbors detail** 命令的输出示例：

```
ciscoasa# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
```

```
0   10.4.9.5                Fa0/0              11 00:04:07  768  4608  0  4    S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0              13 1w0d        1  3000  0  6    S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0              12 1w0d        1  3000  0  4    S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

表 6-5 说明了显示中所示的重要字段。

表 6-5　show ip eigrp neighbors details 字段说明

字段	说明
process	EIGRP 路由进程的自主系统编号。
H	该列列出了与指定邻居建立对等会话的顺序。该顺序由从 0 开始的有序编号指定。
Address	EIGRP 邻居的 IP 地址。
Interface	ASA 在其上接收来自邻居的问候数据包的接口。
Holdtime	ASA 在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。 如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认保持时间，则显示非默认保持时间。 如果该值达到 0，则 ASA 认为邻居不可访问。
Uptime	自 ASA 初次从邻居收到消息后经过的时间（小时：分钟：秒钟格式）。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 ASA 接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 ASA 将数据包从重新传输队列重新发送到邻居之前等待的时间量。
Q Count	ASA 等待发送的 EIGRP 数据包（更新、查询和回复）数。
Seq Num	从邻居接收的上一更新、查询或回复数据包的序列号。
Version	指定的对等设备运行的软件版本。
Retrans	数据包已重传的次数。
Retries	重传数据包的尝试次数。
Restart time	指定从邻居重启之后所经过的时间（格式：小时：分钟：秒）。

相关命令

命令	说明
clear eigrp neighbors	清除 EIGRP 邻居表。
debug eigrp neighbors	显示 EIGRP 邻居调试消息。
debug ip eigrp	显示 EIGRP 数据包调试消息。

show eigrp topology

要显示 EIGRP 拓扑表，请在特权 EXEC 模式下使用 **show eigrp topology** 命令。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

语法说明

active	（可选）仅显示 EIGRP 拓扑表中的活动条目。
all-links	（可选）显示 EIGRP 拓扑表中的所有路由，即使并非可行后续路由。
as-number	（可选）指定 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此您无需指定自主系统编号。
ip-addr	（可选）定义要显示的拓扑表 IP 地址。使用掩码指定时，将提供条目的详细说明。
mask	（可选）定义要应用于 *ip-addr* 参数的网络掩码。
pending	（可选）显示等待来自邻居的更新或等待回复邻居的 EIGRP 拓扑表中的所有条目。
summary	（可选）显示 EIGRP 拓扑表的摘要。
zero-successors	（可选）显示 EIGRP 拓扑表中可用的路由。

默认值

仅显示可行后续路由。使用 **all-links** 关键字以显示所有路由，包括并非可行后续的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

您可以使用 **clear eigrp topology** 命令删除拓扑表的动态条目。

示例

以下是 **show eigrp topology** 命令的输出示例：

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
```

```
P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

表 6-6 说明了显示中所示的重要字段。

表 6-6　show eigrp topology 字段说明

字段	说明
Codes	此拓扑表条目的状态。“ 被动 ” 和 “ 主动 ” 是指与该目的地相关的 EIGRP 状态； “ 更新 ”、“ 查询 ” 和 “ 应答 ” 是指被发送数据包的类型。
P - Passive	路由已知良好并且没有对此目标执行任何 EIGRP 计算。
A - Active	对此目标执行 EIGRP 计算。
U - Update	指示更新数据包已发送到此目标。
Q - Query	指示查询数据包已发送到此目标。
R - Reply	指示回复数据包已发送到此目标。
r - Reply status	软件发送查询后等待回复时设置的标志。
address mask	目标 IP 地址和掩码。
successors	后继路由数量。该数字对应 IP 路由表中下一跳的数量。如果 “successors” 为大写，则路由或下一跃点处于过渡状态。
FD	可行距离。可行距离是到达目的地的最佳度量，或是路由进入活动状态后所获知的最佳度量。该值用于检查可行性条件。如果路由器的报告距离（斜杠后的度量）小于可行距离，则符合可行性条件，且该路径即为可行后继路由。软件确定其有可行后续路由后，无需发送该目标的查询。
via	告知软件此目标的对等设备 IP 地址。前 *n* 个条目（其中 *n* 为后续路由数）为当前后续路由。列表上其余的条目是可行后继。
(*cost*/*adv_cost*)	第一个数字为 EIGRP 度量，表示到达目的地的开销。第二个数字是此对等设备所通告的 EIGRP 度量。
interface	从其获知信息的接口。

以下是 **show eigrp topology** 与 IP 地址配合使用的输出示例。所示输出适用于内部路由。

```
ciscoasa# show eigrp topology 10.2.1.0 255.255.255.0

EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

以下是 **show eigrp topology** 与 IP 地址配合使用的输出示例。所示输出适用于外部路由。

```
ciscoasa# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

相关命令

命令	说明
clear eigrp topology	清除从 EIGRP 拓扑表动态查找的条目。

show eigrp traffic

要显示发送和接收的 EIGRP 数据包数，请在特权 EXEC 模式下使用 **show eigrp traffic** 命令。

show eigrp [*as-number*] **traffic**

语法说明

as-number	（可选）指定您查看事件日志的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此您无需指定自主系统编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

您可以使用 **clear eigrp traffic** 命令清除 EIGRP 流量统计信息。

示例

以下是 **show eigrp traffic** 命令的输出示例：

```
ciscoasa# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

表 6-7 说明了显示中所示的重要字段。

表 6-7　show eigrp traffic 字段说明

字段	说明
process	EIGRP 路由进程的自主系统编号。
Hellos sent/received	发送和接收的问候数据包数。
Updates sent/received	发送和接收的更新数据包数。
Queries sent/received	发送和接收的查询数据包数。
Replies sent/received	发送和接收的回复数据包数。
Acks sent/received	发送和接收的确认数据包数。
Input queue high water mark/drops	接近最大接收阈值的发送数据包数和丢弃数据包数。
SIA-Queries sent/received	发送和接收的 Stuck-in-active 查询。
SIA-Replies sent/received	发送和接收的 Stuck-in-active 回复。

相关命令

命令	说明
debug eigrp packets	显示发送和接收的 EIGRP 数据包的调试信息。
debug eigrp transmit	显示发送的 EIGRP 消息的调试信息。

show environment

要显示系统组件的系统环境信息，请在特权 EXEC 模式下使用 **show environment** 命令。

show environment [**driver** | **fans** | **power-supply** | **temperature**] [**chassis** | **cpu** | **voltage**]

语法说明

chassis	（可选）限制机箱的温度显示。
cpu	（可选）限制处理器的温度显示。ASA 5580-40 显示 4 个处理器的信息。ASA 5580-20 显示 2 个处理器的信息。
driver	（可选）显示环境监控 (IPMI) 驱动程序状态。驱动程序状态可为以下各项之一： • RUNNING（运行）- 驱动程序正常运行。 • STOPPED（已停止）- 错误导致驱动程序停止。
fans	（可选）显示冷却风扇的运行状态。状态为以下各项之一： • OK（正常）- 风扇正常运行。 • Failed（故障）- 风扇出现故障并应进行更换。
power-supply	（可选）显示电源设备的运行状态。每个电源设备的状态均为以下各项之一： • OK（正常）- 电源设备正常运行。 • Failed（故障）- 电源设备出现故障并应进行更换。 • Not Present（不存在）- 指定的电源设备未安装。 电源设备冗余状态也将显示。冗余状态为以下各项之一： • OK（正常）- 设备以完整资源正常运行。 • Lost（丢失）- 设备已丢失冗余但以最低资源正常运行。任何进一步的故障都将导致系统关闭。 • N/A（不适用）- 设备未配置电源设备冗余。
temperature	（可选）显示处理器和机箱的温度和状态。温度以摄氏度为单位指定。状态为以下各项之一： • OK（正常）- 温度位于正常操作范围内。 • Critical（严重）- 温度超出正常操作范围。 操作范围分类如下： • 小于 70 度 - OK（正常） • 70-80 - Warm（热） • 80-90 - Critical（严重） • 大于 90 - Unrecoverable（不可恢复）
voltage	（可选）显示 CPU 电压通道 1-24 的值。不包括运行状态。

默认值

如果没有指定关键字，则显示所有运行信息（驱动程序除外）。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	单个	多个 情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.1(1)	引入了此命令。
8.4(2)	添加了 ASA 5585-X SSP 的输出。此外，添加了对双 SSP 安装的支持。
8.4.4(1)	ASA 5515-X、ASA 5525-X、5545-X 和 ASA 5555-X 的显示电源设备温度值在输出中已更改。
8.6(1)	添加了 ASA 5545-X 和 ASA 5555-X 中 CPU 调压器热事件的输出。添加了电源设备输入状态的输出。添加了电压传感器的输出。

使用指南

您可以显示有关 ASA 5545-X、5555-X、5580 和 5585-X 的操作环境信息。此信息包括风扇和电源设备的运行状态，以及 CPU 和机箱的温度和状态。ASA 5580-40 显示 4 个 CPU 的信息； ASA 5580-20 显示 2 个 CPU 的信息。

注　对于双 SSP 安装，只有主控机箱的传感器显示冷却风扇和电源设备的输出。

示例

以下是 **show environment** 命令的示例通用输出：

```
ciscoasa# show environment

Cooling Fans:
-----------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
```

```
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

以下是 **show environment driver** 命令的输出示例：

```
ciscoasa# show environment driver

Cooling Fans:
-----------------------------------

   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK

   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Power Supplies:
-----------------------------------

   Left Slot (PS0): Not Present
   Right Slot (PS1): Present

   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK

   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Temperature:
-----------------------------------

   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK

   Chassis:
   --------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK

Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
```

```
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

以下是 ASA 5555-X 的 **show environment** 命令的输出示例：

```
ciscoasa# show environment

Cooling Fans:
-----------------------------------

   Chassis Fans:
   -------------------------------

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 9728 RPM - OK
   Right Slot (PS1): 0 RPM - OK

Power Supplies:
-----------------------------------

    Left Slot (PS0): Present
    Right Slot (PS1): Present

    Power Input:
    -------------------------------
    Left Slot (PS0): OK
    Right Slot (PS1): Failure Detected

    Temperature:
    -------------------------------
    Left Slot (PS0): 29 C - OK
    Right Slot (PS1): N/A

   Processors:
   -------------------------------
   Processor 1: 81.0 C - OK

   Chassis:
   -------------------------------
   Ambient 1: 39.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 32.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 47.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 33 C - OK
   Right Slot (PS1): -128 C - OK
```

以下是双 SSP 安装中 ASA 5585-X 主控机箱的 **show environment** 命令的输出示例：

```
ciscoasa(config)# show environment

Cooling Fans:
-----------------------------------

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)
```

```
Power Supplies:
---------------------------------
   Power Supply Unit Redundancy: N/A

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)

Temperature:
---------------------------------

   Processors:
   -------------------------------
   Processor 1: 48.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 47.0 C - OK  (CPU2 Core Temperature)

   Chassis:
   -------------------------------
   Ambient 1: 25.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.50 C - OK  (CPU1 Back Temperature)
   Ambient 4: 27.75 C - OK  (CPU1 Front Temperature)
   Ambient 5: 38.25 C - OK  (CPU2 Back Temperature)
   Ambient 6: 34.0 C - OK  (CPU2 Front Temperature)

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

Voltage:
---------------------------------
   Channel 1:  3.310 V -  (3.3V (U142 VX1))
   Channel 2:  1.492 V -  (1.5V (U142 VX2))
   Channel 3:  1.053 V -  (1.05V (U142 VX3))
   Channel 4:  3.328 V -  (3.3V_STDBY (U142 VP1))
   Channel 5: 11.675 V -  (12V (U142 VP2))
   Channel 6:  4.921 V -  (5.0V (U142 VP3))
   Channel 7:  6.713 V -  (7.0V (U142 VP4))
   Channel 8:  9.763 V -  (IBV (U142 VH))
   Channel 9:  1.048 V -  (1.05VB (U209 VX2))
   Channel 10:  1.209 V -  (1.2V (U209 VX3))
   Channel 11:  1.109 V -  (1.1V (U209 VX4))
   Channel 12:  0.999 V -  (1.0V (U209 VX5))
   Channel 13:  3.324 V -  (3.3V STDBY (U209 VP1))
   Channel 14:  2.504 V -  (2.5V (U209 VP2))
   Channel 15:  1.799 V -  (1.8V (U209 VP3))
   Channel 16:  1.899 V -  (1.9V (U209 VP4))
   Channel 17:  9.763 V -  (IBV (U209 VH))
   Channel 18:  2.048 V -  (VTT CPU0 (U83 VX2))
   Channel 19:  2.048 V -  (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -  (VCC CPU0 (U83 VX4))
   Channel 21:  2.048 V -  (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -  (1.5VA (U83 VP1))
   Channel 23:  1.515 V -  (1.5VB (U83 VP2))
   Channel 24:  8.937 V -  (IBV (U83 VH))
```

如果 ASA 由于 CPU 调压器热事件关闭，则显示以下警告消息：

```
WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the
max thermal operating temperature.The chassis and CPU need to be inspected immediately for
ventilation issues.
```

有关详细信息，请参阅系统日志消息指南中的系统日志消息 735024。

相关命令

命令	说明
show version	显示硬件和软件版本。

show event manager

要显示关于每个配置的事件管理器小应用的信息，请在特权 EXEC 模式下使用 **show event manager** 命令。

show event manager

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下是 **show event manager** 命令的输出示例：

```
ciscoasa# show event manager

event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

相关命令

命令	说明
show running-config event manager	显示事件管理器运行配置。

第 7 章

show failover 至 show ipsec stats traffic 命令

show failover

要显示有关设备故障切换状态的信息，请在特权 EXEC 模式下使用 **show failover** 命令。

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

语法说明

group	显示指定的故障切换组的运行状态。
history	显示故障切换历史记录。故障切换历史记录显示已结束的故障切换状态更改和状态更改的原因。历史记录信息会随设备重启而被清除。
interface	显示故障切换和有状态链路信息。
num	故障切换组编号。
state	显示两个故障切换设备的故障切换状态。显示的信息包括设备的主要或辅助状态、设备的主用 / 备用状态和最新报告的故障切换原因。即使清除了故障的原因，故障原因信息也会保留在输出中。
statistics	显示故障切换命令接口的传输和接收数据包计数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	此命令已修改。输出包括其他信息。
8.2(2)	此命令已修改。输出包括防火墙和故障切换接口的 IPv6 地址。有状态故障切换统计信息输出包括 IPv6 邻居发现表 (IPv6 ND tbl) 更新的信息。

使用指南

show failover 命令显示动态故障切换信息、接口状态和有状态故障切换统计信息。

如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。由于一个接口上可配置多个 IPv6 地址，因此只显示本地链路的地址。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

只有在启用有状态故障切换时，才会出现有状态故障切换逻辑更新统计信息输出。“xerr” 和 “rerr” 值并不指示故障切换中的错误数，而是指示数据包传输或接收错误数。

注意　有状态故障切换（以及相关的有状态故障切换统计信息）输出在 ASA 5505 上不可用。

在 **show failover** 命令输出中，有状态故障切换字段包含以下值：

- 有状态对象具有以下值：
  - xmit - 指示传输的数据包数。
  - xerr - 指示传输错误数。
  - rcv - 指示接收的数据包数。
  - rerr - 指示接收错误数。
- 每行是针对特定对象的静态计数，如下所示：
  - General - 指示所有有状态对象的总和。
  - sys cmd - 指逻辑更新系统命令，例如 **login** 或 **stay alive**。
  - up time - 指示 ASA 正常工作时间的值，即主用 ASA 传递到备用 ASA 的时间。
  - RPC services - 远程过程调用连接信息。
  - TCP conn - 动态 TCP 连接信息。
  - UDP conn - 动态 UDP 连接信息。
  - ARP tbl - 动态 ARP 表信息。
  - Xlate_Timeout - 指示连接转换超时信息。
  - IPv6 ND tbl - IPv6 邻居发现表信息。
  - VPN IKE upd - IKE 连接信息。
  - VPN IPSEC upd - IPsec 连接信息。
  - VPN CTCP upd - cTCP 隧道连接信息。
  - VPN SDI upd - SDI AAA 连接信息。
  - VPN DHCP upd - 隧道化 DHCP 连接信息。
  - SIP Session - SIP 信令会话信息。
  - Route Session - 路由同步更新的 LU 统计信息。

如果不输入故障切换 IP 地址，则 **show failover** 命令显示 IP 地址为 0.0.0.0，且接口的监控仍处于“ 等待 ” 状态。您必须设置一个故障切换 IP 地址，故障切换才能工作。

表 7-1 描述故障切换的接口状态。

表 7-1　　故障切换接口状态

状态	说明
Normal	接口正在运行并正在接收来自对等设备上相应接口的问候数据包。
Normal (Waiting)	接口正在运行，但尚未收到来自对等设备上相应接口的问候数据包。验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。
Normal (Not-Monitored)	接口正在运行，但故障切换进程并未监控它。未受监控的接口发生故障时不会触发故障切换。
No Link	物理链路断开。
No Link (Waiting)	物理链路断开，且接口尚未收到来自对等设备上相应接口的问候数据包。在恢复链路后，验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。
No Link (Not-Monitored)	物理链路断开，但故障切换进程并未监控它。未受监控的接口发生故障时不会触发故障切换。

表 7-1　故障切换接口状态（续）

状态	说明
Link Down	物理链路处于工作状态，但是接口处于管理性关闭状态。
Link Down (Waiting)	物理链路处于工作状态，但是接口处于管理性关闭状态，且接口尚未收到来自对等设备上相应接口的问候数据包。在使接口处于工作状态后（使用接口配置模式下的 **no shutdown** 命令），验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。
Link Down (Not-Monitored)	物理链路处于工作状态，但是接口处于管理性关闭状态，且故障切换进程并未监控它。未受监控的接口发生故障时不会触发故障切换。
Testing	接口由于丢失来自对等设备上相应接口的问候数据包而处于测试模式。
Failed	接口测试失败，并且接口标记为发生故障。如果接口故障符合故障切换条件，则接口故障会导致故障切换到备用设备或故障切换组。

在多配置模式中，仅 **show failover** 命令在安全情景中可用；您无法输入可选关键字。

示例

以下是主用 / 备用故障切换的 **show failover** 命令的输出示例。ASA 是 ASA 5500 系列 ASA，其中每个都配备了 CSC SSM，如每个 ASA 的插槽 1 的详细信息所示。安全设备在故障切换链路 (folink) 和内部接口上使用 IPv6 地址。

```
ciscoasa# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: folink Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3/FE80::20d:29ff:fe1d:69f0): Normal
                  Interface outside (10.132.9.3): Normal
                  Interface folink (0.0.0.0/fe80::2a0:c9ff:fe03:101): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4/FE80::20d:29ff:fe2b:7ba6): Normal
                  Interface outside (10.132.9.4): Normal
                  Interface folink (0.0.0.0/fe80::2e0:b6ff:fe07:3096): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
```

```
sys cmd          1733        0           1733        0
up time          0           0           0           0
RPC services     0           0           0           0
TCP conn         6           0           0           0
UDP conn         0           0           0           0
ARP tbl          106         0           0           0
Xlate_Timeout    0           0           0           0
IPv6 ND tbl      22          0           0           0
VPN IKE upd      15          0           0           0
VPN IPSEC upd    90          0           0           0
VPN CTCP upd     0           0           0           0
VPN SDI upd      0           0           0           0
VPN DHCP upd     0           0           0           0
SIP Session     0           0           0           0
Route Session   165         0           70          6

Logical Update Queue Information
                 Cur     Max     Total
Recv Q:          0       2       1733
Xmit Q:          0       2       15225
```

以下是主用 / 主用故障切换的 **show failover** 命令的输出示例。在本示例中，仅管理员情景可将 IPv6 地址分配给接口。

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
```

```
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
       SIP Session    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

以下是 ASA 5505 上 **show failover** 命令的输出示例：

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

以下是主用 / 主用设置的 **show failover state** 命令的输出示例：

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

以下是主用 / 备用设置的 **show failover state** 命令的输出示例：

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 7-2 说明 **show failover state** 命令的输出。

表 7-2　show failover state 输出说明

字段	说明
Configuration State	显示配置同步状态。 以下是备用设备的可能配置状态： • **Config Syncing - STANDBY（配置同步 - 备用）** - 在执行同步的配置时设置。 • **Interface Config Syncing - STANDBY（接口配置同步 - 备用）** • **Sync Done - STANDBY（完成同步 - 备用）** - 当备用设备完成从主用设备的配置同步时设置。 以下是主用设备的可能配置状态： • **Config Syncing（配置同步）** - 在主用设备执行与备用设备的配置同步时在主用设备上设置。 • **Interface Config Syncing（接口配置同步）** • **Sync Done（完成同步）** - 在主用设备已成功完成到备用设备的配置同步时设置。 • **Ready for Config Sync（准备好进行配置同步）** - 在备用设备发出准备好接收配置同步的信号时在主用设备上设置。

表 7-2　show failover state 输出说明（续）

字段	说明
Communication State	显示 MAC 地址同步状态。 • **Mac set（已设置 Mac）**- MAC 地址已完成从对等设备至此设备的同步。 • **Updated Mac（已更新 Mac）**- 在 MAC 地址已更新并需要同步到另一设备时使用。在设备正在更新从对等设备同步的本地 MAC 地址的过渡期间也使用此状态。
Date/Time	显示故障的日期和时间戳。
Last Failure Reason	显示最后报告故障的原因。此信息不会清除，即使故障情况已清除。只有发生故障切换时，此信息才会变更。 以下是可能的故障原因： • **Ifc Failure（Ifc 故障）**- 发生故障的接口数量符合故障切换条件并导致故障切换。 • **Comm Failure（通信故障）**- 故障切换链路失败或对等设备关闭。 • **Backplane Failure（底板故障）**
状态	显示设备的主要 / 辅助和主用 / 备用状态。
This host/Other host	This host（此主机）指示被执行命令的设备的信息。Other host（其他主机）指示故障切换配对中的另一个设备的信息。

以下是 **show failover history** 命令的输出示例：

```
ciscoasa(config)# show failover history
==========================================================================
Group     From State                To State                  Reason
==========================================================================
. . .
03:42:29 UTC Apr 17 2009
    0     Sync Config               Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    1     Standby Ready             Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    2     Standby Ready             Failed
Backplane failed

3:44:39 UTC Apr 17 2009
    0     Failed                    Negotiation
Backplane operational

3:44:40 UTC Apr 17 2009
    1     Failed                    Negotiation
Backplane operational

3:44:40 UTC Apr 17 2009
    2     Failed                    Negotiation
Backplane operational

==========================================================================
```

每个条目提供状态更改的时间和日期、初始状态、结果状态和状态更改的原因。最新的条目位于显示画面的底部。较旧的条目显示在顶部。最多可以显示 60 个条目。一旦到达条目数上限，随着新条目添加至底部，最旧的条目就会从输出的顶部移除。

表 7-3 显示故障切换状态。有稳定和临时两种状态类型。稳定状态是发生如故障之类的情况而导致状态更改之前设备可保持的状态。临时状态是设备达到稳定状态时所经过的状态。

表 7-3　　故障切换状态

状态	说明
Disabled	禁用故障切换。这是稳定状态。
Failed	设备处于故障状态。这是稳定状态。
Negotiation	设备建立与对等设备的连接，并与其协商确定软件版本兼容性和主用 / 备用角色。根据协商的角色，设备将经历备用设备状态或主用设备状态，或进入故障状态。这是临时状态。
Not Detected	ASA 无法检测到对等设备的存在。若 ASA 启动并启用故障切换而对等设备不存在或关闭，会发生这种情况。
备用设备状态	
Cold Standby	设备等待对等设备进入主用状态。当对等设备进入主用状态时，此设备进入备用配置状态。这是临时状态。
Sync Config	设备请求来自对等设备的运行配置。如果配置同步时发生错误，设备会回到初始化状态。这是临时状态。
Sync File System	设备与对等设备同步文件系统。这是临时状态。
Bulk Sync	设备接收对等设备的状态信息。只有启用有状态故障切换时，才会出现此状态。这是临时状态。
Standby Ready	设备已准备好在主用设备发生故障时接管。这是稳定状态。
主用设备状态	
Just Active	设备成为主用设备时进入的第一个状态。在此状态时会向对等设备发送消息，向对等设备告知该设备成为主用设备并为接口设置 IP 地址和 MAC 地址。这是临时状态。
Active Drain	丢弃来自对等设备的消息队列。这是临时状态。
Active Applying Config	设备正在应用系统配置。这是临时状态。
Active Config Applied	设备已完成应用系统配置。这是临时状态。
Active	设备处于主用状态并在处理流量。这是稳定状态。

每个状态更改后面都附带状态更改原因。在设备从临时状态过渡到稳定状态时，原因通常保持相同。以下是可能的状态更改原因：

- 没有错误
- 通过 CI config 命令设置
- 故障切换状态检查
- 故障切换接口恢复正常
- 未收到对方的问候消息
- 另一设备具有不同的软件版本
- 另一设备操作模式不同

- 另一设备许可证不同
- 另一设备机箱配置不同
- 另一设备卡配置不同
- 另一设备要本设备成为主用设备
- 另一设备要本设备成为备用设备
- 另一设备报告本设备已发生故障
- 另一设备报告该设备已发生故障
- 配置不匹配
- 检测到主用对等设备
- 未找到主用设备
- 已完成配置同步
- 已从通信故障恢复
- 另一设备具有不同的 VLAN 组配置
- 无法验证 VLAN 配置
- 配置同步未完成
- 配置同步失败
- 接口检查
- 我的通信失败
- 针对故障切换消息没有收到 ACK
- 另一设备在同步后进入卡机状态
- 从对等设备中检测不到电源
- 没有故障切换电缆
- 高可用性状态进度失败
- 检测服务卡故障
- 另一设备中的服务卡发生故障
- 本设备与对等设备的服务卡都正常
- LAN 接口变成未配置
- 对等设备刚刚重新加载
- 从串行电缆切换到基于 LAN 的故障切换
- 无法验证配置同步的状态
- 自动更新请求
- 未知原因

以下是 **show failover interface** 命令的输出示例。设备已对故障切换接口配置 IPv6 地址。

```
ciscoasa(config)# sh fail int
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

相关命令

命令	说明
show running-config failover	在当前配置中显示 **failover** 命令。

show failover exec

要对指定设备显示 **failover exec** 命令模式，请在特权 EXEC 模式下使用 **show failover exec** 命令。

show failover exec {**active** | **standby** | **mate**}

语法说明

active	为主用设备显示 **failover exec** 命令模式。
mate	为对等设备显示 **failover exec** 命令模式。
standby	为备用设备显示 **failover exec** 命令模式。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

failover exec 命令会创建与指定设备的会话。默认情况下，该会话在全局配置模式下。您可以通过使用 **failover exec** 命令发送适当命令（例如 **interface** 命令），以更改该会话的命令模式。更改指定设备的 **failover exec** 命令模式不会更改用于访问设备的会话的命令模式。更改设备当前会话的命令模式不会影响 **failover exec** 命令使用的命令模式。

show failover exec 命令显示在指定设备上执行使用 **failover exec** 命令发送的命令的命令模式。

示例

以下是 **show failover exec** 命令的输出示例。此示例表明，在其中输入 **failover exec** 命令的设备的命令模式不必与执行这些命令的 **failover exec** 命令模式相同。

在本示例中，登录到备用设备的管理员将名称添加到主用设备上的接口。在此示例中第二次输入 **show failover exec mate** 命令，会在接口配置模式下显示对等设备。使用 **failover exec** 命令发送到设备的命令在该模式下执行。

```
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
ciscoasa(config)# failover exec mate interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate
```

```
Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
ciscoasa(config)# failover exec mate nameif test
```

相关命令

命令	说明
failover exec	在故障切换对中的指定设备上执行提供的命令。

show file

要显示有关文件系统的信息，请在特权 EXEC 模式下使用 **show file** 命令。

show file descriptors | system | information *filename*

语法说明

descriptors	显示所有打开文件描述符。
filename	指定文件名。
information	显示有关特定文件的信息，包括合作伙伴应用包文件。
system	显示有关磁盘文件系统的大小、可用字节数、介质类型、标志和前缀信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	添加了查看有关合作伙伴应用包文件的信息这一功能。

示例

以下是 **show file descriptors** 命令的输出示例。

```
ciscoasa# show file descriptors
No open file descriptors
ciscoasa# show file system
File Systems:
   Size(b)     Free(b)     Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

以下是 **show file info** 命令的输出示例：

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

相关命令

命令	说明
dir	系统随即会显示目录的内容。
pwd	系统随即会显示当前工作目录。

show firewall

要显示当前防火墙模式（路由或透明），请在特权 EXEC 模式下使用 **show firewall** 命令。

show firewall

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show firewall** 命令的输出示例：

```
ciscoasa# show firewall
Firewall mode: Router
```

相关命令

命令	说明
firewall transparent	设置防火墙模式。
show mode	显示当前情景模式（单模式或多模式）。

show firewall module version

要查看 ASA 服务模块的软件版本编号，请在特权 EXEC 模式下输入 **show firewall module version** 命令。

show firewall switch {**1** | **2**} **module** [*module_number*] **version**

语法说明

module_number	（可选）指定模块编号。
switch {**1** | **2**}	仅适用于 VSS 用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show firewall module version** 命令的输出示例：

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

相关命令

命令	说明
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	创建一组 VLAN。
show module	显示所有已安装的模块。

show flash

要显示内部闪存的内容，请在特权 EXEC 模式下使用 **show flash:** 命令。

show flash: all | controller | filesys

注意　在 ASA 中，**flash** 关键字的别名是 **disk0**。

语法说明

all	显示所有闪存信息。
controller	显示文件系统控制器信息。
filesys	显示文件系统信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show flash:** 命令的输出示例：

```
ciscoasa# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 6:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
```

```
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

相关命令

命令	说明
dir	系统随即会显示目录的内容。
show disk0:	显示内部闪存的内容。
show disk1:	显示外部闪存卡的内容。

show flow-export counters

要显示与 NetFlow 数据相关联的运行时计数器，请在特权 EXEC 模式下使用 **show flow-export counters** 命令。

show flow-export counters

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.1(1)	引入了此命令。
9.0(1)	新增了针对源端口分配故障的错误计数器。

使用指南

运行时间计数器包含统计信息和错误数据。

示例

以下是 **show flow-export counters** 命令的输出示例，显示与 NetFlow 数据相关联的运行时计数器：

```
ciscoasa# show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                      1000
 Errors:
  block allocation failure             0
  invalid interface                    0
  template send failure                0
  no route to collector                0
  source port allocation               0
```

相关命令

命令	说明
clear flow-export counters	将 NetFlow 中的所有运行时计数器重置为零。
flow-export destination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。

show fragment

要显示 IP 分段重组模块的操作数据，请在特权 EXEC 模式下输入 **show fragment** 命令。

show fragment [*interface*]

语法说明

interface	（可选）指定 ASA 接口。

默认值

如果未指定*接口*，此命令将应用于所有接口。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC 模式	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	命令分为两个命令，即 **show fragment** 和 **show running-config fragment**，以将配置数据与操作数据分开。

示例

以下示例展示如何显示 IP 分段重组模块的操作数据：

```
ciscoasa# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

相关命令

命令	说明
clear configure fragment	清除 IP 分段重组配置并重置默认值。
clear fragment	清除 IP 分段重组模块的运行数据。
fragment	提供数据包分段的其他管理并提高与 NFS 的兼容性。
show running-config fragment	显示 IP 分段重组配置。

show gc

要显示垃圾回收进程的统计信息，请在特权 EXEC 模式下使用 **show gc** 命令。

show gc

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show gc** 命令的输出示例：

```
ciscoasa# show gc

Garbage collection process stats:
Total tcp conn delete response             :           0
Total udp conn delete response             :           0
Total number of zombie cleaned             :           0
Total number of embryonic conn cleaned     :           0
Total error response                       :           0
Total queries generated                    :           0
Total queries with conn present response   :           0
Total number of sweeps                     :         946
Total number of invalid vcid               :           0
Total number of zombie vcid                :           0
```

相关命令

命令	说明
clear gc	删除垃圾回收进程统计信息。

show h225

要显示通过 ASA 建立的 H.225 会话的信息，请在特权 EXEC 模式下使用 **show h225** 命令。

show h225

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show h225 命令显示有关通过 ASA 建立的 H.225 会话的信息。此命令与 **debug h323 h225 event**、**debug h323 h245 event** 和 **show local-host** 命令一起使用，用于排查 H.323 检查引擎问题。

在使用 **show h225**、**show h245** 或 **show h323 ras** 命令之前，我们建议您配置 **pager** 命令。如果有很多会话记录且未配置 **pager** 命令，则 **show** 输出可能需要一段时间才能输出全部内容。如果连接数量极大，请基于默认超时值或您设置的值检查会话是否超时。如果未超时，则需要调查问题。

示例

以下是 **show h225** 命令的输出示例：

```
ciscoasa# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
|Local:|10.130.56.3/1040|Foreign: 172.30.254.203/1720
|1.CRV 9861
|Local:|10.130.56.3/1040|Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
|Local:|10.130.56.4/1050|Foreign: 172.30.254.205/1720
```

此输出指示目前在本地终端 10.130.56.3 和外部主机 172.30.254.203 之间有 1 个通过 ASA 的活动 H.323 呼叫，并且在这些特定终端之间有 1 个并发呼叫，其中该呼叫的 CRV（呼叫参考值）是 9861。

对于本地终端 10.130.56.4 和外部主机 172.30.254.205，有 0 个并发呼叫。这意味着即使 H.225 会话仍然存在，终端之间也没有活动呼叫。如果在执行 **show h225** 命令时呼叫已结束但 H.225 会话尚未删除，就可能会发生这种情况。它也可能意味着两个终端之间还有开启的 TCP 连接，因为它们将 “maintainConnection” 设置为 TRUE，所以在它们将其重新设置为 FALSE 或在会话根据您配置中的 H.225 超时值超时之前，会话保持开启。

相关命令

命令	说明
debug h323	启用 H.323 调试信息的显示。
inspect h323	启用 H.323 应用检查。
show h245	显示关于终端使用缓慢启动在 ASA 范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在 ASA 范围内建立的 H.323 RAS 会话的信息。
timeout h225 | h323	配置关闭 H.225 信令连接或 H.323 控制连接前的空闲时间。

show h245

要显示终端使用缓慢启动通过 ASA 建立的 H.245 会话的信息，请在特权 EXEC 模式下使用 **show h245** 命令。

show h245

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show h245 命令显示终端使用缓慢启动通过 ASA 建立的 H.245 会话的信息。（缓慢启动指呼叫的两个终端打开 H.245 的另一个 TCP 控制通道。快速启动指 H.245 消息作为 H.225 控制通道上的 H.225 消息的一部分交换。）此命令与 **debug h323 h245 event**、**debug h323 h225 event** 和 **show local-host** 命令一起使用，用于排查 H.323 检查引擎问题。

示例

以下是 **show h245** 命令的输出示例：

```
ciscoasa# show h245
Total: 1
| LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
| MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
| Local | 10.130.56.3 RTP 49608 RTCP 49609
| MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
| Local | 10.130.56.3 RTP 49606 RTCP 49607
```

目前有一个跨 ASA 的 H.245 控制会话处于活动状态。本地终端是 10.130.56.3，我们期待来自此终端的下一个数据包有 TPKT 报头，因为 TPKT 值为 0。（TKTP 报头是位于每个 H.225/H.245 消息前面的 4 字节的报头。它提供消息的长度，其中包括 4 字节的报头。）外部主机终端是 172.30.254.203，我们期待来自此终端的下一个数据包有 TPKT 报头，因为 TPKT 值为 0。

在这些终端之间协商的媒体具有 LCN（逻辑信道号）258，它具有外部 RTP IP 地址 / 端口对 172.30.254.203/49608、包含本地 RTP IP 地址 / 端口对 10.130.56.3/49608 的 RTCP IP 地址 / 端口 172.30.254.203/49609 和 RTCP 端口 49609。

第二个 LCN 259 具有外部 RTP IP 地址 / 端口对 172.30.254.203/49606、包含本地 RTP IP 地址 / 端口对 10.130.56.3/49606 的 RTCP IP 地址 / 端口对 172.30.254.203/49607 和 RTCP 端口 49607。

相关命令

命令	说明
debug h323	启用 H.323 调试信息的显示。
inspect h323	启用 H.323 应用检查。
show h245	显示关于终端使用缓慢启动在 ASA 范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在 ASA 范围内建立的 H.323 RAS 会话的信息。
timeout h225 | h323	配置 H.225 信号连接或 H.323 控制连接在关闭之前经历的空闲时间。

show h323

要显示有关 H.323 连接的信息，请在特权 EXEC 模式下使用 **show h323** 命令。

show h323 {ras | gup}

语法说明

ras	显示在网守与其 H.323 终端之间跨 ASA 建立的 H323 RAS 会话。
gup	显示有关 H323 网关更新的协议连接的信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show h323 ras 命令显示在网守与其 H.323 终端之间跨 ASA 建立的 H.323 RAS 会话的信息。此命令与 **debug h323 ras event** 和 **show local-host** 命令一起使用，用于排查 H.323 RAS 检查引擎问题。

示例

以下是 **show h323 ras** 命令的输出示例：

```
ciscoasa# show h323 ras
Total: 1
|GK|Caller
|172.30.254.214 10.130.56.14
ciscoasa#
```

此输出显示在网守 172.30.254.214 与其客户端 10.130.56.14 之间存在一个有效注册。

相关命令

命令	说明
debug h323	启用 H.323 调试信息的显示。
inspect h323	启用 H.323 应用检查。
show h245	显示关于终端使用缓慢启动在 ASA 范围内建立的 H.245 会话的信息。
timeout h225 | h323	配置关闭 H.225 信令连接或 H.323 控制连接前的空闲时间。

show history

要显示先前输入的命令，请在用户 EXEC 模式下使用 **show history** 命令。

show history

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show history 命令用于显示先前输入的命令。您可以使用向上和向下箭头分别检查各个命令、输入 **^p** 显示先前输入的行或输入 **^n** 显示下一行。

示例

以下示例展示在用户 EXEC 模式下 **show history** 命令的输出示例：

```
ciscoasa> show history
    show history
    help
    show history
```

以下示例展示在特权 EXEC 模式下 **show history** 命令的输出示例：

```
ciscoasa# show history
    show history
    help
    show history
    enable
    show history
```

以下示例展示在全局配置模式下 **show history** 命令的输出示例：

```
ciscoasa(config)# show history
    show history
    help
    show history
    enable
```

```
show history
config t
show history
```

相关命令

命令	说明
help	显示指定的命令的帮助信息。

show icmp

要显示 ICMP 配置，请在特权 EXEC 模式下使用 **show icmp** 命令。

show icmp

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	此命令以前存在。

使用指南

show icmp 命令显示 ICMP 配置。

示例

以下示例展示 ICMP 配置：

```
ciscoasa# show icmp
```

相关命令

clear configure icmp	清除 ICMP 配置。
debug icmp	启用 ICMP 的调试信息的显示。
icmp	为在 ASA 接口上终止的 ICMP 流量配置访问规则。
inspect icmp	启用或禁用 ICMP 检查引擎。
timeout icmp	配置 ICMP 的空闲超时。

show idb

要显示有关接口描述符块的状态信息，请在特权 EXEC 模式下使用 **show idb** 命令。

show idb

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

IDB 是代表接口资源的内部数据结构。请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show idb** 命令的输出示例：

```
ciscoasa# show idb
Maximum number of Software IDBs 280.In use 23.

                    HWIDBs     SWIDBs
              Active 6          21
            Inactive 1          2
          Total IDBs 7          23
 Size each (bytes) 116          212
        Total bytes 812         4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
```

```
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

表 7-4 显示每个字段的说明。

表 7-4　show idb stats 字段

字段	说明
HWIDBs	显示所有 HWIDB 的统计信息。为系统中的每个硬件端口创建 HWIDB。
SWIDBs	显示所有 SWIDB 的统计信息。为系统中的每个主接口和子接口以及分配给情景的每个接口创建 SWIDB。 其他一些内部软件模块还会创建 IDB。
HWIDB#	指定硬件接口条目。IDB 序列号、地址和接口名称显示在每行中。
SWIDB#	指定软件接口条目。IDB 序列号、地址、对应的 vPif ID 和接口名称显示在每行中。
PEER IDB#	指定分配给情景的接口。IDB 序列号、地址、对应的 vPif ID、情景 ID 和接口名称显示在每行中。

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。

show igmp groups

要显示接收器直接连接至 ASA 的组播组和通过 IGMP 得知的组播组，请在特权 EXEC 模式下使用 **show igmp groups** 命令。

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

语法说明

detail	（可选）提供源的详细说明。
group	（可选）IGMP 组的地址。包括此可选参数可限制只显示指定的组。
if_name	（可选）显示指定接口的组信息。
reserved	（可选）显示有关预留组的信息。
summary	（可选）显示组加入汇总信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果省略所有可选参数和关键字，则 **show igmp groups** 命令会按组地址、接口类型和接口号显示所有直接连接的组播组。

示例

以下是 **show igmp groups** 命令的输出示例：

```
ciscoasa# show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

相关命令

命令	说明
show igmp interface	显示接口的组播信息。

show igmp interface

要显示接口的组播信息，请在特权 EXEC 模式下使用 **show igmp interface** 命令。

show igmp interface [*if_name*]

语法说明

if_name	（可选）显示选定接口的 IGMP 组信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	此命令已修改。删除了 **detail** 关键字。

使用指南

如果省略可选 *if_name* 参数，则 **show igmp interface** 命令会显示有关所有接口的信息。

示例

以下是 **show igmp interface** 命令的输出示例：

```
ciscoasa# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

相关命令

命令	说明
show igmp groups	显示其接收器直接连接到 ASA 并且通过 IGMP 获知的组播组。

show igmp traffic

要显示 IGMP 流量统计信息，请在特权 EXEC 模式下使用 **show igmp traffic** 命令。

show igmp traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show igmp traffic** 命令的输出示例：

```
ciscoasa# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

相关命令

命令	说明
clear igmp counters	清除所有 IGMP 统计信息计数器。
clear igmp traffic	清除 IGMP 流量计数器。

show import webvpn

要列出闪存中用于定制和本地化 ASA 或 AnyConnect 安全移动客户端的文件、定制对象、转换表或插件，请在特权 EXEC 模式下使用 **show import webvpn** 命令。

show import webvpn {**AnyConnect-customization** | **customization** | **mst-translation** | **plug-in** | **translation-table** | **url-list** | **webcontent**}[**detailed** | **xml-output**]

语法说明

AnyConnect-customization	显示 ASA 闪存中用于定制 AnyConnect 客户端 GUI 的资源文件、可执行文件和 MS 转换。
customization	显示 ASA 闪存中用于定制无客户端 VPN 门户的 XML 定制对象（以 base64 解码的文件名）。
mst-translation	显示 ASA 闪存中用于转换 AnyConnect 客户端安装程序的 MS 转换。
plug-in	显示 ASA 闪存中的插件模块（基于 Java 的第三方客户端应用，包括 SSH、VNC 和 RDP）。
translation-table	显示 ASA 闪存中转换无客户端门户、安全桌面和插件所显示的用户消息语言的转换表。
url-list	显示 ASA 闪存中无客户端门户使用的 URL 列表（以 base64 解码的文件名）。
webcontent	显示 ASA 闪存中无客户端门户、无客户端应用和插件对最终用户可见的在线帮助内容。
detailed	显示文件在闪存中的路径和哈希。
xml-output	显示 XML 文件。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC 模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(1)	添加了 **AnyConnect-customization** 关键字。

使用指南

使用 **show import webvpn** 命令标识可供无客户端 SSL VPN 用户使用的定制数据和基于 Java 的客户端应用。显示的列表逐项列出 ASA 上的闪存中所有请求的数据类型。

示例

以下说明通过各种 **show import webvpn** 命令显示的 WebVPN 数据：

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#

ciscoasa#show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization
Template
DfltCustomization
ciscoasa#

ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                                customization
  ua                                                customization
ciscoasa#

ciscoasa# show import webvpn url-list
Template
No bookmarks are currently defined
ciscoasa#

ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

相关命令

命令	说明
revert webvpn all	删除目前在 ASA 上的所有 WebVPN 数据和插件。

show interface

要查看接口统计信息，请在特权 EXEC 模式下使用 **show interface** 命令。

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [**stats** | **detail**]

语法说明

detail	（可选）显示接口详细信息，包括添加接口的顺序、配置状态、真实状态和非对称路由统计信息（如果已通过 **asr-group** 命令启用）。如果显示所有接口，并且在 ASA 5500 系列自适应安全设备上安装了 SSM，则会显示有关其内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
interface_name	（可选）识别通过 **nameif** 命令设置的接口名称。
mapped_name	（可选）在多情景模式下，如果使用 **allocate-interface** 命令分配了映射的名称，则标识该名称。
physical_interface	（可选）标识接口 ID，例如 **gigabitethernet 0/1**。请参阅 **interface** 命令可接受的值。
redundant*number*	（可选）标识冗余接口 ID，例如 **redundant1**。
stats	（默认）显示接口信息和统计信息。此关键字是默认值，而且是可选的。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
vlan *number*	（可选）为具有内置交换机的型号（如 ASA 5505 自适应安全设备）指定 VLAN 接口。

默认值

如果您不标识任何选项，则此命令显示所有接口的基本统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	修改了此命令以包括新接口编号方案，并添加了 **stats** 关键字（为了清楚可见）和 **detail** 关键字。
7.0(4)	此命令添加了对 4GE SSM 接口的支持。
7.2(1)	此命令添加了对交换机接口的支持。
8.0(2)	此命令添加了对冗余接口的支持。此外，为子接口添加了延迟。添加了两个新计数器：输入重置丢弃和输出重置丢弃。

版本	修改
8.2(1)	将无缓冲区号更改为显示块分配的失败数。
8.6(1)	此命令添加了对 ASA 5512-X 到 ASA 5555-X 共享管理接口和软件模块的控制平面接口的支持。使用 **show interface detail** 命令可将管理接口显示为 Internal-Data0/1 ；将控制平面接口显示为 Internal-Control0/0。

使用指南

如果在各情景之间共享接口，并且您在情景内输入此命令，则 ASA 仅显示当前情景中的统计信息。当您在系统执行空间中对物理接口输入此命令时，ASA 显示所有情景的合并统计信息。

为子接口显示的统计信息数量是为物理接口显示的统计信息数量的子集。

不能在系统执行空间中使用接口名称，因为 **nameif** 命令只能用于情景中。同样，如果使用 **allocate-interface** 命令将接口 ID 映射到某个映射名称，则只能在情景中使用该映射名称。如果您在 **allocate-interface** 命令中设置 **visible** 关键字，则 ASA 在 **show interface** 命令输出中显示接口 ID。

注意　硬件中传输或接收的字节数计数和流量统计信息计数不同。

在硬件计数中，数量直接从硬件检索，并反映第 2 层数据包大小。而在流量统计信息中，它反映第 3 层数据包大小。

计数差异因接口卡硬件的具体设计而有所不同。

例如，对于快速以太网卡，因为它包括以太网标头，所以第 2 层计数比流量计数大 14 字节。对于千兆以太网卡，因为它包括以太网标头和 CRC，所以第 2 层计数比流量计数大 18 字节。

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show interface** 命令的输出示例：

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
```

```
     5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
```

```
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

表 7-5 显示每个字段的说明。

表 7-5　show interface 字段

字段	说明
Interface *ID*	接口 ID。在情景中，ASA 显示映射名称（如果已配置），除非您设置 **allocate-interface** 命令 **visible** 关键字。
“*interface_name*”	使用 **nameif** 命令设置的接口名称。在系统执行空间中，此字段为空白，因为您无法在系统中设置名称。如果不配置名称，则在硬件行之后会出现以下消息： `Available but not configured via nameif`
is *state*	管理状态，如下所示： • up - 接口没有关闭。 • administratively down - 使用 **shutdown** 命令关闭接口。
Line protocol is *state*	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。
VLAN identifier	对于子接口，是 VLAN ID。
Hardware	接口类型、最大带宽、延迟、双工和速度。在链路断开时，双工和速度显示配置的值。当链路连通时，这些字段显示配置的值，并在括号中包含实际设置。以下列表说明常见的硬件类型： • i82542 - PIX 平台上使用的 Intel PCI 光纤千兆位卡 • i82543 - PIX 平台上使用的 Intel PCI-X 光纤千兆位卡 • i82546GB - ASA 平台上使用的 Intel PCI-X 铜缆千兆位 • i82547GI - ASA 平台上使用的 Intel CSA 铜缆千兆位 • i82557 - ASA 平台上使用的 Intel PCI 铜缆快速以太网 • i82559 - PIX 平台上使用的 Intel PCI 铜缆快速以太网 • VCS7380 - SSM-4GE 中使用的 Vitesse 四端口千兆交换机
Media-type	（仅适用于 4GE SSM 接口）显示接口是设置为 RJ-45 还是 SFP。

message area	在某些情况下可能显示消息。请参阅以下示例：
	• 在系统执行空间中，您可能看到以下消息：
	`Available for allocation to a context`
	• 如果不配置名称，您会看到以下消息：
	`Available but not configured via nameif`
	• 如果接口是冗余接口的成员，您会看到以下消息：
	`Active member of Redundant5`

MAC address	接口 MAC 地址。
MTU	此接口上允许的最大数据包大小（以字节表示）。如果没有设置接口名称，此字段显示 “MTU not set”（未设置 MTU）。
IP address	使用 **ip address** 命令设置或从 DHCP 服务器接收的接口 IP 地址。在系统执行空间中，此字段显示 “IP address unassigned”（未分配 IP 地址），因为您无法在系统上设置 IP 地址。

表 7-5　show interface 字段（续）

字段	说明
Subnet mask	IP 地址的子网掩码。
Packets input	此接口上接收的数据包数。
Bytes	此接口上接收的字节数。
No buffer	块分配的失败数。
Received:	
Broadcasts	接收的广播数。
Input errors	输入错误总数，包括如下所示的类型。其他与输入有关的错误也可能导致输入错误计数增加，并且一些数据报可能有多个错误；因此，这个总数可能超过以下类型列出的错误数。
Runts	由于小于最小数据包大小（64 字节）而丢弃的数据包数。超短帧通常是由冲突引起的。也可能是由接线不良和电子干扰引起的。
Giants	由于超出最大数据包大小而丢弃的数据包数。例如，大于 1518 字节的所有以太网数据包均被视为超长帧。
CRC	循环冗余检查错误数。当站发送帧时，会将 CRC 附加到帧尾。此 CRC 是使用算法基于帧中的数据生成的。如果在源和目的地之间更改了帧，ASA 会注意到 CRC 不匹配。CRC 数量过大通常是冲突或站传输错误数据引起的。
Frame	帧错误数。错误的帧包含长度不正确或帧校验和错误的数据包。此错误通常是冲突或以太网设备故障引起的。
Overrun	ASA 因输入速度超出 ASA 处理数据的能力而无法将接收的数据传递至硬件缓冲区的次数。
Ignored	不使用此字段。值始终为 0。
Abort	不使用此字段。值始终为 0。
L2 decode drops	因未配置名称（**nameif** 命令）或接收具有无效 VLAN ID 的帧而丢弃的数据包。在冗余接口配置中的备用接口上，此计数器的数值可能因该接口没有配置名称（**nameif** 命令）而增加。
Packets output	在此接口上发送的数据包数。
Bytes	在此接口上发送的字节数。
Underruns	发射器运行速度比 ASA 处理速度更快的次数。
Output Errors	因超过已配置的最大冲突数而未传输的帧数。在网络流量巨大时，此计数器的数值只会增加。
Collisions	由于以太网冲突（单一和多个冲突）而重新传输的消息数。这通常发生在过度扩展的 LAN（以太网或收发器电缆太长、站之间超过两个中继器或层叠的多端口收发器太多）上。输出数据包仅对发生冲突的数据包计数一次。
Interface resets	接口已重置的次数。如果接口在三秒内无法传输，ASA 会重置接口以重启传输。在此时间间隔内，保持连接状态。接口环回或关闭时，也会出现接口重置。
Babbles	未使用。（“babble” 意味着发射器在接口上的时间大于传输最大帧所花费的时间。）

表 7-5　show interface 字段（续）

字段	说明
Late collisions	因冲突发生在正常冲突时间范围之外而未传输的帧数。延迟冲突是在传输数据包中延迟检测到的冲突。通常，这些不应该发生。当两台以太网主机同时尝试通信时，它们应在数据包的早期阶段发生冲突且双方都退出，或者第二台主机应看到第一台正在通信和等待。 如果遇到延迟冲突，设备将迅速行动并尝试在以太网上发送数据包，而 ASA 已部分完成发送数据包。ASA 不重新发送数据包，因为它可能已释放保留数据包第一部分的缓冲区。这不是真正的问题，因为网络协议设计为通过重新发送数据包来解决冲突。但是，延迟冲突指示您的网络中存在问题。常见问题是运行着大量重复的网络和以太网络，超出了指定范围。
Deferred	在传输之前由于链路上的活动而延迟的帧数。
input reset drops	当发生重置时，计算 RX 环中丢弃的数据包数。
output reset drops	计算当发生重置时 TX 环中丢弃的数据包数。
Rate limit drops	（仅适用于 4GE SSM 接口）将接口配置为非千兆速度而尝试传输超过 10 Mbps 或 100 Mbps（具体取决于配置）时丢弃的数据包数。
Lost carrier	在传输期间载波信号丢失的次数。
No carrier	未使用。
Input queue (curr/max packets):	输入队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。对千兆以太网接口不可用。
Output queue (curr/max packets):	输出队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。
input queue (blocks free curr/low)	curr/low（当前 / 低）条目指示接口的接收（输入）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
output queue (blocks free curr/low)	curr/low（当前 / 低）条目指示接口的接收传输（输出）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
Traffic Statistics:	接收、传输或丢弃的数据包数。
Packets input	接收的数据包数和字节数。
Packets output	传输的数据包数和字节数。
Packets dropped	丢弃的数据包数。通常，当加速安全路径 (ASP) 上丢弃数据包（例如，如果数据包由于访问列表拒绝而被丢弃）时，此计数器数值会增加。 有关接口上潜在丢弃的原因，请参阅 **show asp drop** 命令。
1 minute input rate	在过去一分钟内接收的数据包数（包 / 秒和字节 / 秒）。
1 minute output rate	在过去一分钟内传输的数据包数（包 / 秒和字节 / 秒）。

表 7-5　show interface 字段（续）

字段	说明
1 minute drop rate	在过去一分钟内丢弃的数据包数（包 / 秒）。
5 minute input rate	在过去 5 分钟内接收的数据包数（包 / 秒和字节 / 秒）。
5 minute output rate	在过去 5 分钟内传输的数据包数（包 / 秒和字节 / 秒）。
5 minute drop rate	在过去 5 分钟内丢弃的数据包数（包 / 秒）。
Redundancy Information:	对冗余接口，显示成员的物理接口。主用接口在接口 ID 后有 “(Active)”。 如果您尚未指定成员，您会看到以下输出： `Members unassigned`
Last switchover	对冗余接口，显示上次主用接口故障切换到备用接口的时间。

以下是 ASA 5505 上 **show interface** 命令的输出示例（包括交换机端口）：

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

表 7-7 显示针对交换机接口（例如 ASA 5505 自适应安全设备的交换机接口）的 **show interface** 命令的各个字段说明。请参阅表 7-6，了解有关 **show interface** 命令同时显示的字段。

表 7-6　对交换机接口执行 show interface 命令显示的字段

字段	说明
switch ingress policy drops	当端口配置不正确时，通常发生此丢弃。若默认或用户配置的交换机端口设置导致无法在交换机端口中成功转发数据包，则此丢弃会增加。以下配置是此丢弃的可能原因： • VLAN 接口上未配置 **nameif** 命令。 **注**　对于同一 VLAN 中的接口，即使未配置 **nameif** 命令，VLAN 中的交换也会成功，且不会增加此计数器数值。 • VLAN 关闭。 • 接入端口收到带有 802.1Q 标记的数据包。 • 中继端口收到不允许的标记或未标记的数据包。 • ASA 连接到具有以太网 Keepalive 的另一个思科设备。例如，思科 IOS 软件使用以太网环回数据包来确保接口正常运行。此数据包不会被其他任何设备接收；能够发送该数据包即表明正常运行。这些类型的数据包会在交换机端口上丢弃，并且计数器数值会增加。
switch egress policy drops	当前未使用。

以下是 **show interface detail** 命令的输出示例。以下示例展示所有接口的详细接口统计信息，包括内部接口（如果针对您的平台存在）和非对称路由统计信息（如果已通过 **asr-group** 命令启用）：

```
ciscoasa# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
```

```
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 7-7 展示 **show interface detail** 命令的每个字段的说明。请参阅表 7-6，了解有关 **show interface** 命令同时显示的字段。

表 7-7　show interface detail 字段

字段	说明
Demux drops	（仅在内部数据接口上）因 ASA 无法多路复用来自 SSM 接口的数据包而丢弃的数据包数。SSM 接口与背板上的本机接口通信，并在背板上多路复用来自所有 SSM 接口的数据包。
Control Point Interface States:	
Interface number	用于调试的编号，指示此接口创建的顺序，从 0 开始。
Interface config status	管理状态，如下所示： • active - 该接口没有关闭。 • not active - 该接口通过 **shutdown** 命令关闭。
Interface state	接口的实际状态。在大多数情况下，此状态与上述配置状态匹配。如果配置高可用性，则可能不匹配，因为 ASA 会根据需要打开或关闭接口。
Asymmetrical Routing Statistics:	
Received X1 packets	在此接口上接收的 ASR 数据包数。
Transmitted X2 packets	在此接口上发送的 ASR 数据包数。
Dropped X3 packets	在此接口上丢弃的 ASR 数据包数。当尝试转发数据包时，如果接口关闭，则可能丢弃数据包。

以下是 ASA 5512-X 到 ASA 5555-X 上 **show interface detail** 命令的输出示例，显示针对 ASA 和软件模块的管理 0/0 接口（显示为 “Internal-Data0/1”）的合并统计信息。输出还显示 Internal-Control0/0 接口，该接口用于控制软件模块和 ASA 之间的流量。

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
```

```
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active

Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
clear interface	清除 **show interface** 命令的计数器。

命令	说明
delay	更改接口的延迟指标。
interface	配置接口并进入接口配置模式。
nameif	设置接口名称。
show interface ip brief	显示接口 IP 地址和状态。

show interface ip brief

要查看接口 IP 地址和状态，请在特权 EXEC 模式下使用 **show interface ip brief** 命令。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

语法说明

interface_name	（可选）识别通过 **nameif** 命令设置的接口名称。
mapped_name	（可选）在多情景模式下，识别映射名称（如果使用 **allocate-interface** 命令分配了该名称）。
physical_interface	（可选）识别接口 ID（例如 **gigabitethernet0/1**）。请参阅 **interface** 命令可接受的值。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
vlan *number*	（可选）为具有内置交换机的型号（如 ASA 5505 自适应安全设备）指定 VLAN 接口。

默认值

如果不指定接口，ASA 会显示所有接口。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**[1]	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

1. 仅可用于管理 0/0 接口或子接口。

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令添加了对 VLAN 接口的支持和对透明模式的管理 0/0 接口或子接口的支持。

使用指南

在多情景模式下，如果映射了 **allocate-interface** 命令的接口 ID，则您只能指定映射名称或情景中的接口名称。

有关显示输出的说明，请参阅 “ 示例 ” 部分。

示例

以下是 **show ip brief** 命令的输出示例：

```
ciscoasa# show interface ip brief
    Interface                  IP-Address      OK?Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
```

```
GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
GigabitEthernet0/1         unassigned      YES unset   administratively down down
GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
Management0/0              209.165.201.3   YES CONFIG  up
```

表 7-8 显示每个字段的说明。

表 7-8　show interface ip brief 字段

字段	说明
Interface	接口 ID，或多情景模式下的映射名称（如果已使用 **allocate-interface** 命令进行配置）。如果显示所有接口，则显示有关 AIP SSM 内部接口的信息（如果已安装在 ASA 上）。用户无法配置内部接口，该信息只用于调试目的。
IP-Address	接口 IP 地址。
OK?	此列目前没有使用并始终显示为 “Yes”。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 配置了运行配置。 • CONFIG - 已从启动配置载入。 • DHCP - 已从 DHCP 服务器接收。
Status	管理状态，如下所示： • up - 接口没有关闭。 • administratively down - 使用 **shutdown** 命令关闭接口。
Protocol	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
interface	配置接口并进入接口配置模式。
ip address	设置该接口的 IP 地址或设置一个透明防火墙的管理 IP 地址。
nameif	设置接口名称。
show interface	显示接口的运行时状态和统计信息。

show inventory

要显示有关安装在网络设备中并指定了产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN) 的思科产品的所有信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show inventory** 命令。

show inventory [*mod_id*]

语法说明

mod_id	（可选）指定模块 ID 或插槽号码 0-3。

默认值

如果在显示项目的库存时不指定插槽，则会显示所有模块（包括电源）的库存信息。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	—	• 是
用户 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	仅做了几处微小编辑更改。
8.4(2)	添加了 SSP 的输出。此外，添加了对双 SSP 安装的支持。
8.6(1)	添加了 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X（机箱、备用电源和 I/O 扩展卡）的输出。
9.1(1)	添加了 ASA CX 模块的输出。

使用指南

show inventory 命令检索和显示有关每个思科产品的库存信息，这些产品的形式为 UDI，是以下三个不同数据元素的组合：产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN)。

PID 是可用于订购产品的名称；它以前称为 “ 产品名称 ” 或 “ 部件号 ”。这是用来订购具体更换部件的标识符。

VID 是产品的版本。每当修订产品后，VID 即根据 Telcordia GR-209-CORE（管理产品更改通知的行业标准）的严格流程来递增。

SN 是供应商提供的唯一产品序列号。每个产品都具有工厂指定的唯一序列号，无法在实际应用中更改。序列号是用于标识各具体产品实例的方法。对于设备的不同组件，序列号的长度可以不同。

UDI 将每个产品作为一个实体。部分实体（如机箱）具有子实体（像插槽）。每个实体以逻辑排序呈现方式显示在思科实体分层排列的单独行上。

使用 **show inventory** 命令（不带选项）可显示安装在网络设备中并分配了 PID 的思科实体列表。

如果未对思科实体分配 PID，则不会检索或显示该实体。

注意　当两个 SSP 安装在同一机箱中时，模块的编号指示模块在机箱中的物理位置。机箱主控始终是安装在插槽 0 中的 SSP。只有与 SSP 相关联的那些传感器才显示在输出中。

输出中的术语 *module* 等于物理插槽。在 SSP 本身的说明中，输出包括 module: 0（当安装在物理插槽 0 中时），否则包括 module: 1。当目标 SSP 是机箱主控时，**show inventory** 命令输出包括电源和 / 或冷却风扇。否则，会忽略这些组件。

由于 ASA 5500-X 系列的硬件限制，序列号可能不显示。对于这些型号中 PCI-E I/O (NIC) 选项卡的 UDI 显示，根据机箱类型有六种可能的输出，尽管只有两种不同类型的卡。这是因为根据指定的机箱使用了不同的 PCI-E 支架组件。以下示例展示每个 PCI-E I/O 卡组装的预期输出。例如，如果检测到 Silicom SFP NIC 卡，则 UDI 显示取决于安装该 UDI 的设备。VID 和 S/N 值为 N/A，因为没有这些值的电子存储。

对于 ASA 5512-X 或 5515-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

对于 ASA 5512-X 或 5515-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

示例

以下是没有任何关键字或参数的 **show inventory** 命令的输出示例。此输出示例显示安装在 ASA 中且都分配了 PID 的思科实体的列表，包括用于 ASA CX 模块的存储设备。

```
ciscoasa> show inventory
Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555            , VID: V01     , SN: FGL170441BU

Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC         , VID: N/A     , SN: 2CS1AX

Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A                , VID: N/A     , SN: MXA174201RR
```

以下示例展示双 SSP 安装的机箱主控上 **show inventory** 命令的输出：

```
ciscoasa(config)# show inventory
Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40    , VID: V01     , SN: JAF1436ACLJ

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V01     , SN: 123456789AB

Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN       , VID: V01     , SN: POG1434000G

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V01     , SN: POG1434002K
```

表 7-9 说明显示屏幕中显示的字段。

表 7-9　show inventory 的字段说明

字段	说明
Name	分配给思科实体的物理名称（文本字符串）。例如，控制台、SSP 或简单组件号（端口或模块号，如 “1”）取决于设备的物理组件的命名语法。相当于 RFC 2737 中的 entPhysicalName MIB 变量。
DESCR	用于描述对象的思科实体的物理说明。相当于 RFC 2737 中的 entPhysicalDesc MIB 变量。
PID	实体的产品标识符。相当于 RFC 2737 中的 entPhysicalModelName MIB 变量。
VID	实体的版本标识符。相当于 RFC 2737 中的 entPhysicalHardwareRev MIB 变量。
SN	实体的序列号。相当于 RFC 2737 中的 entPhysicalSerialNum MIB 变量。

相关命令

命令	说明
show diag	显示有关网络设备的控制器、接口处理器和端口适配器的诊断信息。
show tech-support	显示报告问题的路由器的一般信息。

show ip address

要查看接口 IP 地址或管理 IP 地址（用于透明模式），请在特权 EXEC 模式下使用 **show ip address** 命令。

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

语法说明

interface_name	（可选）识别通过 **nameif** 命令设置的接口名称。
mapped_name	（可选）在多情景模式下，识别映射名称（如果使用 **allocate-interface** 命令分配了该名称）。
physical_interface	（可选）识别接口 ID（例如 **gigabitethernet0/1**）。请参阅 **interface** 命令可接受的值。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
vlan *number*	（可选）为具有内置交换机的型号（如 ASA 5505 自适应安全设备）指定 VLAN 接口。

默认值

如果不指定接口，则 ASA 显示所有接口的 IP 地址。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	此命令添加了对 VLAN 接口的支持。

使用指南

此命令显示主要 IP 地址（在显示屏幕中称为 “System”，适用于配置高可用性时）以及当前 IP 地址。如果设备处于主用状态，则系统和当前 IP 地址匹配。如果设备处于备用状态，则当前 IP 地址显示备用地址。

示例

以下是 **show ip address** 命令的输出示例：

```
ciscoasa# show ip address
System IP Addresses:
Interface               Name          IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz           209.165.200.225 255.255.255.224   manual
Current IP Addresses:
```

```
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

表 7-10 显示每个字段的说明。

表 7-10　show ip address 字段

字段	说明
Interface	接口 ID，或多情景模式下的映射名称（如果已使用 **allocate-interface** 命令进行配置）。
Name	使用 **nameif** 命令设置的接口名称。
IP address	接口 IP 地址。
Subnet mask	IP 地址子网掩码。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 配置了运行配置。 • CONFIG - 已从启动配置载入。 • DHCP - 已从 DHCP 服务器接收。

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
interface	配置接口并进入接口配置模式。
nameif	设置接口名称。
show interface	显示接口的运行时状态和统计信息。
show interface ip brief	显示接口 IP 地址和状态。

show ip address dhcp

要查看有关接口的 DHCP 租用或服务器的详细信息，请在特权 EXEC 模式下使用 **show ip address dhcp** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp lease** {**proxy** | **server**} {**summary**}

语法说明

interface_name	标识使用 **nameif** 命令设置的接口名称。
lease	显示有关 DHCP 租用的信息。
mapped_name	在多情景模式中，标识使用 **allocate-interface** 命令分配的映射名称。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。请参阅 **interface** 命令可接受的值。
proxy	显示 IPL 表中的代理条目。
server	显示 IPL 表中的服务器条目。
subinterface	标识用于指定逻辑子接口的 1 和 4294967293 之间的整数。
summary	显示条目的汇总。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**[1]	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

1. 仅可用于管理 0/0 接口或子接口。

命令历史

版本	修改
7.0(1)	更改了此命令以包括 **lease** 和 **server** 关键字，从而适应新的服务器功能。
7.2(1)	此命令添加了对 VLAN 接口的支持和对透明模式的管理 0/0 接口或子接口的支持。
9.1(4)	更改了此命令以包括 **proxy** 和 **summary** 关键字，从而适应新的服务器功能。

使用指南

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show ip address dhcp lease** 命令的输出示例：

```
ciscoasa# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

表 7-11 显示每个字段的说明。

表 7-11　show ip address dhcp lease 字段

字段	说明
Temp IP Addr	分配给接口的 IP 地址。
Temp sub net mask	分配给接口的子网掩码。
DHCP Lease server	DHCP 服务器地址。
state	DHCP 租用的状态，如下所示： • Initial - 初始化状态，ASA 启动获取租用进程。当租用结束或租用协商失败时，也会显示此状态。 • Selecting - ASA 正在等待检索来自一个或多个 DHCP 服务器的 DHCPOFFER 消息，从而可从中选择一个。 • Requesting - ASA 正在等待接收所发送请求的目标服务器的回应。 • Purging - ASA 正在删除租用，因为客户端已释放 IP 地址或出现其他错误。 • Bound - ASA 具有有效租用且正在正常运行。 • Renewing - ASA 正在尝试续订租用。它定期将 DHCPREQUEST 消息发送到当前 DHCP 服务器，然后等待回复。 • Rebinding - ASA 无法对原始服务器的租用续约，现在发送 DHCPREQUEST 消息，直到收到任何服务器的回复或租用结束。 • Holddown - ASA 已启动用于删除租用的进程。 • Releasing - ASA 将释放消息发送到服务器，指示不再需要 IP 地址。
DHCP transaction id	客户端选择的随机编号，供客户端和服务器用来关联请求消息。
Lease	DHCP 服务器指定的时间长度，接口可在该时间段内使用此 IP 地址。
Renewal	接口自动尝试续订此租用之前的时间长度。
Rebind	ASA 尝试重新绑定 DHCP 服务器之前的时间长度。如果 ASA 无法与原始 DHCP 服务器通信且租用时间已超过 87.5%，就会进行重新绑定。然后，ASA 尝试通过广播 DHCP 请求与任何可用的 DHCP 服务器联系。

表 7-11　show ip address dhcp lease 字段（续）

字段	说明
Temp default-gateway addr	DHCP 服务器提供的默认网关地址。
Temp ip static route0	默认静态路由。
Next timer fires after	内部计时器触发之前的秒数。
Retry count	如果 ASA 正在尝试建立租用，则此字段显示 ASA 已尝试发送 DHCP 消息的次数。例如，如果 ASA 处于 Selecting（选择中）状态，则此值显示 ASA 已发送发现消息的次数。如果 ASA 处于 Requesting（请求中）状态，则此值显示 ASA 已发送请求消息的次数。
Client-ID	在与服务器的所有通信中使用的客户端 ID。
Proxy	指定此接口是否为 VPN 客户端的代理 DHCP 客户端，值为 True 或 False。
Proxy Network	请求的网络。
Hostname	客户端主机名称。

以下是 **show ip address dhcp server** 命令的输出示例：

```
ciscoasa# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 7-12 显示每个字段的说明。

表 7-12　show ip address dhcp server 字段

字段	说明
DHCP server	向此接口提供租用的 DHCP 服务器的地址。顶部条目（“ANY”）是默认服务器并始终存在。
Leases	从服务器获取的租用数。对于一个接口，租用数通常是 1。如果服务器为正在运行 VPN 代理的接口提供地址，会有数个租用。
Offers	服务器所提供的项的数量。
Requests	发送至服务器的请求数。
Acks	从服务器接收的确认数。
Naks	从服务器接收的否定确认数。
Declines	从服务器接收的拒绝数。
Releases	发送至服务器的释放数。
Bad	从服务器接收的错误数据包数。

表 7-12　show ip address dhcp server 字段（续）

字段	说明
DNS0	从 DHCP 服务器获取的主要 DNS 服务器地址。
DNS1	从 DHCP 服务器获取的辅助 DNS 服务器地址。
WINS0	从 DHCP 服务器获取的主要 WINS 服务器地址。
WINS1	从 DHCP 服务器获取的辅助 WINS 服务器地址。
Subnet	从 DHCP 服务器获取的子网地址。
DNS Domain	从 DHCP 服务器获取的域。

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
ip address dhcp	设置接口以从 DHCP 服务器获取 IP 地址。
nameif	设置接口名称。
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip address pppoe

要查看有关 PPPoE 连接的详细信息，请在特权 EXEC 模式下使用 **show ip address pppoe** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

语法说明

interface_name	标识使用 **nameif** 命令设置的接口名称。
mapped_name	在多情景模式中，标识使用 **allocate-interface** 命令分配的映射名称。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。请参阅 **interface** 命令可接受的值。
subinterface	标识用于指定逻辑子接口的 1 和 4294967293 之间的整数。
vlan *number*	（可选）为具有内置交换机的型号（如 ASA 5505 自适应安全设备）指定 VLAN 接口。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明[1]	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

1. 仅可用于管理 0/0 接口或子接口。

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show ip address pppoe** 命令的输出示例：

```
ciscoasa# show ip address outside pppoe
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
ip address ppoe	设置接口以从 PPPoE 服务器获取 IP 地址。
nameif	设置接口名称。
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip audit count

要显示将审核策略应用到接口时的签名匹配数，请在特权 EXEC 模式下使用 **show ip audit count** 命令。

show ip audit count [**global** | **interface** *interface_name*]

语法说明

global	（默认）显示所有接口的匹配数。
interface *interface_name*	（可选）显示指定接口的匹配数。

默认值

如果未指定关键字，则此命令会显示所有接口的匹配 (**global**)。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要创建审核策略，请使用 **ip audit name** 命令；要应用策略，请使用 **ip audit interface** 命令。

示例

以下是 **show ip audit count** 命令的输出示例：

```
ciscoasa# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
2004 I ICMP Echo Request          10
```

```
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

相关命令

命令	说明
clear ip audit count	清除审核策略的签名匹配计数。
ip audit interface	将审核策略分配至接口。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
show running-config ip audit attack	显示 **ip audit attack** 命令的配置。

show ip verify statistics

要显示由于 Unicast RPF（单播反向路径转发）功能而丢弃的数据包数，请在特权 EXEC 模式下使用 **show ip verify statistics** 命令。使用 **ip verify reverse-path** 命令以启用 Unicast RPF（单播反向路径转发）。

show ip verify statistics [interface *interface_name*]

语法说明

interface *interface_name*	（可选）显示指定接口的统计信息。

默认值

此命令显示所有接口的统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show ip verify statistics** 命令的输出示例：

```
ciscoasa# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

相关命令

命令	说明
clear configure ip verify reverse-path	清除 **ip verify reverse-path** 配置。
clear ip verify statistics	清除单播 RPF 统计信息。
ip verify reverse-path	启用单播反向路径转发功能以防止 IP 欺骗。
show running-config ip verify reverse-path	显示 **ip verify reverse-path** 配置。

show ips

要显示在 AIP SSM 上配置的所有可用 IPS 虚拟传感器，请在特权 EXEC 模式下使用 **show ips** 命令。

show ips [**detail**]

语法说明

detail	（可选）显示传感器 ID 号和名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在多情景模式下，此命令显示进入系统执行空间的所有虚拟传感器，但仅显示分配给情景执行空间中情景的虚拟传感器。请参阅 **allocate-ips** 命令以将虚拟传感器分配给情景。

虚拟传感器在 IPS 6.0 版及更高版本中可用。

示例

以下是 **show ips** 命令的输出示例：

```
ciscoasa# show ips
Sensor name
------------
ips1
ips2
```

以下是 **show ips detail** 命令的输出示例：

```
ciscoasa# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

相关命令

命令	说明
allocate-ips	将虚拟传感器分配到安全情景。
ips	将流量转移至 AIP SSM。

show ipsec sa

要显示 IPsec SA 列表，请在全局配置模式或特权 EXEC 模式下使用 **show ipsec sa** 命令。您还可使用此命令的替代形式：**show crypto ipsec sa**。

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

语法说明

assigned-address	（可选）显示指定的主机名或 IP 地址的 IPsec SA。
detail	（可选）显示有关所显示内容的详细错误信息。
entry	（可选）显示按对等设备地址排序的 IPsec SA
identity	（可选）显示按身份排序的 IPsec SA，不包括 ESP。这是简洁形式。
inactive	（可选）显示无法传递流量的 IPsec SA。
map *map-name*	（可选）显示指定加密映射的 IPsec SA。
peer *peer-addr*	（可选）显示指定对等设备 IP 地址的 IPsec SA。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	添加了对 OSPFv3 和多情景模式的支持。
9.1(4)	更新了输出以反映分配的 IPv6 地址和指示当执行 IKEv2 双流量时的 GRE 传输模式安全关联。

示例

以下示例在全局配置模式下输入，它展示 IPsec SA，包括分配的 IPv6 地址以及传输模式和 GRE 封装指示。

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

以下示例在全局配置模式下输入，它显示 IPsec SA，包括用于将隧道标识为 OSPFv3 的使用中设置。

```
ciscoasa(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

注意　如果 IPsec SA 策略表明在 IPsec 处理前进行碎片整理，则碎片整理统计信息为碎片整理前统计信息。如果 SA 策略表明在 IPsec 处理后进行碎片整理，则显示碎片整理后统计信息。

以下示例在全局配置模式下输入，显示名为 def 的加密映射的 IPsec SA。

```
ciscoasa(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
```

```
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例在全局配置模式下输入，显示关键字 **entry** 的 IPsec SA。

```
ciscoasa(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
```

```
          sa timing: remaining key lifetime (sec): 429
          IV size: 8 bytes
          replay detection support: Y
      outbound esp sas:
        spi: 0xDC15BF68 (3692412776)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 429
          IV size: 8 bytes
          replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例在全局配置模式下输入，显示采用关键字 **entry detail** 的 IPsec SA。

```
ciscoasa(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
        #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
        #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
        #pkts invalid prot (rcv): 0, #pkts verify failed: 0
        #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
        #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
        #pkts replay failed (rcv): 0
        #pkts internal err (send): 0, #pkts internal err (rcv): 0

        local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

        path mtu 1500, ipsec overhead 60, media mtu 1500
        current outbound spi: DC15BF68

      inbound esp sas:
        spi: 0x1E8246FC (511854332)
           transform: esp-3des esp-md5-hmac
           in use settings ={RA, Tunnel, }
           slot: 0, conn_id: 3, crypto-map: def
           sa timing: remaining key lifetime (sec): 322
           IV size: 8 bytes
           replay detection support: Y
      outbound esp sas:
        spi: 0xDC15BF68 (3692412776)
           transform: esp-3des esp-md5-hmac
           in use settings ={RA, Tunnel, }
           slot: 0, conn_id: 3, crypto-map: def
           sa timing: remaining key lifetime (sec): 322
           IV size: 8 bytes
           replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

以下示例展示采用关键字 **identity** 的 IPsec SA。

```
ciscoasa(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例展示采用关键字 **identity** 和 **detail** 的 IPsec SA。

```
ciscoasa(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例展示基于分配 IPv6 地址的 IPSec SA：

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
```

```
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

相关命令

命令	说明
clear configure isakmp	清除所有 ISAKMP 配置。
clear configure isakmp policy	清除所有 ISAKMP 策略配置。
clear isakmp sa	清除 IKE 运行时 SA 数据库。
isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show ipsec sa summary

要显示 IPsec SA 汇总，请在全局配置模式或特权 EXEC 模式下使用 **show ipsec sa summary** 命令。

show ipsec sa summary

语法说明

此命令没有任何参数或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例在全局配置模式下输入，按下列连接类型显示 IPsec SA 汇总：

- IPsec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN 负载平衡

```
ciscoasa(config)# show ipsec sa summary

Current IPsec SA's:             Peak IPsec SA's:
IPsec              :     2          Peak Concurrent SA  :    14
IPsec over UDP     :     2          Peak Concurrent L2L :     0
IPsec over NAT-T   :     4          Peak Concurrent RA  :    14
IPsec over TCP     :     6
IPsec VPN LB       :     0
Total              :    14
ciscoasa(config)#
```

相关命令

命令	说明
clear ipsec sa	全部或基于特定参数删除 IPsec SA。
show ipsec sa	显示 IPsec SA 列表。
show ipsec stats	显示 IPsec 统计信息列表。

show ipsec stats

要显示 IPsec 统计信息列表，请在全局配置模式或特权 EXEC 模式下使用 **show ipsec stats** 命令。

show ipsec stats

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	ESPv3 统计信息与 IPsec 子系统一起显示，并添加了对多情景模式的支持。

使用指南

下表说明了输出条目指示的内容。

输出	说明
IPsec Global Statistics	此部分显示 ASA 支持的 IPsec 隧道总数。
Active tunnels	当前连接的 IPsec 隧道数。
Previous tunnels	已连接的 IPsec 隧道数，包括主用隧道。
Inbound	此部分显示通过 IPsec 隧道接收的入站加密流量。
Bytes	接收的加密流量的字节数。
Decompressed bytes	执行解压缩之后接收的加密流量的字节数（如果适用）。如果未启用压缩，此计数器应始终等于前一个计数器。
Packets	接收的加密 IPsec 数据包数。
Dropped packets	已接收但由于错误而丢弃的加密 IPsec 数据包数。
Replay failures	对接收的加密 IPsec 数据包检测到的反重播故障数。
Authentications	对接收的加密 IPsec 数据包执行的身份验证成功数。
Authentication failures	对接收的加密 IPsec 数据包检测到的身份验证失败数。

输出（续）	说明（续）
Decryptions	对接收的加密 IPsec 数据包执行的解密成功数。
Decryption failures	对接收的加密 IPsec 数据包检测到的解密失败数。
Decapsulated fragments needing reassembly	包括要重组的 IP 分段的解密 IPsec 数据包数。
Outbound	此部分显示要通过 IPsec 流量传输的出站明文流量。
Bytes	要通过 IPsec 隧道加密并传输的明文流量字节数。
Uncompressed bytes	要通过 IPsec 隧道加密并传输的未压缩明文流量字节数。如果未启用压缩，计数器应始终等于前一个计数器。
Packets	要通过 IPsec 隧道加密并传输的明文数据包数。
Dropped packets	要通过 IPsec 隧道加密并传输而由于错误已丢弃的明文数据包数。
Authentications	对要通过 IPsec 隧道传输的数据包执行的身份验证成功数。
Authentication failures	对要通过 IPsec 隧道传输的数据包检测到的身份验证失败数。
Encryptions	对要通过 IPsec 隧道传输的数据包执行的加密成功数。
Encryption failures	对要通过 IPsec 隧道传输的数据包检测到的加密失败数。
Fragmentation successes	作为出站 IPsec 数据包转换的一部分执行的分段操作成功数。
Pre-fragmentation successes	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
Post-fragmentation successes	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
Fragmentation failures	出站 IPsec 数据包转换时发生的分段失败数。
Pre-fragmentation failures	出站 IPsec 数据包转换时发生的预分段失败数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
Post-fragmentation failure	出站 IPsec 数据包转换时发生的后分段失败数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
Fragments created	IPsec 转换过程中创建的分段数。
PMTUs sent	IPsec 系统发送的路径 MTU 消息数。IPsec 将 PMTU 消息发送至内部主机，此主机正在发送封装后由于太大而无法通过 IPsec 隧道传输的数据包。PMTU 消息用于请求主机降低其 MTU 和发送更小的数据包以通过 IPsec 隧道传输。
PMTUs recvd	IPsec 系统接收的路径 MTU 消息数。如果通过隧道发送的数据包太大而无法遍历下游网络元素，IPsec 将接收来自该网络元素的路径 MTU 消息。当接收路径 MTU 消息时，IPsec 通常会降低其隧道 MTU。
Protocol failures	接收的错误 IPsec 数据包数。
Missing SA failures	因指定 IPsec 安全关联不存在而请求的 IPsec 操作数。
System capacity failures	因 IPsec 系统容量不足以支持数据速率而无法完成的 IPsec 操作数。

示例

以下示例在全局配置模式下输入，显示 IPsec 统计信息：

```
ciscoasa(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear ipsec sa	基于指定的参数清除 IPsec SA 或计数器。
crypto ipsec transform-set	定义转换集。
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec sa summary	显示 IPsec SA 摘要。

show ipv6 access-list 至 show ipv6 traffic 命令

show ipv6 access-list

要显示 IPv6 访问列表，请在特权 EXEC 模式下使用 **show ipv6 access-list** 命令。IPv6 访问列表确定哪些 IPv6 流量可通过 ASA。

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*]]

语法说明

any	（可选）IPv6 前缀 ::/0 的缩写。
host *source-ipv6-address*	（可选）特定主机的 IPv6 地址。当提供时，仅显示指定主机的访问规则。
id	（可选）访问列表名称。当提供时，仅显示指定的访问列表。
source-ipv6-prefix /prefix-length	（可选）IPv6 网络地址和前缀。当提供时，仅显示指定的 IPv6 网络的访问规则。

默认值

显示所有 IPv6 访问列表。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show ipv6 access-list 命令的输出类似于 **show ip access-list** 命令，只是前者是特定于 IPv6。

示例

以下是 **show ipv6 access-list** 命令的输出示例。它显示名为 inbound、tcptraffic 和 outbound 的 IPv6 访问列表。

```
ciscoasa# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

相关命令

命令	说明
ipv6 access-list	创建 IPv6 访问列表。

show ipv6 dhcprelay binding

要显示中继代理创建的中继绑定条目，请在特权 EXEC 模式下使用 **show ipv6 dhcprelay binding** 命令。

show ipv6 dhcprelay binding

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show ipv6 dhcprelay binding 命令可允许您检查中继代理创建的中继绑定条目。

示例

以下是 **show ipv6 dhcprelay binding** 命令的输出示例：

```
ciscoasa# show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

相关命令

命令	说明
show ipv6 dhcprelay statistics	显示 IPv6 DHCP 中继代理信息。

show ipv6 dhcprelay statistics

要显示 IPv6 DHCP 中继代理统计信息，请在特权 EXEC 模式下使用 **show ipv6 dhcprelay statistics** 命令。

show ipv6 dhcprelay statistics

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show ipv6 dhcprelay statistics 命令允许您查看 IPv6 DHCP 中继代理信息。

示例

以下是 **show ipv6 dhcprelay statistics** 命令的输出示例：

```
ciscoasa# show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                    1
  ADVERTISE                                  2
  REQUEST                                    1
  CONFIRM                                    1
  RENEW                                    496
  REBIND                                     0
  REPLY                                    498
  RELEASE                                    0
  DECLINE                                    0
  RECONFIGURE                                0
  INFORMATION-REQUEST                        0
  RELAY-FORWARD                            499
  RELAY-REPLY                              500

Relay Errors:
  Malformed message:                         0
  Block allocation/duplication failures:     0
  Hop count limit exceeded:                  0
  Forward binding creation failures:         0
```

```
  Reply binding lookup failures:                0
  No output route:                              0
  Conflict relay server route:                  0
  Failed to add server NP rule:                 0
  Unit or context is not active:                0

Total Relay Bindings Created:                 498
```

相关命令

命令	说明
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。

show ipv6 interface

要显示配置了 IPv6 的接口的状态，请在特权 EXEC 模式下使用 **show ipv6 interface** 命令。

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

语法说明

brief	显示每个接口的 IPv6 状态和配置的简短汇总。
if_name	（可选）由 **nameif** 命令指定的内部或外部接口名称。仅显示指定接口的状态和配置。
prefix	（可选）从本地 IPv6 前缀池生成的前缀。前缀是 IPv6 地址的网络部分。

默认值

显示所有 IPv6 接口。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show ipv6 interface 命令的输出类似于 **show interface** 命令，只是前者是特定于 IPv6。如果接口硬件可用，会将接口标记为 *up*。如果接口可以提供双向通信，会将线路协议标记为 *up*。

当未指定接口名称时，会显示所有 IPv6 接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是 **show ipv6 interface** 命令的输出示例：

```
ciscoasa# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

以下是当输入具有 **brief** 关键字的 **show ipv6 interface** 命令时，该命令的输出示例：

```
ciscoasa# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

以下是 **show ipv6 interface** 命令的输出示例。它显示已从地址生成前缀的接口的特征。

```
ciscoasa# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 mld traffic

要显示组播侦听程序发现 (MLD) 流量计数器信息，请在特权 EXEC 模式下使用 **show ipv6 mld traffic** 命令。

show ipv6 mld traffic

语法说明

此命令没有关键字或变量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(4)	引入了此命令。

使用指南

show ipv6 mld traffic 命令允许您检查是否已接收和发送预计的 MLD 消息数。

show ipv6 mld traffic 命令提供以下信息：

- Elapsed time since counters cleared（清除计数器以后经过的时间）- 自清除计数器以来的时间量。
- Valid MLD Packets（有效 MLD 数据包）- 接收和发送的有效 MLD 数据包数。
- Queries（查询）- 接收和发送的有效查询数。
- Reports（报告）- 接收和发送的有效报告数。
- Leaves（保留）- 接收和发送的有效保留数。
- Mtraee packets（Mtraee 数据包）- 接收和发送的组播跟踪数据包数。
- Errors（错误）- 错误类型和发生的错误数。

示例

以下是 **show ipv6 mld traffic** 命令的输出示例：

```
ciscoasa# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 0:01:19
                   Received           Sent
Valid MLD Packets  1                  3
```

```
Queries            1                   0
Reports            0                   3
Leaves             0                   0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

相关命令

命令	说明
clear ipv6 mld traffic	重置所有 MLD 流量计数器。

show ipv6 neighbor

要显示 IPv6 邻居发现缓存信息，请在特权 EXEC 模式下使用 **show ipv6 neighbor** 命令。

show ipv6 neighbor [*if_name* | *address*]

语法说明

address	（可选）仅显示提供的 IPv6 地址的邻居发现缓存信息。
if_name	（可选）仅显示提供的接口名称（由 **nameif** 命令所配置）的缓存信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show ipv6 neighbor 命令提供以下信息：

- IPv6 Address（IPv6 地址）- 邻居或接口的 IPv6 地址。
- Age（时间）- 自确认地址可到达以来的时间（以分钟为单位）。连字符 (-) 指示静态条目。
- Link-layer Addr（链路层地址）- MAC 地址。如果地址未知，则显示连字符 (-)。
- State（状态）- 邻居缓存条目的状态。

注　可达性检测不会应用于 IPv6 邻居发现缓存中的静态条目；因此，对于动态和静态缓存条目，INCMP（未完成）和 REACH（可达）状态的说明不同。

以下是 IPv6 邻居发现缓存中动态条目的可能状态：

- INCMP -（未完成）正在对条目执行地址解析。邻居请求消息已发送至目标的请求节点组播地址，但是尚未收到对应的邻居通告消息。
- REACH -（可达）在最后 ReachableTime 毫秒内收到正面确认，指示邻居的转发路径运行正常。在 REACH 状态下，由于数据包已发送，设备不执行任何特殊操作。
- STALE - 自收到指示转发路径运行正常的最后一个正面确认以来，已超过 ReachableTime 毫秒。在 STALE 状态下，设备在数据包发送完成之前不执行任何操作。

  - DELAY - 自收到指示转发路径运行正常的最后一个正面确认以来，已超过 ReachableTime 毫秒。数据包在最后 DELAY_FIRST_PROBE_TIME 秒内已发送。在进入 DELAY 状态的 DELAY_FIRST_PROBE_TIME 秒内，如果未收到可达性确认，则发送邻居请求消息并将状态更改为 PROBE。
  - PROBE - 通过每 RetransTimer 毫秒后重新发送邻居请求消息，积极寻找可达性确认，直至收到可达性确认。
  - ???? - 未知状态。

  以下是 IPv6 邻居发现缓存中静态条目的可能状态：

  - INCMP -（未完成）此条目的接口关闭。
  - REACH -（可达）此条目的接口开启。

- Interface

  可从中访问地址的接口。

示例

以下是输入具有接口的 **show ipv6 neighbor** 命令时，该命令的输出示例：

```
ciscoasa# show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

以下是输入具有 IPv6 地址的 **show ipv6 neighbor** 命令时，该命令的输出示例：

```
ciscoasa# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

相关命令

命令	说明
clear ipv6 neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。
ipv6 neighbor	在 IPv6 邻居发现缓存中配置静态条目。

show ipv6 ospf

要显示有关 OSPFv3 路由进程的一般信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf** 命令。

show ipv6 ospf [*process_id*] [*area_id*]

语法说明

area_id	（可选）仅显示有关指定区域的信息。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。当启用 OSPFv3 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show ipv6 ospf 命令列出以下设置：

- 事件记录
- 路由类型
- 重分布路由类型
- SPF 计划延时
- 两个连续 SPF 之间的保持时间
- 两个连续 SPF 之间的等待时间
- 最小 LSA 间隔
- 最小 LSA 到达

示例

以下是 **show ipv6 ospf** 命令的输出示例：

```
ciscoasa# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

```
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

相关命令

命令	说明
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。
show ipv6 ospf database	显示与特定路由器的 OSPFv3 数据库相关的信息列表。

show ipv6 ospf border-routers

要显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf border-routers** 命令。

show ipv6 ospf [*process_id*] **border-routers**

语法说明

process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。当启用 OSPFv3 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

show ipv6 ospf border-routers 命令列出以下设置：

- 区域内路由
- 区域间路由
- IPv6 地址
- 接口类型
- 区域 ID
- SPF 编号

示例

以下是 **show ipv6 ospf border-routers** 命令的输出示例：

```
ciscoasa# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf database	显示与特定路由器的 OSPFv3 数据库相关的信息列表。

show ipv6 ospf database

要显示与特定路由器的 OSPFv3 数据库相关的信息列表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf database** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]

语法说明

adv-router *router-id*	（可选）显示通告路由器的所有 LSA。路由器 ID 必须是 RFC 2740 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
area	（可选）仅显示有关区域 LSA 的信息。
area_id	（可选）仅显示有关指定区域的信息。
as	（可选）过滤未知自主系统 (AS) LSA。
database-summary	（可选）显示数据库中每个区域的每种类型的 LSA 数以及总数。
destination-router-id	（可选）仅显示有关指定目标路由器的信息。
external	（可选）仅显示有关外部 LSA 的信息。
interface	（可选）显示有关依据接口情景过滤的 LSA 的信息。
interface-name	（可选）指定 LSA 接口名称。
internal	（可选）仅显示有关内部 LSA 的信息。
inter-area prefix	（可选）仅显示有关基于区域间前缀的 LSA 的信息。
inter-area router	（可选）仅显示有关基于区域间路由器 LSA 的 LSA 的信息。
link	（可选）显示有关链路 LSA 的信息。当后面有 **unknown** 关键字时，**link** 关键字会过滤链路范围 LSA。
link-state-id	（可选）指定用于区分 LSA 的整数。在网络和链路 LSA 中，链路状态 ID 与接口索引匹配。
network	（可选）显示有关网络 LSA 的信息。
nssa-external	（可选）仅显示有关末节区域 (NSSA) 外部 LSA 的信息。
prefix *ipv6-prefix*	（可选）显示邻居的本地链路 IPv6 地址。IPv6 前缀必须是 RFC 2373 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。
ref-lsa	（可选）进一步过滤前缀 LSA 类型。
router	（可选）显示有关路由器 LSA 的信息。
self-originate	（可选）仅显示来自本地路由器的自发 LSA。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	单个	多个 情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

多种形式的命令提供有关不同 OSPFv3 LSA 的信息。

示例

以下是 **show ipv6 ospf database** 命令的输出示例：

```
ciscoasa# show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3
            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf events

要显示 OSPFv3 内部事件信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf events** 命令。

show ipv6 ospf [*process_id*] **events**

语法说明

process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示 OSPFv3 事件信息。

示例

以下是 **show ipv6 ospf events** 命令的输出示例：

```
ciscoasa# show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,
   Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age
   0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,
   Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
```

```
12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0, Adv-Rtr
50.100.168.192
16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf flood-list

要显示等待在接口上泛洪的 OSPFv3 LSA 列表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf flood-list** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

语法说明

area_id	（可选）仅显示有关指定区域的信息。
interface-number	指定泛洪 LSA 所在的接口号。
interface-type	指定泛洪 LSA 所在的接口类型。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。当启用 OSPFv3 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示 OSPFv3 数据包节奏信息。

示例

以下是 **show ipv6 ospf flood-list** 命令的输出示例：

```
ciscoasa# show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf graceful-restart

要显示有关 OSPFv3 平滑重启的信息，请在特权 EXEC 模式下使用 **show ipv6 ospf graceful-restart** 命令。

show ipv6 ospf graceful-restart

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.3(1)	引入了此命令。

示例

以下是 **show ipv6 ospf graceful-restart** 命令的输出示例：

```
ciscoasa# show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。

show ipv6 ospf interface

要显示 OSPFv3 相关的接口信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf interface** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

语法说明

area_id	（可选）仅显示有关指定区域的信息。
brief	（可选）显示路由器上 OSPFv3 接口、状态、地址和掩码以及区域的简要概述信息。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。
type-number	（可选）指定接口类型和号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示路由器上 OSPFv3 接口、状态、地址和掩码以及区域的概述信息。

示例

以下是 **show ipv6 ospf interface** 命令的输出示例：

```
ciscoasa# show ipv6 ospf interface

ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
```

```
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 0:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf neighbor

要基于每个接口显示 OSPFv3 邻居信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf neighbor** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

语法说明

area_id	（可选）仅显示有关指定区域的信息。
detail	（可选）详细显示所有邻居信息。
interface-type interface-number	（可选）指定接口类型和号码。
neighbor-id	（可选）指定邻居 ID。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可按接口显示 OSPFv3 邻居的详细信息。

示例

以下是 **show ipv6 ospf neighbor** 命令的输出示例：

```
ciscoasa# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4        1   FULL/  -        00:00:31    14              POS4/0
172.16.3.3        1   FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5        1   FULL/  -        0:00:33    13              ATM3/0
```

以下是 **show ipv6 ospf neighbor detail** 命令的输出示例：

```
Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 0:00:33
    Neighbor is up for 0:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 0:00:33
    Neighbor is up for 0:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 0:00:38
    Neighbor is up for 0:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf request-list

要显示路由器已请求的所有 LSA 的列表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf request-list** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

语法说明

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定路由器从此接口请求的所有 LSA 的列表。
interface-neighbor	（可选）指定路由器在此接口上从此邻居请求的所有 LSA 的列表。
neighbor	（可选）指定路由器从此邻居请求的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可列出路由器请求的所有 LSA。

示例

以下是 **show ipv6 ospf request-list** 命令的输出示例：

```
ciscoasa# show ipv6 ospf request-list


           OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
```

```
1       0.0.0.0         192.168.255.1   0x800000C5  1       0x008CD1
2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf retransmission-list

要显示等待重新发送的所有 LSA 的列表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf retransmission-list** 命令。

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

语法说明

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定在此接口上等待重新发送的所有 LSA 的列表。
interface-neighbor	（可选）指定针对此接口等待从此邻居重新发送的所有 LSA 的列表。
neighbor	（可选）指定等待针对此邻居重新发送的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可列出等待重新发送的所有 LSA。

示例

以下是 **show ipv6 ospf retransmission-list** 命令的输出示例：

```
ciscoasa# show ipv6 ospf retransmission-list


       OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1

Type    LS ID           ADV RTR         Seq NO      Age    Checksum
0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf statistic

要显示各种 OSPFv3 统计信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf statistic** 命令。

show ipv6 ospf [*process_id*] **statistic** [**detail**]

语法说明

detail	（可选）指定详细 SPF 信息，包括触发点。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可列出 SPF 的执行次数、原因和持续时间。

示例

以下是 **show ipv6 ospf statistic** 命令的输出示例：

```
ciscoasa# show ipv6 ospf 10 statistic detail


Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
```

```
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0            0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf summary-prefix

要显示在 OSPFv3 进程下配置的所有汇总地址重分布信息列表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf summary-prefix** 命令。

show ipv6 ospf [*process_id*] **summary-prefix**

语法说明

process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示在 OSPFv3 进程下配置的所有汇总地址重分布信息列表。

示例

以下是 **show ipv6 ospf summary-prefix** 命令的输出示例：

```
ciscoasa# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf timers

要显示 OSPFv3 计时器信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf timers** 命令。

show ipv6 ospf [*process_id*] **timers** [**lsa-group** | **rate-limit**]

语法说明

lsa-group	（可选）指定 OSPFv3 LSA 组信息。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。
rate-limit	（可选）指定 OSPFv3 LSA 速率限制信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示在 OSPFv3 进程下配置的 LSA 信息。

示例

以下是 **show ipv6 ospf timers lsa-group** 命令的输出示例：

```
ciscoasa# show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)
```

```
Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

以下是 **show ipv6 ospf timers rate-limit** 命令的输出示例：

```
ciscoasa# show ipv6 ospf timers rate-limit

List of LSAs that are in rate limit Queue
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf traffic

要显示当前可用接口的 OSPFv3 流量相关的统计信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf traffic** 命令。

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

语法说明

interface_name	（可选）指定接口的名称（例如，接口 GigabitEthernet0/0）。使用此选项将流量隔离至特定接口。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由进程时，此 ID 是管理性分配的号码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示可用接口的 OSPFv3 流量相关信息。

示例

以下是 **show ipv6 ospf traffic** 命令的输出示例：

```
ciscoasa# show ipv6 ospf 10 traffic inside

Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                        0 0
  RX Hello                       1232 53132
  RX DB des                        27 896
  RX LS req                         3 216
  RX LS upd                        28 2436
  RX LS ack                        14 1064
  RX Total                       1304 57744
```

```
TX Failed                       0 0
TX Hello                      753 32072
TX DB des                      27 1056
TX LS req                       2 92
TX LS upd                       9 1128
TX LS ack                      15 900
TX Total                      806 35248
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf virtual-links

要显示 OSPFv3 虚拟链路的参数和当前状态，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show ipv6 ospf virtual-links** 命令。

show ipv6 ospf virtual-links

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显示 OSPFv3 虚拟链路的参数和当前状态。

示例

以下是 **show ipv6 ospf virtual-links** 命令的输出示例：

```
ciscoasa# show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

相关命令

命令	说明
show ipv6 ospf	显示 OSPFv3 路由进程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 route

要显示 IPv6 路由表的内容，请在特权 EXEC 模式下使用 **show ipv6 route** 命令。

show ipv6 route [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]

语法说明

cluster	（可选）显示集群中 IPv6 路由表序列号、IPv6 重新收敛计时器状态和 IPv6 路由条目序列号。
failover	（可选）显示 IPv6 路由表序列号、IPv6 重新收敛计时器状态和 IPv6 路由条目序列号。
interface	（可选）显示 IPv6 接口特定的路由。
ospf	（可选）显示 OSPFv3 路由。
summary	（可选）显示 IPv6 路由汇总。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	添加了对 **failover**、**cluster**、**ospf**、**interface** 和 **summary** 关键字的支持。

使用指南

show ipv6 route 命令的输出类似于 **show route** 命令，只是信息是特定于 IPv6。

以下信息出现在 IPv6 路由表中：

- Codes（代码）- 指示派生路由的协议。值如下所示：
  - C - 连接
  - L - 本地
  - S - 静态
  - R - 派生的 RIP
  - B - 派生的 BGP
  - I1 - ISIS L1（派生的集成 IS-IS 级别 1）
  - I2 - ISIS L2（派生的集成 IS-IS 级别 2）
  - IA - ISIS interarea（派生的集成 ISIS interarea）

- fe80::/10 - 指示远程网络的 IPv6 前缀。
- [0/0] - 中括号中的第一个数字是信息源的管理距离；第二个数字是路由的指标。
- via :: - 指定到远程网络的下一个路由器的地址。
- inside - 指定可到达所指定网络的下一个路由器所使用的接口。

注　**clustering** 和 **failover** 关键字不会显示，除非在 ASA 上配置了那些功能。

示例

以下是 **show ipv6 route** 命令的输出示例：

```
ciscoasa# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

以下是 **show ipv6 route failover** 命令的输出示例：

```
ciscoasa# show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

以下是主设备上 **show ipv6 route cluster** 命令的输出示例：

```
ciscoasa/LB1/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

以下是在角色更改时，对从属设备执行 **show ipv6 route cluster** 命令的输出示例：

```
ciscoasa/LB2/slave(config)# cluster master
INFO: Wait for existing master to quit.Use "show cluster info"
to check status.Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
ciscoasa/LB2/slave(config)#
ciscoasa/LB2/master(config)#
ciscoasa/LB2/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

相关命令

命令	说明
debug ipv6 route	显示 IPv6 路由表更新和路由缓存更新的调试消息。
ipv6 route	将静态条目添加至 IPv6 路由表。

show ipv6 routers

要显示从链路上路由器接收的 IPv6 路由器通告信息，请在特权 EXEC 模式下使用 **show ipv6 routers** 命令。

show ipv6 routers [*if_name*]

语法说明

if_name	（可选）要显示其有关信息的内部或外部接口名称，由 **nameif** 命令所指定。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当未指定接口名称时，会显示所有 IPv6 接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是输入时没有接口名称的 **show ipv6 routers** 命令的输出示例：

```
ciscoasa# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

相关命令

命令	说明
ipv6 route	将静态条目添加至 IPv6 路由表。

show ipv6 traffic

要显示有关 IPv6 流量的统计信息，请在特权 EXEC 模式下使用 **show ipv6 traffic** 命令。

show ipv6 traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **clear ipv6 traffic** 命令可清除流量计数器。

示例

以下是 **show ipv6 traffic** 命令的输出示例：

```
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

相关命令

命令	说明
clear ipv6 traffic	清除 IPv6 流量计数器。

show isakmp ipsec-over-tcp stats 至 show mroute 命令

show isakmp ipsec-over-tcp stats

要显示基于 TCP 的 IPsec 的运行时统计信息，请在全局配置模式或特权 EXEC 模式下使用 **show isakmp ipsec-over tcp stats** 命令。

show isakmp ipsec-over-tcp stats

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	• 是	—
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
ASAv(1)	引入了 **show isakmp ipsec-over-tcp stats** 命令。
7.2(1)	弃用了 **show isakmp ipsec-over-tcp stats** 命令。**show crypto isakmp ipsec-over-tcp stats** 命令取而代之。
9.0(1)	增加了多情景模式支持。

使用指南

此命令的输出包括以下字段：

- Embryonic connections（初期连接数）
- Active connections（活动连接数）
- Previous connections（先前连接数）
- Inbound packets（入站数据包数）
- Inbound dropped packets（入站丢弃的数据包数）
- Outbound packets（出站数据包数）
- Outbound dropped packets（出站丢弃的数据包数）
- RST packets（RST 数据包）
- Received ACK heart-beat packets（收到的 ACK 心跳数据包数）
- Bad headers（错误报头数）
- Bad trailers（错误报尾数）
- Timer failures（计时器故障数）

- Checksum errors（校验和错误数）
- Internal errors（内部错误数）

示例

以下示例在全局配置模式下发出命令，显示 ISAKMP 统计信息：

```
ciscoasa(config)# show isakmp ipsec-over-tcp stats
Global IPsec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
crypto isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show isakmp sa

要显示 IKE 运行时 SA 数据库，请在全局配置模式或特权 EXEC 模式下使用 **show isakmp sa** 命令。

show isakmp sa [detail]

语法说明

detail	显示关于 SA 数据库的详细输出。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	• 是	—
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了 **show isakmp sa** 命令。
7.2(1)	此命令已弃用。**show crypto isakmp sa** 命令取代了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令的输出包括以下字段：

详细信息未指定。

IKE 对等设备	Type	Dir	Rky	状态
209.165.200.225	L2L	初始	否	MM_Active

详细信息已指定。

IKE 对等设备	Type	Dir	Rky	状态	加密	Hash	Auth	使用时间
209.165.200.225	L2L	初始	否	MM_Active	3des	md5	preshrd	86400

示例

以下示例在全局配置模式下输入，显示关于 SA 数据库的详细信息：

```
ciscoasa(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
```

```
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

相关命令

命令	说明
clear configure isakmp	清除所有 ISAKMP 配置。
clear configure isakmp policy	清除所有 ISAKMP 策略配置。
clear isakmp sa	清除 IKE 运行时 SA 数据库。
isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show isakmp stats

要显示运行时统计信息，请在全局配置模式或特权 EXEC 模式下使用 **show isakmp stats** 命令。

show isakmp stats

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	• 是	—
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
ASAv(1)	引入了 **show isakmp stats** 命令。
7.2(1)	此命令已弃用。**show crypto isakmp stats** 命令取代了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

每个计数器都映射到一个关联的 cikePhase1GW 计数器。有关每个计数器的详细信息，请参阅 CISCO-IPSEC-FLOW-MONITOR-MIB.my。

- Active/Standby Tunnels（主用 / 备用隧道数）- cikePhase1GWActiveTunnels
- Previous Tunnels（先前隧道数）- cikePhase1GWPreviousTunnels
- In Octets（输入八位字节数）- cikePhase1GWInOctets
- In Packets（输入数据包数）- cikePhase1GWInPkts
- In Drop Packets（输入丢弃数据包数）- cikePhase1GWInDropPkts
- In Notifys（输入通知数）- cikePhase1GWInNotifys
- In P2 Exchanges（输入 P2 交换数）- cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids（输入 P2 交换无效次数）- cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects（输入 P2 交换拒绝次数）- cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests（输入 P2 Sa 删除请求数）- cikePhase1GWInP2SaDelRequests
- Out Octets（输出八位字节数）- cikePhase1GWOutOctets
- Out Packets（输出数据包数）- cikePhase1GWOutPkts

- Out Drop Packets（输出丢弃数据包数）- cikePhase1GWOutDropPkts
- Out Notifys（输出通知数）- cikePhase1GWOutNotifys
- Out P2 Exchanges（输出 P2 交换数）- cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids（输出 P2 交换无效次数）- cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects（输出 P2 交换拒绝次数）- cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests（输出 P2 Sa 删除请求数）- cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels（发起方隧道数）- cikePhase1GWInitTunnels
- Initiator Fails（发起方失败次数）- cikePhase1GWInitTunnelFails
- Responder Fails（响应方失败次数）- cikePhase1GWRespTunnelFails
- System Capacity Fails（系统容量故障次数）- cikePhase1GWSysCapFails
- Auth Fails（验证失败次数）- cikePhase1GWAuthFails
- Decrypt Fails（解密失败次数）- cikePhase1GWDecryptFails
- Hash Valid Fails（哈希有效失败次数）- cikePhase1GWHashValidFails
- No Sa Fails（无 Sa 故障次数）- cikePhase1GWNoSaFails

此命令的输出包括以下字段：

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails

- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

示例

以下示例在全局配置模式下发出命令，显示 ISAKMP 统计信息：

```
ciscoasa(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

相关命令

命令	说明
clear configure isakmp	清除所有 ISAKMP 配置。
clear configure isakmp policy	清除所有 ISAKMP 策略配置。
clear isakmp sa	清除 IKE 运行时 SA 数据库。
isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show kernel

要显示 Linux brctl 实用程序提供的可用于调试的信息，请在特权 EXEC 模式下使用 **show kernel** 命令。

show kernel [process | bridge | cgroup-controller | ifconfig | module]

语法说明

bridge	显示 tap 网桥。
cgroup-controller	显示 cgroup-controller 统计信息。
ifconfig	显示 tap 和网桥接口统计信息。
module	显示已安装并且正在运行的模块。
process	显示 ASA 上运行的活动内核进程的当前状态。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。
8.4(1)	增加了 **cgroup-controller** 关键字。
8.6(1)	增加了 **ifconfig**、**module** 和 **bridge** 关键字。

使用指南

此命令显示内核中运行的各个进程的统计信息。

示例

以下示例展示 **show kernel process** 命令的输出：

```
ciscoasa# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
```

```
 69     5  20 -5           0         0 3725736671    S         0 aio/0
171     1  16  0      991232        80 3725684979    S         0 init
172   171  19  0      983040       268 3725684979    S         0 rcS
201   172  21  0     1351680       344 3725712932    S         0 lina_monitor
202   201  16  0 1017602048    899932 3725716348    S       212 lina
203   202  16  0 1017602048    899932           0    S         0 lina
204   203  15  0 1017602048    899932           0    S         0 lina
205   203  15  0 1017602048    899932 3725712932    S         6 lina
206   203  25  0 1017602048    899932           0    R 13069390 lina
ciscoasa#
```

表 9-1 显示每个字段的说明。

表 9-1　　show kernel process 字段

字段	说明
PID	进程 ID。
PPID	父进程 ID。
PRI	进程的优先级。
NI	nice（友好）值，用于优先级计算。值范围为 19（最友好）到 -19（对其他进程不友好）。
VSIZE	虚拟内存大小（以字节为单位）。
RSS	进程的驻留集大小（以千字节为单位）。
WCHAN	进程处于等待状态时所处的通道。
STAT	进程的状态： • R - 正在运行 • S - 在可中断等待状态下休眠 • D - 在不可中断磁盘休眠状态下等待 • Z - 僵停 • T - 跟踪或停止（基于信号） • P - 分页
RUNTIME	进程在用户模式和内核模式中已计划的节拍数。运行时是 utime 和 stime 的总和。
COMMAND	进程名。

以下示例展示 **show kernel module** 命令的输出：

```
ciscoasa# show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

以下示例展示 **show kernel ifconfig** 命令的输出：

```
ciscoasa# show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

相关命令

命令	说明
show module	显示有关 ASA 中安装的模块的信息。

show kernel bridge

要显示 Linux 网桥、其成员端口以及在每个端口获知的可用于调试的 MAC 地址，请在特权 EXEC 模式下使用 **show kernel bridge** 命令。

show kernel bridge [**mac-address** *bridge name*]

语法说明

bridge name	显示网桥名称。
mac-address	显示与每个端口关联的 MAC 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。

使用指南

此命令显示 Linux 网桥、其成员端口以及在每个端口获知的可用于调试的 MAC 地址（包括远程 MAC 地址）。

示例

以下示例展示 **show kernel bridge** 命令的输出：

```
ciscoasa# show kernel bridge

bridge name    bridge id        STP enabled interfaces
br0         8000.0e3cd8a8909f    no        tap1
                                tap3
br1        8000.26d29f51a490     no        tap2
                                tap4
                                tap5hostname#
```

以下示例展示 **show kernel bridge mac-address** 命令的输出：

```
ciscoasa# show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

相关命令

命令	说明
show kernel	显示有关 ASA 中安装的模块的信息。

show lacp

要显示流量统计信息、系统标识符和邻居详细信息等 EtherChannel LACP 信息，请在特权 EXEC 模式下输入此命令。

show lacp {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

语法说明

channel_group_number	（可选）指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
counters	显示用于已发送和接收的 LACPDU 和标记数量的计数器。
internal	显示内部信息。
neighbor	显示邻居信息。
sys-id	显示 LACP 系统 ID。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.4(1)	我们引入了此命令。

示例

以下是 **show lacp sys-id** 命令的输出示例：

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

以下是 **show lacp counters** 命令的输出示例：

```
ciscoasa# show lacp counters

              LACPDUs          Marker       Marker Response    LACPDUs
Port        Sent    Recv     Sent    Recv     Sent     Recv      Pkts Err
--------------------------------------------------------------------------
Channel group: 1
Gi3/1       736     728      0       0        0        0         0
Gi3/2       739     730      0       0        0        0         0
Gi3/3       739     732      0       0        0        0         0
```

以下是 **show lacp internal** 命令的输出示例：

```
ciscoasa# show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

以下是 **show lacp neighbor** 命令的输出示例：

```
ciscoasa# show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

show lacp cluster

要显示 cLACP 系统 MAC 和 ID，请在特权 EXEC 模式下使用 **show lacp cluster** 命令。

show lacp cluster {**system-mac** | **system-id**}

语法说明

system-mac	显示系统 ID 以及它是自动生成还是手动输入的。
system-id	显示系统 ID 和优先级。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

使用 **clacp system-mac** 命令设置 cLACP 系统 ID 和优先级。

示例

以下是 **show lacp cluster system-mac** 命令的输出示例：

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

以下是 **show lacp cluster system-id** 命令的输出示例：

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5    ,a300.010a.010a
```

相关命令

命令	说明
clacp system-mac	设置 cLACP 系统 ID 和优先级。

show license

要显示智能许可状态，请在特权 EXEC 模式下使用 **show license** 命令。

注　此功能仅适用于 ASAv。

show license [all | entitlement | cert | pool | registration | features

语法说明

all	显示智能许可的状态、智能代理版本、UDI 信息、智能代理状态、全球合规性状态、授权状态、许可证书信息和计划智能代理任务。
entitlement	显示每个使用中的授权及其句柄（即整数 ID）、计数、标记、实施模式（例如，合规、不合规等）、版本和授权请求时间的详细信息。
cert	显示 ID 证书内容、签发日期和到期日期。
pool	显示此设备分配到的授权池。
registration	显示当前的智能许可证注册状态。
features	显示当前许可证。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.3(2)	我们引入了此命令。

使用指南

show activation-key 命令提供与 show license features 命令相同的输出。

示例

以下示例展示只有基本许可证（无最新许可证授权）的 ASAv：

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
```

```
Inside Hosts                        : Unlimited      perpetual
Failover                            : Active/Standby perpetual
Encryption-DES                      : Enabled        perpetual
Encryption-3DES-AES                 : Enabled        perpetual
Security Contexts                   : 0              perpetual
GTP/GPRS                            : Disabled       perpetual
AnyConnect Premium Peers            : 2              perpetual
AnyConnect Essentials               : Disabled       perpetual
Other VPN Peers                     : 250            perpetual
Total VPN Peers                     : 250            perpetual
Shared License                      : Disabled       perpetual
AnyConnect for Mobile               : Disabled       perpetual
AnyConnect for Cisco VPN Phone      : Disabled       perpetual
Advanced Endpoint Assessment        : Disabled       perpetual
UC Phone Proxy Sessions             : 2              perpetual
Total UC Proxy Sessions             : 2              perpetual
Botnet Traffic Filter               : Enabled        perpetual
Intercompany Media Engine           : Disabled       perpetual
Cluster                             : Disabled       perpetual
```

相关命令

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clear configure license	清除智能许可配置。
feature tier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
license smart	让您为智能许可请求许可证授权。
license smart deregister	从许可证颁发机构注销设备。
license smart register	向许可证颁发机构注册设备。
license smart renew	续订注册或许可证授权。
service call-home	启用 Smart Call Home。
show running-config license	显示智能许可配置。
throughput level	设置智能许可的吞吐量级别。

show local-host

要显示本地主机的网络状态，请在特权 EXEC 模式下使用 **show local-host** 命令。

show local-host | include interface [*ip_address*] [**detail**] [**all**][**brief**] [**connection** {**tcp** *start*[-*end*] | **udp** *start*[-*end*] | **embryonic** *start*[-*end*]}] [**zone** [*zone-name*]]

语法说明

all	（可选）包括连接到 ASA 和连接自 ASA 的本地主机。
brief	（可选）显示有关本地主机的简要信息。
connection	（可选）根据连接的编号和类型显示三种类型的过滤器：TCP、UDP 和初期。这些过滤器可以单独使用也可以联合使用。
detail	（可选）显示本地主机信息的详细网络状态，包括有关活动 xlate 和网络连接的详细信息。
include interface	指定每个接口上将使用的 IP 地址。
ip_address	（可选）指定本地主机 IP 地址。
zone [*zone_name*]	（可选）指定每个区域的本地主机。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	对于有主机限制的型号，此命令现在显示将哪个接口视为外部接口。
7.2(4)	**show local-host** 命令增加了两个新选项 **connection** 和 **brief**，以便按内部主机的连接数过滤输出。
9.1(2)	发送到思科用于基于遥测的警报的 Smart Call Home 信息以前来自 **show local-host** 命令，此版本更改为来自 **show local-host	include interface** 命令。
9.3(2)	添加了 **zone** 关键字。

使用指南

show local-host 命令可显示本地主机的网络状态。对于任何将流量转发到 ASA 或通过其转发流量的主机，将为其创建一个本地主机。

此命令可显示本地主机的转换和连接插槽。当常规转换和连接状态可能不适用时，此命令为使用 **nat 0 access-list** 命令配置的主机提供信息。

此命令还显示连接限制值。如果未设置连接限制，值将显示为 0 并且不应用限制。

对于有主机限制的型号，在路由模式下，仅当内部主机（工作和家庭区域）与外部（互联网区域）通信时，它们才计入限制范围。互联网主机不计入限制范围。在工作区域和家庭区域之间发起流量的主机也不计入限制范围。与默认路由关联的接口被视为互联网接口。如果没有默认路由，所有接口上的主机都计入限制范围。在透明模式下，主机数量最低的接口计入主机限制范围。

发生 SYN 攻击（已配置 TCP 拦截）时，**show local-host** 命令输出将已拦截连接数包括在使用计数中。此字段通常仅显示完全开放的连接。

在 **show local-host** 命令输出中，当为使用静态连接的主机配置了最大初期限制（TCP 拦截水印）时，使用**主机的 TCP 初期连接计数器**。此计数器显示从其他主机到该主机的初期连接总数。如果此总数超过配置的最大限制，将对到主机的新连接应用 TCP 拦截。

示例

以下是 **show local-host** 命令的输出示例：

```
ciscoasa# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

以下是对具有主机限制的 ASA 执行 **show local-host** 命令的输出示例：

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface.Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

以下是对具有主机限制的 ASA 执行 **show local-host** 命令的输出示例。但在没有默认路由时，主机限制将应用到所有接口。如果默认路由或该路由使用的接口发生故障，则可能检测不到默认路由接口。

```
ciscoasa# show local-host
Unable to determine Internet interface from default route.Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

以下是对不限制主机的 ASA 执行 **show local-host** 命令的输出示例：

```
ciscoasa# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

以下示例展示本地主机的网络状态：

```
ciscoasa# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
```

```
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

以下示例展示具有至少 4 个 UDP 连接以及同时具有 1 到 10 个 TCP 连接的所有主机：

```
ciscoasa# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
        watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
        Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
        10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
        10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
        maximum active, 0 denied
```

以下示例展示当使用 **brief** 选项时的本地主机地址和连接计数器：

```
ciscoasa# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited
        TCP embryonic count to host = 0
        TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

以下示例展示当使用 **brief** 和 **connection** 选项时的输出：

```
ciscoasa# show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

ciscoasa# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

相关命令

命令	说明
clear local-host	释放通过 **show local-host** 命令显示的本地主机的网络连接。
nat	将网络与全局 IP 地址池关联。

show logging

要显示缓冲区中的日志或其他记录设置，请在特权 EXEC 模式下使用 **show logging** 命令。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

语法说明

all	（可选）显示所有系统日志消息 ID，以及它们是启用还是禁用。
asdm	（可选）显示 ASDM 记录缓冲区内容。
message	（可选）显示非默认级别的消息。请参阅 **logging message** 命令来设置消息级别。
queue	（可选）显示系统日志消息队列。
setting	（可选）显示记录设置，而不显示记录缓冲区。
syslog_id	（可选）指定要显示的消息编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	指示是否将系统日志服务器配置为使用 SSL/TLS 连接。
8.4(1)	对于 **show logging** 命令，输出包括审核块当前状态的条目。

使用指南

如果正在使用 **logging buffered** 命令，不带任何关键字的 **show logging** 命令将显示当前消息缓冲区和当前设置。

show logging queue 命令可用于显示以下内容：

- 队列中的消息数量
- 队列中记录的最大消息数量
- 由于块内存无法处理而被丢弃的消息数量
- 用于陷阱和其他系统日志消息的单独队列

注　零是可接受的已配置队列大小，表示允许最大队列大小。如果配置的队列大小为零，**show logging queue** 命令的输出将显示实际队列大小。

示例

以下是 **show logging** 命令的输出示例：

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

注　*state* 的有效值为 enabled（启用）、disabled（禁用）、disabled-blocking（禁用阻塞）和 disabled-not blocking（禁用未阻塞）。

以下是配置了安全系统日志服务器后 **show logging** 命令的输出示例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
ciscoasa(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

以下是 **show logging queue** 命令的输出示例：

```
ciscoasa(config)# show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

以下是 **show logging message all** 命令的输出示例：

```
ciscoasa(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
```

```
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

相关命令

命令	说明
logging asdm	启用记录到 ASDM。
logging buffered	启用记录到缓冲区。
logging host	Defines a syslog server.
logging message	设置消息级别或禁用消息。
logging queue	配置记录队列。

show logging flow-export-syslogs

要显示其信息还会被 NetFlow 捕获以及将受到 **logging flow-export-syslogs enable | disable** 命令影响的所有系统日志消息，请在特权 EXEC 模式下使用 **show logging flow-export-syslogs** 命令。

show logging flow-export-syslogs

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.1(1)	引入了此命令。

使用指南

在输入 **logging flow-export syslogs disable** 命令后，请确保您了解哪些系统日志消息已被禁用。禁用的系统日志消息如下：

系统日志消息	说明
106015	TCP 流量被拒绝，因为第一个数据包不是 SYN 数据包。
106023	通过 **access-group** 命令连接到接口的入口 ACL 或出口 ACL 拒绝流。
106100	ACL 允许或拒绝的流。
302013 和 302014 的流量	TCP 连接和删除。
302015 和 302016 的流量	UDP 连接和删除。
302017 和 302018 的流量	GRE 连接和删除。
302020 和 302021 的流量	ICMP 连接和删除。
313001	发送到 ASA 的 ICMP 数据包被拒绝。
313008	发送到 ASA 的 ICMPv6 数据包被拒绝。
710003	连接到 ASA 的尝试被拒绝。

示例

以下是 **show logging flow-export-syslogs** 命令的输出示例，其中列出了将禁用的系统日志消息：

```
ciscoasa(config)# show logging flow-export-syslogs

Syslog ID          Type                 Status
302013           Flow Created          Enabled
302015           Flow Created          Enabled
302017           Flow Created          Enabled
302020           Flow Created          Enabled
302014           Flow Deleted          Enabled
302016           Flow Deleted          Enabled
302018           Flow Deleted          Enabled
302021           Flow Deleted          Enabled
106015           Flow Denied           Enabled
106023           Flow Denied           Enabled
313001           Flow Denied           Enabled
313008           Flow Denied           Enabled
710003           Flow Denied           Enabled
106100           Flow Created/Denied   Enabled
```

相关命令

命令	说明
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate *minutes*	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

show logging rate-limit

要显示禁止的系统日志消息，请在特权 EXEC 模式下使用 **show logging rate-limit** 命令。

show logging rate-limit

语法说明

此命令没有任何参数或关键字。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

清除信息后，不会再显示任何内容，直到主机重新建立连接。

示例

以下示例展示 **show logging rate-limit** 命令的输出：

```
ciscoasa(config)# show logging rate-limit
%ASA-7-710005: TCP request discarded from 171.69.39.0/2678 to management:10.89.130.244/443
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =   0x0807C0FA
%ASA-6-106015: Deny TCP (no connection) from 171.69.39.0/2685 to 10.89.130.244/443 flags
FIN PSH ACK  on interface management
%ASA-7-710005: TCP request discarded from 171.69.39.0/2685 to management:10.89.130.244/443
%ASA-6-302013: Built inbound TCP connection 2116 for management:171.69.39.0/2689
(171.69.39.0/2689) to identity:10.89.130.244/443 (10.89.130.244/443)
%ASA-6-725001: Starting SSL handshake with client management:171.69.39.0/2689 for TLSv1
session.
%ASA-6-725003: SSL client management:171.69.39.0/2689 request to resume previous session.
%ASA-6-725002: Device completed SSL handshake with client management:171.69.39.0/2689
%ASA-6-605005: Login permitted from 171.69.39.0/2689 to management:10.89.130.244/https for
user "enable_15"
%ASA-5-111007: Begin configuration: 171.69.39.0 reading from http [POST]
```

相关命令

命令	说明
show logging	显示已启用的日志记录选项。

show mac-address-table

要显示 MAC 地址表，请在特权 EXEC 模式下使用 **show mac-address-table** 命令。

show mac-address-table [*interface_name* | **count** | **static**]

语法说明

count	（可选）列出动态和静态条目的总数。
interface_name	（可选）标识要查看其 MAC 地址表条目的接口名称。
static	（可选）仅列出静态条目。

默认值

如果不指定接口，将显示所有接口 MAC 地址条目。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	—	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mac-address-table** 命令的输出示例：

```
ciscoasa# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

以下是对内部接口执行 **show mac-address-table** 命令的输出示例：

```
ciscoasa# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

以下是 **show mac-address-table count** 命令的输出示例：

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

相关命令

命令	说明
firewall transparent	将防火墙模式设置为透明。
mac-address-table aging-time	为动态 MAC 地址条目设置超时。
mac-address-table static	向 MAC 地址表添加静态 MAC 地址条目。
mac-learn	禁用 MAC 地址学习。

show management-access

要显示为管理访问配置的内部接口的名称，请在特权 EXEC 模式下使用 show management-access 命令。

show management-access

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

通过 **management-access** 命令，您可使用在 *mgmt_if* 中指定的防火墙接口的 IP 地址定义内部管理接口。（接口名称通过 **nameif** 命令定义，并在 **show interface** 命令的输出中用引号 " " 括起显示。）

示例

以下示例展示如何将名为 “inside” 的防火墙接口配置为管理访问接口并显示结果：

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show management-access
management-access inside
```

相关命令

命令	说明
clear configure management-access	删除 ASA 的管理访问内部接口的配置。
management-access	配置用于管理访问的内部接口。

show mdm-proxy sessions

显示当前活动的 MDM 代理会话。

show mdm-proxy sessions [checkin | enrollment]

语法说明

仅指定 **checkin** 则仅显示签入会话，仅指定 **enrollment** 则仅显示已注册会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(1)	引入了此命令。

相关命令

命令	说明
mdm-proxy	进入 config-mdm-proxy 模式以配置 MDM 代理服务。

show mdm-proxy statistics

显示 MDM 代理服务统计信息。

show mdm-proxy statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(1)	引入了此命令。

示例

```
ciscoasa (config)# show mdm-proxy statistics<cr>

MDM proxy statistics:
=====================
Total number of successful MDM enrollments: 1230
Number of active MDM enrollments: 10
Maximum number of simultaneously active MDM enrollments: 90
Minimum duration of an MDM enrollment: 4 seconds
Maximum duration of an MDM enrollment: 25 seconds
Total number of failed MDM enrollments due to authentication failure: 23
Total number of failed MDM enrollments due to SCEP enrollment failure: 28.
Total number of failed MDM enrollments: 61
Total number of successful MDM check-ins: 3167
Number of active MDM check-ins: 26
Maximum number of simultaneously active MDM check-ins: 316
Minimum duration of an MDM check-in: 3 seconds
Maximum duration of an MDM check-in: 21 seconds
Total number of failed MDM check-ins: 118
```

相关命令

命令	说明
clear mdm-proxy statistics	清除 MDM 代理计数器，将其设置为零。
mdm-proxy	进入 config-mdm-proxy 模式以配置 MDM 代理服务。

show memory

要显示最大物理内存及操作系统当前可用空闲内存的摘要，请在特权 EXEC 模式下使用 **show memory** 命令。

[cluster exec] show memory [detail]

语法说明

cluster exec	（可选）在集群环境中，让您在一个设备中发出 **show memory** 命令，同时在所有其他设备中运行该命令。
detail	（可选）显示空闲和已分配的系统内存的详细视图。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了 **cluster exec** 选项。
9.2(1)	向输出中增加了虚拟机 (VM) 统计信息以支持 ASAv。
9.3(2)	在 **show memory detail** 命令中，内存管理器已被标准 glibc 库取代。

使用指南

show memory 命令可显示最大物理内存及操作系统当前可用空闲内存的摘要。内存会根据需要进行分配。

还可以使用 SNMP 显示 **show memory** 命令的信息。

可以将 **show memory detail** 输出与 **show memory binsize** 命令一起使用来调试内存泄漏。

show memory detail 命令输出可分为三个部分：摘要、DMA 内存和 HEAP 内存。摘要显示内存的总体分配方式。未绑定到 DMA 或保留的内存被视为 HEAP 内存。Free Memory（空闲内存）值是 HEAP 中的未使用内存。Allocated memory in use（使用中的已分配内存）值是已分配的 HEAP 数量。HEAP 分配的细目随后显示在输出中。保留内存和 DMA 保留内存主要被 VPN 服务使用，也被不同的系统进程使用。

空闲内存分为两部分：空闲内存堆和空闲内存系统。空闲内存堆是 glibc 堆中的空闲内存量。当 glibc 堆按需增长和缩减时，空闲堆内存的量并不指示系统中剩余的总内存。空闲内存系统表示 ASA 可用的空闲内存量。

保留内存 (DMA) 是为 DMA 池保留的内存量。内存开销是各种运行进程的 glibc 开销和进程开销。

在 **show memory detail** 命令输出中，已分配内存统计合计（字节）列中显示的值未反映实际值 (MEMPOOL_GLOBAL_SHARED POOL STATS)。

输出表明，先分配了大小为 49,152 的块，随后该块返回到空闲池，并分配了另一个大小为 131,072 的块。在这种情况下，您会认为空闲内存减少了 131,072-49,152=81,920 字节，但实际上减少了 100,000 字节（请参阅 Free memory 行）。

```
ciscoasa# show memory detail

MEMPOOL_GLOBAL_SHARED POOL STATS:           MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =   1862270976  Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99  Number of free chunks       =          100
Number of mmapped regions   =            0  Number of mmapped regions   =            0
Mmapped bytes allocated     =            0  Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976  Max memory footprint        =   1862270976
Keepcost                    =   1762019304  Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304  Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944  Allocated memory in use     =    100233944
Free memory                 =   1762137032  Free memory                 =   1762037032


----- fragmented memory statistics -----    ----- fragmented memory statistics -----

 fragment size       count          total     fragment size       count          total
    (bytes)                        (bytes)       (bytes)                        (bytes)
----------------  ----------  -------------- ----------------  ----------  --------------
        32768             1          33176           32768             1          33176
                                                      49152             1          50048
   1762019304             1     1762019304*     1761869256             1     1761869256*


----- allocated memory statistics -----     ----- allocated memory statistics -----

 fragment size       count          total     fragment size       count          total
    (bytes)                        (bytes)       (bytes)                        (bytes)
----------------  ----------  -------------- ----------------  ----------  --------------
        49152            10         491520           49152             9         442368
        65536           125        8192000           65536           125        8192000
        98304             3         294912           98304             3         294912
       131072            18        2359296          131072            19        2490368
```

以下输出确认分配了大小为 150,000 而不是 131,072 的块：

```
ciscoasa# show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

按照设计，**show memory detail** 命令输出中显示的总字节数是近似值。这有两个原因：

- 对于每个分段大小，如果您需要获取所有分段的总和，将会影响性能，因为可能有大量分配对应单个分段大小，要获得准确值，需要查遍数千个区块。
- 对于每个 binsize，您需要查遍双重链接的分配列表，并且可能有多个分配。在这种情况下，您不能长时间占用 CPU，需要定期暂停分配。在恢复分配之后，其他进程可能已分配或取消分配内存，内存状态可能已发生变化。因此，总字节数列提供近似值而不是实际值。

示例

以下是 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

以下是 **show memory detail** 命令的输出示例：

```
ciscoasa# show memory detail
Free memory heap:                 2473071872 bytes (xx%)
 Free memory system:               xxxxxxxxxx bytes (xx%)
 Used memory:
      Allocated memory in use:      308939520 bytes (xx%)
      Reserved memory (DMA):        1512955904 bytes (xx%)
      Memory overhead:              xxxxxxxxx bytes (xx%)
 ----------------------------   ------------------
 Total memory:                    4294967296 bytes (100%)
------------------------------------------------------
Total memory:                   268435456 bytes (100%)
Dynamic Shared Objects(DSO):           0 bytes
DMA memory:
  Unused memory:                 3212128 bytes (8%)
  Crypto reserved memory:        2646136 bytes (7%)
  Crypto free:                   1605536 bytes (4%)
  Crypto used:                   1040600 bytes (3%)
  Block reserved memory:        33366816 bytes (85%)
  Block free:                   31867488 bytes (81%)
  Block used:                    1499328 bytes (4%)
  Used memory:                    178440 bytes (0%)
------------------------------------------------------
  Total memory:                 39403520 bytes (100%)
  HEAP memory:
  Free memory:                 130546920 bytes (80%)
  Used memory:                  33030808 bytes (20%)
  Init used memory by library:   4218752 bytes (3%)
  Allocated memory:            28812056 bytes (18%)
------------------------------------------------------
  Total memory:                 163577728 bytes (100%)

Least free memory: 122963528 bytes (75%)
Most used memory:   40614200 bytes (25%)

----- fragmented memory statistics -----

fragment size    count      total
(bytes)                     (bytes)
---------------- ---------- --------------
16               113        1808

<More>
```

以下是在 ASA 5525 上启用 **jumbo-frame reservation** 命令并发出 **write memory** 命令和 **reload** 命令后 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        3008918624 bytes (70%)
Used memory:        1286048672 bytes (30%)
-------------       ----------------------
Total memory:       4294967296 bytes (100%)
```

以下是在 ASA 5525 上未启用 **jumbo-frame reservation** 命令时 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        3318156400 bytes (77%)
Used memory:         976810896 bytes (23%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

以下是在 ASA 5515 上启用 **jumbo-frame reservation** 命令后 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        3276619472 bytes (76%)
Used memory:        1018347824 bytes (24%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

以下是在 ASA 5515 上未启用 **jumbo-frame reservation** 命令时 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        3481145472 bytes (81%)
Used memory:         813821824 bytes (19%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

以下是在 ASA 5585 上启用 **jumbo-frame reservation** 命令后 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        8883297824 bytes (69%)
Used memory:        4001604064 bytes (31%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

以下是在 ASA 5585 上未启用 **jumbo-frame reservation** 命令时 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:        9872205104 bytes (77%)
Used memory:        3012696784 bytes (23%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

以下是在不支持 **jumbo-frame** 命令的 ASA 5520 上 **show memory** 命令的输出示例：

```
ciscoasa# show memory
ree memory:         206128232 bytes (38%)
Used memory:         330742680 bytes (62%)
-------------       -----------------
Total memory:        536870912 bytes (100%)
```

以下是在不支持 **jumbo-frame** 命令的 ASA 5505 上 **show memory** 命令的输出示例：

```
ciscoasa# show memory
Free memory:          48457848 bytes (18%)
Used memory:         219977608 bytes (82%)
-------------        -----------------
Total memory:        268435456 bytes (100%
```

以下是 ASAv 上 **show memory** 命令的输出示例：

```
Free memory:        2694133440 bytes (63%)
Used memory:        1600833856 bytes (37%)
-------------     ------------------
Total memory:       4294967296 bytes (100%)

Virtual platform memory
-----------------------
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

相关命令

命令	说明
show memory profile	显示 ASA 内存使用情况（分析）的信息。
show memory binsize	显示为特定存储空间分配的区块的摘要信息。

show memory api

要显示系统中注册的 malloc 栈 API，请在特权 EXEC 模式下使用 **show memory api** 命令。

show memory api

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示系统中注册的 malloc 栈 API。

如果开启任意内存调试功能（即无延迟毒化器、内存跟踪器或内存分析器），其 API 将显示在 **show memory api** 命令输出中。

示例

以下是 **show memory api** 命令的输出示例：

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

相关命令

命令	说明
show memory profile	显示 ASA 内存使用情况（分析）的信息。
show memory binsize	显示为特定存储空间分配的区块的摘要信息。

show memory app-cache

要按应用观察内存使用情况，请在特权 EXEC 模式下使用 **show memory app-cache** 命令。

show memory app-cache [**threat-detection** | **host** | **flow** | **tcb** | **http** | **access-list**] [**detail**]

语法说明

access-list	（可选）显示用于访问列表的应用级别内存缓存。
detail	（可选）显示空闲和已分配的系统内存的详细视图。
flow	（可选）显示用于流的应用级别内存缓存。
host	（可选）显示用于主机的应用级别内存缓存。
http	（可选）显示用于 HTTP 的应用级别内存缓存。
tcb	（可选）显示 TCB 的应用级别内存缓存。
threat-detection	（可选）显示用于威胁检测的应用级别内存缓存。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(1)	引入了此命令。
8.1(1)	增加了 **access-list** 和 **http** 选项。

使用指南

此命令可用于按应用观察内存使用情况。

示例

以下是 **show memory app-cache threat-detection** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache threat-detection
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

以下是 **show memory app-cache threat-detection detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
```

```
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

以下是 **show memory app-cache host detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

以下是 **show memory app-cache flow detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

以下是 **show memory app-cache access-list detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768
```

以下是 **show memory app-cache http detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
```

```
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0
```

以下是 **show memory app-cache tcb detail** 命令的输出示例：

```
ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

相关命令

命令	说明
show memory profile	显示 ASA 内存使用情况（分析）的信息。
show memory binsize	显示为特定存储空间分配的区块的摘要信息。
show memory	显示最大物理内存及操作系统当前可用内存的摘要。

show memory binsize

要显示为特定 bin 大小分配的区块的摘要信息，请在特权 EXEC 模式下使用 **show memory binsize** 命令。

show memory binsize *size*

语法说明

size	显示特定 bin 大小的区块（内存块）。bin 大小来自于 **show memory detail** 命令输出的 “fragment size”（分段大小）列。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令没有使用指南。

示例

以下示例展示为一个大小为 500 的 bin 分配的区块的摘要信息：

```
ciscoasa# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

相关命令

命令	说明
show memory-caller address	显示 ASA 上配置的地址范围。
show memory profile	显示 ASA 内存使用情况（分析）的信息。
show memory	显示最大物理内存及操作系统当前可用内存的摘要。

show memory delayed-free-poisoner

要显示 **memory delayed-free-poisoner** 队列使用情况的摘要，请在特权 EXEC 模式下使用 **show memory delayed-free-poisoner** 命令。

show memory delayed-free-poisoner

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **clear memory delayed-free-poisoner** 命令可清除队列和统计信息。

示例

以下是 **show memory delayed-free-poisoner** 命令的输出示例：

```
ciscoasa# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
         3335600:  memory held in queue
            6095:  current queue count
               0:  elements dequeued
               3:  frees ignored by size
            1530:  frees ignored by locking
              27:  successful validate runs
               0:  aborted validate runs
        01:09:36:  local time of last validate
```

表 9-2 介绍了 **show memory delayed-free-poisoner** 命令输出中的重要字段。

表 9-2　　show memory delayed-free-poisoner 命令输出说明

字段	说明
memory held in queue	无延迟内存毒化器工具队列中保留的内存。如果未启用无延迟内存毒化器工具，则此类内存在 **show memory** 输出中通常为 “ 任意 ” 数量。
current queue count	队列中的元素数量。
elements dequeued	已从队列中删除的元素的数量。当系统中的大部分或全部其他空闲内存最终保留在队列中时，此数量开始增加。
frees ignored by size	由于请求过小无法保留所需跟踪信息而导致未放入队列的自由请求的数量。
frees ignored by locking	由于多个应用正在使用内存而导致被工具拦截且未放入队列的自由请求的数量。最后一个将内存释放回系统的应用最终会将此类内存区域放入队列。
successful validate runs	自启用监控或使用 **clear memory delayed-free-poisoner** 命令清除监控以来，验证队列内容（自动或通过 **memory delayed-free-poisoner validate** 命令）的次数。
aborted validate runs	自启用监控或使用 **clear memory delayed-free-poisoner** 命令清除监控以来，由于一次有多个任务试图使用队列而导致检查队列内容的请求（定期运行或来自 CLI 的验证请求）被中止的次数。
local time of last validate	上次验证运行完成时的本地系统时间。

相关命令

命令	说明
clear memory delayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。
memory delayed-free-poisoner enable	启用 delayed free-memory poisoner 工具。
memory delayed-free-poisoner validate	强制验证 delayed free-memory poisoner 工具队列中的元素。

show memory profile

要显示有关 ASA 的内存使用（内存分析）的信息，请在特权 EXEC 模式下使用 **show memory profile** 命令。

show memory profile [peak] [detail | collated | status]

语法说明

collated	（可选）整理显示的内存信息。
detail	（可选）显示详细的内存信息。
peak	（可选）显示峰值捕获缓冲区而不是 “ 使用中 ” 缓冲区。
status	（可选）显示内存分析和峰值捕获缓冲区的当前状态。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **show memory profile** 命令可对内存使用级别和内存泄漏进行故障排除。即使内存分析已停止，您仍然可以查看分析缓冲区内容。开始内存分析将自动清除该缓冲区。

注　启用内存分析时，ASA 的性能可能会临时下降。

示例

以下是 **show memory profile** 命令的输出示例：

```
ciscoasa# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail 命令的输出分为六个数据列和最左侧的一个标题列。与第一个数据列对应的内存桶的地址在标题列给定（十六进制数）。数据本身是通过桶地址中的文本 / 代码保存的字节数。数据列中的句点 (.) 表示此内存桶处的文本未保留内存。行中的其他列对应于大于前一列增量的桶地址。例如，第一行中第一个数据列的地址桶为 0x001069e0。第一行中第二个数据列的地址桶为 0x001069e4，依此类推。通常标题列地址是下一个桶地址；即，前一行的最后一个数据列的地址加上增量。所有未使用的行都不会显示。若不显示多个连续的此类行，用标题列中的三个句点 (...) 指示。

以下是 **show memory profile detail** 命令的输出示例：

```
ciscoasa# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

以下是 **show memory profile collated** 命令的输出示例：

```
ciscoasa# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

以下是 **show memory profile peak** 命令的输出示例，其中显示了峰值捕获缓冲区：

```
ciscoasa# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

以下是 **show memory profile peak detail** 命令的输出示例，其中显示了峰值捕获缓冲区和通过相应桶地址中的文本 / 代码保存的字节数：

```
ciscoasa# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c .. 102400 ...
```

以下是 **show memory profile status** 命令的输出示例，其中显示了内存分析和峰值捕获缓冲区的当前状态：

```
ciscoasa# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

相关命令

命令	说明
memory profile enable	启用对内存使用（内存分析）的监控。
memory profile text	配置要分析的内存的程序文本范围。
clear memory profile	清除内存分析功能保留的内存缓冲区。

show memory top-usage

要显示 **show memory detail** 命令输出中数量排在前面的已分配分段大小，请在特权 EXEC 模式下使用 **show memory top-usage** 命令。

show memory top-usage [*num*]

语法说明

num	（可选）在列表中显示 bin 大小的数量。有效值为 1 到 64。

默认值

num 的默认值为 10。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.4(6)	引入了此命令。

使用指南

使用 **show memory top-usage** 命令可显示 **show memory detail** 命令输出中数量排在前面的已分配分段大小。

此命令不使用集群，因此在启用集群时不需要禁用。

示例

以下是 **show memory top-usage** 命令的输出示例：

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
      1572864             9       14155776
     12582912             1       12582912
      6291456             1        6291456

----- Binsize PC top usage -----

Binsize: 1572864               total (bytes): 14155776

pc = 0x805a870, size = 16422399 , count = 9
```

```
Binsize: 12582912               total (bytes): 12582912

pc = 0x805a870, size = 12960071 , count = 1

Binsize: 6291456                total (bytes): 6291456

pc = 0x9828a6c, size = 7962695  , count = 1


MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912             1       12582912
      2097152             6       12582912
        65536           181       11862016

----- Binsize PC top usage -----

Binsize: 12582912               total (bytes): 12582912

pc = 0x8249763, size = 37748736 , count = 1

Binsize: 2097152                total (bytes): 12582912

pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1

Binsize: 65536                  total (bytes): 11862016

pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1
```

相关命令

命令	说明
show memory tracking	显示所有当前已收集的信息。

show memory tracking

要显示工具跟踪的当前已分配内存，请在特权 EXEC 模式下使用 **show memory tracking** 命令。

show memory tracking [**address** | **dump** | **detail**]

语法说明

address	（可选）按地址显示内存跟踪。
detail	（可选）显示内存跟踪状态。
dump	（可选）显示内存跟踪地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

使用 **show memory tracking** 命令可显示工具跟踪的当前已分配内存。

示例

以下是 **show memory tracking** 命令的输出示例：

```
ciscoasa# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

以下是 **show memory tracking address** 命令的输出示例：

```
ciscoasa# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154

memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
```

```
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2
```

以下是 **show memory tracking dump** 命令的输出示例：

```
ciscoasa# show memory tracking dump
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

相关命令

命令	说明
clear memory tracking	清除所有当前已收集的信息。

show memory webvpn

要生成 WebVPN 的内存使用情况统计信息，请在特权 EXEC 模式下使用 **show memory webvpn** 命令。

show memory webvpn [**allobjects** | **blocks** | **dumpstate** [**cache** | **disk0** | **disk1** | **flash** | **ftp** | **system** | **tftp**] | **pools** | **profile** [**clear** | **dump** | **start** | **stop**] | **usedobjects** {{**begin** | **exclude** | **grep** | **include**} **line** *line*}]

语法说明

allobjects	显示池、块以及所有已使用和已释放对象的 WebVPN 内存消耗详细信息。
begin	从匹配的行开始。
blocks	显示内存块的 WebVPN 内存消耗详细信息。
cache	指定 WebVPN 内存缓存状态转储的文件名。
clear	清除 WebVPN 内存配置。
disk0	指定 WebVPN 内存 disk0 状态转储的文件名。
disk1	指定 WebVPN 内存 disk1 状态转储的文件名。
dump	将 WebVPN 内存配置放入文件。
dumpstate	将 WebVPN 内存状态放入文件。
exclude	排除匹配的行。
flash	指定 WebVPN 内存闪存状态转储的文件名。
ftp	指定 WebVPN 内存 FTP 状态转储的文件名。
grep	包括或排除匹配的行。
include	包括匹配的行。
line	标识要匹配的行。
line	指定要匹配的行。
pools	显示内存池的 WebVPN 内存消耗详细信息。
profile	获取 WebVPN 内存配置并将其放入文件。
system	指定 WebVPN 内存系统状态转储的文件名。
start	开始收集 WebVPN 内存分析。
stop	停止获取 WebVPN 内存分析。
tftp	指定 WebVPN 内存 TFTP 状态转储的文件名。
usedobjects	显示已使用对象的 WebVPN 内存消耗详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

示例

以下是 **show memory webvpn allobjects** 命令的输出示例：

```
ciscoasa# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

相关命令

命令	说明
memory-size	设置 WebVPN 服务在 ASA 上可以使用的内存量。

show memory-caller address

要显示 ASA 上配置的地址范围，请在特权 EXEC 模式下使用 **show memory-caller address** 命令。

show memory-caller address

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

必须先使用 **memory caller-address** 命令配置地址范围，才能使用 **show memory-caller address** 命令显示它们。

示例

以下示例展示如何使用 **memory caller-address** 命令配置地址范围，以及 **show memory-caller address** 命令生成的输出：

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

如果在输入 **show memory-caller address** 命令之前未配置地址范围，则不会显示任何地址：

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
```

相关命令

命令	说明
memory caller-address	配置调用方 PC 的内存块。

show mfib

要显示有关转发条目和接口的 MFIB 信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib** 命令。

show mfib [*group* [*source*]] [**verbose**] [**cluster**]

语法说明

cluster	（可选）显示 MFIB 日期和当前计时器值。
group	（可选）显示组播组的 IP 地址。
source	（可选）显示组播路由源的 IP 地址。这是采用四点分十进制记数法的单播 IP 地址。
verbose	（可选）显示有关条目的附加信息。

默认值

如果没有可选参数，则显示所有组的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	**修改**
7.0(1)	引入了此命令。
9.0(1)	增加了 **cluster** 关键字。仅适用于 ASA 5580 和 5585-X。

示例

以下是 **show mfib** 命令的输出示例：

```
ciscoasa# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

相关命令

命令	**说明**
show mfib verbose	显示有关转发条目和接口的详细信息。

show mfib active

要显示活动组播源，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib active** 命令。

show mfib [*group*] **active** [*kbps*]

语法说明

group	（可选）组播组的 IP 地址。
kbps	（可选）将显示限制为大于或等于此值的组播流。

此命令没有任何参数或关键字。

默认值

kbps 的默认值为 4。如果未指定 *group*，将显示所有组。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show mfib active 命令的输出显示表示速率 PPS 的正数或负数。当 RPF 数据包发生故障或路由器观察到具有传出接口 (OIF) 列表的 RPF 数据包时，ASA 显示负数。此类型的活动可能指示组播路由问题。

示例

以下是 **show mfib active** 命令的输出示例：

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

相关命令

命令	说明
show mroute active	显示活动的组播流。

show mfib count

要显示 MFIB 路由和数据包计数数据，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib count** 命令。

show mfib [*group* [*source*]] **count**

语法说明

group	（可选）组播组的 IP 地址。
source	（可选）组播路由源的 IP 地址。这是采用四点分十进制记数法的单播 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示数据包丢弃统计信息。

示例

以下是 **show mfib count** 命令的输出示例：

```
ciscoasa# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

相关命令

命令	说明
clear mfib counters	清除 MFIB 路由器数据包计数器。
show mroute count	显示组播路由计数器。

show mfib interface

要显示与 MFIB 过程有关的接口的数据包统计信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib interface** 命令。

show mfib interface [*interface*]

语法说明

interface	（可选）接口名称。将显示限制为指定的接口。

默认值

显示所有 MFIB 接口的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mfib interface** 命令的输出示例：

```
ciscoasa# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

相关命令

命令	说明
show mfib	显示有关转发条目和接口的 MFIB 信息。

show mfib reserved

要显示预留组，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib reserved** 命令。

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

语法说明

active	（可选）显示活动组播源。
count	（可选）显示数据包和路由计数数据。
kpbs	（可选）将显示限制为大于或等于此值的活动组播源。
verbose	（可选）显示附加信息。

默认值

kbps 的默认值为 4。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示 224.0.0.0 到 224.0.0.225 范围内的 MFIB 条目。

示例

以下是 **show mfib reserved** 命令的输出示例：

```
ciscoasa# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

相关命令

命令	说明
show mfib active	显示活动的组播流。

show mfib status

要显示常规 MFIB 配置和运行状态，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib status** 命令。

show mfib status

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mfib status** 命令的输出示例：

```
ciscoasa# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

相关命令

命令	说明
show mfib	显示有关转发条目和接口的 MFIB 信息。

show mfib summary

要显示有关 MFIB 条目和接口数量的摘要信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib summary** 命令。

show mfib summary

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mfib summary** 命令的输出示例：

```
ciscoasa# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

相关命令

命令	说明
show mroute summary	显示组播路由表摘要信息。

show mfib verbose

要显示有关转发条目和接口的详细信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show mfib verbose** 命令。

show mfib verbose

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mfib verbose** 命令的输出示例：

```
ciscoasa# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

相关命令

命令	说明
show mfib	显示有关转发条目和接口的 MFIB 信息。
show mfib summary	显示有关 MFIB 条目和接口数量的摘要信息。

show mgcp

要显示 MGCP 配置和会话信息，请在特权 EXEC 模式下使用 **show mgcp** 命令。

show mgcp {**commands** | **sessions**} [**detail**]

语法说明

commands	列出命令队列中 MGCP 命令的数量。
detail	（可选）在输出中列出每个命令（或会话）的附加信息。
sessions	列出现有 MGCP 会话的数量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show mgcp commands 命令用于列出命令队列中 MGCP 命令的数量。**show mgcp sessions** 命令用于列出现有 MGCP 会话的数量。**detail** 选项用于在输出中包括每个命令（或会话）的附加信息。

示例

以下是 **show mgcp** 命令选项的示例：

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#

ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP | host-pc-2
       Transaction ID  2052
       Endpoint name | aaln/1
       Call ID | 9876543210abcdef
       Connection ID |
       Media IP | 192.168.5.7
       Media port | 6058
ciscoasa#
```

```
ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#

ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP | host-pc-2
       Call ID | 9876543210abcdef
       Connection ID | 6789af54c9
       Endpoint name | aaln/1
       Media lcl port  6166
       Media rmt IP | 192.168.5.7
       Media rmt port  6058
ciscoasa#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug mgcp	启用 MGCP 调试信息。
inspect mgcp	启用 MGCP 应用检查。
mgcp-map	定义 MGCP 映射并启用 mgcp 映射配置模式。
show conn	显示不同连接类型的连接状态。

show mmp

要显示有关现有 MMP 会话的信息，请在特权 EXEC 模式下使用 **show mmp** 命令。

show mmp [*address*]

语法说明

address	指定 MMP 客户端 / 服务器的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。

示例

以下示例展示如何使用 **show mmp** 命令显示有关现有 MMP 会话的信息：

```
ciscoasa# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

相关命令

命令	说明
debug mmp	显示检查 MMP 事件。
inspect mmp	配置 MMP 检查引擎。
show debug mmp	显示 MMP 检查模块的当前调试设置。

show mode

要显示正在运行的软件映像和闪存中任意映像的安全情景模式，请在特权 EXEC 模式下使用 **show mode** 命令。

show mode

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show mode** 命令的输出示例： 以下示例展示当前模式和未运行的映像 “image.bin” 的模式：

```
ciscoasa# show mode flash:/image.bin
Firewall mode: multiple
```

模式可以是多模式或单模式。

相关命令

命令	说明
context	在系统配置中创建安全情景并进入情景配置模式。
mode	将情景模式设置为单个或多个。

show module

要显示有关 ASA 上安装的模块的信息，请在用户 EXEC 模式下使用 **show module** 命令。

show module [*id* | **all**] [**details** | **recover** | **log** [**console**]

语法说明

all	（默认）显示所有模块的信息。
console	（可选）显示模块的控制台日志信息。
details	（可选）显示附加信息，包括模块的远程管理配置。
id	指定模块 ID。对于硬件模块，指定插槽编号，可以是 **0**（用于 ASA）或 **1**（用于安装的模块）。对于软件模块，指定以下名称之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块
log	（可选）显示模块的日志信息。
recover	（可选）显示 **hw-module** 或 **sw-module module recover** 命令的设置。

默认值

默认情况下，显示所有模块的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**[1]	**系统**
用户 EXEC	• 是	• 是	• 是	• 是	• 是

1. **show module recover** 命令仅在系统执行空间中可用。

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令修改为在输出中包括更多详细信息。
8.2(1)	有关 SSC 的信息包括在输出中。
8.2(5)	增加了有关对 ASA 5585-X 以及 ASA 5585-X 上的 IPS SSP 的支持的信息。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
8.6(1)	对于 ASA 5512-X 到 ASA 5555-X：增加了 **log** 和 **console** 关键字；增加了 **ips** 设备 ID。
9.1(1)	通过添加 **cxsc** 模块 ID，增加了对 ASA CX 软件模块的支持。
9.2(1)	添加了对 ASA FirePOWER 模块的支持，包括 **sfr** 关键字。

使用指南

此命令显示有关 ASA 中安装的模块的信息。ASA 本身也会以模块形式出现在显示中（在插槽 0 中）。

示例

以下是 **show module** 命令的输出示例。模块 0 为基本设备；模块 1 为 CSC SSM。

```
ciscoasa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

下表说明了输出中列出的每个字段。

表 9-3　show module 输出字段

字段	说明
Mod	模块编号，0 或 1。
Ports	端口数量。
Card Type	对于模块 0 中显示的设备，类型为平台型号。对于模块 1 中的 SSM，类型为 SSM 型。
type	此模块的型号。
Serial No.	序列号。
MAC Address Range	此 SSM 上的接口的 MAC 地址范围，或者内置接口（对于设备）。
Hw Version	硬件版本。
Fw Version	固件版本。
Sw Version	软件版本。
SSM Application Name	SSM 上运行的应用的名称。
SSM Application Version	SSM 上运行的应用的版本。

表 9-3　show module 输出字段（续）

字段	说明
Status	对于模块 0 中的设备，状态为 Up Sys。模块 1 中的 SSM 的状态可以是以下状态之一： • Initializing（正在初始化）- 检测到 SSM，并且设备正在初始化控制通信。 • Up（开启）- SSM 已完成设备初始化。 • Unresponsive（无响应）- 设备在与此 SSM 通信时遇到错误。 • Reloading（正在重新加载）- SSM 正在重新加载。 • Shutting Down（正在关闭）- SSM 正在关闭。 • Down（关闭）- SSM 已关闭。 • Recover（恢复）- SSM 正在尝试下载恢复映像。 • No Image Present（不存在映像）- IPS 软件尚未安装。
Data Plane Status	数据层面的当前状态。
Compatibility	SSM 相对于设备其余部分的兼容性。
Slot	物理插槽编号（仅用于双 SSP 模式）。

show module details 命令的输出会根据已安装的模块而有所不同。例如，CSC SSM 的输出包括有关 CSC SSM 软件组件的字段。

以下是 **show module 1 details** 命令的输出示例：

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

下表说明了输出中的附加字段。

表 9-4　show module details 附加输出字段

字段	说明
DC address （未显示）	（仅限 ASA FirePOWER）。管理模块的 FireSIGHT 管理中心 的地址。
Mgmt IP addr	显示模块的管理接口的 IP 地址。
Mgmt Network Mask （未显示）	显示管理地址的子网掩码。

表 9-4　show module details 附加输出字段（续）

字段	说明
Mgmt Gateway （未显示）	管理地址的网关。
Mgmt web ports	显示为模块的管理接口配置的端口。
Mgmt TLS enabled	显示是否为模块的管理接口的连接启用传输层安全（true 或 false）。

对于允许配置软件模块的型号，**show module** 命令会列出所有可能的模块。状态消息指示是否已安装其中一个模块。

```
ciscoasa# show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt     ASA5555            FCH1714J6HP
 ips Unknown                                      N/A                FCH1714J6HP
cxsc Unknown                                      N/A                FCH1714J6HP
 sfr FirePOWER Services Software Module           ASA5555            FCH1714J6HP

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 bc16.6520.1dcd to bc16.6520.1dd6  1.0          2.1(9)8      100.8(66)11
 ips bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
 sfr bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A          5.3.1-100

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr ASA FirePOWER                  Up               5.3.1-100

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Up                 Up

Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         172 days
```

以下是 **show module 1 recover** 命令的输出示例：

```
ciscoasa# show module 1 recover
Module 1 recover parameters.。。
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

以下是安装 SSC 后 **show module 1 details** 命令的输出示例：

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
```

```
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App.Name: IPS
App.Status: Up
App.Status Desc:
App.Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

以下是在 ASA 5585-X 中安装 IPS SSP 后 **show module 1 details** 命令的输出示例：

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: V1.0
Serial Number: 12345678
Firmware version: 1.0(7)2
Software version: 4.1(1.1)S47(0.1)
MAC Address Range: 000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status: Up
Status: Up
Mgmt IP addr: 10.89.147.13
Mgmt web ports: 443
Mgmt TLS enabled: true
```

以下是在 ASA 5585-X 中安装 CXSC SSP 后 **show module all** 命令的输出示例：

```
ciscoasa# show module all

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1504CBRM
  1 ASA 5585-X CXSC Security Services Processor-1 ASA5585-SSP-IPS10  JAF1510BLSE

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1d54 to 5475.d05b.1d5f  1.0          2.0(7)0      100.7(14)13
  1 5475.d05b.248c to 5475.d05b.2497  1.0          0.0(0)0      1.0

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CXSC Security Module             Up               1.0

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

以下是在 ASA 5585-X 中安装 CXSC SSP 后 **show module 1 details** 命令的输出示例：

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version:   1.0
Serial Number:      123456789
Firmware version:   1.0(9)0
Software version:   CXSC Security Module Version 1.0
App.name:           CXSC Security Module
App.version:        Version 1.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Activated:          Yes
Mgmt IP addr:       100.0.1.4
Mgmt web port:      8443
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
hw-module module recover	通过从 TFTP 服务器加载恢复映像来恢复模块。
hw-module module reset	关闭模块并执行硬件复位。
hw-module module reload	重新加载模块软件。
hw-module module shutdown	关闭模块软件，以确保断电不会导致丢失配置数据。
sw-module	配置软件模块。

show monitor-interface

要显示有关用于故障切换的监控接口的信息，请在特权 EXEC 模式下使用 **show monitor-interface** 命令。

show monitor-interface

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(2)	此命令已修改。输出包括 IPv6 地址。

使用指南

由于一个接口可配置多个 IPv6 地址，因此在 **show monitor-interface** 命令中仅显示链路本地地址。如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

监测的故障切换接口可以具有以下状态：

- Unknown（未知）- 初始状态。此状态也可能意味着状态无法确定。
- Normal（正常）- 接口正在接收流量。
- Normal (Waiting)（正常 [等待]）- 接口开启，但尚未从对等设备上的相应接口收到问候数据包。验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。
- Testing（测试）- 该接口上有 5 个轮询时间未收听到问候消息。
- Link Down（链路关闭）- 接口或 VLAN 被管理性关闭。
- No Link（无链路）- 接口的物理链路已关闭。
- Failed（故障）- 在该接口上没有收到流量，但在对等设备接口上收听到流量。

示例

以下是 **show monitor-interface** 命令的输出示例：

```
ciscoasa# show monitor-interface

This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
                Interface management (0.0.0.0): Unknown (Waiting)
                Interface failif (0.0.0.0): Unknown (Waiting)
```

相关命令

命令	说明
monitor-interface	在特定接口上启用状况监控。

show mrib client

要显示有关 MRIB 客户端连接的信息，请在用户 EXEC 或特权 EXEC 模式下使用 **show mrib client** 命令。

show mrib client [**filter**] [**name** *client_name*]

语法说明

filter	（可选）显示客户端过滤器。用于查看有关每个客户端拥有的 MRIB 标志以及每个客户端感兴趣的标志的信息。
name *client_name*	（可选）用作 MRIB 客户端的组播路由协议的名称，如 PIM 或 IGMP。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

filter 选项用于显示各 MRIB 客户端已注册的路由和接口级别标志更改。此命令选项还显示哪些标志由 MRIB 客户端所有。

示例

以下是使用 **filter** 关键字的 **show mrib client** 命令的输出示例：

```
ciscoasa# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
```

```
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

相关命令

命令	说明
show mrib route	显示 MRIB 表条目。

show mrib route

要显示 MRIB 表中的条目，请在用户 EXEC 或特权 EXEC 模式下使用 **show mrib route** 命令。

show mrib route [[*source* | *****] [*group*[*/prefix-length*]]]

语法说明

*	（可选）显示共享树条目。
/prefix-length	（可选）MRIB 路由的前缀长度。十进制值，表示地址的多少个高位连续位构成前缀（地址的网络部分）。十进制值前面必须有斜线标记。
group	（可选）组的 IP 地址或名称。
source	（可选）路由源的 IP 地址或名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

MFIB 表维护从 MRIB 更新的条目和标志子集。标志根据组播数据包的转发规则集来确定转发和信令行为。

除了接口和标志的列表外，每个路由条目都显示各种计数器。字节数是转发的总字节数。数据包数是针对此条目接收的数据包数。**show mfib count** 命令显示与路由无关的全局计数器。

示例

以下是 **show mrib route** 命令的输出示例：

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS
```

```
(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

相关命令

命令	说明
show mfib count	显示 MFIB 表的路由和数据包计数数据。
show mrib route summary	显示 MRIB 表条目的摘要。

show mroute

要显示 IPv4 组播路由表，请在特权 EXEC 模式下使用 **show mroute** 命令。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

语法说明

active *rate*	（可选）仅显示活动组播源。活动源是正在以指定 *rate* 或更高速率发送的源。如果未指定 *rate*，则活动源是正在以 4 kbps 或更高速率发送的源。
count	（可选）显示有关组和源的统计信息，包括数据包数、每秒数据包数，平均数据包大小和 bps。
group	（可选）组播组的 IP 地址或名称，如 DNS 主机表中所定义。
pruned	（可选）显示修剪的路由。
reserved	（可选）显示预留组。
source	（可选）源主机名或 IP 地址。
summary	（可选）在组播路由表中显示每个条目的单行缩写摘要。

默认值

如果未指定，则 *rate* 参数默认为 4 kbps。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show mroute 命令显示组播路由表的内容。ASA 通过创建基于 PIM 协议消息、IGMP 报告和流量的 (S,G) 和 (*,G) 条目来填充组播路由表。星号 (*) 指所有源地址，“S” 指单个源地址，“G” 是目标组播组地址。在创建 (S, G) 条目时，软件使用在单播路由表中找到的到该目标组的最佳路径（通过 RPF）。

要查看运行配置中的 **mroute** 命令，请使用 **show running-config mroute** 命令。

示例

以下是 **show mroute** 命令的输出示例：

```
ciscoasa(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
```

```
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 8:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute 输出中显示以下字段：

- **Flags** - 提供有关条目的信息。
  - **D - 致密**。条目在密集模式下工作。
  - **S - 稀疏**。条目在稀疏模式下工作。
  - **B - 双向组**。指示组播组在双向模式下工作。
  - **s - SSM 组**。指示组播组在 IP 地址的 SSM 范围内。如果 SSM 范围更改，此标志将重置。
  - **C - 已连接**。组播组的成员出现在直接连接的接口上。
  - **L - 本地**。ASA 本身是组播组的成员。通过 **igmp join-group** 命令以本地方式加入组（对于已配置的组）。
  - **I - 已接收源特定主机报告**。指示通过 (S, G) 报告创建了 (S, G) 条目。此 (S, G) 报告可能通过 IGMP 创建。此标志仅在 DR 上设置。
  - **P - 已修剪**。路由已修剪。软件将保留此信息，以便下游成员加入源。
  - **R - RP 位已设置**。指示 (S, G) 条目指向 RP。
  - **F - 注册标志**。指示软件正在注册组播源。
  - **T - SPT 未已设置**。指示已在最短路径源树上收到数据包。
  - **J - 联合 SPT**。对于 (*, G) 条目，指示流量流下共享树的速率超过为组设置的 SPT 阈值。（默认 SPT 阈值设置为 0 kbps）。当设置 J - Join 最短路径树 (SPT) 标志后，在共享树收到的下一个 (S, G) 数据包将触发源方向上的 (S, G) 加入，从而使 ASA 加入源树。

    对于 (S, G) 条目，指示由于超过了组的 SPT 阈值而创建了条目。当为 (S, G) 条目设置 J - Join SPT 标志后，ASA 监控源树上的流量速率，并在源树上的流量速率低于组的 SPT 阈值超过 1 分钟时尝试切换回此源的共享树。

    注　ASA 会测量共享树上的流量速率，并将测量出的速率与组的 SPT 阈值进行比较，每秒比较一次。如果流量速率超过 SPT 阈值，将在 (*, G) 条目上设置 J - Join SPT 标志，直到下一次测量流量速率。当下一个数据包到达共享树并且开始新的测量间隔时，清除该标志。

    如果组使用默认 SPT 阈值 0 Kbps，将始终在 (*, G) 条目上设置 J - Join SPT 标志，并且不会清除。当使用默认 SPT 阈值时，如果收到来自新源的流量，ASA 会立即切换到最短路径源树。

- **Timers:Uptime/Expires（计时器：正常运行时间 / 到期时间）**- Uptime（正常运行时间）针对接口指示条目在 IP 组播路由表中的时长（以小时、分钟和秒为单位）。Expires（到期时间）针对接口指示从 IP 组播路由表中删除条目之前的时长（以小时、分钟和秒为单位）。
- **Interface state（接口状态）**- 指示传入或传出接口的状态。
  - **Interface（接口）**- 传入或传出接口列表中列出的接口名称。
  - **State（状态）**- 指示数据包在接口上被转发、修剪还是变空，具体取决于是否因访问列表或生存时间 (TTL) 阈值而存在限制。
- **(*, 239.1.1.40)** 和 **(* , 239.2.2.1)** - IP 组播路由表中的条目。条目包含源的 IP 地址，后面紧跟组播组的 IP 地址。用星号 (*) 代替源则表示所有源。
- **RP** - RP 的地址。对于在稀疏模式下运行的路由器和接入服务器，此地址始终为 224.0.0.0。
- **Incoming interface（传入接口）**- 预期用于来自源的组播数据包的接口。如果数据包未在此接口上接收到，则将其丢弃。
- **RPF nbr** - 上游路由器相对于源的 IP 地址。
- **Outgoing interface list（传出接口列表）**- 用于转发数据包的接口。

相关命令

命令	说明
clear configure mroute	从运行配置中删除 **mroute** 命令。
mroute	配置静态组播路由。
show mroute	显示 IPv4 组播路由表。
show running-config mroute	显示已配置的组播路由。

第 10 章

show nac-policy 至 show ospf virtual-links 命令

show nac-policy

要显示 NAC 策略使用统计信息并将 NAC 策略分配到组策略，请在特权 EXEC 模式下使用 **show nac-policy** 命令。

show nac-policy [*nac-policy-name*]

语法说明

nac-policy-name	（可选）要显示使用统计信息的 NAC 策略的名称。

默认值

如果没有指定名称，则 CLI 列出所有 NAC 策略名称及其各自的统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例展示名为 framework1 和 framework2 的 NAC 策略的数据：

```
ciscoasa(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

每个 NAC 策略的第一行指示其名称和类型 (nac-framework)。如果策略没有分配到任何组策略，则 CLI 在策略类型旁边显示文本 “is not in use”。否则，CLI 显示组策略的使用数据。表 10-1 说明了 **show nac-policy** 命令中的字段。

表 10-1　show nac-policy 命令字段

字段	说明
applied session count	此 ASA 应用 NAC 策略的 VPN 会话累计数。
applied group-policy count	此 ASA 应用 NAC 策略的组策略累计数。
group-policy list	此 NAC 策略分配到的组策略列表。在这种情况下，使用组策略不会确定其是否在此列表中显示；如果 NAC 策略分配到运行的配置中的组策略，则该组策略在此列表中显示。

相关命令

clear nac-policy	重置 NAC 策略使用统计信息。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。
show vpn-session_summary.db	显示数字 IPSec、Cisco WebVPN 和 NAC 会话。

show nameif

要查看使用 **nameif** 命令的接口名称集，请在特权 EXEC 模式下使用 **show nameif** 命令。

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name* | **zone**]

语法说明

mapped_name	（可选）在多情景模式下，如果使用 **allocate-interface** 命令分配了映射的名称，则标识该名称。
physical_interface	（可选）识别接口 ID（例如 **gigabitethernet0/1**）。请参阅 **interface** 命令可接受的值。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
zone	（可选）显示区域名称。

默认值

如果没有指定接口，则 ASA 显示所有接口名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(2)	添加了 **zone** 关键字。

使用指南

在多情景模式下，如果映射 **allocate-interface** 命令中的接口 ID，则只能在一个情景中指定映射名称。此命令的输出仅显示 Interface（接口）列中的映射名称。

示例

以下是 **show nameif** 命令的输出示例：

```
ciscoasa# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

请参阅 **show nameif zone** 命令的以下输出：

```
ciscoasa# show nameif zone
Interface               Name                zone-name   Security
GigabitEthernet0/0      inside-1            inside-zone   100
GigabitEthernet0/1.21   inside              inside-zone   100
GigabitEthernet0/1.31   4                                 0
```

```
GigabitEthernet0/2       outside                 outside-zone  0
Management0/0            lan                                   0
```

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
interface	配置接口并进入接口配置模式。
nameif	设置接口名称。
show interface ip brief	显示接口 IP 地址和状态。

show nat

要显示 NAT 策略的统计信息，请在特权 EXEC 模式下使用 **show nat** 命令。

show nat [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]
[**translated** [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]] [**detail**]
[**divert-table** [**ipv6**] [**interface** *name*]]

语法说明

detail	（可选）包括对象字段更详细的扩展。
divert-table	（可选）显示 NAT 转移表。
interface *name*	（可选）指定源接口。
ip_addr mask	（可选）指定 IP 地址和子网掩码。
ipv6	（可选）显示转移表中的 IPv6 条目。
object *name*	（可选）指定网络对象或服务对象。
object-group *name*	（可选）指定网络对象组
translated	（可选）指定转换参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。
9.0(1)	此命令现已支持 IPv6 流量，以及 IPv4 与 IPv6 之间的转换。

使用指南

使用 **show nat** 命令以显示 NAT 策略的运行时表示。使用 **detail** 可选关键字以展开对象并查看对象值。使用其他选择器字段以限制 **show nat** 命令输出。

示例

以下是 **show nat** 命令的输出示例：

```
ciscoasa# show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
```

```
   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0

ciscoasa# show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
    1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

以下是 **show nat detail** 命令在 IPv6 与 IPv4 之间的输出示例：

```
ciscoasa# show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

以下是 **show nat divert ipv6** 命令的输出示例：

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

相关命令

命令	说明
clear nat counters	清除 NAT 策略计数器。
nat	识别一个接口上转换为另一个接口上的映射地址的地址。

show nat divert-table

要显示 NAT 转移表的统计信息，请在特权 EXEC 模式下使用 **show nat divert-table** 命令。

show nat divert-table [**ipv6**] [**interface** *name*]

语法说明

divert-table	显示 NAT 转移表。
ipv6	（可选）显示转移表中的 IPv6 条目。
interface *name*	（可选）指定源接口。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show nat divert-table** 命令以显示 NAT 转移表的运行时表示。使用 **ipv6** 可选关键字以查看转移表中的 IPv6 条目。使用 **interface** 可选关键字以查看特定源接口的 NAT 转移表。

示例

以下是 **show nat divert-table** 命令的输出示例：

```
ciscoasa# show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
```

```
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

相关命令

命令	说明
clear nat counters	清除 NAT 策略计数器。
nat	识别一个接口上转换为另一个接口上的映射地址的地址。
show nat	显示 NAT 策略的运行时表示。

show nat pool

要显示 NAT 池使用的统计信息，请在特权 EXEC 模式下使用 **show nat pool** 命令。

show nat pool [**cluster**]

语法说明

cluster	（可选）启用 ASA 集群后，将显示当前分配到所有者设备和备用设备的 PAT 地址。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。
8.4(3)	输出已修改为显示扩展 PAT 的目标地址。PAT 范围也将根据 **flat** 和 **include-reserve** 关键字的使用进行修改。
9.0(1)	此命令现已支持 IPv6 流量。我们添加了 **cluster** 关键字以显示当前分配到所有者设备和备用设备的 PAT 地址。

使用指南

为每个映射的协议 /IP 地址 / 端口范围创建 NAT 池，其中端口范围默认为 1-511、512-1023 和 1024-65535。如果在 **nat** 命令中对 PAT 池使用 **flat** 关键字，您将看到更小、更大的范围。

每个 NAT 池在上次使用后存在至少 10 分钟。如果您使用 **clear xlate** 清除转换，则 10 分钟抑制计时器将被取消。

示例

以下是通过 **show running-config object network** 命令所示的动态 PAT 规则创建的 NAT 池的输出示例。

```
ciscoasa(config)# show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

ciscoasa# show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

以下是 **show nat pool** 命令展示如何使用 PAT 池 **flat** 选项的输出示例。如果没有 **include-reserve** 关键字，则显示两个范围；低于 1024 的源端口映射到同一端口时使用较低的范围。

```
ciscoasa# show nat pool

ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

以下是 **show nat pool** 命令展示如何使用 PAT 池 **flat include-reserve** 选项的输出示例。

```
ciscoasa# show nat pool

ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

以下是 **show nat pool** 命令展示如何使用 PAT 池 **extended flat include-reserve** 选项的输出示例。重要的项目是括号内的地址。这些是用于扩展 PAT 的目标地址。

```
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

相关命令

命令	说明
nat	识别一个接口上转换为另一个接口上的映射地址的地址。
show nat	显示 NAT 策略统计信息。

show ntp associations

要查看 NTP 关联信息，请在用户 EXEC 模式下使用 **show ntp associations** 命令。

show ntp associations [detail]

语法说明

detail	（可选）显示关于每个关联的其他详细信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show ntp associations** 命令的输出示例：

```
ciscoasa> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

表 10-2 显示每个字段的说明。

表 10-2　show ntp associations 字段

字段	说明
（显示行中的前导字符）	显示行中开头的字符可以是以下一个或多个字符： • * - 同步到此对等设备。 • # - 几乎同步到此对等设备。 • + - 为可能的同步选择的对等设备。 • - - 对等设备作为候选可供选择。 • ~ - 对等设备已静态配置，但未同步。

表 10-2　show ntp associations 字段（续）

字段	说明
address	NTP 对等设备的地址。
ref clock	对等设备参考时钟的地址。
st	对等设备的层。
when	从对等设备接收上一 NTP 数据包后经过的时间。
poll	轮询间隔（以秒为单位）。
reach	对等设备可达性（作为位串，八进制）。
delay	对等设备的往返延迟（以毫秒为单位）。
offset	对等设备时钟与本地时钟的相对时间（以毫秒为单位）。
disp	分散值。

以下是 **show ntp associations detail** 命令的输出示例：

```
ciscoasa> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

表 10-3 显示每个字段的说明。

表 10-3　show ntp associations detail 字段

字段	说明
IP-address configured	服务器（对等设备）IP 地址。
（状态）	• our_master - ASA 已同步到此对等设备。 • selected - 为可能的同步选择对等设备。 • candidate - 对等设备作为候选可供选择。
（健全性）	• sane - 对等设备已通过基本健全性检查。 • insane - 对等设备未通过基本健全性检查。
（有效性）	• valid - 对等设备时间被视为有效。 • invalid - 对等设备时间被视为无效。 • leap_add - 对等设备发出将添加闰秒的信令。 • leap-sub - 对等设备发出将减去闰秒的信令。
stratum	对等设备的层。

表 10-3　show ntp associations detail 字段（续）

字段	说明
（参考对等设备）	unsynced - 对等设备未同步到任何其他机器。 ref ID - 对等设备同步到的机器的地址。
time	上次从其主控设备接收对等设备的时间戳。
our mode client	我们相对于对等设备的模式，即始终为客户端。
peer mode server	相对于服务器的对等设备模式。
our poll intvl	我们相对于对等设备的轮询间隔。
peer poll intvl	对等设备相对于我们的轮询间隔。
root delay	沿路径到根目录（最终第 1 层时间来源）的延迟。
root disp	路径到根目录的分散。
reach	对等设备可达性（作为八进制位串）。
sync dist	对等设备同步距离。
delay	对等设备的往返延迟。
offset	对等设备时钟相对于我们的时钟的偏差。
dispersion	对等设备时钟的分散。
precision	对等设备时钟的精度（以赫兹为单位）。
version	对等设备使用的 NTP 版本号。
org time	发起时间戳。
rcv time	接收时间戳。
xmt time	传输时间戳。
filtdelay	每个示例的往返延迟（以毫秒为单位）。
filtoffset	每个示例的时钟偏差（以毫秒为单位）。
filterror	每个示例的近似误差。

相关命令

命令	说明
ntp authenticate	启用 NTP 身份验证。
ntp authentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntp server	标识 NTP 服务器。
ntp trusted-key	提供 ASA 在数据包中使用的密钥 ID 以向 NTP 服务器进行身份验证。
show ntp status	显示 NTP 关联的状态。

show ntp status

要显示每个 NTP 关联的状态，请在用户 EXEC 模式下使用 **show ntp status** 命令。

show ntp status

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

请参阅 “ 示例 ” 部分，了解显示输出的说明。

示例

以下是 **show ntp status** 命令的输出示例：

```
ciscoasa> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

表 10-4 显示每个字段的说明。

表 10-4　show ntp status 字段

字段	说明
Clock	• synchronized - ASA 已同步到 NTP 服务器。 • unsynchronized - ASA 未同步到 NTP 服务器。
stratum	此系统的 NTP 层。
reference	ASA 同步到的 NTP 服务器的地址。
nominal freq	系统硬件时钟的标称频率。

表 10-4　show ntp status 字段（续）

字段	说明
actual freq	系统硬件时钟的测量频率。
precision	此系统时钟的精度（以赫兹为单位）。
reference time	参考时间戳。
clock offset	系统时钟相对于同步对等设备的偏差。
root delay	沿路径到根目录时钟的总延迟。
root dispersion	根路径的分散。
peer dispersion	同步对等设备的分散。

相关命令

命令	说明
ntp authenticate	启用 NTP 身份验证。
ntp authentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntp server	标识 NTP 服务器。
ntp trusted-key	提供 ASA 在数据包中使用的密钥 ID 以向 NTP 服务器进行身份验证。
show ntp associations	显示与 ASA 关联的 NTP 服务器。

show object-group

要显示对象组信息和对象组为网络对象组类型时相关的命中计数，请在特权 EXEC 模式下使用 **show object-group** 命令。

show object-group [**protocol** | **service** | **icmp-type** | **id** *object-group name*]

语法说明

icmp-type	（可选）ICMP 类型对象组。
id	（可选）标识现有的对象组。
object-group name	（可选）将指定名称分配到对象组。
protocol	（可选）协议类型对象组。
service	（可选）服务类型对象。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

如果对象组为网络对象组类型，则尝试显示对象组的例行程序也会显示对象命中计数。服务、协议和 icmp 类型对象组不会显示命中计数。

示例

以下是 **show object-group** 命令的输出示例，显示关于名为 “Anet” 的网络对象组的信息：

```
ciscoasa# show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

以下是 **show object-group** 命令的输出示例，显示关于服务组的信息：

```
ciscoasa (config)# show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp

   object-group protocol C-grp-proto
   protocol-object ospf
```

以下是 **show object-group** 命令的输出示例，显示关于协议的信息：

```
ciscoasa (config)# show object-group protocol
object-group protocol C-grp-proto
   protocol-object ospf
```

相关命令

命令	说明
clear object-group	清除指定对象组的网络对象命中计数。
show access list	显示所有访问列表、相关扩展访问列表条目以及命中计数。

show ospf

要显示关于 OSPF 路由进程的一般信息，请在特权 EXEC 模式下使用 **show ospf** 命令。

show ospf [*pid* [*area_id*]]

语法说明

area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
pid	（可选）OSPF 进程的 ID。

默认值

如果没有指定 *pid*，则列出所有 OSPF 进程。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果已包含 *pid*，则仅包含指定路由进程的信息。

示例

以下是 **show ospf** 命令的输出示例，展示如何显示关于特定 OSPF 路由进程的一般信息：

```
ciscoasa# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs.Minimum LSA arrival 1 secs
 Number of external LSA 0.Checksum Sum 0x     0
 Number of opaque AS LSA 0.Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0.0 normal 0 stub 0 nssa
 External flood list length 0
```

以下是 **show ospf** 命令的输出示例，展示如何显示关于所有 OSPF 路由进程的一般信息：

```
ciscoasa# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
```

```
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs.Minimum LSA arrival 1 secs
Number of external LSA 0.Checksum Sum 0x     0
Number of opaque AS LSA 0.Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0.0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs.Minimum LSA arrival 1 secs
Number of external LSA 0.Checksum Sum 0x     0
Number of opaque AS LSA 0.Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0.0 normal 0 stub 0 nssa
External flood list length 0
```

相关命令

命令	说明
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf border-routers

要显示到 ABR 和 ASBR 的内部 OSPF 路由表条目，请在特权 EXEC 模式下使用 **show ospf border-routers** 命令。

show ospf border-routers

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下是 **show ospf border-routers** 命令的输出示例：

```
ciscoasa# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

相关命令

命令	说明
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf database

要显示 ASA 上 OSPF 拓扑数据库中包含的信息，请在特权 EXEC 模式下使用 **show ospf database** 命令。

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

语法说明

addr	（可选）路由器地址。
adv-router	（可选）通告的路由器。
area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
asbr-summary	（可选）显示 ASBR 列表摘要。
database	显示数据库信息。
database-summary	（可选）显示完整的数据库摘要列表。
external	（可选）显示指定自主系统外部的路由。
internal	（可选）指定自主系统内部的路由。
lsid	（可选）LSA ID。
network	（可选）显示关于网络的 OSPF 数据库信息。
nssa-external	（可选）显示外部末节区域列表。
pid	（可选）OSPF 进程的 ID。
router	（可选）显示路由器。
self-originate	（可选）显示指定自主系统的信息。
summary	（可选）显示列表的摘要。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

OSPF 路由相关的 **show** 命令在 ASA 上的特权模式下可用。您无需处于 OSPF 配置模式即可使用 OSPF 相关的 **show** 命令。

示例

以下是 **show ospf database** 命令的输出示例：

```
ciscoasa# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

以下是 **show ospf database asbr-summary** 命令的输出示例：

```
ciscoasa# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

以下是 **show ospf database router** 命令的输出示例：

```
ciscoasa# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

以下是 **show ospf database network** 命令的输出示例：

```
ciscoasa# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

以下是 **show ospf database summary** 命令的输出示例：

```
ciscoasa# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

以下是 **show ospf database external** 命令的输出示例：

```
ciscoasa# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

相关命令

命令	说明
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf flood-list

要显示等待在接口上泛洪的 OSPF LSA 列表，请在特权 EXEC 模式下使用 **show ospf flood-list** 命令。

show ospf flood-list *interface_name*

语法说明

interface_name	要显示邻居信息的接口的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

OSPF 路由相关的 **show** 命令在 ASA 上的特权模式下可用。您无需处于 OSPF 配置模式即可使用 OSPF 相关的 **show** 命令。

示例

以下是 **show ospf flood-list** 命令的输出示例：

```
ciscoasa# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

相关命令

命令	说明
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf interface

要显示 OSPF 相关接口信息，请在特权 EXEC 模式下使用 **show ospf interface** 命令。

show ospf interface [*interface_name*]

语法说明

interface_name	（可选）要显示 OSPF 相关信息的接口的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果使用时不带 *interface_name* 参数，则显示所有接口的 OSPF 信息。

示例

以下是 **show ospf interface** 命令的输出示例：

```
ciscoasa# show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

相关命令

命令	说明
interface	进入接口配置模式。

show ospf nsf

要显示 OSPFv2 相关 NSF 信息，请在特权 EXEC 模式下使用 **show ospf nsf** 命令。

show ospf nsf

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.3(1)	引入了此命令。

示例

以下是 **show ospf nsf** 命令的输出示例：

```
ciscoasa# show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

相关命令

命令	说明
nsf cisco	在支持 NSF 的路由器上启用思科 NSF。
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf neighbor

要基于每个接口显示 OSPF 邻居信息，请在特权 EXEC 模式下使用 **show ospf neighbor** 命令。

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

语法说明

detail	（可选）列出指定路由器的详细信息。
interface_name	（可选）要显示邻居信息的接口的名称。
nbr_router_id	（可选）邻居路由器的路由器 ID。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下是 **show ospf neighbor** 命令的输出示例。它基于每个接口展示如何显示 OSPF 邻居信息。

```
ciscoasa# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

以下是 **show ospf neighbor detail** 命令的输出示例。它展示如何显示指定 OSPF 邻居的详细信息。

```
ciscoasa# show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
```

```
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
Dead timer due in 0:00:24
Neighbor is up for 1:42:15
Index 5/5, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

相关命令

命令	说明
neighbor	配置 OSPF 路由器与非广播网络的互连。
router ospf	启用 OSPF 路由并配置全局 OSPF 路由参数。

show ospf request-list

要显示路由器请求的所有 LSA 的列表，请在特权 EXEC 模式下使用 **show ospf request-list** 命令。

show ospf request-list *nbr_router_id interface_name*

语法说明

interface_name	要显示邻居信息的接口的名称。显示路由器从此接口请求的所有 LSA 的列表。
nbr_router_id	邻居路由器的路由器 ID。显示路由器从此邻居请求的所有 LSA 的列表。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下是 **show ospf request-list** 命令的输出示例：

```
ciscoasa# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

相关命令

命令	说明
show ospf retransmission-list	显示等待重新发送的所有 LSA 的列表。

show ospf retransmission-list

要显示等待重新发送的所有 LSA 的列表，请在特权 EXEC 模式下使用 **show ospf retransmission-list** 命令。

show ospf retransmission-list *nbr_router_id interface_name*

语法说明

interface_name	要显示邻居信息的接口的名称。
nbr_router_id	邻居路由器的路由器 ID。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

OSPF 路由相关的 **show** 命令在 ASA 上的特权模式下可用。您无需处于 OSPF 配置模式即可使用 OSPF 相关的 **show** 命令。

nbr_router_id 参数显示等待为此邻居重新发送的所有 LSA 的列表。

interface_name 参数显示等待为此接口重新发送的所有 LSA 的列表。

示例

以下是 **show ospf retransmission-list** 命令的输出示例，其中 *nbr_router_id* 参数为 192.168.1.11 而 *if_name* 参数为 outside：

```
ciscoasa# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

相关命令

命令	说明
show ospf request-list	显示路由器请求的所有 LSA 的列表。

show ospf summary-address

要显示在 OSPF 进程下配置的所有摘要地址重分布信息的列表，请在特权 EXEC 模式下使用 **show ospf summary-address** 命令。

show ospf summary-address

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下内容展示 **show ospf summary-address** 命令的输出示例。它展示如何在为 ID 为 5 的 OSPF 进程配置摘要地址之前显示所有摘要地址重分布信息的列表。

```
ciscoasa# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

相关命令

命令	说明
summary-address	创建 OSPF 的汇聚地址。

show ospf traffic

要显示特定 OSPF 实例处理（发送或接收）的不同类型数据包列表，请在特权 EXEC 模式下使用 **show ospf traffic** 命令。通过此命令，您可以获取处理的不同类型 OSPF 数据包的快照而无需启用调试。如果配置了两个 OSPF 实例，则 show ospf traffic 命令会显示两个实例的统计信息及每个实例的进程 ID。您还可以通过使用 **show ospf** *process_id* **traffic** 命令显示单一实例的统计信息。

show ospf traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

通过此命令，您可以获取处理的不同类型 OSPF 数据包的快照而无需启用调试。如果配置了两个 OSPF 实例，则 **show ospf traffic** 命令会显示两个实例的统计信息及每个实例的进程 ID。您还可以通过使用 **show ospf** *process_id* **traffic** 命令显示单一实例的统计信息。

示例

以下内容展示 **show ospf traffic** 命令的输出示例。

```
ciscoasa# show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

相关命令

命令	说明
show ospf virtual-links	显示 OSPF 虚拟链路的参数和当前状态。

show ospf virtual-links

要显示 OSPF 虚拟链路的参数和当前状态，请在特权 EXEC 模式下使用 **show ospf virtual-links** 命令。

show ospf virtual-links

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

示例

以下是 **show ospf virtual-links** 命令的输出示例：

```
ciscoasa# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

相关命令

命令	说明
area virtual-link	定义 OSPF 虚拟链路。

第 11 章

show pager 至 show route 命令

show pager

要显示接口的默认路由或静态路由，请在特权 EXEC 模式下使用 **show pager** 命令。

show pager

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
4.0(1)	引入了此命令。

示例

以下是 **show pager** 命令的输出示例：

```
ciscoasa(config)# show pager
pager lines 0
```

相关命令

命令	说明
clear configure pager	从运行配置中删除设置为在 Telnet 会话中出现 “---More---” 提示符之前显示的行数。
show running-config pager	在运行配置中显示设置为在 Telnet 会话中出现 “---More---” 提示符之前显示的行数。
terminal pager	设置在出现 “---More---” 提示符之前要在 Telnet 会话中显示的行数。此命令不会保存到运行配置中。

show password encryption

要显示密码加密配置设置，请在特权 EXEC 模式下使用 **show password encryption** 命令。

show password encryption

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.3(1)	引入了此命令。
8.4(1)	允许在用户情景中显示密码加密。

使用指南

如果已使用 **write memory** 命令保存了密钥，“saved” 将会显示在哈希密钥旁边。如果没有密钥或者密钥已从运行配置中删除，将会显示 “Not set” 而不是哈希值。

示例

以下是 **show password encryption** 命令的输出示例：

```
ciscoasa# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

相关命令

命令	说明
password encryption aes	启用密码加密。
key config-key password-encrypt	设置用于生成加密密钥的口令。

show perfmon

要显示有关 ASA 性能的信息，请在特权 EXEC 模式下使用 **show perfmon** 命令。

show perfmon [**detail**]

语法说明

detail	（可选）显示其他统计信息。这些统计信息与思科统一防火墙 MIB 的全局和单一协议连接对象收集的统计信息相一致。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	ASA 已引入对此命令的支持。
7.2(1)	添加了 **detail** 关键字。

使用指南

此命令的输出不显示在 Telnet 会话中。

perfmon 命令按定义的时间间隔持续显示性能统计信息。使用 **show perfmon** 命令可立即显示这些信息。

示例

以下是 **show perfmon** 命令的输出示例：

```
ciscoasa(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

以下是 **show perfmon detail** 命令的输出示例：

```
ciscoasa(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

相关命令

命令	说明
perfmon	按定义的时间间隔显示详细的性能监控信息。

show phone-proxy

要显示电话代理特定信息，请在全局配置模式下使用 **show phone-proxy** 命令。

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

语法说明

detail	显示详细信息。
media-sessions	显示电话代理存储的相应媒体会话。此外，还显示为建立了媒体会话的接口配置的媒体终端地址。
secure-phones	显示数据库中存储的支持安全模式的电话。
signaling-sessions	显示电话代理存储的相应信令会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。
8.2(1)	更新了此命令，现在，指定 **media-sessions** 关键字还会显示为建立了媒体会话的接口配置的媒体终端地址。

示例

以下示例使用 **show phone proxy** 命令来显示电话代理特定信息：

```
ciscoasa(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
ciscoasa(config)#
```

以下示例展示使用 **show phone proxy** 命令来显示数据库中存储的支持安全模式的电话：

```
ciscoasa(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
ciscoasa(config)#
```

以下示例使用 **show phone proxy** 命令来显示成功呼叫的输出以及为建立了媒体会话的接口配置的媒体终端地址：

```
ciscoasa(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

相关命令

命令	说明
debug phone-proxy	显示电话代理实例的调试消息。
phone proxy	配置电话代理实例。

show pim df

要显示集合点 (RP) 或接口的双向 DF“ 获胜者 ”，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim df** 命令。

show pim df [**winner**] [*rp_address* | *if_name*]

语法说明

rp_address	可以是以下各项之一： • RP 的名称，由域名系统 (DNS) 主机表或者域 **ipv4 host** 命令定义。 • RP 的 IP 地址。这是采用四点分十进制表示法的组播 IP 地址。
if_name	物理或逻辑接口名称。
winner	（可选）显示每个 RP 的每个接口在 DF 选定中的获胜者。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令还显示适用于 RP 的优胜衡量标准。

示例

以下是 **show pim df** 命令的输出示例：

```
ciscoasa# show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

要显示组 - 协议映射表，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim group-map** 命令。

show pim group-map [**info-source**] [*group*]

语法说明

group	（可选）可以是以下各项之一： • 组播组的名称，由 DNS 主机表或者域 **ipv4 host** 命令定义。 • 组播组的 IP 地址。这是采用四点分十进制表示法的组播 IP 地址。
info-source	（可选）显示组范围信息源。

默认值

显示所有组的组 - 协议映射。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示 RP 的所有组协议地址映射。在 ASA 上从不同的客户端获知映射。

在 ASA 上实施 PIM 会在映射表中填充各种特殊条目。自动 RP 组范围会从稀疏模式组范围中专门排除。SSM 组范围也不属于稀疏模式范围。链路本地组播组（224.0.0.0 至 224.0.0.225，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。最后一个条目使用给定 RP 在稀疏模式下显示所有剩余的组。

如果使用 **pim rp-address** 命令配置了多个 RP，则会显示适当的组范围及相应的 RP。

示例

以下是 **show pim group-map** 命令的输出示例：

```
ciscoasa# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

在行 1 和行 2 中，自动 RP 组范围会从稀疏模式组范围中专门排除。

在行 3 中，链路本地组播组（224.0.0.0 至 224.0.0.255，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。

在行 4 中，PIM 源特定组播 (PIM-SSM) 组范围映射到 232.0.0.0/8。

最后一个条目显示，所有剩余的组都处于稀疏模式并映射到 RP 10.10.3.2。

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。
pim rp-address	配置 PIM 集合点 (RP) 的地址。

show pim interface

要显示 PIM 的接口特定信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim interface** 命令。

show pim interface [*if_name* | **state-off** | **state-on**]

语法说明

if_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
state-off	（可选）显示禁用了 PIM 的接口。
state-on	（可选）显示启用了 PIM 的接口。

默认值

如果不指定接口，将会显示所有接口的 PIM 信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在 ASA 上实施 PIM 会将 ASA 本身视为 PIM 邻居。因此，此命令的输出中的 “ 邻居数 ” 列显示的邻居数会比实际邻居数大 1。

示例

以下示例展示内部接口的 PIM 信息：

```
ciscoasa# show pim interface inside
Address     Interface      Ver/     Nbr     Query      DR     DR
                           Mode     Count   Intvl      Prior
172.16.1.4 inside          v2/S     2       100 ms     1      172.16.1.4
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

show pim join-prune statistic

要显示 PIM 联接 / 修剪汇聚统计信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim join-prune statistics** 命令。

show pim join-prune statistics [*if_name*]

语法说明

if_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

默认值

如果不指定接口，此命令将会显示所有接口的联接 / 修剪统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **clear pim counters** 命令可清除 PIM 联接 / 修剪统计信息。

示例

以下是 **show pim join-prune statistic** 命令的输出示例：

```
ciscoasa# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

相关命令

命令	说明
clear pim counters	清除 PIM 流量计数器。

show pim neighbor

要显示 PIM 邻居表中的条目，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim neighbor** 命令。

show pim neighbor [**count** | **detail**] [*interface*]

语法说明

interface	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
count	（可选）显示 PIM 邻居总数以及每个接口的 PIM 邻居数。
detail	（可选）显示通过上游检测问候选项获知的邻居的其他地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令用于确定路由器通过 PIM 问候消息获知的 PIM 邻居。此外，此命令还指明哪个接口是指定路由器 (DR) 以及邻居何时能够双向运行。

在 ASA 上实施 PIM 会将 ASA 本身视为 PIM 邻居。因此，ASA 接口会显示在此命令的输出中。ASA 的 IP 地址旁边带有一个星号。

示例

以下是 **show pim neighbor** 命令的输出示例：

```
ciscoasa# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

show pim range-list

要显示 PIM 的范围列表信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim range-list** 命令。

show pim range-list [*rp_address*]

语法说明

rp_address	可以是以下各项之一： • RP 的名称，由域名系统 (DNS) 主机表或者域 **ipv4 host** 命令定义。 • RP 的 IP 地址。这是采用四点分十进制表示法的组播 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令用于确定组映射的组播转发模式。此命令的输出还指明范围的集合点 (RP) 地址（如果适用）。

示例

以下是 **show pim range-list** 命令的输出示例：

```
ciscoasa# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 3:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 3:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

相关命令

命令	说明
show pim group-map	显示组到 PIM 模式的映射和活动 RP 信息。

show pim topology

要显示 PIM 拓扑表信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim topology** 命令。

show pim topology [*group*] [*source*]

语法说明

group	（可选）可以是以下各项之一： • 组播组的名称，由 DNS 主机表或者域 **ipv4 host** 命令定义。 • 组播组的 IP 地址。这是采用四点分十进制表示法的组播 IP 地址。
source	（可选）可以是以下各项之一： • 组播源的名称，由 DNS 主机表或者域 **ipv4 host** 命令定义。 • 组播源的 IP 地址。这是采用四点分十进制表示法的组播 IP 地址。

默认值

显示所有组和源的拓扑信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 PIM 拓扑表可显示给定组、(*, G)、(S, G) 和 (S, G)RPT（它们分别有自己的接口列表）的各个条目。

PIM 通过 MRIB 传达这些条目的内容； MRIB 是组播路由协议（例如 PIM）、本地成员协议（例如互联网组管理协议 [IGMP]）和系统的组播转发引擎之间的通信中介。

MRIB 显示对于给定 (S, G) 条目应在哪个接口接收数据包以及应在哪个接口转发数据包。此外，在转发过程中会使用组播转发信息库 (MFIB) 表，以决定每个数据包的转发操作。

注　要转发信息，请使用 **show mfib route** 命令。

示例

以下是 **show pim topology** 命令的输出示例：

```
ciscoasa# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
```

```
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

相关命令

命令	说明
show mrib route	显示 MRIB 表。
show pim topology reserved	显示保留组的 PIM 拓扑表信息。

show pim topology reserved

要显示保留组的 PIM 拓扑表信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim topology reserved** 命令。

show pim topology reserved

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show pim topology reserved** 命令的输出示例：

```
ciscoasa# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside             00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside              00:00:48  off II
```

相关命令

命令	说明
show pim topology	显示 PIM 拓扑表。

show pim topology route-count

要显示 PIM 拓扑表条目数，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim topology route-count** 命令。

show pim topology route-count [**detail**]

语法说明

detail	（可选）显示每个组更详细的计数信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令显示 PIM 拓扑表的条目数。要显示有关条目的更多信息，请使用 **show pim topology** 命令。

示例

以下是 **show pim topology route-count** 命令的输出示例：

```
ciscoasa# show pim topology route-count

PIM Topology Table Summary
  No.of group ranges = 5
  No.of (*,G) routes = 0
  No.of (S,G) routes = 0
  No.of (S,G)RPT routes = 0
```

相关命令

命令	说明
show pim topology	显示 PIM 拓扑表。

show pim traffic

要显示 PIM 流量计数器，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim traffic** 命令。

show pim traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **clear pim counters** 命令可清除 PIM 流量计数器。

示例

以下是 **show pim traffic** 命令的输出示例：

```
ciscoasa# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

相关命令

命令	说明
clear pim counters	清除 PIM 流量计数器。

show pim tunnel

要显示有关 PIM 隧道接口的信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show pim tunnel** 命令。

show pim tunnel [*if_name*]

语法说明

if_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

默认值

如果不指定接口，此命令会显示所有接口的 PIM 隧道信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC 或特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

PIM 注册数据包通过虚拟封装隧道接口从源第一跳 DR 路由器发送到 RP。在 RP 上，虚拟解封隧道用于代表 PIM 注册数据包的接收接口。此命令显示这两种接口的隧道信息。

注册隧道是通过共享树从源发送到 RP 以供分布的（PIM 注册消息中的）封装组播数据包。注册仅适用于 SM，而不适用于 SSM 和双向 PIM。

示例

以下是 **show pim tunnel** 命令的输出示例：

```
ciscoasa# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

相关命令

命令	说明
show pim topology	显示 PIM 拓扑表。

show port-channel

要在详细的单行摘要表单中显示 EtherChannel 信息或者要显示端口和端口通道信息，请在特权 EXEC 模式下使用 **show port-channel** 命令。

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

语法说明

brief	（默认设置）显示简要信息。
channel_group_number	（可选）指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
detail	（可选）显示详细信息。
port	（可选）显示每个接口的信息。
protocol	（可选）显示 EtherChannel 协议，例如 LACP（如果已启用）。
summary	（可选）显示端口通道摘要。

命令默认

默认设置为 **brief**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.4(1)	我们引入了此命令。

示例

以下是 **show port-channel** 命令的输出示例：

```
ciscoasa# show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

以下是 **show port-channel summary** 命令的输出示例：

```
ciscoasa# show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

以下是 **show port-channel detail** 命令的输出示例：

```
ciscoasa# show port-channel detail
       Channel-group listing:
       ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d
```

```
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel port** 命令的输出示例：

```
ciscoasa# show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
        Ports in the group:
        -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
```

```
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel protocol** 命令的输出示例：

```
ciscoasa# show port-channel protocol
        Channel-group listing:
        ----------------------

Group: 1
----------
Protocol: LACP
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。

命令	说明
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

show port-channel load-balance

对于 EtherChannel，要显示当前的端口通道负载平衡算法，或者要查看为给定参数集选择的成员接口，请在特权 EXEC 模式下输入此命令。

show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **mac** | **l4port** | **mixed** | **vlan-only** *number*} *parameters*]

语法说明

channel_group_number	指定 EtherChannel 信道组编号（1 到 48）。
hash-result	（可选）显示在为当前负载平衡算法输入的哈希值之后选择的成员接口。
ip	（可选）指定 IPv4 数据包参数。
ipv6	（可选）指定 IPv6 数据包参数。
l4port	（可选）指定端口数据包参数。
mac	（可选）指定 MAC 地址数据包参数。
mixed	（可选）指定 IP 或 IPv6 参数的组合以及端口和 / 或 VLAN ID。
parameters	（可选）数据包参数（取决于类型）。例如，对于 **ip**，可以指定源 IP 地址、目标 IP 地址和 / 或 VLAN ID。
vlan-only	（可选）指定数据包的 VLAN ID。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.4(1)	我们引入了此命令。

使用指南

默认情况下，ASA 根据数据包的源 IP 地址和目标 IP 地址 (**src-dst-ip**) 来平衡接口上的数据包负载。要更改算法，请参阅 **port-channel load-balance** 命令。

使用此命令可查看当前负载平衡算法；如果与 **hash-result** 关键字结合使用，此命令还可以测试将为带有给定参数的数据包选择哪个成员接口。此命令仅测试当前负载平衡算法。例如，如果算法是 src-dst-ip，请输入 IPv4 或 IPv6 源 IP 地址和目标 IP 地址。如果您输入当前算法没有使用的其他参数，这些参数将被忽略，且当前算法实际使用的而您没有输入的值将会默认为 0。例如，如果算法是 vlan-src-ip，请输入：

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

如果您输入以下内容，则 vlan-src-ip 算法会假设使用的是源 IP 地址 0.0.0.0 和 VLAN 0，并会忽略您输入的值：

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

示例

以下是 **show port-channel 1 load-balance** 命令的输出示例：

```
ciscoasa# show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 相匹配：

```
ciscoasa# show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination
10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 不匹配，且使用的哈希值为 0：

```
ciscoasa# show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。

show power inline

对于带有 PoE 接口的型号（例如 ASA 5505），可在用户 EXEC 模式下使用 **show power inline** 命令来显示接口的电源状态。

show power inline

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

可以使用 PoE 接口连接需要电源的设备，例如 IP 电话或无线接入点。

示例

以下是 **show power inline** 命令的输出示例：

```
ciscoasa# show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

表 11-1 显示每个字段的说明：

表 11-1　show power inline 字段

字段	说明
Interface	显示 ASA 上的所有接口（包括没有 PoE 可用的接口）。
Power	显示电源是否已开启。如果设备不需要电源，或者该接口上没有设备，或者接口已关闭，则值为 Off。如果接口不支持 PoE，则值为 n/a。
Device	显示正在对其供电的设备类型（Cisco 或 IEEE）。如果设备不需要电源，值为 n/a。如果设备是思科设备，显示屏会显示 Cisco。IEEE 表示设备是符合 IEEE 802.3af 标准的设备。

相关命令

命令	说明
clear configure interface	清除接口的所有配置。
clear interface	清除 **show interface** 命令的计数器。
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。

show priority-queue statistics

要显示接口的优先级队列统计信息，请在特权 EXEC 模式下使用 **show priority-queue statistics** 命令。

show priority-queue statistics [*interface-name*]

语法说明

interface-name	（可选）指定要显示尽力而为队列和低延迟队列详细信息的接口的名称。

默认值

如果省略接口名称，此命令会显示所有配置的接口的优先级队列统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示对名为 test 的接口使用 **show priority-queue statistics** 命令以及命令输出。在以下输出中，BE 表示 “ 尽力而为 ” 队列，LLQ 表示低延迟队列：

```
ciscoasa# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
ciscoasa#
```

相关命令

命令	说明
clear configure priority-queue	从指定接口删除优先级队列配置。
clear priority-queue statistics	清除某个接口或所有配置的接口的优先队列统计信息计数器。
priority-queue	配置优先级队列。在接口上。
show running-config priority-queue	显示指定接口的当前优先级队列配置。

show processes

要显示正在 ASA 上运行的进程的列表，请在特权 EXEC 模式下使用 **show processes** 命令。

show processes [**cpu-usage** [[**non-zero**][**sorted**]] [**cpu-hog** | **memory** | **internals**]

语法说明

cpu-hog	显示正在大量占用 CPU（即使用 CPU 超过 100 毫秒）的进程的数量及详细信息。
cpu-usage	显示在最近的 5 秒、1 分钟和 5 分钟内每个进程的 CPU 使用率。
internals	显示每个进程的内部详细信息。
memory	显示每个进程的内存分配。
non-zero	（可选）显示 CPU 使用率不是 0 的进程。
sorted	（可选）显示已排序的进程 CPU 使用率。

默认值

默认情况下，此命令显示正在 ASA 上运行的进程。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	我们引入了此命令。
7.0(4)	改进了运行时间值，现在的准确性达到 1 毫秒以内。
7.2(1)	改进了输出，现在可显示有关大量占用 CPU 的进程的更多详细信息。
8.0(1)	增加了 **cpu-usage** 关键字。
9.2(1)	改进了输出，现在可显示 CPU 大量占用检测信息。

使用指南

进程是只需要几个指令的轻量级线程。**show processes** 命令显示正在 ASA 上运行的进程的列表，如下所示：

命令	显示的数据	说明
show processes	PC	程序计数器。
show processes	Stack Pointer	堆栈指针。
show processes	STATE	线程队列的地址。
show processes	Runtime	线程根据 CPU 时钟周期已运行的毫秒数。对于基于 CPU 时钟周期（小于 10 纳秒分辨率）而非时钟计时周期（10 毫秒分辨率）的完整、准确的进程 CPU 使用率计算，准确性达到 1 毫秒以内。

命令	显示的数据	说明
show processes	SBASE	堆栈基址。
show processes	Stack	当前使用中的字节数以及堆栈的总大小。
show processes	Process	线程的功能。
show processes cpu-usage	MAXHOG	最大 CPU 大量占用运行时间，以毫秒为单位。
show processes cpu-usage	NUMHOG	CPU 大量占用运行次数。
show processes cpu-usage	LASTHOG	上一次 CPU 大量占用运行时间，以毫秒为单位。
show processes cpu-usage	PC	CPU 大量占用进程的指令指针。
show processes cpu-usage	Traceback	CPU 大量占用进程的堆栈跟踪。最多可回溯 14 个地址。
show processes internals	Invoked Calls	调度程序运行进程的次数。
show processes internals	Giveups	进程将 CPU 归还给调度程序的次数。

使用 **show processes cpu-usage** 命令可将匹配范围缩小到 ASA 上可能正在使用 ASA 的 CPU 的特定进程。可使用 **sorted** 和 **non-zero** 命令进一步定制 **show processes cpu-usage** 命令的输出。

借助调度程序和总摘要行，您可以连续运行两个 **show proccesses** 命令，并比较输出以确定：

- CPU 占用率。
- 每个线程的 CPU 使用率（通过将具体线程的运行时间增量与总运行时间增量作比较来确定）。

示例

以下示例展示如何显示正在 ASA 上运行的进程的列表：

```
ciscoasa# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
```

以下示例展示如何显示每个进程的 CPU 使用率：

```
ciscoasa# show proc cpu-usage non-zero
PC          Thread      5Sec    1Min    5Min    Process
0818af8e    d482f92c    0.1%    0.1%    0.1%    Dispatch Unit
08bae136    d48180f0    0.1%    0.0%    0.2%    ssh
-------------------------------------
```

以下示例展示如何显示正在大量占用 CPU 的进程的数量及详细信息：

```
ciscoasa# show processes cpu-hog
Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
```

CPU 大量占用回溯的剩余部分如下：

```
Process:      DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
LASTHOG At:   15:42:21 UTC Jan 6 2014
PC:           0x0000000000000000 (suspend)
```

```
Call stack:   0x000000000041c98c  0x000000000041cc99  0x000000000069b0f0
              0x00000000013619af  0x000000000136cbbd  0x0000000001372203
              0x00007ffffeab2f3a
              Interrupt based hog #1
              Hog #1, traceback #1, at:   15:41:16 UTC Jan 6 2014, hog 20 ms
              PC:           0x0000000000eb616b
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
                            0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af
              Hog #1, traceback #2, at:   15:41:16 UTC Jan 6 2014, hog 21 ms
              PC:           0x0000000000e8fc41
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af  0x000000000136cbbd
                            0x0000000001372203  0x00007ffffeab2f3a
              Interrupt based hog #2
              Hog #2, traceback #1, at:   15:41:36 UTC Jan 6 2014, hog 9 ms
              PC:           0x0000000000eb6167
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
                            0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af
              Interrupt based hog #3
              Hog #3, traceback #1, at:   15:42:21 UTC Jan 6 2014, hog 2 ms
              PC:           0x000000000068a223
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x000000000069bbba
                            0x000000000069b0a4  0x00000000013619af  0x000000000136cbbd
                            0x0000000001372203  0x00007ffffeab2f3a
```

以下示例展示如何显示每个进程的内存分配：

```
ciscoasa# show processes memory

------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
```

以下示例展示如何显示每个进程的内部详细信息：

```
ciscoasa# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

相关命令

命令	说明
show cpu	显示 CPU 使用情况信息。

show quota management-session

要显示当前管理会话的统计信息，请在特权 EXEC 模式下使用 **show quota management-session** 命令。

show quota management-session

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令显示当前管理会话的以下统计信息：

- 限制
- 警告级别
- 当前计数
- 上限
- 生成的警告数量
- 生成的错误数量

示例

以下示例展示当前管理会话的统计信息：

```
ciscoasa# show quota management-session
quota management-session limit 250
quota management-session warning level 225
quota management-session level 1
quota management-session high water 1
quota management-session errors 0
quota management-session warnings 0
```

相关命令

命令	说明
show running-config quota management-session	显示管理会话配额的当前值。
quota management-session	设置设备上允许的并发 ASDM、SSH 和 Telnet 会话的数量。

show reload

要显示 ASA 的重新加载状态，请在特权 EXEC 模式下使用 **show reload** 命令。

show reload

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令没有使用指南。

示例

以下示例展示计划在 4 月 20 日（周六） 12:00 a.m（午夜）重新加载：

```
ciscoasa# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

相关命令

命令	说明
reload	重新启动并重新加载配置。

show resource allocation

要显示所有类和类成员的每个资源的分配情况，请在特权 EXEC 模式下使用 **show resource allocation** 命令。

show resource allocation [**detail**]

语法说明

detail	显示其他信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	创建了一个新的资源类 (routes)，以在每个情景中设置路由表条目的最大数量。 创建了新的资源类型（即 vpn other 和 vpn burst other），以在每个情景中设置站点间 VPN 隧道的最大数量。

使用指南

此命令显示资源分配情况，但不显示实际正在使用的资源。有关实际资源使用情况的更多信息，请参阅 **show resource usage** 命令。

示例

以下是 **show resource allocation** 命令的输出示例。在以下输出中，每个资源的总体分配情况显示为绝对值以及可用系统资源所占的百分比。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Routes                     25000           0.00%
 Xlates                     91749           N/A
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

表 11-2 显示每个字段的说明。

表 11-2　show resource allocation 字段

字段	说明
Resource	可限制的资源的名称。
Total	在所有情景中分配的资源总量。此数量是每秒并发实例或实例的绝对数量。如果您在类定义中指定了百分比，ASA 会在显示此值时将百分比转换为绝对数量。
% of Avail	在所有情景中分配的总系统资源的百分比（如果可用）。如果资源没有系统限制，此列将显示 N/A。

以下是 **show resource allocation detail** 命令的输出示例：

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
```

```
                  All Contexts:      3                              20      20.00%
Routes            default          all       C  unlimited                   N/A
                  gold               1       D  unlimited             5     N/A
                  silver             1      CA         10            10     N/A
                  bronze             0      CA          5                   N/A
                  All Contexts:      3                              20      N/A

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040      N/A
                  bronze             0      CA      11520
                  All Contexts:      3                         23040      N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535   100.00%
                  silver             1      CA       6553       6553     9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                        137623   209.99%
```

表 11-3 显示每个字段的说明。

表 11-3　show resource allocation detail 字段

字段	说明
Resource	可限制的资源的名称。
Class	每个类（包括默认类）的名称。 All contexts 字段显示所有类的总值。
Mmbrs	分配给每个类的情景数量。
Origin	资源限制的起源，如下所示： • A - 限制是通过 **all** 选项设置的，而不是作为单个资源设置的。 • C - 限制源于成员类。 • D - 限制未在成员类中定义，但源于默认类。对于分配给默认类的情景，值将会是 “C” 而不是 “D”。 ASA 可以将 “A” 和 “C” 或 “D” 结合使用。
Limit	每个情景的资源限制，显示为绝对数量。如果您在类定义中指定了百分比，ASA 会在显示此值时将百分比转换为绝对数量。
Total	在类的所有情景中分配的资源总量。此数量是每秒并发实例或实例的绝对数量。如果资源没有限制，将显示为空白。
% of Avail	在类的所有情景中分配的总系统资源的百分比（如果可用）。如果资源没有限制，将显示为空白。如果资源没有系统限制，此列将显示 N/A。

相关命令

命令	说明
class	Creates a resource class.
context	添加安全情景。
limit-resource	设置类的资源限制。
show resource types	显示可为其设置限制的资源类型。
show resource usage	显示 ASA 的资源使用情况。

show resource types

要查看 ASA 跟踪其使用情况的资源类型，请在特权 EXEC 模式下使用 **show resource types** 命令。

show resource types

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令显示您可以为每个情景管理的其他资源类型。
9.0(1)	创建了一个新的资源类 (routes)，以在每个情景中设置路由表条目的最大数量。 创建了新的资源类型（即 vpn other 和 vpn burst other），以在每个情景中设置站点间 VPN 隧道的最大数量。

示例

以下示例展示资源类型：

```
ciscoasa# show resource types

Rate limited resource types:
Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  Routes          Routing Table Entries
  Other-vpn       Other VPN licenses
  Other-vpn-burst Allowable burst for Other VPN licenses
  All             All Resources
```

相关命令

命令	说明
clear resource usage	清除资源使用统计信息
context	添加安全情景。
show resource usage	显示 ASA 的资源使用情况。

show resource usage

要查看 ASA 的资源使用情况或多模式下每个情景的资源使用情况，请在特权 EXEC 模式下使用 **show resource usage** 命令。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**]
[**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

语法说明

context *context_name*	（仅限多模式）指定要查看统计信息的情景名称。指定 **all** 可查看所有情景的统计信息； ASA 列出每个情景的使用情况。
count_threshold	设置要显示资源须达到的资源使用量下限。默认值为 1。如果资源使用量低于所设置的数值，则不会显示资源。如果为计数器名称指定 **all**，则 *count_threshold* 适用于当前使用量。 **注**　要显示所有资源，请将 *count_threshold* 设置为 **0**。
counter *counter_name*	显示以下计数器类型的计数： • **current** - 显示活动并发实例数或资源的当前使用率。 • **peak** - 显示峰值并发实例数或者自上一次清除统计信息以来（使用 **clear resource usage** 命令或由于设备重新启动）资源的峰值使用率。 • **denied** - 显示由于超过 Limit 列所示的资源限制而被拒绝的实例的数量。 • **all** -（默认设置）显示所有统计信息。
detail	显示所有资源（包括不能管理的资源）的使用情况。例如，可以查看 TCP 拦截次数。
resource [**rate**] *resource_name*	显示特定资源的使用情况。为所有资源指定 **all**（默认值）。指定 **rate** 可显示资源的使用率。按使用率测量的资源包括 **conns**、**inspects** 和 **syslogs**。对于这些资源类型，必须指定 **rate** 关键字。conns 资源也可以按并发连接数来测量；要查看每秒连接数，必须使用 **rate** 关键字。 资源包括以下类型： • **asdm** - ASDM 管理会话。 • **conns** - 任意两台主机（包括一台主机和多台其他主机之间的连接）之间的 TCP 或 UDP 连接。 • **inspects** - 应用检查。 • **hosts** - 可通过 ASA 连接的主机。 • **mac-addresses** - 对于透明防火墙模式，MAC 地址表中允许的 MAC 地址数量。 • **routes -** 路由表条目。 • **ssh** - SSH 会话。 • **syslogs** - 系统日志消息。 • **telnet** - Telnet 会话。 • （仅限多模式）**VPN Other** - 站点间 VPN 会话。 • （仅限多模式）**VPN Burst Other** - 站点间 VPN 突发会话。 • **xlates** - NAT 转换。

summary	（仅限多模式）显示汇总的所有情景使用情况。
system	（仅限多模式）显示汇总的所有情景使用情况，但显示资源的系统限制而不显示汇总的情景限制。
top *n*	（仅限多模式）显示是指定资源的前 *n* 个用户的情景。对于此选项，必须指定一种资源类型，而不能指定 **resource all**。

默认值

对于多情景模式，默认情景为 **all**（显示每个情景的资源使用情况）。对于单模式，情景名称将被忽略，且输出将 “context” 显示为 “System”。

默认资源名称为 **all**（显示所有资源类型）。

默认计数器名称为 **all**（显示所有统计信息）。

默认计数阈值为 **1**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令显示被拒绝的资源，因为您可以限制每个情景的资源。
9.0(1)	创建了一个新的资源类 (routes)，以在每个情景中设置路由表条目的最大数量。 创建了新的资源类型（即 vpn other 和 vpn burst other），以在每个情景中设置站点间 VPN 隧道的最大数量。

示例

以下是 **show resource usage context** 命令的输出示例，其中显示管理情景的资源使用情况：

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

以下是 **show resource usage summary** 命令的输出示例，其中显示所有情景和所有资源的资源使用情况。以下示例展示 6 个情景的限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
```

```
Conns [rate]                270          535        42200        1704 Summary
Inspects [rate]             270          535       100000(S)        0 Summary
Other VPN Sessions            0           10           10         740 Summary
Other VPN Burst               0           10           10         730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下是 **show resource usage system** 命令的输出示例，其中显示所有情景的资源使用情况，但显示系统限制而不显示汇总的情景限制：

```
ciscoasa# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

以下是 **show resource usage detail counter all 0** 命令的输出示例，其中显示所有资源（而非只显示可以管理的资源）：

```
ciscoasa# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
chunk:ether                 0            0  unlimited             0 admin
chunk:est                   0            0  unlimited             0 admin

...

Telnet                      0            0          5             0 admin
SSH                         1            1          5             0 admin
ASDM                        0            1          5             0 admin
Syslogs [rate]              0           68  unlimited             0 admin
aaa rate                    0            0  unlimited             0 admin
url filter rate             0            0  unlimited             0 admin
Conns                       1            6  unlimited             0 admin
Xlates                      0            0  unlimited             0 admin
tcp conns                   0            0  unlimited             0 admin
Hosts                       2            3  unlimited             0 admin
Other VPN Sessions          0           10        750           740 admin
Other VPN Burst             0           10        750           730 admin
udp conns                   0            0  unlimited             0 admin
smtp-fixups                 0            0  unlimited             0 admin
Conns [rate]                0            7  unlimited             0 admin
establisheds                0            0  unlimited             0 admin
pps                         0            0  unlimited             0 admin
syslog rate                 0            0  unlimited             0 admin
bps                         0            0  unlimited             0 admin
Fixups [rate]               0            0  unlimited             0 admin
non tcp/udp conns           0            0  unlimited             0 admin
tcp-intercepts              0            0  unlimited             0 admin
```

```
globals                    0           0  unlimited           0 admin
np-statics                 0           0  unlimited           0 admin
statics                    0           0  unlimited           0 admin
nats                       0           0  unlimited           0 admin
ace-rules                  0           0        N/A           0 admin
aaa-user-aces              0           0        N/A           0 admin
filter-rules               0           0        N/A           0 admin
est-rules                  0           0        N/A           0 admin
aaa-rules                  0           0        N/A           0 admin
console-access-rul         0           0        N/A           0 admin
policy-nat-rules           0           0        N/A           0 admin
fixup-rules                0           0        N/A           0 admin
aaa-uxlates                0           0  unlimited           0 admin
CP-Traffic:IP              0           0  unlimited           0 admin
CP-Traffic:ARP             0           0  unlimited           0 admin
CP-Traffic:Fixup           0           0  unlimited           0 admin
CP-Traffic:NPCP            0           0  unlimited           0 admin
CP-Traffic:Unknown         0           0  unlimited           0 admin
```

相关命令

命令	说明
class	创建一个资源类。
clear resource usage	清除资源使用统计信息
context	添加安全情景。
limit-resource	设置类的资源限制。
show resource types	显示资源类型列表。

show rest-api agent

要确定 REST API 代理当前是否已启用，请在特权 EXEC 模式下使用 **show rest-api agent** 命令。

show rest-api agent

注　所有版本的 ASAv、ASA 5585-X、ASA 5506-X 和 ASA 5508-X 以外的所有 ASA 5500-X 系列设备上支持此命令。

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	是	—	—

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

使用此命令可确定 REST API 代理当前是否已启用。

示例

以下示例指明 REST API 代理已启用：

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

如果代理被禁用，消息将显示为 “REST API agent is currently disabled”。

相关命令

命令	说明
rest-api	验证并安装 REST API 软件包。启用 REST API 代理。
show version	如果 REST API 代理已启用，其版本号将包含在 **show version** 输出中。

show rip database

要显示存储在 RIP 拓扑数据库中的信息，请在特权 EXEC 模式下使用 **show rip database** 命令。

show rip database [*ip_addr* [*mask*]]

语法说明

ip_addr	（可选）限制要为指定网络地址显示的路由。
mask	（可选）指定可选网络地址的网络掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	•	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

与 RIP 路由相关的 **show** 命令可在 ASA 的特权 EXEC 模式下使用。您无需处于 RIP 配置模式即可使用 RIP 相关的 **show** 命令。

RIP 数据库包含通过 RIP 获知的所有路由。在该数据库中出现的路由不一定出现在路由表中。有关如何用路由协议数据库中的条目填充路由表的信息，请参阅*《思科安全设备命令行配置指南》*。

示例

以下是 **show rip database** 命令的输出示例：

```
ciscoasa# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

以下是 **show rip database** 命令的输出示例，其中包含网络地址和网络掩码：

```
Router# show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
    [1] via 172.19.67.38, 0:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

相关命令

命令	说明
router rip	启用 RIP 路由并配置全局 RIP 路由参数。

show route

要显示路由表，请在特权 EXEC 模式下使用 **show route** 命令。

show route [*interface_name* [*ip_address* [*netmask* [**static**]]]] [**failover**] [**cluster**] [**zone**]

语法说明

cluster	（可选）显示路由信息库 (RIB) 代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。
failover	（可选）显示出现故障切换且备用设备变为主用设备后的当前路由表序列号和路由条目数。
interface_name	（可选）限制为仅显示使用指定接口的路由条目。
ip_address	（可选）限制为仅显示指向指定目标的路由。
netmask	（可选）定义要应用于指定目标的网络掩码。
static	（可选）限制为仅显示静态路由。
zone	（可选）显示区域接口的路由。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	增加了 **failover** 关键字。输出显示 RIB 代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。
9.0(1)	增加了 **cluster** 关键字。适用于动态路由协议（EIGRP、OSPF 和 RIP），仅在 ASA 5580 和 5585-X 上可用。
9.2(1)	现在，此命令显示本地主机路由和连接的路由。引入了新代码（L、I、E、su 和 +），用于表示所显示的路由的协议或类型。
9.3(2)	添加了 **zone** 关键字。

使用指南

show route 命令的输出类似于 **show ipv6 route** 命令的输出，唯一不同之处是，前者显示的信息是 IPv4 特定信息。

注　**clustering** 和 **failover** 关键字不会显示，除非在 ASA 上配置了那些功能。

show route 命令列出可用于新连接的 “ 最佳 ” 路由。如果您将允许的 TCP SYN 发送到备用接口，ASA 只能使用同一个接口作出响应。如果该接口上的 RIB 中没有默认路由，ASA 将会由于没有相邻关系而丢弃数据包。**show running-config route** 命令中所示的所有配置将保留在系统的某些数据结构中。

使用 **show asp table routing** 命令可查看特定于后端接口的路由表。这一设计类似于 OSPF 或 EIGRP，其中的协议特定路由数据库不同于全局路由表，后者仅显示 “ 最佳 ” 路由。此行为是有意设计的行为。

注意　在思科 IOS 中使用 **show ip route** 命令时，**longer-prefix** 关键字可用。如果在思科 IOS 中使用此关键字，仅在指定网络和掩码对相匹配的情况下才会显示路由。

在 ASA 上，**longer-prefix** 关键字是 **show route** 命令的默认行为；也就是说，CLI 中不需要其他关键字。因此，键入 **ip** 不能看到路由。要获取超级网络路由，必须与 IP 地址一起传递掩码值。

示例

以下是 **show route** 命令的输出示例：

```
ciscoasa# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

以下是 **show route** 命令在 ASA 5555 的管理情景中的输出示例： 以下输出显示内部环回地址（VPN 硬件客户端使用该地址进行个人用户身份验证）。

```
ciscoasa/admin(config)# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

以下是 **show route failover** 命令的输出示例，其中显示在故障切换后 OSPF 和 EIGRP 路由与备用设备之间的同步情况：

```
ciscoasa(config)# show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

以下是 **show route cluster** 命令的输出示例：

```
ciscoasa(cfg-cluster)# show route cluster

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route


Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

请参阅 **show route zone** 命令的以下输出：

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

show route bgp

要显示路由表，请在特权 EXEC 模式下使用 **show route bgp** 命令。

show route [bgp [*as_number*]**]**

语法说明

bgp	（可选）显示 BGP 路由的路由信息库 (RIB) 代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。
as_number	（可选）限制为仅显示使用指定 AS 编号的路由条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

show route bgp 命令的输出类似于 **show route** 命令的输出，唯一不同之处是，前者显示的信息是 BGP 特定信息。

show route bgp 命令列出可用于新 BGP 连接的 “ 最佳 ” 路由。

以下是 **show route bgp** 命令的输出示例：

```
ciscoasa# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

show route eigrp

要显示路由表，请在特权 EXEC 模式下使用 **show route eigrp** 命令。

show route [eigrp [*process-id*]**]**

语法说明

eigrp	（可选）显示路由信息库 (RIB) 纪元号（序列号）、当前计时器值，以及 EIGRP 路由的网络描述符块纪元号（序列号）。
process-id	（可选）限制为仅显示使用指定进程 ID 的路由条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

show route eigrp 命令的输出类似于 **show route** 命令的输出，唯一不同之处是，前者显示的信息是 EIGRP 特定信息。

show route eigrp 命令列出可用于新 BGP 连接的 “ 最佳 ” 路由。

以下是 **show route eigrp** 命令的输出示例：

```
ciscoasa# show route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

show route summary

要显示路由表的当前状态，请在特权 EXEC 模式下使用 **show route summary** 命令。

show route summary

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

show route summary 命令显示路由表的当前状态。

以下是 **show route summary** 命令的输出示例：

```
ciscoasa# show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

第 12 章

show running-config 至 show switch vlan 命令

show running-config

要显示 ASA 上当前运行的配置，请在特权 EXEC 模式下使用 **show running-config** 命令。

show running-config [**all**] [*command*]

语法说明

all	显示整个运行配置，包括默认设置。
command	显示与特定命令关联的配置。有关可用命令，请使用 **show running-config ?** 参阅 CLI 帮助。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.3(1)	命令输出会显示加密密码。

使用指南

show running-config 命令用于显示 ASA 上的内存中的活动配置（包括保存的配置更改）。

要显示 ASA 上的闪存中保存的配置，请使用 **show configuration** 命令。

show running-config 命令输出显示当启用或禁用密码加密时的加密、屏蔽或明文密码。

注　当使用 ASDM 命令连接或配置 ASA 后，该命令将出现在配置中。

示例

以下是 **show running-config** 命令的输出示例：

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
```

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
```

```
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

以下是 **show running-config access-group** 命令的输出示例：

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

以下是 **show running-config arp** 命令的输出示例：

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

相关命令

命令	说明
clear configure	清除运行配置。
show configuration	显示启动配置。

show scansafe server

要显示云网络安全代理服务器的状态，请在特权 EXEC 模式下使用 **show scansafe server** 命令。

show scansafe server

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

此命令显示服务器的状态，是当前活动服务器、备用服务器还是无法访问。

示例

以下是 **show scansafe server** 命令的输出示例：

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。

命令	说明
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

show scansafe statistics

要显示有关 云网络安全 活动的信息，请在特权 EXEC 模式下使用 **show scansafe statistics** 命令。

show scansafe statistics

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

show scansafe statistics 命令用于显示有关 云网络安全 活动的信息，如重新定向到代理服务器的连接数、当前正在重新定向的连接数以及白名单连接数。

示例

以下是 **show scansafe statistics** 命令的输出示例：

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。

命令	说明
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

show service-policy

要显示服务策略统计信息，请在特权 EXEC 模式下使用 **show service-policy** 命令。

show service-policy [**global** | **interface** *intf*] [**csc** | **cxsc** | **inspect** *inspection* [*arguments*] | **ips** | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

语法说明

csc	（可选）显示有关包括 **csc** 命令的策略的详细信息。
cxsc	（可选）显示有关包括 **cxsc** 命令的策略的详细信息。
dest_ip dest_mask	对应 **flow** 关键字，指流量流的目标 IP 地址和子网掩码。
details	（可选）对应 **set connection** 关键字，如果启用每客户端连接限制，则显示每客户端连接信息。
eq *dest_port*	（可选）对应 **flow** 关键字，等于流的目标端口。
eq *src_port*	（可选）对应 **flow** 关键字，等于流的源端口。
flow *protocol*	（可选）显示与通过 5 元组（协议、源 IP 地址、源端口、目标 IP 地址、目标端口）标识的特定流匹配的策略。您可以使用此命令检查服务策略配置是否将提供特定连接所需的服务。 由于流以 5 元组的形式描述，因此并非所有策略都受到支持。请参阅以下受支持的策略匹配： • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	（可选）限制全局策略的输出。
host *dest_host*	对应 **flow** 关键字，指流量流的主机目标 IP 地址。
host *src_host*	对应 **flow** 关键字，指流量流的主机源 IP 地址。
icmp_control_message	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 控制消息。
icmp_number	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 协议编号。
inspect *inspection* [*arguments*]	（可选）显示有关包括 **inspect** 命令的策略的详细信息。并非所有 **inspect** 命令都受到详细输出支持。要查看所有检查，请使用 **show service-policy** 命令且不带任何参数。各个检查的可用参数各不相同；请参阅 CLI 帮助以获取更多信息。
interface *intf*	（可选）显示应用到通过 *intf* 参数指定的接口的策略，其中 *intf* 是 **nameif** 命令给定的接口名称。
ips	（可选）显示有关包括 **ips** 命令的策略的详细信息。
police	（可选）显示有关包括 **police** 命令的策略的详细信息。
priority	（可选）显示有关包括 **priority** 命令的策略的详细信息。
set connection	（可选）显示有关包括 **set connection** 命令的策略的详细信息。

sfr	（可选）显示有关包括 **sfr** 命令的策略的详细信息。
shape	（可选）显示有关包括 **shape** 命令的策略的详细信息。
src_ip src_mask	对应 **flow** 关键字，指流量流中使用的源 IP 地址和子网掩码。
user-statistics	（可选）显示有关包括 **user-statistics** 命令的策略的详细信息。此命令用于显示身份防火墙的用户统计信息，包括发送的数据包计数，发送的丢弃计数、收到的数据包计数和针对选定用户发送的丢弃计数。

默认值

如果不指定任何参数，此命令将显示所有全局接口策略。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	增加了 **csc** 关键字。
7.2(4)/8.0(4)	增加了 **shape** 关键字。
8.4(2)	我们增加了对用于身份防火墙的 **user-statistics** 关键字的支持。
8.4(4.1)	我们增加了对用于 ASA CX 模块的 **cxsc** 关键字的支持。
9.2(1)	我们增加了对用于 ASA FirePOWER 模块的 **sfr** 关键字的支持。

使用指南

show service-policy 命令输出中显示的初期连接数指示到通过 **class-map** 命令定义的用于匹配流量的接口的当前初期连接数。“embryonic-conn-max” 字段展示了针对使用模块化策略框架配置的流量类最大初期限制。如果所显示的当前初期连接数等于或超过最大值，将对与通过 **class-map** 命令定义的流量类型相匹配的新 TCP 连接应用 TCP 拦截。

当对配置进行服务策略更改后，所有*新*连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。**show** 命令输出不会包含有关旧连接的数据。例如，如果从接口删除 QoS 服务策略，然后重新添加一个修改版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；基于旧策略的现有连接不再显示在命令输出中。要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略重新连接。请参阅 **clear conn** 或 **clear local-host** 命令。

注　对于 **inspect icmp** 和 **inspect icmp error** 策略，数据包计数只包括回应请求和应答数据包。

示例

以下是 **show service-policy global** 命令的输出示例：

```
ciscoasa# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

以下是 **show service-policy priority** 命令的输出示例：

```
ciscoasa# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

以下是 **show service-policy flow** 命令的输出示例：

```
ciscoasa# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

以下是 **show service-policy inspect http** 命令的输出示例： 此示例展示 match-any 类映射中的每个匹配命令的统计信息。

```
ciscoasa# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
```

```
        Match: request method connect, 0 packets
        log, packet 648
```

以下是 **show service-policy inspect waas** 命令的输出示例： 此示例展示 waas 统计信息。

```
ciscoasa# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
       SYN with WAAS option 4
       SYN-ACK with WAAS option 4
       Confirmed WAAS connections 4
       Invalid ACKs seen on WAAS connections 0
       Data exceeding window size on WAAS connections 0
```

以下是 **show gtp requests** 命令的输出示例：

```
ciscoasa# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

您可以使用垂直线 | 过滤显示，如以下示例所示：

```
ciscoasa# show service-policy gtp statistics | grep gsn
```

此示例展示了输出中带 gsn 一词的 GTP 统计信息。

以下命令显示 GTP 检查的统计信息：

```
ciscoasa# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

表 12-1 介绍了 **show service-policy inspect gtp statistics** 命令输出的每个列。

表 12-1　GPRS GTP Statistics

列标题	说明
version_not_support	显示具有不支持的 GTP 版本字段的数据包。
msg_too_short	显示长度小于 8 字节的数据包。
unknown_msg	显示未知类型消息。
unexpected_data_msg	显示意外数据消息。
mandatory_ie_missing	显示缺少必需信息元素 (IE) 的消息。
mandatory_ie_incorrect	显示具有格式不正确的必需信息元素 (IE) 的消息。
optional_ie_incorrect	显示具有格式不正确的可选信息元素 (IE) 的消息。
ie_unknown	显示具有未知信息元素 (IE) 的消息。

表 12-1　GPRS GTP Statistics（续）

列标题	说明
ie_out_of_order	显示具有失序信息元素 (IE) 的消息。
ie_unexpected	显示具有意外信息元素 (IE) 的消息。
total_forwarded	显示转发的消息总数。
total_dropped	显示丢弃的消息总数。
signalling_msg_dropped	显示丢弃的信令消息数。
data_msg_dropped	显示丢弃的数据消息数。
signalling_msg_forwarded	显示转发的信令消息数。
data_msg_forwarded	显示转发的数据消息数。
total created_pdp	显示所创建的数据包数据协议 (PDP) 情景总数。
total deleted_pdp	显示删除的数据包数据协议 (PDP) 情景总数。
total created_pdpmcb	显示所创建的 PDPMCB 会话总数。
total deleted_pdpmcb	显示删除的 PDPMCB 会话总数。
pdp_non_existent	显示为不存在的 PDP 情景接收的消息数。

以下命令显示有关 PDP 情景的信息：

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 12-2 介绍了 **show service-policy inspect gtp pdp-context** 命令输出的每个列。

表 12-2　PDP 情景

列标题	说明
Version	显示 GTP 版本。
TID	显示隧道标识符。
MS Addr	显示移动站地址。
SGSN Addr	显示服务网关服务节点。
Idle	显示未使用 PDP 情景的时间。
APN	显示接入点名称。

相关命令

命令	说明
clear configure service-policy	清除服务策略配置。
clear service-policy	清除所有服务策略配置。
service-policy	配置服务策略。
show running-config service-policy	显示在运行配置中配置的服务策略。

show shared license

要显示共享许可证统计信息，请在特权 EXEC 模式下使用 **show shared license** 命令。可选关键字仅适用于许可服务器。

show shared license [**detail** | **client** [*hostname*] | **backup**]

语法说明

backup	（可选）显示有关备用服务器的信息。
client	（可选）限制对参与者的显示。
detail	（可选）显示所有统计信息，包括每个参与者的统计信息。
hostname	（可选）限制对特定参与者的显示。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

要清除统计信息，请输入 **clear shared license** 命令。

示例

以下是许可证参与者上 **show shared license** 命令的输出示例：

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
```

```
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

表 12-3 介绍了 **show shared license** 命令的输出。

表 12-3　show shared license 说明

字段	说明
Primary License Server	主服务器的 IP 地址。
Version	共享许可证版本。
Status	如果在备用服务器上发出该命令，则 “Active”（活动）表示此设备已承担主共享许可服务器的角色。“Inactive”（非活动）表示设备处于备用模式，并且设备正在与主服务器通信。 如果在主许可服务器上配置了故障切换，备用服务器可能在故障切换期间短暂变为 “Active”（活动）状态，但在通信重新同步后应恢复 “Inactive”（非活动）状态。
Shared license utilization	
SSLVPN	
Total for network	显示可用共享会话的总数。
Available	显示剩余的可用共享会话数。
Utilized	显示为活动许可证服务器获取的共享会话数。
This device	
Platform limit	显示此设备的符合已安装许可证的 SSL VPN 会话总数。
Current usage	显示此设备在共享池中当前拥有的共享 SSL VPN 会话数。
High usage	显示此设备拥有的共享 SSL VPN 会话的最大数。
Messages Tx/Rx/Error	
Registration Get Release Transfer	显示每种连接类型的 “ 已发送 ”、“ 已接收 ” 和 “ 错误 ” 数据包数。
Client ID	唯一客户端 ID。
Usage	显示正在使用的会话数。
Hostname	显示此设备的主机名。

以下是许可证服务器上 **show shared license detail** 命令的输出示例：

```
ciscoasa# show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
```

```
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	清除共享许可证统计信息。
license-server address	标识参与者的共享许可服务器的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

show shun

要显示 shun 信息，请在特权 EXEC 模式下使用 **show shun** 命令。

show shun [*src_ip* | *statistics*]

语法说明

src_ip	（可选）显示该地址的信息。
statistics	（可选）仅显示接口计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

示例

以下是 **show shun** 命令的输出示例：

```
ciscoasa# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

相关命令

命令	说明
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
shun	阻止新连接并禁止通过任何现有连接传输数据包，从而允许对攻击主机作出动态响应。

show sip

要显示 SIP 会话，请在特权 EXEC 模式下使用 **show sip** 命令。

show sip

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show sip 命令协助排查 SIP 检查引擎问题，通过 **inspect protocol sip udp 5060** 命令描述。**show timeout sip** 命令显示指定协议的超时值。

show sip 命令显示 ASA 中建立的 SIP 会话的信息。连同 **debug sip** 和 **show local-host** 命令，此命令用于排查 SIP 检查引擎问题。

注　建议先配置 **pager** 命令，再使用 **show sip** 命令。如果有许多 SIP 会话记录并且未配置 **pager** 命令，则 **show sip** 命令输出需要一段时间才能输出全部内容。

示例

以下是 **show sip** 命令的输出示例：

```
ciscoasa# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
|state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
|state Active, idle 0:00:06
```

此示例展示了 ASA 上的两个活动 SIP 会话（如 `Total`（总数）字段中所示）。每个 `call-id` 代表一个呼叫。

第一个会话的 `call-id` 为 `c3943000-960ca-2e43-228f@10.130.56.44`，其处于 `Call Init` 状态，表示会话仍在呼叫设置中。只有看到 ACK 时，才说明呼叫设置完成。此会话已空闲 1 秒。

第二个会话处于 `Active` 状态，其中呼叫设置已完成，终端正在交换媒介。此会话已空闲 6 秒。

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug sip	启用 SIP 的调试信息。
inspect sip	启用 SIP 应用检查。
show conn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。

show skinny

要排查 SCCP (Skinny) 检查引擎问题，请在特权 EXEC 模式下使用 **show skinny** 命令。

show skinny

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show skinny 命令辅助排查 SCCP (Skinny) 检查引擎问题。

示例

以下是 **show skinny** 命令在下列条件下的输出示例。ASA 中设置了两个活动 Skinny 会话。第一个建立在位于本地地址 10.0.0.11 的内部思科 IP 电话与位于 172.18.1.33 的外部 Cisco CallManager 之间。TCP 端口 2000 为 CallManager。第二个建立在位于本地地址 10.0.0.22 的另一个内部思科 IP 电话与同一 Cisco CallManager 之间。

```
ciscoasa# show skinny

        LOCAL                   FOREIGN                 STATE

----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

输出指示已在两个内部思科 IP 电话之间建立呼叫。第一个电话和第二个电话的 RTP 侦听端口分别为 UDP 22948 和 20798。

以下是这些 Skinny 连接的 xlate 信息：

```
ciscoasa# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug skinny	显示 SCCP 调试信息
inspect skinny	启用 SCCP 应用检查。
show conn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。

show sla monitor configuration

要显示 SLA 操作的配置值（包括默认值），请在用户 EXEC 模式下使用 **show sla monitor configuration** 命令。

show sla monitor configuration [*sla-id*]

语法说明

sla-id	（可选）SLA 操作的 ID 编号。有效值为从 1 到 2147483647。

默认值

如果未指定 *sla-id*，将显示所有 SLA 操作的配置值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

使用 **show running config sla monitor** 命令可查看运行配置中的 SLA 操作命令。

示例

以下是 **show sla monitor** 命令的输出示例。它显示 SLA 操作 123 的配置值。**show sla monitor** 命令输出的后面是同一 SLA 操作的 **show running-config sla monitor** 命令的输出。

```
ciscoasa> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
```

```
Status of entry (SNMP RowStatus): Active
Enhanced History:

ciscoasa# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

相关命令

命令	说明
show running-config sla monitor	显示运行配置中的 SLA 操作配置命令。
sla monitor	定义 SLA 监控操作。

show sla monitor operational-state

要显示 SLA 操作的运行状态，请在用户 EXEC 模式下使用 **show sla monitor operational-state** 命令。

show sla monitor operational-state [*sla-id*]

语法说明

sla-id	（可选）SLA 操作的 ID 编号。有效值为从 1 到 2147483647。

默认值

如果未指定 *sla-id*，将显示所有 SLA 操作的统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

使用 **show running-config sla monitor** 命令可显示运行配置中的 SLA 操作命令。

示例

以下是 **show sla monitor operational-state** 命令的输出示例：

```
ciscoasa> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

相关命令

命令	说明
show running-config sla monitor	显示运行配置中的 SLA 操作配置命令。
sla monitor	定义 SLA 监控操作。

show snmp-server engineid

要显示 ASA 上已配置的 SNMP 引擎的标识，请在特权 EXEC 模式下使用 **show snmp-server engineid** 命令。

show snmp-server engineid

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下是 **show snmp-server engineid** 命令的输出示例：

```
ciscoasa# show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

使用指南

SNMP 引擎是可以驻留在本地设备上的 SNMP 副本。引擎 ID 是为每个 ASA 情景的每个 SNMP 代理分配的唯一值。引擎 ID 不能在 ASA 上配置。引擎 ID 的长度为 25 字节，用于生成加密密码。加密密码随后存储在闪存中。引擎 ID 可以缓存。在故障切换对中，引擎 ID 与对等设备同步。

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
show running-config snmp-server	显示 SNMP 服务器配置。
snmp-server	配置 SNMP 服务器。

show snmp-server group

要显示已配置的 SNMP 组的名称、正在使用的安全模式、不同视图的状态以及每个组的存储类型，请在特权 EXEC 模式下使用 **show snmp-server group** 命令。

show snmp-server group

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下是 **show snmp-server group** 命令的输出示例：

```
ciscoasa# show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                     security model:v3 priv
readview : def_read_view                 writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

使用指南

根据 SNMP 的基于视图的访问控制模型 (VACM) 来使用 SNMP 用户和组。SNMP 组确定要使用的安全模型。SNMP 用户应当符合 SNMP 组的安全模型。每个 SNMP 组名称和安全级别对必须唯一。

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
show running-config snmp-server	显示 SNMP 服务器配置。
snmp-server	配置 SNMP 服务器。

show snmp-server statistics

要显示 SNMP 服务器统计信息，请在特权 EXEC 模式下使用 **show snmp-server statistics** 命令。

show snmp-server statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下是 **show snmp-server statistics** 命令的输出示例：

```
ciscoasa# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
clear snmp-server statistics	清除 SNMP 数据包输入和输出计数器。
show running-config snmp-server	显示 SNMP 服务器配置。
snmp-server	配置 SNMP 服务器。

show snmp-server user

要显示有关 SNMP 用户的已配置特性的信息，请在特权 EXEC 模式下使用 **show snmp-server user** 命令。

show snmp-server user [*username*]

语法说明

username	（可选）标识要显示其 SNMP 信息的特定用户或多个用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下是 **show snmp-server user** 命令的输出示例：

```
ciscoasa# show snmp-server user authuser
User name: authuser
Engine ID: 00000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

输出提供以下信息：

- 用户名，是标识 SNMP 用户名称的字符串。
- 引擎 ID，是标识 ASA 上的 SNMP 副本的字符串。
- 存储类型，指示在 ASA 上的易失性或临时内存中还是在非易失性或永久内存中设定设置，如果为后者，则关闭 ASA 再重新开启后，设置仍然保留。
- 活动访问列表，是与 SNMP 用户关联的标准 IP 访问列表。
- Rowstatus，指示其是否处于活动状态。
- 身份验证协议，标识正在使用哪种身份验证协议。选项为 MD5、SHA 或无。如果您的软件映像不支持身份验证，则此字段不显示。
- 隐私协议，指示是否启用 DES 数据包加密。如果您的软件映像不支持隐私，则此字段不显示。
- 组名称，指示用户所属的 SNMP 组。SNMP 组按照基于视图的访问控制模型 (VACM) 进行定义。

使用指南

SNMP 用户必须是 SNMP 组的一部分。如果不输入 *username* 参数，则 **show snmp-server user** 命令将显示所有已配置用户的信息。如果输入 *username* 参数并且相应用户存在，则显示该用户的信息。

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
show running-config snmp-server	显示 SNMP 服务器配置。
snmp-server	配置 SNMP 服务器。

show software authenticity file

要显示与特定映像文件的软件验证有关的数字签名信息，请在特权 EXEC 模式下使用 **show software authenticity file** 命令。

show software authenticity [*filename*]

语法说明

filename	（可选）标识特定的映像文件。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(2)	引入了此命令。

示例

以下是 **show software authenticity file** 命令的输出示例：

```
ciscoasa# show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

输出提供以下信息：

- 文件名，是内存中文件的名称。
- 映像类型，是所显示映像的类型。
- 签名者信息指定签名信息，其中包括以下内容：
  - 公用名称，是软件制造商的名称。
  - 组织单位，指示部署软件映像的硬件。
  - 组织名称，是软件映像的所有者。
- 证书序列号，是数字签名的证书序列号。

- 哈希算法，指示数字签名验证中使用的哈希算法类型。
- 签名算法，标识数字签名验证中使用的签名算法类型。
- 密钥版本，指示用于验证的密钥版本。

相关命令

命令	说明
show version	显示软件版本、硬件配置、许可证密钥和相关运行时间数据。

show ssh sessions

要显示有关 ASA 上的活动 SSH 会话的信息，请在特权 EXEC 模式下使用 **show ssh sessions** 命令。

show ssh sessions [**hostname** or **A.B.C.D**] [**hostname** or **X:X:X:X::X**] [**detail**]

语法说明

hostname or **A.B.C.D**	（可选）仅显示指定的 SSH 客户端 IPv4 地址的 SSH 会话信息。
hostname or **X:X:X:X::X**	（可选）仅显示指定的 SSH 客户端 IPv6 地址的 SSH 会话信息。
detail	显示详细的 SSH 会话信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.1(2)	增加了 **detail** 选项。

使用指南

SID 是标识 SSH 会话的唯一编号。Client IP（客户端 IP）是运行 SSH 客户端的系统的 IP 地址。Version（版本）是 SSH 客户端支持的协议版本号。如果 SSH 仅支持 SSH 版本 1，则 Version（版本）列显示 1.5。如果 SSH 客户端同时支持 SSH 版本 1 和 SSH 版本 2，则 Version（版本）列显示 1.99。如果 SSH 客户端仅支持 SSH 版本 2，则 Version（版本）列显示 2.0。Encryption（加密）列显示 SSH 客户端使用的加密类型。State（状态）列显示客户端与 ASA 交互时所取得的进展。Username（用户名）列显示已通过会话身份验证的登录用户名。Mode（模式）列说明 SSH 数据流的方向。

对于可以使用相同或不同加密算法的 SSH 版本 2，Mode（模式）字段显示 in（输入）和 out（输出）。对于在两个方向上使用相同加密的 SSH 版本 1，Mode（模式）字段显示无 (“-”)，并且每连接仅允许一个条目。

示例

以下是 **show ssh sessions** 命令的输出示例：

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

```
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

以下是 **show ssh sessions detail** 命令的输出示例：

```
ciscoasa# show ssh sessions detail
SSH Session ID              : 0
>   Client IP               : 161.44.66.200
>   Username                : root
>   SSH Version             : 2.0
>   State                   : SessionStarted
>   Inbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Received         : 2224
>   Outbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Transmitted      : 2856
>   Rekey Information
>    Time Remaining (sec)   : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey             : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys      : 0
>    Time-Based Rekeys      : 0
```

相关命令

命令	说明
ssh disconnect	断开活动的 SSH 会话。
ssh timeout	设置空闲 SSH 会话的超时值。

show ssl

要显示有关 ASA 上的活动 SSL 会话的信息，请在特权 EXEC 模式下使用 **show ssl** 命令。

show ssl [cache | ciphers | errors | mib | objects]

语法说明

cache	（可选）显示 SSL 会话缓存统计信息。
ciphers	（可选）显示可用的 SSL 密码。
errors	（可选）显示 SSL 错误。
mib	（可选）显示 SSL MIB 统计信息。
objects	（可选）显示 SSL 对象统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(1)	引入了此命令。
9.1(2)	增加了 **detail** 选项。
9.3(2)	增加了对 TLSv1.1 和 TLSv1.2 的支持。

使用指南

此命令显示有关当前 SSLv2 和 SSLv3 会话的信息，包括启用的密码顺序、禁用了哪些密码、正在使用的 SSL 信任点，以及是否启用证书身份验证。

示例

以下是 **show ssl** 命令的输出示例：

```
ciscoasa# show ssl

Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2

SSL trust-points:
Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

相关命令

命令	说明
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。

show ssl ciphers

要显示有关指定级别的可用密码的信息，请在特权 EXEC 模式下使用 **show ssl ciphers** 命令。

show ssl ciphers *level*

语法说明

level	指定密码的强度并指示所支持的最低密码级别。有效值（按强度的升序排列）如下： • **all** - 包括所有密码，其中包括 NULL-SHA。 • **low** - 包括除 NULL-SHA 以外的所有密码。 • **medium** - 包括除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 以外的所有密码。 • **fips** - 包括所有符合 FIPS 的密码（不包括 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA）。 • **high**（仅适用于 TLSv1.2 ）- 仅包括使用 SHA-2 密码的 AES-256。

默认值

所有协议版本的默认值均为 **medium**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

使用 **show ssl ciphers** 命令可显示根据使用 **ssl cipher** 命令配置的级别所配置的可用密码。使用 **show ssl ciphers** *level* 命令可显示有关指定级别的可用密码的信息。

示例

以下是 **show ssl ciphers** 命令的输出示例：

```
ciscoasa# show ssl ciphers

Current cipher configuration:
default (medium):
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
```

```
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
sslv3 (medium):
  AES256-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

以下是 **show ssl ciphers fips** 命令的输出示例：

```
ciscoasa# show ssl ciphers fips

DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

相关命令

命令	说明
show ssl	显示 SSL 配置信息，包括证书。
ssl ciphers	指定 SSL、DTLS 和 TLS 协议的加密算法。

show startup-config

要显示启动配置或显示当加载启动配置时出现的任何错误，请在特权 EXEC 模式下使用 **show startup-config** 命令。

show startup-config [**errors**]

语法说明

errors	（可选）显示当 ASA 加载启动配置时生成的任何错误。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统[1]
特权 EXEC	• 是	• 是	• 是	• 是	• 是

1. **errors** 关键字仅适用于单模式和系统执行空间。

命令历史

版本	修改
7.0(1)	增加了 **errors** 关键字。
8.3(1)	命令输出会显示加密密码。

使用指南

在多情景模式下，**show startup-config** 命令显示当前执行空间的启动配置：系统配置或安全情景。

show startup-config 命令输出显示当启用或禁用密码加密时的加密、屏蔽或明文密码。

要从内存中清除启动错误，请使用 **clear startup-config errors** 命令。

示例

以下是 **show startup-config** 命令的输出示例：

```
ciscoasa# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 209.165.200.224
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
```

```
 nameif test
 security-level 0
 ip address 209.165.200.225
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 209.165.200.226
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

以下是 **show startup-config errors** 命令的输出示例：

```
ciscoasa# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done.(1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', "nameif inside"
.....
*** Output from config line 37, "config-url disk:/admin..."
```

相关命令

命令	说明
clear startup-config errors	从内存中清除启动错误。
show running-config	显示运行的配置。

show sunrpc-server active

要显示为 Sun RPC 服务开放的针孔，请在特权 EXEC 模式下使用 **show sunrpc-server active** 命令。

show sunrpc-server active

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **show sunrpc-server active** 命令可显示为 Sun RPC 服务（如 NFS 和 NIS）开放的针孔。

示例

要显示为 Sun RPC 服务开放的针孔，请输入 **show sunrpc-server active** 命令。以下是 **show sunrpc-server active** 命令的输出示例：

```
ciscoasa# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

相关命令

命令	说明
clear configure sunrpc-server	从 ASA 清除 Sun 远程处理器调用服务。
清除 sunrpc 服务器活动	清除为 Sun RPC 服务（如 NFS 或 NIS）开放的针孔。
inspect sunrpc	启用或禁用 Sun RPC 应用检查并配置使用的端口。
show running-config sunrpc-server	显示有关 SunRPC 服务配置的信息。

show switch mac-address-table

对于具有内置交换机的型号（如 ASA 5505 自适应安全设备），请在特权 EXEC 模式下使用 **show switch mac-address-table** 命令查看交换机 MAC 地址表。

show switch mac-address-table

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令仅适用于具有内置交换机的型号。交换机 MAC 地址表为交换机硬件中的每个 VLAN 内的流量维护 MAC 地址到交换机端口的映射。如果您在透明防火墙模式下，在 ASA 软件中使用 **show mac-address-table** 命令可查看网桥 MAC 地址表。网桥 MAC 地址表为 VLAN 之间传递的流量维护 MAC 地址到 VLAN 接口的映射。

MAC 地址条目的有效期为 5 分钟。

示例

以下是 **show switch mac-address-table** 命令的输出示例。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

表 12-4 显示每个字段的说明：

表 12-4　show switch mac-address-table 字段

字段	说明
Mac Address	显示 MAC 地址。
VLAN	显示与 MAC 地址关联的 VLAN。
Type	显示 MAC 地址是动态获知、作为静态组播地址获知还是静态获知的。唯一的静态条目用于内部背板接口。
Age	显示 MAC 地址表中的动态条目的期限。
Port	显示用于通过 MAC 地址访问主机的交换机端口。

相关命令

命令	说明
show mac-address-table	显示没有内置交换机的型号的 MAC 地址表。
show switch vlan	显示 VLAN 和物理 MAC 地址关联。

show switch vlan

对于具有内置交换机的型号（如 ASA 5505 自适应安全设备），请在特权 EXEC 模式下使用 **show switch vlan** 命令查看 VLAN 和关联的交换机端口。

show switch vlan

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令仅适用于具有内置交换机的型号。对于其他型号，请使用 **show vlan** 命令。

示例

以下是 **show switch vlan** 命令的输出示例。

```
ciscoasa# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

表 12-4 显示每个字段的说明：

表 12-5　show switch vlan 字段

字段	说明
VLAN	显示 VLAN 编号。
Name	显示 VLAN 接口的名称。如果未使用 **nameif** 命令设置名称或者不存在 **interface vlan** 命令，则显示破折号 (-)。

表 12-5　show switch vlan 字段（续）

字段	说明
Status	显示状态（up 或 down）以从 / 向交换机中的 VLAN 接收 / 发送流量。VLAN 中需要至少一个交换机端口处于 up 状态才能使 VLAN 处于 up 状态。
Ports	显示为每个 VLAN 分配的交换机端口。如果某个交换机端口为多个 VLAN 列出，则该端口是中继端口。上面的输出示例显示 Ethernet0/1 是承载 VLAN 100 和 VLAN 300 的中继端口。

相关命令

命令	说明
clear interface	清除 **show interface** 命令的计数器。
interface vlan	创建 VLAN 接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。
show vlan	显示没有内置交换机的型号的 VLAN。
switchport mode	将交换机端口的模式设置为访问模式或中继模式。

第 13 章

show tcpstat 至 show traffic 命令

show tcpstat

要显示 ASA TCP 堆栈以及 ASA 上终止的 TCP 连接的状态（用于调试），请在特权 EXEC 模式下使用 **show tcpstat** 命令。此命令支持 IPv4 和 IPv6 地址。

show tcpstat

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show tcpstat 命令可用于显示 TCP 堆栈和 ASA 上终止的 TCP 连接的状态。表 13-1 说明了所显示的 TCP 统计信息。

表 13-1　show tcpstat 命令中的 TCP 统计信息

统计	说明
tcb_cnt	TCP 用户数。
proxy_cnt	TCP 代理数。TCP 代理被用户授权使用。
tcp_xmt pkts	TCP 堆栈发送的数据包数。
tcp_rcv good pkts	TCP 堆栈接收的良好数据包数。
tcp_rcv drop pkts	TCP 堆栈丢弃的已接收数据包数。
tcp bad chksum	校验和错误的已接收数据包数。
tcp user hash add	已添加到哈希表的 TCP 用户数。
tcp user hash add dup	当尝试添加新用户时发现哈希表中已存在 TCP 用户的次数。
tcp user srch hash hit	当搜索时在哈希表中找到 TCP 用户的次数。
tcp user srch hash miss	当搜索时在哈希表中找不到 TCP 用户的次数。
tcp user hash delete	从哈希表中删除 TCP 用户的次数。
tcp user hash delete miss	当尝试删除 TCP 用户时在哈希表中找不到该用户的次数。

表 13-1　show tcpstat 命令中的 TCP 统计信息（续）

统计	说明
lip	TCP 用户的本地 IP 地址。
fip	TCP 用户的外部 IP 地址。
lp	TCP 用户的本地端口。
fp	TCP 用户的外部端口。
st	TCP 用户的状态（请参阅 RFC 793）。可能值如下： 1　CLOSED 2　LISTEN 3　SYN_SENT 4　SYN_RCVD 5　ESTABLISHED 6　FIN_WAIT_1 7　FIN_WAIT_2 8　CLOSE_WAIT 9　CLOSING 10　LAST_ACK 11　TIME_WAIT
rexqlen	TCP 用户的重新传输队列的长度。
inqlen	TCP 用户的输入队列的长度。
tw_timer	TCP 用户的 time_wait 计时器的值（以毫秒为单位）。
to_timer	TCP 用户的非活动超时计时器的值（以毫秒为单位）。
cl_timer	TCP 用户的关闭请求计时器的值（以毫秒为单位）。
per_timer	TCP 用户的持续计时器的值（以毫秒为单位）。
rt_timer	TCP 用户的重新传输计时器的值（以毫秒为单位）。
tries	TCP 用户的重新传输计数。

示例

以下示例展示如何显示 ASA 上的 TCP 堆栈的状态：

```
ciscoasa# show tcpstat
                CURRENT MAX      TOTAL
tcb_cnt         2       12       320
proxy_cnt       0       0        160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

相关命令

命令	说明
show conn	显示使用的连接和可用的连接。

show tech-support

要显示用于技术支持分析人员进行诊断的信息，请在特权 EXEC 模式下使用 **show tech-support** 命令。

show tech-support [**detail** | **file** | **no-config** | **performance**]

语法说明

detail	（可选）列出详细信息。
file	（可选）将命令的输出写入文件。
no-config	（可选）排除运行配置的输出。
performance	（可选）显示性能信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	增加了 **detail** 和 **file** 关键字。
7.2(1)	改进了输出，现在可显示有关大量占用 CPU 的进程的更多详细信息。
9.1(2)	输出已增强以包括 **show environment** 命令的信息。
9.1(3)	输出已增强以包括 **show memory detail**、**show memory top-usage** 和 **show vlan** 命令的信息。
9.2(1)	输出已增强以包括 **show memory detail**、**show cpu detail**、**show blocks queue history core-local**、**show asp drop**、**show asp event dp-cp**、**show cpu usage history** 和 **show traffic summary** 命令的信息。删除了 **show kernel cgroup-controller detail** 命令的输出。增加了 **performance** 关键字。
9.2(1)	输出已增强以包括 **show vlan** 命令的信息。
9.3(2)	**show tech-support detail** 命令增加了 **show route-summary** 命令输出。

使用指南

show tech-support 命令可列出技术支持分析人员帮助您诊断问题时所需的信息。此命令将多个 **show** 命令的输出结合在一起，这些命令为技术支持分析人员提供大多数信息。

示例

以下示例展示如何显示用于技术支持分析的信息。输出缩短为以 **show module** 命令的输出开头。

```
ciscoasa# show tech-support | beg show module

------------------ show module ------------------

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAD1626056J

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 a493.4c43.0d68 to a493.4c43.0d73  2.0          2.0(13)0     100.8(0)229

Mod SSP Application Name           Status           SSP Application Version
--- ------------------------------ ---------------- --------------------------

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable

------------------ show environment ------------------

Cooling Fans:
-------------------------------------

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7200 RPM - OK  (Fan Module Fan)

Power Supplies:
-------------------------------------
   Power Supply Unit Redundancy: N/A

   Temperature:
   --------------------------------
   Left Slot (PS0): 30 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 31 C - OK  (Fan Module Temperature)

   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7100 RPM - OK  (Fan Module Fan)

Temperature:
-------------------------------------

   Processors:
   --------------------------------
   Processor 1: 47.0 C - OK  (CPU1 Core Temperature)

   Chassis:
   --------------------------------
   Ambient 1: 31.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.25 C - OK  (CPU1 Front Temperature)
   Ambient 4: 32.0 C - OK  (CPU1 Back Temperature)

   IO Hub:
   --------------------------------
   Circuit Die: 49.0 C - OK  (Circuit Die Temperature)
```

```
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 30 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 31 C - OK  (Fan Module Temperature)

Voltage:
----------------------------------
   Channel 1:  3.325 V -   (3.3V (U142 VX1))
   Channel 2:  1.496 V -   (1.5V (U142 VX2))
   Channel 3:  1.048 V -   (1.05V (U142 VX3))
   Channel 4:  3.337 V -   (3.3V_STDBY (U142 VP1))
   Channel 5: 11.665 V -   (12V (U142 VP2))
   Channel 6:  4.950 V -   (5.0V (U142 VP3))
   Channel 7:  6.853 V -   (7.0V (U142 VP4))
   Channel 8:  9.616 V -   (IBV (U142 VH))
   Channel 9:  1.046 V -   (1.05VB (U209 VX2))
   Channel 10:  1.213 V -   (1.2V (U209 VX3))
   Channel 11:  1.110 V -   (1.1V (U209 VX4))
   Channel 12:  1.006 V -   (1.0V (U209 VX5))
   Channel 13:  3.335 V -   (3.3V STDBY (U209 VP1))
   Channel 14:  2.499 V -   (2.5V (U209 VP2))
   Channel 15:  1.803 V -   (1.8V (U209 VP3))
   Channel 16:  1.894 V -   (1.9V (U209 VP4))
   Channel 17:  9.611 V -   (IBV (U209 VH))
   Channel 18:  2.048 V -   (VTT CPU0 (U83 VX2))
   Channel 19:  0.000 V -   (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -   (VCC CPU0 (U83 VX4))
   Channel 21:  1.772 V -   (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -   (1.5VA (U83 VP1))
   Channel 23:  0.000 V -   (1.5VB (U83 VP2))
   Channel 24:  8.937 V -   (IBV (U83 VH))

------------------ show memory ------------------

Free memory:        4927975152 bytes (76%)
Used memory:        1514475792 bytes (24%)
-------------     ------------------
Total memory:       6442450944 bytes (100%)

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show vpn-sessiondb summary ------------------


No sessions to display.


------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     0   1450   1450   1450
     4    100     99     99
    80   1000   1000   1000

------------------ show asp drop ------------------
Frame drop:
Flow is denied by configured rule (acl-drop)                           290272
  Slowpath security checks failed (sp-security-failed)                    22489
```

```
  Interface is down (interface-down)                                    49
Last clearing: Never
Flow drop:
Last clearing: Never

------------------ show asp event dp-cp ------------------
DP-CP EVENT QUEUE                   QUEUE-LEN  HIGH-WATER
Punt Event Queue                            0           1
Identity-Traffic Event Queue                0           1
General Event Queue                         0           2
Syslog Event Queue                          0           3
Non-Blocking Event Queue                    0          22
Midpath High Event Queue                    0           0
Midpath Norm Event Queue                    0           1
SRTP Event Queue                            0           0
HA Event Queue                              0           3
Threat-Detection Event Queue                0           0
ARP Event Queue                             0          10
IDFW Event Queue                            0           0
CXSC Event Queue                            0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                18079          0    18079        0    18079           0
  inspect-gtp       18079          0    18079        0    18079           0
drop-flow             0            0    36158        0    36158           0
midpath-norm          9            0        9        0        9           0
adj-absent          18079          0    18079        0    18079           0
arp-in            7683820          0  7683820        0  7683820           0
identity-traffic       16          0       16        0       16           0
syslog             117503          0   117503        0   117503           0
scheduler              89          0       89        0       89           0
ha-msg           48812863          0 48812863        0 48812863           5

------------------ show blocks queue history core-local ------------------

History buffer memory usage: 3744 bytes (default)
History analysis time limit: 100 msec

------------------ show blocks core ------------------
CORE  LIMIT  ALLOC   HIGH    CNT       FAILED
   0  24576     24     25   1111            0
   1  24576   4425   6155    899            0
   2  24576   2045   2873    743            0
   3  24576   3129   4648    817            0
   4  24576     18     18   1994            0
   5  24576    338    936   1412            0
   6  24576     40     44   2011            0
   7  24576    124    129   1155            0

------------------ show cpu detail ------------------

Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 4       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 5       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 6       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 7       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 66.7%; 1 minute: 66.7%; 5 minutes: 66.7%
```

```
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.3%; 1 minute: 0.1%; 5 minutes: 0.1%

------------------ show memory detail ------------------
Free memory:                    10213725472 bytes (79%)
Used memory:
     Allocated memory in use:      789891808 bytes ( 6%)
     Reserved memory:             1881284608 bytes (15%)
----------------------------   ------------------
Total memory:                   12884901888 bytes (100%)

Least free memory:      10213420912 bytes (79%)
Most used memory:        2671480976 bytes (21%)

MEMPOOL_DMA_ALT1 POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    263907584
Max contiguous free mem     =    263907584
Allocated memory in use     =     27858592
Free memory                 =    263907680

----- fragmented memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96**
    263907584             1      263907584*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
         8192            16         131072
     12582912             1       12582912

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =          131
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    252590992
Max contiguous free mem     =    252590992
Allocated memory in use     =     39118960
Free memory                 =    252647312

----- fragmented memory statistics -----
```

```
fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96**
          256            64          20480
          384            32          15360
          512            33          20208
    252590992             1      252590992*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96
          144             2            288
          256             2            512
          384             3           1152
          512             3           1536
         1024           128         131072
         2048             1           2048
         8192             5          40960
        12288            25         307200
        16384             1          16384
        32768             2          65536
        65536             1          65536
        98304             2         196608
       131072             3         393216
       196608             5         983040
       262144             3         786432
       393216             1         393216
       524288             2        1048576
       786432             2        1572864
      1048576             1        1048576
      1572864             2        3145728
      2097152             2        4194304
      3145728             2        6291456
     12582912             1       12582912

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =  11003617280
Number of free chunks       =          492
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =  11003617280
Keepcost                    =  10213402128
Max contiguous free mem     =  10213402128
Allocated memory in use     =    789891808
Free memory                 =  10213725472

----- fragmented memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           32           201           6432
           48           131           6288
           64           138           8832
           96             1             96**
          112             2            224
```

```
          256             5           1392
          512             1            592
         2048             1           2160
        24576            11         284784
  10213402128             1    10213402128*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           80          1485         118800
           96          8525         818400
          112          3287         368144
          128          1867         238976
          144         10842        1561248
          160           876         140160
          176           476          83776
          192           448          86016
          208           795         165360
          224          1130         253120
          240           191          45840
          256          2733         699648
          384           415         159360
          512          1225         627200
          768           869         667392
         1024          1507        1543168
         1536          5345        8209920
         2048           329         673792
         3072           186         571392
         4096          5001       20484096
         6144            58         356352
         8192           349        2859008
        12288            94        1155072
        16384            85        1392640
        24576            17         417792
        32768           172        5636096
        49152            38        1867776
        65536           172       11272192
        98304            44        4325376
       131072            41        5373952
       196608            36        7077888
       262144            40       10485760
       393216            20        7864320
       524288            15        7864320
       786432            50       39321600
      1048576            32       33554432
      1572864             1        1572864
      2097152            12       25165824
      3145728             2        6291456
      4194304             1        4194304
      6291456             1        6291456
      8388608             1        8388608
     12582912             5       62914560

Summary for all pools:

Non-mmapped bytes allocated =  11587149824
Number of free chunks       =          624
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
```

```
Max memory footprint        =  11587149824
Keepcost                    =  10729900704
Allocated memory in use     =    856869360
Free memory                 =  10730280464


------------------ show memory top-usage ------------------

MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912             1       12582912
      2097152             2        4194304
      3145728             1        3145728
      1048576             2        2097152
      1572864             1        1572864
       786432             1         786432
       196608             3         589824
       262144             2         524288
       393216             1         393216
        98304             3         294912

----- Binsize PC top usage -----

Binsize: 12582912               total (bytes): 12582912

pc = 0x805ada0, size = 12960071 , count = 1

Binsize: 2097152                total (bytes): 4194304

pc = 0x805ada0, size = 5758350  , count = 2

Binsize: 3145728                total (bytes): 3145728

pc = 0x987071c, size = 3178567  , count = 1

Binsize: 1048576                total (bytes): 2097152

pc = 0x805ada0, size = 2309774  , count = 2

Binsize: 1572864                total (bytes): 1572864

pc = 0x805ada0, size = 1740871  , count = 1

Binsize: 786432                 total (bytes): 786432

pc = 0x805ada0, size = 915271   , count = 1

Binsize: 196608                 total (bytes): 589824

pc = 0x805ada0, size = 484622   , count = 2
pc = 0x80567f1, size = 259271   , count = 1

Binsize: 262144                 total (bytes): 524288

pc = 0x805ada0, size = 352071   , count = 1
pc = 0x80567f1, size = 310471   , count = 1

Binsize: 393216                 total (bytes): 393216
```

```
pc = 0x805ada0, size = 505671   , count = 1

Binsize: 98304                  total (bytes): 294912

pc = 0x805ada0, size = 129671   , count = 1
pc = 0x80567f1, size = 227342   , count = 2


MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
      8388608             2       16777216
        65536           126        8257536
       524288            14        7340032
      4194304             1        4194304
      3145728             1        3145728
       131072            21        2752512
      1048576             2        2097152
      2097152             1        2097152
        16384           127        2080768
       262144             7        1835008

----- Binsize PC top usage -----

Binsize: 8388608                total (bytes): 16777216

pc = 0x825b333, size = 16777216 , count = 2

Binsize: 65536                  total (bytes): 8257536

pc = 0x916e48d, size = 7531232  , count = 107
pc = 0x982de33, size = 263056   , count = 4
pc = 0x982db72, size = 324956   , count = 4
pc = 0x82d9092, size = 65536    , count = 1
pc = 0x819b8f9, size = 77824    , count = 1
pc = 0x819b65e, size = 77824    , count = 1
pc = 0x9334871, size = 65536    , count = 1
pc = 0x8a01e5a, size = 65536    , count = 1
pc = 0x8a109f0, size = 65536    , count = 1
pc = 0x9162fb0, size = 163968   , count = 2
pc = 0x8f13da8, size = 66048    , count = 1
pc = 0x8056c11, size = 66528    , count = 1
pc = 0x8056bf5, size = 66528    , count = 1

Binsize: 524288                 total (bytes): 7340032

pc = 0x8a9f8eb, size = 643264   , count = 1
pc = 0x982db72, size = 5325112  , count = 8
pc = 0x807bcb4, size = 524312   , count = 1
pc = 0x821944f, size = 1282600  , count = 2
pc = 0x9187575, size = 524312   , count = 1
pc = 0x8056a14, size = 524352   , count = 1

Binsize: 4194304                total (bytes): 4194304

pc = 0x8cc1f27, size = 5242924  , count = 1

Binsize: 3145728                total (bytes): 3145728
```

```
pc = 0x821944f, size = 3698788  , count = 1

Binsize: 131072                 total (bytes): 2752512

pc = 0x9137bc4, size = 163904   , count = 1
pc = 0x806e421, size = 393216   , count = 3
pc = 0x8f3f649, size = 154136   , count = 1
pc = 0x911894b, size = 131072   , count = 1
pc = 0x89f3fd0, size = 141212   , count = 1
pc = 0x982de33, size = 593580   , count = 4
pc = 0x8167e2b, size = 160864   , count = 1
pc = 0x982db72, size = 983250   , count = 6
pc = 0x9162fb0, size = 327808   , count = 2
pc = 0x806e024, size = 184800   , count = 1

Binsize: 1048576                total (bytes): 2097152

pc = 0x982de33, size = 1081507  , count = 1
pc = 0x821944f, size = 1120100  , count = 1

Binsize: 2097152                total (bytes): 2097152

pc = 0x8aa1252, size = 2097152  , count = 1

Binsize: 16384                  total (bytes): 2080768

pc = 0x806e421, size = 1474560  , count = 90
pc = 0x982de33, size = 135545   , count = 7
pc = 0x9173a77, size = 36928    , count = 2
pc = 0x88a6fec, size = 163840   , count = 10
pc = 0x8f3f649, size = 24160    , count = 1
pc = 0x982db72, size = 96195    , count = 5
pc = 0x8a765c0, size = 17408    , count = 1
pc = 0x92cb71b, size = 17388    , count = 1
pc = 0x982dbee, size = 119925   , count = 7
pc = 0x879defa, size = 19456    , count = 1
pc = 0x8ebd433, size = 16432    , count = 1
pc = 0x8ebd415, size = 16432    , count = 1

Binsize: 262144                 total (bytes): 1835008

pc = 0x982db72, size = 1573315  , count = 5
pc = 0x982de33, size = 580878   , count = 2

------------------ show route-summary----------

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          0           1           0           88          288
eigrp 11        0           3000        0           324000      864000
bgp 200         2           45          0           4136        13536
  External: 47 Internal: 0 Local: 0
ospf 100        0           538         0           47344       157096
  Intra-area: 38 Inter-area: 0 External-1: 500 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal        7                                               288976
Total           9           3586        0           375744      1324472

------------------ show vlan ------------------

64, 66, 70-72, 80-82, 142, 151, 950-951, 960-961
```

相关命令

命令	说明
show clock	显示用于 Syslog 服务器 (PFSS) 以及公共密钥基础设施 (PKI) 协议的时钟。
show conn count	显示已使用和可用的连接。
show cpu	显示 CPU 利用率信息。
show failover	显示连接的状态以及哪个 ASA 处于活动状态
show memory	显示最大物理内存和可用于操作系统的当前空闲内存的摘要。
show perfmon	显示有关 ASA 的性能的信息
show processes	显示正在运行的进程的列表。
show running-config	显示 ASA 上当前正在运行的配置。
show xlate	显示有关转换插槽的信息。

show threat-detection memory

要显示高级威胁检测统计（通过 **threat-detection statistics** 命令启用）使用的内存，请在特权 EXEC 模式下使用 **show threat-detection memory** 命令。

show threat-detection memory

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

某些统计可使用大量内存，并会影响 ASA 性能。此命令可监控内存使用情况，以便您在必要时调整配置。

示例

以下是 **show threat-detection memory** 命令的输出示例：

```
ciscoasa# show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks              70265072


Regular memory                BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888


Total TD memory:                70460960
```

相关命令

命令	说明
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics port	显示端口统计信息。
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。
threat-detection statistics	启用高级威胁检测统计。

show threat-detection rate

当使用 **threat-detection basic-threat** 命令启用基本威胁检测后，可以在特权 EXEC 模式下使用 **show threat-detection rate** 命令查看统计信息。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

语法说明

acl-drop	（可选）显示由于访问列表拒绝而产生丢弃数据包的速率。
min-display-rate *min_display_rate*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位）的统计信息。可以将 *min_display_rate* 设置在 0 和 2147483647 之间。
bad-packet-drop	（可选）显示由于数据包格式错误（如 invalid-ip-header 或 invalid-tcp-hdr-length）而被拒绝所产生丢弃数据包的速率。
conn-limit-drop	（可选）显示由于超过连接限制（系统范围的资源限制和配置中设置的限制）而产生丢弃数据包的速率。
dos-drop	（可选）显示由于检测到 DoS 攻击（如无效的 SPI，状态防火墙检查失败）而产生丢弃数据包的速率。
fw-drop	（可选）显示由于基本防火墙检查失败而产生丢弃数据包的速率。此选项是包括此命令中所有防火墙相关丢包的组合速率。它不包括非防火墙相关丢包（例如 **interface-drop**、**inspect-drop** 和 **scanning-threat**）。
icmp-drop	（可选）显示由于检测到可疑 ICMP 数据包而被拒绝所产生丢弃数据包的速率。
inspect-drop	（可选）显示由于数据包导致应用检查失败而产生丢弃数据包的速率限制。
interface-drop	（可选）显示由于接口过载而产生丢弃数据包的速率限制。
scanning-threat	（可选）显示由于检测到扫描攻击而产生丢弃数据包的速率。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。全面扫描威胁检测（请参阅 **threat-detection scanning-threat** 命令）采用此扫描攻击速率信息，然后通过例如将主机归类为攻击者并自动回避以采取相应措施。
syn-attack	（可选）显示由于会话不完整（如 TCP SYN 攻击或无数据 UDP 会话攻击）而产生丢弃数据包的速率。

默认值

如果不指定事件类型，则显示所有事件。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

显示输出显示以下信息：

- 固定时间段内的平均速率（以事件数 / 秒为单位）
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）
- 超过速率的次数
- 固定时间段内的事件总数。

ASA 会在平均速率间隔内计算 30 次事件计数，换句话说，ASA 在每个突发周期的末尾检查速率，总共检查 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 10 分钟，则突发间隔为 10 秒。如果上一个突发间隔为 3:00:00 至 3:00:10，并且您在 3:00:15 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 59 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection rate** 命令的输出示例：

```
ciscoasa# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

相关命令

命令	说明
clear threat-detection rate	清除基本威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
threat-detection basic-threat	启用基本威胁检测。
threat-detection rate	设置每种事件类型的威胁检测速率限制。
threat-detection scanning-threat	启用扫描威胁检测。

show threat-detection scanning-threat

如果使用 **threat-detection scanning-threat** 命令启用扫描威胁检测，则在特权 EXEC 模式下使用 **show threat-detection scanning-threat** 命令查看被分类为攻击者和目标的主机。

show threat-detection scanning-threat [**attacker** | **target**]

语法说明

attacker	（可选）显示攻击主机 IP 地址。
target	（可选）显示目标主机 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.0(4)	显示修改为在报头文本中包括 “& Subnet List”（& 子网列表）。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

示例

以下是 **show threat-detection scanning-threat** 命令的输出示例：

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
```

相关命令

命令	说明
clear threat-detection shun	释放被避开的主机。
show threat-detection shun	显示当前避开的主机。
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。
threat-detection scanning-threat	启用扫描威胁检测。

show threat-detection shun

如果使用 **threat-detection scanning-threat** 命令启用扫描威胁检测并自动避开攻击主机，则在特权 EXEC 模式下使用 **show threat-detection shun** 命令查看当前避开的主机。

show threat-detection shun

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

要释放回避的主机，请使用 **clear threat-detection shun** 命令。

示例

以下是 **show threat-detection shun** 命令的输出示例：

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

相关命令

命令	说明
clear threat-detection shun	释放被避开的主机。
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。
threat-detection scanning-threat	启用扫描威胁检测。

show threat-detection statistics host

在使用 **threat-detection statistics host** 命令启用威胁统计后，请在特权 EXEC 模式下使用 **show threat-detection statistics host** 命令查看主机统计信息。威胁检测统计信息显示允许和丢弃的流量速率。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

语法说明

ip_address	（可选）显示特定主机的统计信息。
mask	（可选）设置主机 IP 地址的子网掩码。
min-display-rate *min_display_rate*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位）的统计信息。可以将 *min_display_rate* 设置在 0 和 2147483647 之间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

显示输出显示以下信息：

- 固定时间段内的平均速率（以事件数 / 秒为单位）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

ASA 会在平均速率间隔内计算 30 次事件计数，换句话说，ASA 在每个突发周期的末尾检查速率，总共检查 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection statistics host** 命令的输出示例：

```
ciscoasa# show threat-detection statistics host

                          Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

表 13-2 显示每个字段的说明。

表 13-2　show threat-detection statistics host 字段

字段	说明
Host	显示主机 IP 地址。
tot-ses	显示此主机自添加到数据库以来的会话总数。
act-ses	显示当前所涉及主机的活动会话总数。
fw-drop	显示防火墙丢弃数。防火墙丢弃是包含基本威胁检测中跟踪的所有防火墙相关数据包丢弃的合并速率，包括访问列表拒绝、错误数据包、超过连接限制、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包和无数据 UDP 攻击数据包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
insp-drop	显示由于使应用检查失败而被丢弃的数据包数。
null-ses	显示空会话的数量，这些会话是在 30 秒超时期间内未完成的 TCP SYN 会话以及在会话开始 3 秒后其服务器未发送任何数据的 UDP 会话。
bad-acc	显示对处于关闭状态的主机端口的错误访问尝试数量。当确定某个端口处于空会话时（请参阅上文），该主机的端口状态设置为 HOST_PORT_CLOSE。任何访问该主机端口的客户端都会被立即分类为错误访问，无需等待超时。

表 13-2　show threat-detection statistics host 字段（续）

字段	说明
Average(eps)	显示每个时间段内的平均速率（以事件数 / 秒为单位）。 安全设备在每个突发周期的末尾存储计数，总共处理 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）。对于 Average(eps) 说明中指定的示例，最新速率为 3:19:30 至 3:20:00 的速率
Trigger	显示超过丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
20-min, 1-hour, 8-hour, and 24-hour	默认情况下，显示三个速率间隔。可以使用 **threat-detection statistics host number-of-rate** 命令减少速率间隔数。由于主机统计使用大量内存，减少默认值为 3 的速率间隔数可降低内存使用。如果将此关键字设置为 1，则仅保持最短的速率间隔统计。如果将该值设置为 2，则保持两个最短的间隔。
Sent byte	显示成功从主机发送的字节数。
Sent pkts	显示成功从主机发送的数据包数。
Sent drop	显示从主机发送的由于是扫描攻击的一部分而被丢弃的数据包数。
Recv byte	显示主机成功接收的字节数。
Recv pkts	显示主机成功接收的数据包数。
Recv drop	显示主机接收的由于是扫描攻击的一部分而被丢弃的数据包数。

相关命令

命令	说明
threat-detection scanning-threat	启用扫描威胁检测。
show threat-detection statistics top	显示前 10 个统计信息。
show threat-detection statistics port	显示端口统计信息。
show threat-detection statistics protocol	显示协议统计信息。
threat-detection statistics	启用威胁统计。

show threat-detection statistics port

在使用 **threat-detection statistics port** 命令启用威胁统计后，请在特权 EXEC 模式下使用 **show threat-detection statistics port** 命令查看 TCP 和 UDP 端口统计信息。威胁检测统计信息显示允许和丢弃的流量速率。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]

语法说明

start_port[**-***end_port*]	（可选）显示特定端口或一系列端口（0 到 65535 之间）的统计信息。
min-display-rate *min_display_rate*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位）的统计信息。可以将 *min_display_rate* 设置在 0 和 2147483647 之间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

显示输出显示以下信息：

- 固定时间段内的平均速率（以事件数 / 秒为单位）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

ASA 会在平均速率间隔内计算 30 次事件计数，换句话说，ASA 在每个突发周期的末尾检查速率，总共检查 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection statistics port** 命令的输出示例：

```
ciscoasa# show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

表 13-3 显示每个字段的说明。

表 13-3　show threat-detection statistics port 字段

字段	说明
Average(eps)	显示每个时间段内的平均速率（以事件数 / 秒为单位）。 安全设备在每个突发周期的末尾存储计数，总共处理 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）。对于 Average(eps) 说明中指定的示例，最新速率为 3:19:30 至 3:20:00 的速率
Trigger	显示超过丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
port_number/*port_name*	显示发送、接收或丢弃数据包或字节的端口的端口号和名称。
tot-ses	显示此端口的会话总数。

表 13-3　show threat-detection statistics port 字段（续）

字段	说明
act-ses	显示端口当前涉及的活动会话的总数。
20-min, 1-hour, 8-hour, and 24-hour	显示这些固定速率间隔的统计信息。
Sent byte	显示从端口成功发送的字节数。
Sent pkts	显示从端口发送的成功数据包数。
Sent drop	显示从端口发送的由于是扫描攻击的一部分而被丢弃的数据包数。
Recv byte	显示端口成功接收的字节数。
Recv pkts	显示端口成功接收的数据包数。
Recv drop	显示端口接收的由于是扫描攻击的一部分而被丢弃的数据包数。

相关命令

命令	说明
threat-detection scanning-threat	启用扫描威胁检测。
show threat-detection statistics top	显示前 10 个统计信息。
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics protocol	显示协议统计信息。
threat-detection statistics	启用威胁统计。

show threat-detection statistics protocol

在使用 **threat-detection statistics protocol** 命令启用威胁统计后，请在特权 EXEC 模式下使用 **show threat-detection statistics protocol** 命令查看 IP 协议统计信息。威胁检测统计信息显示允许和丢弃的流量速率。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

语法说明

protocol_number	（可选）显示特定协议编号（0 到 255 之间）的统计信息。
min-display-rate *min_display_rate*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位）的统计信息。可以将 *min_display_rate* 设置在 0 和 2147483647 之间。
protocol_name	（可选）显示特定协议名称的统计信息： • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	单个	多个 情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.2(2)	对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

显示输出显示以下信息：

- 固定时间段内的平均速率（以事件数 / 秒为单位）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

ASA 会在平均速率间隔内计算 30 次事件计数，换句话说，ASA 在每个突发周期的末尾检查速率，总共检查 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection statistics protocol** 命令的输出示例：

```
ciscoasa# show threat-detection statistics protocol

                          Average(eps)     Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0                0       0                 1000
  8-hour Sent byte:                  0                2       0                 1000
 24-hour Sent byte:                  0                0       0                 1000
  1-hour Sent pkts:                  0                0       0                   10
  8-hour Sent pkts:                  0                0       0                   10
 24-hour Sent pkts:                  0                0       0                   10
```

表 13-4 显示每个字段的说明。

表 13-4　show threat-detection statistics protocol 字段

字段	说明
Average(eps)	显示每个时间段内的平均速率（以事件数 / 秒为单位）。 安全设备在每个突发周期的末尾存储计数，总共处理 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）。对于 Average(eps) 说明中指定的示例，最新速率为 3:19:30 至 3:20:00 的速率
Trigger	显示超过丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
protocol_number/ *protocol_name*	显示发送、接收或丢弃数据包或字节的协议的协议号和名称。
tot-ses	当前未使用。
act-ses	当前未使用。
20-min, 1-hour, 8-hour, and 24-hour	显示这些固定速率间隔的统计信息。
Sent byte	显示从协议成功发送的字节数。
Sent pkts	显示从协议成功发送的数据包数。
Sent drop	显示从协议发送的由于是扫描攻击的一部分而被丢弃的数据包数。
Recv byte	显示协议成功接收的字节数。
Recv pkts	显示协议成功接收的数据包数。
Recv drop	显示协议接收的由于是扫描攻击的一部分而被丢弃的数据包数。

相关命令

命令	说明
threat-detection scanning-threat	启用扫描威胁检测。
show threat-detection statistics top	显示前 10 个统计信息。
show threat-detection statistics port	显示端口统计信息。
show threat-detection statistics host	显示主机统计信息。
threat-detection statistics	启用威胁统计。

show threat-detection statistics top

在使用 **threat-detection statistics** 命令启用威胁统计后，请在特权 EXEC 模式下使用 **show threat-detection statistics top** 命令查看前 10 名统计信息。如果未启用特定类型的威胁检测统计，则无法使用此命令查看这些统计信息。威胁检测统计信息显示允许和丢弃的流量速率。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**] [**long**]]

语法说明

access-list	（可选）显示与数据包匹配的前 10 名 ACE，包括允许和拒绝 ACE。允许和拒绝的流量在此显示中没有区别。如果使用 **threat-detection basic-threat** 命令启用基本威胁检测，则可以使用 **show threat-detection rate access-list** 命令跟踪访问列表拒绝。
all	（可选）对于 TCP 拦截，显示所有跟踪服务器的历史记录数据。
detail	（可选）对于 TCP 拦截，显示历史采样数据。
host	（可选）显示每个固定时间段的前 10 名主机统计信息。 **注**　由于威胁检测算法的原因，用于故障切换链路或状态链路的接口可能显示为前 10 名主机之一。当将一个接口同时用于故障切换和状态链路时，更有可能出现这种情况。这是预期行为，您可以在显示中忽略此 IP 地址。
long	（可选）显示长格式的统计历史记录，其中含有服务器的实际 IP 地址和未转换 IP 地址。
min-display-rate *min_display_rate*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位）的统计信息。可以将 *min_display_rate* 设置在 0 和 2147483647 之间。
port-protocol	（可选）显示 TCP/UDP 端口和 IP 协议类型的前 10 名合并统计信息。TCP（协议 6 ）和 UDP（协议 17）未包含在 IP 协议的显示中；但是，TCP 和 UDP 端口包含在端口的显示中。如果只启用端口或协议类型中的一个，则只能查看启用的统计信息。
rate-1	（可选）展示显示中的最小固定速率间隔的统计信息。例如，如果显示中含有前 1 小时、8 小时和 24 小时的统计信息，则当您使用 **rate-1** 关键字时，ASA 仅显示 1 小时间隔。
rate-2	（可选）展示显示中的中等固定速率间隔的统计信息。例如，如果显示中含有前 1 小时、8 小时和 24 小时的统计信息，则当您使用 **rate-2** 关键字时，ASA 仅显示 8 小时间隔。
rate-3	（可选）展示显示中的最大固定速率间隔的统计信息。例如，如果显示中含有前 1 小时、8 小时和 24 小时的统计信息，则当您使用 **rate-3** 关键字时，ASA 仅显示 24 小时间隔。
tcp-intercept	显示 TCP 拦截统计信息。显示包含遭受攻击的前 10 名受保护服务器。

默认值

如果不指定事件类型，则显示所有事件。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	单个	多个	
				情景	系统
特权 EXEC	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.0(4)	增加了 **tcp-intercept** 关键字。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.2(2)	为 **tcp-intercept** 增加了 **long** 关键字。对于威胁事件，严重性级别从警告更改为通知。威胁事件可每隔五分钟触发。

使用指南

显示输出显示以下信息：

- 固定时间段内的平均速率（以事件数 / 秒为单位）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

ASA 会在平均速率间隔内计算 30 次事件计数，换句话说，ASA 在每个突发周期的末尾检查速率，总共检查 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection statistics top access-list** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top access-list

                    Top     Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]              173               0       0               623488
              200/2[1]               43               0       0               156786
              100/1[2]               43               0       0               156786
  8-hour ACL hits:
              100/3[0]               21            1298       0               623488
              200/2[1]                5             326       0               156786
              100/1[2]                5             326       0               156786
```

表 13-5 显示每个字段的说明。

表 13-5　show threat-detection statistics top access-list 字段

字段	说明
Top	显示一定时间段内的 ACE 排名，从 [0]（最高计数）到 [9]（最低计数）。统计信息可能不足以覆盖全部 10 个位置，因此可能列出不到 10 个 ACE。
Average(eps)	显示每个时间段内的平均速率（以事件数 / 秒为单位）。 安全设备在每个突发周期的末尾存储计数，总共处理 30 个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的最新突发速率（以事件数 / 秒为单位）。对于 Average(eps) 说明中指定的示例，最新速率为 3:19:30 至 3:20:00 的速率。
Trigger	此列始终为 0，因为不存在访问列表流量触发的速率限制；拒绝和允许的流量在此显示中没有区别。如果使用 **threat-detection basic-threat** 命令启用基本威胁检测，则可以使用 **show threat-detection rate access-list** 命令跟踪访问列表拒绝。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，ASA 会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
1-hour（1 小时），8-hour（8 小时）	显示这些固定速率间隔的统计信息。
acl_name/line_number	显示访问列表名称和导致拒绝的 ACE 的行号。

以下是 **show threat-detection statistics top access-list rate-1** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top access-list rate-1

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
               100/3[0]              173                0       0               623488
               200/2[1]               43                0       0               156786
               100/1[2]               43                0       0               156786
```

以下是 **show threat-detection statistics top port-protocol** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top port-protocol

Top          Name    Id     Average(eps)     Current(eps) Trigger      Total events
  1-hour Recv byte:
 1          gopher   70               71                0       0          32345678
 2   btp-clnt/dhcp   68               68                0       0          27345678
 3          gopher   69               65                0       0          24345678
 4    Protocol-96 * 96               63                0       0          22345678
```

```
 5      Port-7314 7314              62              0       0          12845678
 6 BitTorrent/trc 6969              61              0       0          12645678
 7     Port-8191-65535              55              0       0          12345678
 8           SMTP  366              34              0       0           3345678
 9         IPinIP *  4              30              0       0           2345678
10          EIGRP * 88              23              0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

表 13-6 显示每个字段的说明。

表 13-6　show threat-detection statistics top port-protocol 字段

字段	说明
Top	显示一定时间段 / 统计类型范围内的端口或协议排名，从 [0]（最高计数）到 [9]（最低计数）。统计信息可能不足以覆盖全部 10 个位置，因此可能列出不到 10 个端口 / 协议。
Name	显示端口 / 协议名称。
Id	显示端口 / 协议 ID 编号。星号 (*) 表示 ID 是 IP 协议编号。
Average(eps)	请参阅表 13-2 中的说明。
Current(eps)	请参阅表 13-2 中的说明。
Trigger	显示超过丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	请参阅表 13-2 中的说明。
Time_interval Sent byte	显示从针对每个时间段列出的端口和协议成功发送的字节数。
Time_interval Sent packet	显示从针对每个时间段列出的端口和协议成功发送的数据包数。
Time_interval Sent drop	显示从针对每个时间段列出的端口和协议发送的由于是扫描攻击的一部分而被丢弃的数据包数。
Time_interval Recv byte	显示针对每个时间段列出的端口和协议成功接收的字节数。
Time_interval Recv packet	显示针对每个时间段列出的端口和协议成功接收的数据包数。
Time_interval Recv drop	显示针对每个时间段列出的端口和协议接收的由于是扫描攻击的一部分而被丢弃的数据包数。

表 13-6　show threat-detection statistics top port-protocol 字段（续）

字段	说明
port_number/ port_name	显示发送、接收或丢弃数据包或字节的端口的端口号和名称。
protocol_number/ protocol_name	显示发送、接收或丢弃数据包或字节的协议的协议号和名称。

以下是 **show threat-detection statistics top host** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top host

                  Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]             2938                0       0              10580308
  1-hour Sent pkts:
          10.0.0.1[0]               28                0       0                104043
  20-min Sent drop:
          10.0.0.1[0]                9                0       1                 10851
  1-hour Recv byte:
          10.0.0.1[0]             2697                0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]               29                0       0                104846
  20-min Recv drop:
          10.0.0.1[0]               42                0       3                 50567
  8-hour Sent byte:
          10.0.0.1[0]              367                0       0              10580308
  8-hour Sent pkts:
          10.0.0.1[0]                3                0       0                104043
  1-hour Sent drop:
          10.0.0.1[0]                3                0       1                 10851
  8-hour Recv byte:
          10.0.0.1[0]              337                0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]                3                0       0                104846
  1-hour Recv drop:
          10.0.0.1[0]               14                0       1                 50567
 24-hour Sent byte:
          10.0.0.1[0]              122                0       0              10580308
 24-hour Sent pkts:
          10.0.0.1[0]                1                0       0                104043
 24-hour Recv byte:
          10.0.0.1[0]              112                0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]                1                0       0                104846
```

表 13-7 显示每个字段的说明。

表 13-7　show threat-detection statistics top host 字段

字段	说明
Top	显示一定时间段 / 统计类型范围内的主机排名，从 [0]（最高计数）到 [9]（最低计数）。统计信息可能不足以覆盖全部 10 个位置，因此可能列出不到 10 个主机。
Average(eps)	请参阅表 13-2 中的说明。
Current(eps)	请参阅表 13-2 中的说明。

表 13-7　show threat-detection statistics top host 字段（续）

字段	说明
Trigger	请参阅表 13-2 中的说明。
Total events	请参阅表 13-2 中的说明。
Time_interval Sent byte	显示成功发送到针对每个时间段列出的主机的字节数。
Time_interval Sent packet	显示成功发送到针对每个时间段列出的主机的数据包数。
Time_interval Sent drop	显示发送到针对每个时间段列出的主机的由于是扫描攻击的一部分而被丢弃的数据包数。
Time_interval Recv byte	显示针对每个时间段列出的主机成功接收的字节数。
Time_interval Recv packet	显示针对每个时间段列出的端口和协议成功接收的数据包数。
Time_interval Recv drop	显示针对每个时间段列出的端口和协议接收的由于是扫描攻击的一部分而被丢弃的数据包数。
host_ip_address	显示发送、接收或丢弃数据包或字节的主机 IP 地址。

以下是 **show threat-detection statistics top tcp-intercept** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
----------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2     192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3     192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4     192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5     192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6     192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7     192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8     192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9     192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10    192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

表 13-8 显示每个字段的说明。

表 13-8　show threat-detection statistics top tcp-intercept 字段

字段	说明
Monitoring window size:	显示 ASA 采样统计信息的时间段。默认值为 30 分钟。可以使用 **threat-detection statistics tcp-intercept rate-interval** 命令更改此设置。ASA 在此间隔内采样 30 次数据。
Sampling interval:	显示采样的间隔。此值始终为速率间隔除以 30。
rank	显示排名 1 到 10，其中 1 是最受攻击的服务器，10 是最不受攻击的服务器。
server_ip:port	显示正受到攻击的服务器 IP 地址和端口。

表 13-8　show threat-detection statistics top tcp-intercept 字段（续）

字段	说明
interface	显示服务器受到攻击的接口。
avg_rate	显示采样期间内的平均攻击速率（以攻击数 / 秒为单位）。
current_rate	显示当前攻击速率（以攻击数 / 秒为单位）。
total	显示攻击总数。
attacker_ip	显示攻击者 IP 地址。
(*last_attack_time* ago)	显示上一次攻击发生的时间。

以下是 **show threat-detection statistics top tcp-intercept long** 命令的输出示例，括号中为实际源 IP 地址：

```
ciscoasa# show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total>
<Source IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

以下是 **show threat-detection statistics top tcp-intercept detail** 命令的输出示例：

```
ciscoasa# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
     Sampling History (30 Samplings):
             95348      95337      95341      95339      95338      95342
             95337      95348      95342      95338      95339      95340
             95339      95337      95342      95348      95338      95342
             95337      95339      95340      95339      95347      95343
             95337      95338      95342      95338      95337      95342
             95348      95338      95342      95338      95337      95343
             95337      95349      95341      95338      95337      95342
             95338      95339      95338      95350      95339      95570
             96351      96351      96119      95337      95349      95341
             95338      95337      95342      95338      95338      95342
.......
```

表 13-9 显示每个字段的说明。

表 13-9　show threat-detection statistics top tcp-intercept detail 字段

字段	说明
Monitoring window size:	显示 ASA 采样统计信息的时间段。默认值为 30 分钟。可以使用 **threat-detection statistics tcp-intercept rate-interval** 命令更改此设置。ASA 在此间隔内采样 30 次数据。
Sampling interval:	显示采样的间隔。此值始终为速率间隔除以 30。
rank	显示排名 1 到 10，其中 1 是最受攻击的服务器，10 是最不受攻击的服务器。
server_ip:port	显示正受到攻击的服务器 IP 地址和端口。
interface	显示服务器受到攻击的接口。
avg_rate	显示通过 **threat-detection statistics tcp-intercept rate-interval** 命令设置的速率间隔（默认情况下，速率间隔为 30 分钟）内的平均攻击速率（以攻击数 / 秒为单位）。ASA 在速率间隔内每 30 秒采样一次数据。
current_rate	显示当前攻击速率（以攻击数 / 秒为单位）。
total	显示攻击总数。
attacker_ip or <*various*> Last: *attacker_ip*	显示攻击者 IP 地址。如果有多个攻击者，则 “<various>” 后面紧跟上一个攻击者 IP 地址。
(*last_attack_time* ago)	显示上一次攻击发生的时间。
sampling data	显示所有 30 个采样数据值，这些值显示了每个间隔的攻击数。

相关命令

命令	说明
threat-detection scanning-threat	启用扫描威胁检测。
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics port	显示端口统计信息。
show threat-detection statistics protocol	显示协议统计信息。
threat-detection statistics	启用威胁统计。

show tls-proxy

要显示 TLS 代理和会话信息，请在全局配置模式下使用 **show tls-proxy** 命令。

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**] [**statistics**]]

语法说明

cert-dump	转储本地动态证书。输出是 LDC 的十六进制转储。
count	仅显示会话计数器。
detail	显示详细 TLS 代理信息，包括每个 SSL 段和 LDC 的密码。
host *host_addr*	指定要显示关联会话的特定主机。
session	显示活动 TLS 代理会话。
statistics	显示监控和管理 TLS 会话的统计信息。
tls_name	要显示的 TLS 代理的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC 模式	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(2)	引入了此命令。
8.3(1)	增加了 **statistics** 关键字。

示例

以下是 **show tls-proxy** 命令的输出示例：

```
ciscoasa# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

以下是 **show tls-proxy session** 命令的输出示例：

```
ciscoasa# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

以下是 **show tls-proxy session detail** 命令的输出示例：

```
ciscoasa# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

以下是 **show tls-proxy session statistics** 命令的输出示例：

```
ciscoasa# show tls-proxy session stastics
    TLS Proxy Sessions (Established: 600)
        Mobility:                              200
        UC-IME:                                400

    Per-Session Licensed TLS Proxy Sessions
    (Established: 222, License Limit: 250)
        SIP:                                     2
        SCCP:                                   20
        Phone Proxy:                           200

    Total TLS Proxy Sessions
        Established:                           822
        Platform Limit:                       1000
```

相关命令

命令	说明
client	定义密码套件以及设置本地动态证书颁发者或密钥对。
ctl-provider	定义 CTL 提供程序实例，然后进入提供程序配置模式。
show running-config tls-proxy	显示所有或指定的 TLS 代理的运行配置。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

show track

要显示跟踪过程跟踪的对象的信息，请在用户 EXEC 模式下使用 **show track** 命令。

show track [*track-id*]

语法说明

track-id	跟踪条目对象 ID。有效值为从 1 到 500。

默认值

如果未提供 *track-id*，则显示所有跟踪对象的信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下是 **show track** 命令的输出示例：

```
ciscoasa(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

相关命令

命令	说明
show running-config track	显示运行配置中的 **track rtr** 命令。
track rtr	创建用于轮询 SLA 的跟踪条目。

show traffic

要显示接口发送和接收活动，请在特权 EXEC 模式下使用 **show traffic** 命令。

show traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	增加了 ASA 5550 的输出。
9.3(1)	增加了物理接口上的汇聚流量的输出。

使用指南

show traffic 命令列出了自上次输入 **show traffic** 命令以来或 ASA 上线以来通过每个接口的数据包和字节数。秒数是 ASA 自上次重启以来的在线持续时间，除非自上次重启以来输入过 **clear traffic** 命令。如果是这种情况，则秒数是自输入命令以来的持续时间。

对于 ASA 5550，**show traffic** 命令还显示每个插槽的汇聚吞吐量。由于 ASA 5550 要求流量均匀分配到各个插槽才能实现最大吞吐量，因此此输出可帮助您确定流量是否均匀分配。

要显示物理接口上的汇聚流量，必须先输入 **sysopt traffic detailed-statistics** 命令开启此功能。

示例

以下是 **show traffic** 命令的输出示例：

```
ciscoasa# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
```

```
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

对于 ASA 5550，以下文本显示在末尾：

```
----------------------------------------
        Per Slot Throughput Profile
----------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************

  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

以下示例显示为物理接口上的汇聚流量增加的输出：

```
IP packet size distribution (values listed in percentages)
Total Packets = 1278:
      32    64    96   128   192   256   512
    00.0  43.5  10.4  10.1  26.1  01.4  03.6

    1024  1536  2048  4096  8192  9216
    03.6  06.6  00.0  00.0  00.0  00.0

Protocol         Total    Conns   Packets   Bytes  Packets    Total
--------         Conns     /Sec     /Conn    /Pkt     /Sec  Packets
TCP                  8      0.2        98     215     26.8     1279
TCP-inspected        0      0.0       N/A     N/A      0.0        0
UDP                  3      0.0         0      90      0.0        2
UDP-inspected        5      0.0         1     189      0.0       56
ICMP                 0      0.0         1      98      0.0        2
IP                   0      0.0       N/A     N/A      0.0        0
Total:              16      0.2        22     207     26.8     1433

Last clearing of statistics: Never
```

相关命令

命令	说明
clear traffic	重置用于发送和接收活动的计数器。

show uauth 至 show xlate 命令

show uauth

要显示一个或当前所有已验证的用户、用户所绑定的主机 IP 以及任何缓存的 IP 和端口授权信息，请在特权 EXEC 模式下使用 **show uauth** 命令。

show uauth [*username*]

语法说明

username	（可选）按用户名指定用户身份验证和授权信息。

默认值

省略用户名将显示所有用户的授权信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	空闲时间已添加到输出。
7.2(2)	从输出中移除空闲时间。

使用指南

show uauth 命令显示一个用户或所有用户的 AAA 授权和身份验证缓存。

此命令与 **timeout** 命令配合使用。

每个用户主机 IP 地址都有一个与之连接的授权缓存。缓存允许每个用户主机最多可以有 16 个地址和服务对。如果有用户尝试从正确的主机访问已缓存的服务，ASA 会认为该用户已获得预授权，并会立即充当连接代理。例如，一旦获得授权访问网站，就无需每次加载图像时都连接授权服务器（假设图像来自同一个 IP 地址）。此过程可大大提高性能并减少授权服务器的负载。

show uauth 命令的输出显示提供给授权服务器以进行身份验证和授权的用户名、用户名绑定的 IP 地址以及用户是仅经过身份验证还是缓存了服务。

注　如果启用扩展身份验证，将为分配给客户端的 IP 地址向用户身份验证表添加一个条目（可通过 **show uauth** 命令显示）。但是，如果在网络扩展模式下将扩展身份验证与简易虚拟专用网 (VPN) 远程接入功能结合使用，会在网络间创建 IPsec 隧道，如此一来，位于防火墙后面的用户将无法与单个 IP 地址关联。因此，完成扩展身份验证后将无法创建用户身份验证条目。如果需要 AAA 授权或计费服务，可以启用 AAA 身份验证代理对防火墙后面的用户进行身份验证。有关 AAA 身份验证代理的详细信息，请参阅 **aaa** 命令。

可使用 **timeout uauth** 命令指定在用户连接进入空闲状态后应保留缓存多长时间。可使用 **clear uauth** 命令删除所有用户的所有授权缓存，这样将强制用户在下一次创建连接时重新进行身份验证。

示例

此示例显示在没有验证用户以及正在对一位用户进行身份验证时 **show uauth** 命令的输出示例：

```
ciscoasa(config)# show uauth
                        Current    Most Seen
Authenticated Users       1            1
Authen In Progress        0            1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
   access-list #ACSACL#-IP-v039294-521b0b8b (*)
   absolute   timeout: 0:00:00
   inactivity timeout: 0:05:00
```

此示例显示三个用户已经过验证和授权以通过 ASA 使用服务时 **show uauth** 命令的输出示例：

```
ciscoasa(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

相关命令

命令	说明
clear uauth	清除当前用户身份验证和授权信息。
timeout	设置最长空闲持续时间。

show url-block

要显示 url 块缓冲区中保留的数据包数量以及由于超过缓冲区限制或重新传输而丢失的包数量（如果有），请在特权 EXEC 模式下使用 **show url-block** 命令。

show url-block [**block statistics**]

语法说明

block statistics	（可选）显示块缓冲区使用率统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show url-block block statistics 命令显示 url 块缓冲区中保留的数据包数量以及由于超过缓冲区限制或重新传输而丢失的包数量（如果有）。

示例

以下是 **show url-block** 命令的输出示例的示例：

```
ciscoasa# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

这显示 URL 块缓冲区的配置。

以下是来自 **show url-block block statistics** 命令的输出示例：

```
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

相关命令

命令	说明
clear url-block block statistics	清除数据块缓冲区使用计数器。
filter url	将流量引导至 URL 过滤服务器。
url-block	管理用于 Web 服务器响应的 URL 缓冲区。
url-cache	在来自 N2H2 或 Websense 服务器的响应挂起时，启用 URL 缓存并设置缓存的大小。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

show url-cache statistics

要显示有关 URL 缓存的信息（用于从 N2H2 或 Websense 过滤服务器收到的 URL 响应），请在特权 EXEC 模式下使用 **show url-cache statistics** 命令。

show url-cache statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show url-cache statistics 命令显示下列条目：

- Size - 用 **url-cache** *size* 选项设置的缓存的大小（以千字节为单位）。
- Entries - 基于缓存大小的缓存条目最大数量。
- In Use - 缓存中当前的条目数。
- Lookups - ASA 查找某个缓存条目的次数。
- Hits - ASA 在缓存中找到某个条目的次数。

您可以使用 **show perfmon** 命令查看有关 N2H2 Sentian 或 Websense 过滤活动的其他信息。

示例

以下是 **show url-cache statistics** 命令的输出示例：

```
ciscoasa# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 Hits :     290
```

相关命令

命令	说明
clear url-cache statistics	从配置中删除 **url-cache** 命令语句。
filter url	将流量引导至 URL 过滤服务器。
url-block	管理用于 Web 服务器响应的 URL 缓冲区。
url-cache	对从 N2H2 或 Websense 服务器收到的响应启用 URL 缓存并设置缓存的大小。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

show url-server

要显示有关 URL 过滤服务器的信息，请在特权 EXEC 模式下使用 **show url-server** 命令。

show url-server statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

show url-server statistics 命令显示 URL 服务器供应商； URL 的总数量、允许的数量和拒绝的数量； HTTPS 连接的总数量、允许和拒绝的数量； TCP 连接的总数量、允许和拒绝的数量；以及 URL 服务器的状态。

show url-server 命令显示以下信息：

- 对于 N2H2：**url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol** [{**TCP | UDP**}{**version 1 | 4**}]
- 对于 Websense：**url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol** [{**TCP | UDP**}]

示例

以下是 **show url-server statistics** 命令的输出示例：

```
ciscoasa## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
```

```
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                       DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
。。。
URL Packets Sent and Received Stats:
------------------------------------
Message                  Sent     Received
STATUS_REQUEST           411      0
LOOKUP_REQUEST           366519   365952
LOG_REQUEST              0        NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis.The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

相关命令

命令	说明
clear url-server	清除 URL 过滤服务器统计信息。
filter url	将流量引导至 URL 过滤服务器。
url-block	管理用于 Web 服务器响应的 URL 缓冲区。
url-cache	在来自 N2H2 或 Websense 服务器的响应挂起时，启用 URL 缓存并设置缓存的大小。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

show user-identity ad-agent

要显示有关身份防火墙的 AD 代理的信息，请在特权 EXEC 模式下使用 **show user-identity ad-agent** 命令。

show user-identity ad-agent [**statistics**]

语法说明

statistics	（可选）显示关于 AD 代理的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• **是**	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

您可以监视身份防火墙的 AD 代理组件。

使用 **show user-identity ad-agent** 命令来获取 AD 代理的故障排除信息。此命令显示有关主要和辅助 AD 代理的以下信息：

- AD 代理状态
- 域状态
- AD 代理统计信息

表 14-1　命令输出的说明

类型	值	说明
Mode	配置模式	指定全部下载或按需下载。
AD Agent IP Address	IP address	显示活动 AD 代理 IP 地址。
Backup	IP address	显示备用 AD 代理 IP 地址。
AD Agent Status	• Disabled • Down • Up（已注册） • Probing	• 身份防火墙已禁用。 • AD 代理已关闭。 • AD 代理已启动且正在运行。 • ASA 已注册，并且 AD 代理已启动且正在运行。 • ASA 正在尝试连接到 AD 代理。

表 14-1　命令输出的说明（续）

类型	值	说明
Authentication Port	udp/1645	显示 AD 代理身份验证端口。
Accounting Port	udp/1646	显示 AD 代理记账端口。
ASA Listening Port	udp/3799	显示 ASA 侦听端口。
Interface	Interface	显示 ASA 用于联系 AD 代理的接口。
IP Address	IP address	显示 ASA 用于联系 AD 代理的 IP 地址。
Uptime	Time	显示 AD 代理可运行时间。
Average RTT	Milliseconds	显示 ASA 用于联系 AD 代理的平均往返时间。
Domain	域昵称 状态：up 状态：down	显示 AD 代理的 Microsoft Active Directory 域。

示例

本示例显示如何展示身份防火墙的 AD 代理信息：

```
ciscoasa# show user-identity ad-agent
Primary AD Agent:
Status                    up (registered)
 Mode:                     full-download
 IP address:               172.23.62.125
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  15 mins 41 secs
 Average RTT:              57 msec

Secondary AD Agent:
Status                    up
 Mode:                     full-download
 IP address:               172.23.62.136
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  7 mins 56 secs
 Avg RTT:                  15 msec
```

相关命令

命令	说明
clear user-identity ad-agent statistics	清除 ASA 为身份防火墙维护的 AD 代理统计信息。
user-identity enable	创建思科身份防火墙实例。
show user-identity ad-group-members	显示身份防火墙的 AD 代理域中的组成员。

show user-identity ad-group-members

要显示身份防火墙的 AD 代理域中的组成员，请在特权 EXEC 模式下使用 **show user-identity ad-group-members** 命令。

show user-identity ad-group-members [*domain_nickname*\]*user_group_name* [**timeout seconds** *seconds*]

语法说明

domain_nickname	（可选）指定身份防火墙的域名。
timeout seconds *seconds*	（可选）设置用于检索组成员统计信息的计时器并指定计时器的时间长度。
user_group_name	（可选）指定为其检索统计信息的组名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

show user-identity ad-group-members 命令显示指定用户组的直接成员（用户和组）。

注　此命令不显示在 ASA 上用 **object-group user** 命令配置的本地定义组的信息。

ASA 发送 LDAP 一个查询，以查找在 Active Directory 服务器上配置的 Active Directory 组。运行此命令等同于运行使您能够您选中指定用户组的成员的 LDAP 浏览器命令。ASA 发出一个 LDAP 层级的查询以检索指定组的直接成员（distinguishedName 格式）。运行此命令不会更新已导入用户组的 ASA 内部缓存。

未指定 *domain_nickname* 时，ASA 显示默认域中具有 *user_group_name* 的组的信息。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

组名是 AD 组的唯一 sAMAccountName，不是 CN 名称。要显示特定组 sAMAccountName 的信息，请使用 **show user-identity ad-groups filter** *filter_string* 命令来检索组的 sAMAccountName。

示例

本示例展示如何显示身份防火墙的 sample1 组的成员：

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO        AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。
show user-identity ad-groups	显示有关身份防火墙的 AD 代理的信息。

show user-identity ad-groups

要显示身份防火墙的特定组的信息，请在特权 EXEC 模式下使用 **show user-identity ad-groups** 命令。

show user-identity ad-groups *domain_nickname* {**filter** *filter_string* | **import-user-group** [**count**]}

语法说明

count	（可选）显示激活组的数量。
domain_nickname	指定身份防火墙的域名。
filter *filter_string*	指定要显示的组，该组中包含 Microsoft Active Directory 域控制器的 CN 属性中的指定过滤字符串。
import-user-group	仅显示身份防火墙的激活组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

在运行 **show user-identity ad-groups** 命令时，ASA 将 LDAP 查询发送到 Microsoft Active Directory 以检索属于指定域昵称的所有用户组。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。ASA 仅检索具有组 objectclass 属性的组。ASA 显示 distinguishedName 格式的检索组。

指定**过滤器** *filter_string* 关键字和参数时，ASA 将显示包含域控制器的 CN 属性中的指定过滤字符串的组。因为 **access-list** 和 **object-group** 命令只获取 sAMAccountName，所以您可以运行 **show user-identity ad-users filter** *filter_string* 命令来检索组的 sAMAccountName。未指定**过滤器** *filter_string* 时，ASA 将显示所有 Active Directory 组。

指定 **import-user-group count** 关键字时，ASA 显示所有激活的（因为它们是访问组、导入用户组或服务策略配置的一部分）和存储在本地数据库中的 Active Directory 组。ASA 只显示组的 sAMAccountName。

示例

以下示例展示如何显示属于身份防火墙的指定域昵称的用户组：

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO        AAA Server Group:       CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups       6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...


ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2


ciscoasa# show user-identity ad-groups CSCO import-user-group
Domain: CSCO
Groups:
        group.SampleGroup1
        group.SampleGroup2
...
```

本示例展示如何运行此命令将过滤字符串应用于访问列表和对象组命令的结果。运行 **show user-identity ad-users CSCO filter SampleGroup1** 命令将获得指定字符串的 sAMAccountName：

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1
Domain:CSCO    AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity ad-users

要显示身份防火墙的 Microsoft Active Directory 用户，请在特权 EXEC 模式下使用 **show user-identity ad-users** 命令。

show user-identity ad-users *domain_nickname* [**filter** *filter_string*]

语法说明

domain_nickname	指定身份防火墙的域名。
filter *filter_string*	（可选）指定以显示包含 Microsoft Active Directory 域控制器的 CN 属性中的指定过滤字符串的用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

在运行 **show user-identity ad-users** 命令时，ASA 将 LDAP 查询发送到 Microsoft Active Directory 以检索属于指定域昵称的所有用户。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

指定**过滤器** *filter_string* 关键字和参数时，ASA 将显示包含域控制器的 CN 属性中的指定过滤字符串的用户。ASA 发送 LDAP 一个查询，以查找在 Active Directory 服务器上配置的 Active Directory 组。

ASA 只检索具有 user objectclass 属性和 samAccountType 属性 805306368 的用户。其他对象（例如，机器对象）可以包含在 user objectclass 中；但是，samAccountType 805306368 将过滤掉非用户对象。未指定过滤字符串时，ASA 显示所有 Active Directory 用户。

ASA 显示 distinguishedName 格式的检索的用户。

示例

本示例展示如何显示关于身份防火墙的 Active Directory 用户信息：

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO        AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
```

```
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity group

要显示为身份防火墙配置的用户组，请在特权 EXEC 模式下使用 **show user-identity group** 命令。

show user-identity group

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show user-identity group** 命令获取为身份防火墙配置的用户组的故障排除信息。ASA 发送 LDAP 一个查询，以查找在 Active Directory 服务器上配置的 Active Directory 组。此命令按以下格式显示激活的用户组列表：

domain\group_name

ASA 仅显示应用于安全策略的顶级组。激活的顶级组的最大数量为 256。当组属于访问组、导入用户组或服务策略组配置的一部分时，组已激活。

示例

本示例展示如何显示身份防火墙的已激活组：

```
ciscoasa# show user-identity group
Group ID        Activated Group Name (Domain\\Group)
--------        ------------------------------------
       1        LOCAL\\og1
       2        LOCAL\\marketing
       3        CISCO\\group.sampleuser1
       4        IDFW\\grp1
...
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity ip-of-user

要显示身份防火墙的指定用户的 IP 地址，请在特权 EXEC 模式下使用 **show user-identity ip-of-user** 命令。

show user-identity ip-of-user [*domain_nickname*\]*user-name* [**detail**]

语法说明

detail	（可选）显示关于用户和 IP 地址的详细输出。
domain_nickname	（可选）指定身份防火墙的域名。
user-name	指定为其获取 IP 地址的用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

此命令显示指定用户的用户信息和 IP 地址。用户可以具有多个与其关联的 IP 地址。

未指定 *domain_nickname* 参数时，ASA 显示默认域中名为 *user_name* 的用户的信息。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

指定 **detail** 关键字时，ASA 显示活动连接总数、用户统计信息时间段和丢失数，以及此时间段内通过指定用户的所有 IP 地址的输入数据包和输出数据包。未指定 **detail** 选项时，ASA 只显示每个 IP 地址的域昵称和状态。

注　只有当您为身份防火墙启用用户统计信息扫描或记账时，ASA 才显示详细的用户统计信息，例如，指定时间段内接收的数据包数、发送数据包数和丢弃数。请参阅 CLI 配置指南以了解关于配置身份防火墙的信息。

示例

以下示例展示如何显示身份防火墙的指定用户的 IP 地址：

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)
```

```
ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins;  Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins;  Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560


ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user


ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

IPv6 support

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)


ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins;  Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。
show user-identity user-of-ip	显示与指定 IP 地址关联的用户信息

show user-identity memory

要显示身份防火墙的各种模块的内存，请在特权 EXEC 模式下使用 **show user-identity memory** 命令。

show user-identity memory

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

您可以在 ASA 上监视身份防火墙的内存使用情况。运行 **show user-identity memory** 命令将显示用户记录、组记录、主机记录及其相关哈希表的内存。ASA 还显示基于身份的 tmatch 表所使用的内存。

该命令显示身份防火墙中各种模块的内存使用情况（以字节为单位）：

- 用户
- 群组
- 用户统计信息
- LDAP

ASA 发送 LDAP 一个查询，以查找在 Active Directory 服务器上配置的 Active Directory 组。Active Directory 服务器验证用户并生成用户登录安全日志。

- AD 代理
- 其他
- 总内存使用情况

配置身份防火墙以从 AD 代理检索用户信息的方法，会影响功能使用的内存量。指定 ASA 使用按需检索还是完全下载检索。选择 “ 按需 ” 的优势是使用的内存较少，因为只查询和存储接收的数据包的用户。请参阅 CLI 配置指南中的 “ 配置身份选项 ” 以了解对这些选项的说明。

示例

本示例展示如何显示身份防火墙模块的内存状态：

```
ciscoasa# show user-identity memory
Users:       22416048 bytes
Groups:           320 bytes
User stats:         0 bytes
LDAP:             300 bytes
AD agent:         500 bytes
Misc:           32428 bytes
Total:       22449596 bytes
Users:       22416048 bytes
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity statistics

要显示身份防火墙的用户或用户组的统计信息，请在特权 EXEC 模式下使用 **show user-identity statistics** 命令。

show user-identity statistics [**user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\]*user_group_name*]

语法说明

domain_nickname	（可选）指定身份防火墙的域名。
user *user_name*	（可选）指定从其检索统计信息的用户名。
user-group *domain_nickname*\ *user_group_name*	（可选）指定为其检索统计信息的组名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

运行 **show user-identity statistics** 命令以显示用户或用户组的统计信息。

未指定 **user** 关键字和 *domain_nickname* 参数时，ASA 显示默认域中名为 *user_name* 的用户的信息。

未指定 **user-group** 关键字和 *domain_nickname* 时，ASA 显示默认域中具有 *user_group_name* 的组的信息。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

示例

以下示例展示如何显示身份防火墙的用户的相关统计信息：

```
ciscoasa# show user-identity statistics user
Current monitored users:11  Total not monitored users:0
                         Average(eps)    Current(eps) Trigger      Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                4              10      14              4861
    1-hour Recv pkts:                  1               10        0               4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
  20-min Sent attack:                4              10        4              4862
  1-hour Sent pkts:                    0               5         0              2451
...
```

```
ciscoasa# show user-identity statistics user user1
Current                          Average(eps)    Current(eps) Trigger      Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                4              10       14              4861
  1-hour Recv pkts:                   1              10       0               4901
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity statistics top user

要显示身份防火墙的前 10 位用户的统计信息，请在特权 EXEC 模式下使用 **show user-identity statistics top user** 命令。

show user-identity statistics top user

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

show user-identity statistics top user 命令显示前 10 位用户的已接收 EPS 数据包、发送的 EPS 数据包和发送的攻击的统计信息。对于每个用户（显示为*域\用户名*），ASA 显示该用户的平均 EPS 数据包、当前 EPS 数据包、触发器和事件总数。

示例

本示例展示如何显示身份防火墙的前 10 位用户的相关信息：

```
ciscoasa# show user-identity statistics top user
Top          Name    Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv pkts:
01    APAC\sampleuser1
                                   0               0       0               391
  1-hour Sent pkts:
01    APAC\sampleuser2
                                   0               0       0               196
02    CSCO\sampleuser3
                                   0               0       0               195
  10-min Sent attack:
01    CSCO\sampleuser4
                                   0               0       0               352
02    CSCO\sampleuser3
                                   0               0       0               350
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity user active

要显示身份防火墙的活动用户，请在特权 EXEC 模式下使用 **show user-identity user active** 命令。

show user-identity user active [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name* | **user** [*domain_nickname*\]*user_name*] [**list** [**detail**]]

语法说明

detail	（可选）显示活动用户会话的详细输出。
domain *domain_nickname*	显示指定域中活动用户的统计信息。
list	（可选）显示活动用户统计信息的总结列表。
user *domain_nickname\user_name*	（可选）显示指定用户的统计信息。
user-group *domain_nickname\user_group_name*	（可选）显示指定用户组的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

可以显示身份防火墙使用的 IP 用户映射数据库中包含的所有用户的相关信息。

show user-identity user active 命令显示用户的以下信息：

- *域\用户名*
- 活动连接
- 空闲分钟数

默认域名可以是真实域名、特殊保留字或 LOCAL。身份防火墙为所有本地定义的用户组或本地定义的用户（使用 VPN 或 Web 门户登录和验证的用户）使用 LOCAL 域名。未指定默认域时，默认域为 LOCAL。

用户名后附加了空闲分钟数。按用户（而不是按用户的 IP 地址）存储登录时间和空闲时间。

指定了**用户组**关键字时，只显示激活的用户组。当组属于访问组、导入用户组或服务策略组配置的一部分时，组已激活。

未指定 **user-group** 关键字和 *domain_nickname* 时，ASA 显示默认域中具有 *user_group_name* 的组的信息。

注　用 **disable-user-identity-rule** 关键字配置了 **user-identity action domain-controller-down** 且指定的域关闭时，或者以 **disable-user-identity-rule** 关键字配置了 **user-identity action ad-agent-down** 命令且 AD 代理已关闭时，所有已登录用户都在用户统计信息中显示为禁用。

注　只有当您为身份防火墙启用用户统计信息扫描或记账时，ASA 才显示详细的用户统计信息，例如，指定时间段内接收的数据包数、发送数据包数和丢弃数。请参阅 CLI 配置指南以了解关于配置身份防火墙的信息。

示例

以下示例展示如何显示身份防火墙的活动用户的相关信息：

```
ciscoasa# show user-identity user active
Total active users: 30  Total IP addresses: 35
  LOCAL: 0 users, 0 IP addresses
  cisco.com: 0 users, 0 IP addresses
  d1: 0 users, 0 IP addresses
  IDFW: 0 users, 0 IP addresses
  idfw.com: 0 users, 0 IP addresses
  IDFWTEST: 30 users, 35 IP addresses


ciscoasa# show user-identity user active domain CSCO
Total active users: 48020 Total IP addresses:10000
  CSCO: 48020 users, 10000 IP addresses


ciscoasa# show user-identity user active domain CSCO list
Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 5 mins
   CSCO\member-2: 20 active conns; idle 20 mins
   CSCO\member-3: 3 active conns; idle 101 mins
   …


ciscoasa# show user-identity user active list
Total active users: 48032  Total IP addresses: 10000
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 6 mins
   APAC\sampleuser2: 20 active conns; idle 0 mins
   CSCO\member-2: 20 active conns; idle 1 mins
   CSCO\member-3: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 22 mins
   CSCO\member-4: 3 active conns; idle 101 mins
   …
ciscoasa# show user-identity user active list detail
Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
     172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
```

```
     172.100.3.23: login 200 min, idle 15 mins , 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
   CSCO\member-1: 4 active connections;  idle 350 mins
   …
  APAC\sampleuser12: 3 active conns; idle 101 mins
     172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
     172.100.3.23: login 200 min, idle 150 mins, 2 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active list detail
Total users: 25  Total IP addresses: 5
   LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...


ciscoasa# show user-identity user active user sampleuser1 list detail
CSCO\sampleuser1: 20 active conns; idle 3 mins
     172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
     172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active user APAC\sampleuser2
APAC\sampleuser2: 20 active conns; idle 2 mins


ciscoasa# show user-identity user active user-group APAC\\marketing list

   APAC\sampleuser1: 20 active conns; idle 2 mins
   APAC\member-1: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 0 mins
   APAC\member-3: 20 active conns; idle 6 mins
...

ciscoasa# show user-identity user active user-group APAC\\inactive list
ERROR: group is not activated
```

相关命令

命令	说明
clear user-identity active-user-database	设置指定用户的状态，所有用户都属于指定用户组，或所有用户注销身份防火墙。
user-identity enable	创建思科身份防火墙实例。

show user-identity user all

要显示关于身份防火墙的用户的统计信息，请在特权 EXEC 模式下使用 **show user-identity user all** 命令。

show user-identity user all [**list**] [**detail**]

语法说明

detail	（可选）显示关于身份防火墙的所有用户的详细输出。
list	（可选）显示汇总身份防火墙的所有用户的统计信息的列表。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 show user-identity all 命令显示身份防火墙使用的 IP 用户映射数据库中包含的所有用户的信息。

将详细信息关键字包含在此命令中且该命令输出显示 IP 地址处于非活动状态时，IP 地址未与用户关联。搜索与该 IP 地址关联的用户将返回错误。

注　用 **disable-user-identity-rule** 关键字配置了 **user-identity action domain-controller-down** 且指定的域关闭时，或者以 **disable-user-identity-rule** 关键字配置了 **user-identity action ad-agent-down** 命令且 AD 代理已关闭时，所有已登录用户都在用户统计信息中显示为禁用。

注　只有当您为身份防火墙启用用户统计信息扫描或记账时，ASA 才显示详细的用户统计信息，例如，指定时间段内接收的数据包数、发送数据包数和丢弃数。请参阅 CLI 配置指南以了解关于配置身份防火墙的信息。

示例

以下示例展示如何显示身份防火墙的所有用户的相关统计信息：

```
ciscoasa# show user-identity user all list
Total inactive users: 1201  Total IP addresses: 100
```

```
ciscoasa# show user-identity user all list
Total users: 7
  LOCAL\idfw: 0 active conns
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
  cisco.com\sampleuser4: 0 active conns; idle 300 mins
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
  cisco.com\sampleuser7: 0 active conns


ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
  LOCAL\idfw: 0 active conns
    10.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns; idle 300 mins
    171.69.42.8: inactive
    10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
  cisco.com\sampleuser4: 0 active conns
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity user inactive

要显示有关身份防火墙的非活动用户的信息，请在特权 EXEC 模式下使用 **show user-identity user inactive** 命令。

show user-identity user inactive [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name*]

语法说明

domain *domain_nickname*	（可选）显示身份防火墙的指定域名中非活动用户的统计信息。
user-group *domain_nickname*\ *user_group_name*	（可选）显示指定用户组中非活动用户的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show user-identity user inactive** 命令显示在此 **user-identity inactive-user-timer** 命令所配置的值更长的时间内没有活动流量的用户的相关信息。

指定了**用户组**关键字时，只显示激活的用户组。当组属于访问组、导入用户组或服务策略组配置的一部分时，组已激活。

未指定 **user-group** 关键字和 *domain_nickname* 时，ASA 显示默认域中具有 *user_group_name* 的组的信息。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

示例

以下示例展示如何显示身份防火墙的非活动用户的状态：

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
   APAC\sampleuser1
   CSCO\sampleuser2
172.1.1.1: inactive     …
...
```

```
ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
    CSCO: 1101
   CSCO\sampleuser1
   CSCO\sampleuser2
   CSCO\sampleuser3
...


ciscoasa# show user-identity user inactive user-group CSCO\\marketing
Total inactive users: 21
   CSCO\sampleuser1
   CSCO\sampleuser2
...
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。
user-identity inactive-user-timer	指定某个用户被思科身份防火墙实例视为空闲之前所经过的时间量。

show user-identity user-not-found

要显示身份防火墙未找到的 Active Directory 用户的 IP 地址，请在特权 EXEC 模式下使用 **show user-identity user-not-found** 命令。

show user-identity user-not-found

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show user-identity user-not-found** 命令可显示未能在 Microsoft Active Directory 中找到的用户的 IP 地址。

ASA 维护这些 IP 地址的本地 “ 找不到的用户 ” 数据库。ASA 仅保留 “ 找不到的用户 ” 列表的最新 1024 个数据包（来自同一个源的连续数据包将被当作一个数据包），而不会在数据库中保留整个列表。

示例

本示例展示如何显示身份防火墙未找到的用户的相关信息：

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
…
```

相关命令

命令	说明
clear user-identity user-not-found	清除身份防火墙的 ASA 本地 “ 找不到的用户 ” 数据库。
user-identity enable	创建思科身份防火墙实例。
user-identity user-not-found	为身份防火墙启用 “ 找不到的用户 ” 跟踪。

show user-identity user-of-group

要显示身份防火墙的指定用户组的用户，请在特权 EXEC 模式下使用 **show user-identity user-of-group** 命令。

show user-identity user-of-group [*domain_nickname*\]*user_group_name*

语法说明

domain_nickname	指定身份防火墙的域名。
user_group_name	指定要显示统计信息的用户组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show user-identity user-of-group** 命令显示其组 ID 与指定的用户组匹配的用户。（ASA 扫描 IP 用户哈希列表以查找此信息，而不是向 Active Directory 发送 LDAP 查询。AD 代理维护用户 ID 和 IP 地址映射的缓存并向 ASA 通报更改。）

必须激活指定的用户组，这意味着，指定的用户组必须是导入用户组（在访问列表或服务策略配置中被定义为用户组）或本地用户组（使用 object-group user 定义）。

该组可以拥有多个用户成员。用户组的成员都是指定组的直接成员（包括用户和组）。

未用 *user_group_name* 参数指定 *domain_nickname* 时，ASA 显示默认域中具有 *user_group_name* 的组的信息。参数 *domain_nickname* 可以是真实域昵称或 LOCAL。

命令输出指示用户处于非活动状态时，用户可能已注销或者从未登录。

示例

以下示例展示如何显示身份防火墙的指定用户组的用户：

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) …
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....
```

```
ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\\group.local1    Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show user-identity user-of-ip

要显示身份防火墙的特定 IP 地址的用户的相关信息，请在特权 EXEC 模式下使用 **show user-identity user-of-ip** 命令。

show user-identity user-of-ip *ip_address* [**detail**]

语法说明

detail	（可选）显示具有指定 IP 地址的用户的相关详细输出。
ip_address	指出显示其信息的用户的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **show user-identity user-of-ip** 命令来显示与指定 IP 地址关联的用户信息。

指定 **detail** 关键字时，ASA 显示用户登录时间、空闲时间、活动连接数、用户统计信息时间段和丢失数，以及此时间段内的输入数据包和输出数据包。未指定 **detail** 关键字时，ASA 仅显示域昵称、用户名和状态。

用户处于非活动状态时，用户可能已注销或者从未登录。

将 **detail** 关键字包含于此命令中且 IP 地址的命令输出显示错误时，此 IP 地址处于非活动状态，意味着此 IP 地址未与用户关联。

注　只有当您为身份防火墙启用用户统计信息扫描或记账时，ASA 才显示详细的用户统计信息，例如，指定时间段内接收的数据包数、发送数据包数和丢弃数。请参阅 CLI 配置指南以了解关于配置身份防火墙的信息。

示例

以下示例展示如何显示身份防火墙的活动用户的状态：

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
```

```
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

IPv6 support

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60

ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

相关命令

命令	说明
user-identity enable	创建思科身份防火墙实例。

show version

要显示软件版本、硬件配置、许可证密钥和相关正常运行数据，请在用户 EXEC 模式下使用 **show version** 命令。

show version

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.2(1)	在全状态故障切换模式中，将显示额外的一行，其中显示集群正常运行时间。
8.3(1)	输出现在显示某功能使用永久还是时效性密钥，以及时效性密钥的使用时长。
8.4(1)	增加了对 “ 无负载加密 ” 型号 (NPE) 的支持。
9.3(2)	如果 REST API 代理已启用，将显示其版本号。

使用指南

show version 命令可显示软件版本、自上次重新启动以来的运行时间、处理器类型、闪存分区类型、接口板、序列号（BIOS ID）、激活密钥值、许可类型以及上次修改配置时的时间戳。

如果 REST API 代理已安装并启用，也会显示其版本号。

以 **show version** 命令列出的序列号是针对闪存分区 BIOS。此号码与机箱上的序列号不同。您获得软件升级时，需要在 **show version** 命令中显示序列号，而不是机箱号。

故障切换集群正常运行时间值指出故障切换设置已运行多长时间。如果一个设备停止运行，只要活动设备继续运行，正常运行时间值就会持续增长。因此，故障切换集群正常运行时间可能大于单个设备的正常运行时间。如果您暂时禁用故障切换，然后重新启用它，则故障切换集群正常运行时间报告禁用故障切换之前设备正常运行的时间以及禁用故障切换时设备正常运行的时间。

如果您有无负载加密型号，则在查看许可证时，VPN 和 Unified Communications 许可证不会列出。

对于 ASA 5505 上的完全 VPN 对等点，所有类型的 VPN 会话的合计总数取决于您的许可证。如果启用 AnyConnect Essentials，则总数为型号最大值：25。如果启用 AnyConnect Premium，则总数为 AnyConnect Premium 值加上其他 VPN 值，不超过 25 个会话。与其他型号不同，其他 VPN 值等于所有 VPN 会话的型号限制，ASA 5505 的其他 VPN 值小于型号限制，因此总值会因 AnyConnect Premium 许可证而异。

示例

以下是 **show version** 命令的输出示例，并显示软件版本、硬件配置、许可证密钥和相关正常运行时间信息。注意，在配置了全状态故障切换的环境中，将显示额外的一行，其中显示故障切换集群正常运行时间。如果未配置故障切换，不会显示该行。此显示将展示有关最低内存需求的警告消息。

```
**************************************************************************
**                                                                      **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***    **
**                                                                      **
**          ----> Minimum Memory Requirements NOT Met! <----            **
**                                                                      **
**  Installed RAM:  512 MB                                              **
**  Required  RAM: 2048 MB                                              **
**  Upgrade part#: ASA5520-MEM-2GB=                                     **
**                                                                      **
**  This ASA does not meet the minimum memory requirements needed to    **
**  run this image. Please install additional memory (part number       **
**  listed above) or downgrade to ASA version 8.2 or earlier.           **
**  Continuing to run without a memory upgrade is unsupported, and      **
**  critical system features will not function properly.                **
**                                                                      **
**************************************************************************

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.06
 0: Ext: GigabitEthernet0/0  : address is 0013.c480.82ce, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0013.c480.82cf, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0013.c480.82d0, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0013.c480.82d1, irq 9
 4: Ext: Management0/0       : address is 0013.c480.82cd, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
```

```
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012
```

如果您在执行 **eject** 命令之后输入 **show version** 命令，但尚未实际移除此设备，则显示以下消息：

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

相关命令

命令	说明
eject	允许外部紧凑型闪存设备从 ASA 实际移除之前关闭。
show hardware	显示详细硬件信息。
show serial	显示硬件串行信息。
show uptime	显示 ASA 已正常运行的时间长度。

show vlan

要显示在 ASA 上配置的所有 VLAN，请在特权 EXEC 模式下使用 **show vlan 命令。**

show vlan

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示已配置的 VLAN：

```
ciscoasa# show vlan
10-11,30,40,300
```

相关命令

命令	说明
clear interface	清除 **show interface** 命令的计数器。
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。

show vm

要显示有关 ASAv 的虚拟平台信息，请在特权 EXEC 模式下使用 **show vm** 命令。

show vm

语法说明

此命令没有关键字或参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

对于 ASAv，请注意以下许可准则：

- 允许的 vCPU 的数量由安装的 vCPU 平台许可确定。
  - 如果许可的 vCPU 的数量与调配的 vCPU 的数量匹配，则状态为 “ 兼容 ”。
  - 如果许可的 vCPU 的数量少于调配的 vCPU 的数量，则状态为 “ 不兼容：超额调配 ”。
  - 如果许可的 vCPU 的数量多于调配的 vCPU 的数量，则状态为 “ 兼容：调配不足 ”。
- 内存限制由调配的 vCPU 的数量确定。
  - 如果调配的内存位于允许的限制内，则状态为 “ 兼容 ”。
  - 如果调配的内存高于允许的限制，则状态为 “ 不兼容：超额调配 ”。
  - 如果调配的内存低于允许的限制，则状态为 “ 兼容：调配不足 ”。
- 频率预留限制由调配的 vCPU 的数量确定。
  - 如果频率预留内存等于或高于需要的最小值 (1000 MHz)，则状态为 “ 兼容 ”。
  - 如果频率预留内存低于需要的最小值 (1000 MHz)，则状态为 “ 兼容：调配不足 ”。

例如，以下输出展示尚未应用任何许可。允许的 vCPU 的数量是指许可的数量，且 “ 不兼容：超额调配 ” 表示产品正在使用比已许可的资源多的资源运行。

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

示例

以下示例展示虚拟平台信息：

```
ciscoasa# show vm

Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     4
Processor Memory             :  8192 MB
Minimum Processor Frequency  :  1000 MHz
Maximum Processor Frequency  :  20000 MHz

Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     4     (Compliant)
Processor Memory                :  8192 MB  (Compliant)
Processor Frequency Reservation :  1000 MHz (Compliant)
Processor Frequency Limit       :  20000 MHz (Compliant)
Average Usage (30 seconds)      :   103 MHz
```

相关命令

命令	说明
show cpu detail	显示每个 vCPU 的 vCPU 信息。

show vpn load-balancing

要显示 VPN 负载平衡虚拟集群配置的运行时统计信息，请在全局配置、特权 EXEC 或 VPN 负载平衡模式下使用 **show vpn-load-balancing** 命令。

show vpn load-balancing

语法说明

此命令没有变量或参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—
VPN 负载平衡	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	在输出示例中为负载 (%) 显示和会话显示添加了单独的 IPsec 和 SSL 列。
8.4(2)	已将新信息添加到显示的输出。

使用指南

show vpn load-balancing 命令显示虚拟 VPN 负载平衡集群的统计信息。如果本地设备未参与 VPN 负载平衡集群，此命令指示尚未为此设备配置 VPN 负载平衡。

输出中的星号 (*) 指示您连接到的 ASA 的 IP 地址。

示例

此示例显示 **show vpn load-balancing** 命令以及该命令在本地设备参与 VPN 负载平衡集群的情况下的输出：

```
ciscoasa# sh vpn load-balancing
------------------------------------------------------------------------------
    Status     Role   Failover   Encryption        Cluster IP   Peers
------------------------------------------------------------------------------
   Enabled   Master        n/a     Disabled 192.0.2.255   0

Peers:
------------------------------------------------------------------------------
       Public IP     Role  Pri             Model  Load-Balancing Version
------------------------------------------------------------------------------
        192.0.2.255    Master    5          ASA-5520            3
```

```
Total License Load:
-------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials          Other VPN
                   ------------------------------   ---------------------
                        Limit    Used   Load          Limit    Used   Load
-------------------------------------------------------------------------
     192.0.2.255       750       0     0%            750       1     0%

Licenses Used By Inactive Sessions :
-------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials     Inactive Load
-------------------------------------------------------------------------
     192.0.2.255                      0                0%
```

在主设备上，总许可证负载输出包括关于主设备和备用设备的信息；但是，备用设备仅显示关于自身的信息，而不显示主设备的信息。因此，主设备了解所有许可的成员，但是许可的成员只了解自己的许可证。

输出中还包含 “ 非活动会话使用的许可证 ” 部分。AnyConnect 会话进入非活动状态时，只要会话尚未以正常方式终止，ASA 就保留该会话。这样，AnyConnect 会话可以使用相同的 webvpn cookie 来重新连接且不必重新验证。非活动会话将保持该状态，直至 AnyConnect 客户端恢复会话或发生空闲超时为止。将维持这些非活动会话的许可证，并在此 “ 非活动会话使用的许可证 ” 部分中表示这些许可证。

如果本地设备未参与 VPN 负载平衡集群，则 **show vpn load-balancing** 命令显示不同的结果：

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

相关命令

命令	说明
clear configure vpn load-balancing	从配置中删除 **vpn load-balancing** 命令语句。
show running-config vpn load-balancing	随即会显示当前 VPN 负载均衡虚拟集群配置。
vpn load-balancing	进入 vpn 负载均衡模式。

show vpn-sessiondb

要显示有关 VPN 会话的信息，请在特权 EXEC 模式下使用 **show vpn-sessiondb** 命令。该命令包括完整或详细显示信息的选项，使您能够指定要显示的会话类型，并提供选项将信息过滤和排序。语法表和用法注释将相应地组织这些选项

show vpn-sessiondb [**detail**] [**ospfv3**] [**failover**] [**full**] [**summary**] [**ratio** {**encryption** | **protocol**}] [**license-summary**] {**anyconnect** | **email-proxy** | **index** *indexnumber* | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **vpn-lb** | **webvpn**} [**filter** {**name** username | **ipaddress** *IPaddr* | **a-ipaddress** *IPaddr* | **p-ipaddress** *IPaddr* | **tunnel-group** *groupname* | **protocol** *protocol-name* | **encryption** *encryption-algo* | **inactive**}] [**sort** {**name** | **ipaddress** | **a-ipaddress** | **p-ip address** | **tunnel-group** | **protocol** | **encryption** | **inactivity**}]

语法说明

anyconnect	显示 AnyConnect VPN 客户端会话，包括 OSPFv3 会话信息。
detail	（可选）显示会话的相关扩展详细信息。例如，**detail** 选项用于 IPsec 会话，会显示其他详细信息，例如 IKE 哈希算法、身份验证模式和再生密钥时间间隔。 如果您选择 **detail** 和 **full** 选项，则 ASA 以机器可读格式显示详细输出。
email-proxy	显示邮件代理会话。
encryption	将加密类型比率显示为会话总数比率形式。
failover	显示故障切换 IPsec 隧道的会话信息。
filter *filter_criteria*	（可选）过滤输出以仅显示您使用一个或多个过滤选项指定的信息。有关 *filter_criteria* 选项的列表，请参阅 “ 使用指南 ” 部分。
full	（可选）显示流式未截断输出。在记录之间用 | 字符和 || 字符串对输出进行分段。
index *indexnumber*	按索引编号显示单个会话。指定会话的索引编号（范围为 1 - 750）。
l2l	显示 VPN LAN-to-LAN 会话信息。
license-summary	显示 VPN 许可证摘要信息。
ospfv3	显示 OSPFv3 会话信息。
protocol	将协议类型比率显示为会话总数比率形式。
ra-ikev1-ipsec	显示 IPsec IKEv1 会话。
ra-ikev2-ipsec	显示 IKEv2 远程访问客户端连接的详细信息。
sort *sort_criteria*	（可选）根据您指定的排序选项将输出排序。有关 *sort_criteria* 选项的列表，请参阅 “ 使用指南 ” 部分。
summary	显示 VPN 会话摘要信息。
vpn-lb	显示 VPN 负载平衡管理会话。
webvpn	显示无客户端 SSL VPN 会话，包括 OSPFv3 会话信息。

默认值

没有默认行为和默认值。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	单个	多个 情景	系统
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	添加了 VLAN 字段说明。
8.0(5)	将 **inactive** 添加为 **filter** 选项，并将 **inactivity** 添加为 **sort** 选项。
8.2(1)	许可证信息已添加到输出。
8.4(1)	**svc** 关键字已更改为 **anyconnect**。**远程**关键字已更改为 **ra-ikev1-ipsec**。添加了 **ratio** 关键字。
9.0(1)	添加了 **ospfv3** 关键字，并且 OSPFv3 会话信息现在包含在 VPN 会话摘要中。 添加了 **fitler a-ipversion** 和 **filter p-ipversion** 选项，以允许对所有 AnyConnect、LAN-to-LAN 和无客户端 SSL VPN 会话分配的 IPv4 或 IPv6 地址进行过滤。
9.1(2)	我们添加了故障切换隧道类型和 **failover** 关键字以支持故障切换 IPsec 隧道。请参阅 **failover ipsec pre-shared-key** 命令。
9.1(4)	使用 **detail anyconnect** 选项时的输出已更新来反映分配的 IPv6 地址且指出执行 IKEv2 双流量时的 GRE 传输模式安全关联。
9.3(2)	我们添加 **ra-ikev2-ipsec** 关键字以显示 IKEv2 远程访问客户端连接的详细信息。更新了 VPN 会话摘要输出以包括 IKEv2 远程访问客户端连接以及 IKEv2 和 IPsec 隧道计数。更新了 VPN 许可证使用概要输出以添加 IKEv2 远程访问客户端连接。

使用指南

您可以使用以下选项对会话显示进行过滤和排序：

Filter/Sort 选项	说明
filter a-ipaddress *IPaddr*	过滤输出以仅显示指定的分配 IP 地址的信息。
sort a-ipaddress	按分配的 IP 地址排序显示。
filter a-ipversion {v4 | v6}	过滤输出以显示所有 AnyConnect 会话分配的 IPv4 或 IPv6 地址的相关信息。
filter encryption *encryption-algo*	过滤输出以仅显示使用指定加密算法的会话的信息。
sort encryption	按加密算法将显示排序。加密算法包括：aes128、aes192、aes256、des、3des、rc4

Filter/Sort 选项	说明
filter inactive	过滤空闲和可能失去连接（由于休眠、移动设备断开连接等等）的非活动会话。从 ASA 发送 TCP keepalive 而没有收到来自 AnyConnect 客户端的响应时，非活动会话数量会增长。用 SSL 隧道丢弃时间为每个会话加上时间戳。如果会话主动通过 SSL 隧道传输流量，则显示 00:00m:00s。 **注**　ASA 不会将 TCP keepalive 发送到一些设备（例如 iPhone、iPad 和 iPod）以延长电池续航时间，因此故障检测无法区分断开连接与休眠。因此，按照设计，非活动状态计数器将保持为 00:00:00。
sort inactivity	将非活动会话排序。
filter ipaddress *IPaddr*	过滤输出以仅显示指定的内部 IP 地址的信息。
sort ipaddress	按内部 IP 地址将显示排序。
filter name *username*	过滤输出以显示指定用户名的会话。
sort name	按用户名的字母顺序将显示排序。
filter p-address *IPaddr*	过滤输出以仅显示指定的外部 IP 地址的信息。
sort p-address	按指定的外部 IP 地址将显示排序。
filter p-ipversion {v4 | v6}	过滤输出以显示源自具有 IPv4 或 IPv6 地址的终端的所有 AnyConnect 会话的相关信息。
filter protocol *protocol-name*	过滤输出以仅显示使用指定协议的会话的信息。
sort protocol	按协议将显示排序。协议包括：IKE、IMAP4S、IPsec、IPsecLAN2LAN、IPsecLAN2LANOverNatT、IPsecOverNatT、IPsecoverTCP、IPsecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN
filter tunnel-group *groupname*	过滤输出以仅显示指定的隧道组的信息。
sort tunnel-group	按隧道组将显示排序。
|	使用以下参数来修改输出：{begin | include | exclude | grep | [-v]} {reg_exp}

示例

以下是 **show vpn-sessiondb** 命令的输出示例：

```
ciscoasa# show vpn-sessiondb

--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         78 :           2 :        0
  SSL/TLS/DTLS              :      1 :         72 :           2 :        0
  IKEv2 IPsec               :      0 :          6 :           1 :        0
IKEv2 Generic IPsec Client  :      0 :          0 :           0
Clientless VPN              :      0 :          8 :           2
  Browser                   :      0 :          8 :           2
--------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     86
Device Total VPN Capacity   :    750
Device Load                 :     0%
--------------------------------------------------------------------------
```

```
-----------------------------------------------------------------------------
Tunnels Summary
-----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
IKEv2                       :      0 :          6 :               1
IPsecOverNatT               :      0 :          6 :               1
Clientless                  :      0 :         17 :               2
AnyConnect-Parent           :      1 :         69 :               2
SSL-Tunnel                  :      1 :         75 :               2
DTLS-Tunnel                 :      1 :         56 :               2
-----------------------------------------------------------------------------
Totals                      :      3 :        229
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
IPv6 Usage Summary
-----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :            :
  IPv6 Peer                 :      1 :         41 :           2
  Tunneled IPv6             :      1 :         70 :           2
AnyConnect IKEv2            :        :            :
  IPv6 Peer                 :      0 :          4 :           1
Clientless                  :        :            :
  IPv6 Peer                 :      0 :          1 :           1
-----------------------------------------------------------------------------
```

以下是来自 **show vpn-sessiondb detail l2l** 命令的输出示例，显示关于 LAN-to-LAN 会话的详细信息：

```
ciscoasa# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection   : 172.16.0.0
Index        : 1
IP Addr      : 172.16.0.0
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 240                    Bytes Rx     : 160
Login Time   : 14:50:35 UTC Tue May 1 2012
Duration     : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 1.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86389 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                 Hashing      : SHA1
```

```
  Encapsulation: Tunnel                  PFS Group    : 5
  Rekey Int (T): 120 Seconds             Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes         Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes              Idle TO Left : 29 Minutes
  Bytes Tx     : 240                     Bytes Rx     : 160
  Pkts Tx      : 3                       Pkts Rx      : 2

NAC:
  Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds               EoU Age(T)   : 13 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
  Redirect URL :
```

以下是 **show vpn-sessiondb detail index 1** 命令的输出示例：

```
AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : user1
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPsec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                      Bytes Rx     : 604533
  Pkts Tx      : 0                      Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds           Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds            EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds              Posture Token: Healthy
  Redirect URL : www.cisco.com
```

以下是 **show vpn-sessiondb ospfv3** 命令的输出示例：

```
asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s
```

以下是 **show vpn-sessiondb detail ospfv3** 命令的输出示例：

```
asa# show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
  Tunnel ID    : 1.1
  Local Addr   : ::/0/89/0
  Remote Addr  : ::/0/89/0
  Encryption   : none                   Hashing      : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes              Idle TO Left : 0 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 0
  Pkts Tx      : 0                      Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 105268 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

以下是来自 **show vpn-sessiondb summary** 命令的输出示例：

```
ciscoasa# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
OSPFv3 IPsec               :      1 :          1 :           1
----------------------------------------------------------------------------
Total Active and Inactive  :      1             Total Cumulative :      1
Device Total VPN Capacity  :  10000
Device Load                :     0%
----------------------------------------------------------------------------
```

以下是常规 IKEv2 IPsec 远程访问会话的 **show vpn-sessiondb summary** 命令的输出示例：

```
ciscoasa# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
```

```
-----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concur : Inactive
                             ----------------------------------------------
Generic IKEv2 Remote Access  :      1 :          1 :           1
-----------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :      1
Device Total VPN Capacity    :    250
Device Load                  :     0%
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
Tunnels Summary
-----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
IKEv2                        :      1 :          1 :               1
IPsec                        :      1 :          1 :               1
-----------------------------------------------------------------------------
Totals                       :      2 :          2
-----------------------------------------------------------------------------
```

以下是 **show vpn-sessiondb det anyconnect** 命令的输出示例：

```
ciscoasa# show vpn-sessiondb det anyconnect

Session Type: AnyConnect Detailed

Username     : userab                 Index        : 2
Assigned IP  : 65.2.1.100             Public IP    : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)3DES  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 21248
Pkts Tx      : 0                      Pkts Rx      : 238
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : test1
Login Time   : 22:44:59 EST Tue Aug 13 2013
Duration     : 0h:02m:42s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 75.2.1.60
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 400 Minutes            Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : 3.1.05050

IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 64251                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
```

```
  Encryption   : 3DES                    Hashing      : SHA1
  Rekey Int (T): 86400 Seconds           Rekey Left(T): 86241 Seconds
  PRF          : SHA1                    D/H Group    : 2
  Filter Name  : mixed1
  Client OS    : Windows

IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 75.2.1.23/255.255.255.255/47/0
  Remote Addr  : 75.2.1.60/255.255.255.255/47/0
  Encryption   : 3DES                    Hashing      : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds           Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes             Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes             Conn TO Left : 497 Minutes
  Bytes Tx     : 0                       Bytes Rx     : 21326
  Pkts Tx      : 0                       Pkts Rx      : 239

NAC:
  Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds               EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
  Redirect URL :
```

以下示例是来自 **show vpn-sessiondb ra-ikev2-ipsec** 命令的输出示例：

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username     : IKEV2TG                 Index        : 1
Assigned IP  : 95.0.225.200            Public IP    : 85.0.224.12
Protocol     : IKEv2 IPsec
License      : AnyConnect Essentials
Encryption   : IKEv2: (1)3DES  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                       Bytes Rx     : 17844
Pkts Tx      : 0                       Pkts Rx      : 230
Pkts Tx Drop : 0                       Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG     Tunnel Group : IKEV2TG
Login Time   : 11:39:54 UTC Tue May 6 2014
Duration     : 0h:03m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

以下是来自 **show vpn-sessiondb license-summary** 命令的输出示例：

```
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                    Status : Capacity : Installed :  Limit
                                   ----------------------------------------
AnyConnect Premium                : DISABLED :      250 :        10 :   NONE
AnyConnect Essentials             :  ENABLED :      250 :       250 :   NONE
Other VPN (Available by Default)  :  ENABLED :      250 :       250 :   NONE
Shared License Server             : DISABLED
Shared License Participant        : DISABLED
AnyConnect for Mobile             : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment      : DISABLED(Requires Premium)
```

```
AnyConnect for Cisco VPN Phone   : DISABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
VPN Licenses Usage Summary
-----------------------------------------------------------------------------
                         Local : Shared :   All   :    Peak :  Eff.:
                        In Use : In Use : In Use : In Use :  Limit : Usage
                       ---------------------------------------------------
AnyConnect Essentials  :      1 :      0 :      1 :      1 :    250 :    0%
  AnyConnect Client    :                :      0 :      0           :    0%
    AnyConnect Mobile  :                :      0 :      0           :    0%
  Generic IKEv2 Client :                :      1 :      1           :    0%
Other VPN              :                :      0 :      0 :    250 :    0%
  Cisco VPN Client     :                :      0 :      0           :    0%

-----------------------------------------------------------------------------
Shared License Network Summary
-----------------------------------------------------------------------------
AnyConnect Premium
  Total shared licenses in network                                  : 500
  Shared licenses held by this participant                          :  0
  Shared licenses held by all participants in the network           :  0
-----------------------------------------------------------------------------
```

如示例中所示，为响应 **show vpn-sessiondb** 命令而显示的字段因您输入的关键字而异。表 14-2 描述这些字段。

表 14-2　show vpn-sessiondb 命令字段

字段	说明
Auth Mode	用于验证该会话的协议或模式。
Bytes Rx	ASA 从远程对等设备或客户端接收的字节总数。
Bytes Tx	ASA 传输到远程对等设备或客户端的字节数。
Client Type	在远程对等设备上运行的客户端软件（如果可用）。
Client Ver	在远程对等设备上运行的客户端软件的版本。
Connection	连接或专用 IP 地址的名称。
D/H Group	Diffie-Hellman 组。用于生成 IPsec SA 加密密钥的算法和密钥大小。
Duration	会话登录时间与上次屏幕刷新之间经过的时间 (HH:MM:SS)。
EAPoUDP Session Age	上次成功的状态验证以来的秒数。
Encapsulation	用于应用 IPsec ESP（封装安全负载协议）加密和验证的模式（即，应用了 ESP 的原始 IP 包的一部分）。
Encryption	此会话使用的数据加密算法（如果有）。
EoU Age (T)	EAPoUDP 会话寿命。上次成功的状态验证以来的秒数。
Filter Name	指定的用来限制会话信息显示的用户名。
Hashing	用于创建数据包的哈希的算法，该算法用于 IPsec 数据身份验证。
Hold Left (T)	剩余的延缓时间。如果上一状态验证成功，则为 0 秒。否则，为下一状态验证尝试之前剩余的秒数。

表 14-2　show vpn-sessiondb 命令字段（续）

字段	说明
Hold-Off Time Remaining	如果上一状态验证成功，则为 0 秒。否则，为下一状态验证尝试之前剩余的秒数。
IKE Neg Mode	用于交换密钥信息和设施 SA 的 IKE（IPsec 阶段 1）模式：积极或主要。
IKE Sessions	IKE（IPsec 阶段 1）会话数；通常为 1。这些会话为 IPsec 流量建立隧道。
Index	此记录的唯一标识符。
IP Addr	为此会话分配给远程客户端的专用 IP 地址。这也称为“内部”或“虚拟”IP 地址。它允许客户端在专用网络中显示为主机。
IPsec Sessions	IPsec（阶段 2）会话数，即通过隧道的数据流量会话。每个 IPsec 远程访问会话可以有两个 IPsec 会话：一个包含隧道终端，而另一个包含可通过隧道访问的专用网络。
License Information	显示关于共享 SSL VPN 许可证的信息。
Local IP Addr	分配给隧道本地终端（这是 ASA 上的接口）的 IP 地址。
Login Time	会话登录的日期和时间 (MMM DD HH:MM:SS)。以 24 小时计时法显示时间。
NAC Result	网络准入控制状态验证的状态。它可以是下列类型之一： • Accepted（已接受）- ACS 成功验证远程主机的状态。 • Rejected（已拒绝）- ACS 无法成功验证远程主机的状态。 • Exempted（豁免）- 根据在 ASA 上配置的状态验证例外列表，该远程主机免于进行状态验证。 • Non-Responsive（无响应）- 远程主机未响应 EAPoUDP Hello 消息。 • Hold-off（隔断）- ASA 在成功进行状态验证之后，与远程主机失去 EAPoUDP 通信。 • N/A（不适用）- 根据 VPN NAC 组策略，为远程主机禁用了 NAC。 • Unknown（未知）- 正在进行状态验证。
NAC Sessions	网络准入控制（EAPoUDP）会话数。
Packets Rx	ASA 从远程对等设备接收的数据包的数量。
Packets Tx	ASA 传输到远程对等设备的数据包的数量。
PFS Group	完全转发保密组编号。
Posture Token	访问控制服务器上可配置的信息文本字符串。ACS 为了参考信息将状态令牌下载到 ASA 以协助进行系统监控、报告、调试和记录。典型的状态令牌为正常、检查、隔离、感染或未知。
Protocol	会话使用的协议。
Public IP	分配给客户端的公共可路由 IP 地址。
Redirect URL	在状态验证或无客户端身份验证后，ACS 将会话的访问策略下载到 ASA。重新定向 URL 是访问策略负载的可选部分。ASA 将所有 HTTP（端口 80）和 HTTPS（端口 443）请求从远程主机重新定向到重新定向 URL（如果存在）。如果访问策略没有包含重新定向 URL，ASA 不会重新定向来自远程主机的 HTTP 和 HTTPS 请求。 重新定向 URL 保持有效，直到 IPsec 会话结束或直到状态重新验证为止，对此，ACS 下载新的访问策略，其中可以包含其他重新定向 URL 或不包含重新定向 URL。

表 14-2　show vpn-sessiondb 命令字段（续）

字段	说明
Rekey Int (T)	IPsec（IKE）SA 加密密钥的生命期。
Rekey Left (T)	IPsec（IKE）SA 加密密钥的剩余生命期。
Rekey Time Interval	IPsec（IKE）SA 加密密钥的生命期。
Remote IP Addr	分配给隧道的远程终端（即远程对等设备上的接口）的 IP 地址。
Reval Int (T)	重新验证时间间隔。每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Reval Left (T)	到下次重新验证的时间。如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功状态验证以来的秒数之间的差值。
Revalidation Time Interval	每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Session ID	会话组件（子会话）的标识符。每个 SA 都有自己的标识符。
Session Type	会话的类型：LAN-to-LAN 或 Remote
SQ Int (T)	Status Query Time Interval. 每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是 ASA 向远程主机提出的请求，用于指出自上次状态验证以来主机是否经历任何状态变化。
Status Query Time Interval	每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是 ASA 向远程主机提出的请求，用于指出自上次状态验证以来主机是否经历任何状态变化。
Time Until Next Revalidation	如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功状态验证以来的秒数之间的差值。
Tunnel Group	此隧道针对属性值引用的隧道组的名称。
UDP Dst Port 或 UDP Destination Port	远程对等设备用于 UDP 的端口号。
UDP Src Port 或 UDP Source Port	ASA 用于 UDP 的端口号。
Username	建立会话所使用的用户登录名称。
VLAN	分配给此会话的出口 VLAN 接口。ASA 将所有流量转发到此 VLAN。以下要素之一指定值： • 组策略 • 继承的组策略

相关命令

命令	说明
show running-configuration vpn-sessiondb	显示 VPN 会话数据库运行配置（max-other-vpn-limit、max-anyconnect-premium-or-essentials-limit）。
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。

show vpn-sessiondb ratio

要按协议或加密算法以百分比形式显示当前会话比率，请在特权 EXEC 模式下使用 **show vpn-sessiondb ratio** 命令。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

语法说明

encryption	确定要显示的加密协议。指阶段 2 加密。加密算法包括：	
	aes128	des
	aes192	3des
	aes256	rc4
filter *groupname*	过滤输出以仅包含所指定的隧道组的会话比率。	
protocol	确定要显示的协议。协议包括：	
	IKEv1	L2TPOverIPsecOverNatT
	IKEv2	Clientless
	IPsec	Port-Forwarding
	IPsecLAN2LAN	IMAP4S
	IPsecLAN2LANOverNatT	POP3S
	IPsecOverNatT	SMTPS
	IPsecOverTCP	AnyConnect-Parent
	IPsecOverUDP	SSL-Tunnel
	L2TPOverIPsec	DTLS-Tunnel

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	输出增强以包含 IKEv2。
9.0(1)	增加了多情景模式支持。

示例

以下是 **show vpn-sessiondb ratio** 命令的输出示例（以 **encryption** 作为参数）：

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

以下是 **show vpn-sessiondb ratio** 命令的输出示例（以 **protocol** 作为参数）：

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPsec                    1              20%
IPsecLAN2LAN             0               0%
IPsecLAN2LANOverNatT     0               0%
IPsecOverNatT            0               0%
IPsecOverTCP             1 20%
IPsecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPsec            0               0%
L2TPOverIPsecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

相关命令

命令	说明
show vpn-sessiondb	显示按您指定的标准过滤和排序（可选）的会话（具有或没有扩展的详细信息）。
show vpn-sessiondb summary	显示会话摘要，包括当前会话总数、每种类型的当前会话、峰值和累积总值、最大并发会话数

show vpn-sessiondb summary

要显示 IPsec、Cisco AnyConnect 和 NAC 会话数，请在特权 EXEC 模式下使用 **show vpn-sessiondb summary** 命令。

show vpn-sessiondb summary

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	—	• 是	• 是

命令历史

版本	修改
7.0(7)	引入了此命令。
8.0(2)	添加 VLAN 映射会话表。
8.0(5)	为活动、累计、峰值并发和非活动添加新输出。
9.0(1)	增加了多情景模式支持。

示例

以下是具有一个 IPsec IKEv1 和一个无客户端会话的 **show vpn-sessiondb summary** 命令的输出示例：

注　待机状态的设备不区分活动与非活动会话。

```
ciscoasa# show vpn-sessiondb summary

VPN Session Summary
Sessions:
                        Active :Cumulative :Peak Concurrent :Inactive :
    Clientless VPN            :       1:         2:             1
    Browser                   :       1:         2:             1
    IKEv1 IPsec/L2TP IPsec0   :       1:         1:             1

Total Active and Inactive: 2      Total Cumulative: 3
Device Total VPN Capacity: 10000
Device Load            : 0%

License Information:
    Shared VPN License Information:
        SSL VPN                      : 12000
            Allocated to this device :    0
            Allocated to network     :    0
            Device limit             : 750
```

```
IPsec   :   750     Configured :750    Active : 0     Load : 0%
SSL VPN :   750     Configured :750    Active : 0     Load : 0%
                        Active : Cumulative : Peak Concurrent
SSL VPN         :           0 :         1 :            1
Totals          :           0 :         1 :

Active NAC Sessions:
  Accepted               : 0
  Rejected               : 0
  Exempted               : 0
  Non-responsive         : 0
Hold-off               : 0
  N/A                    : 0

Active VLAN Mapping Sessions:
  Static                 : 0
  Auth                   : 0
  Access                 : 0
  Guest                  : 0
  Quarantine             : 0
  N/A                    : 0

ciscoasa#
```

您可以使用 SSL 输出在许可证数量方面确定物理设备资源。单用户会话可能占用一个许可证，但可能使用多个隧道。例如，具有 DTLS 的 AnyConnect 用户通常具有关联的父会话、SSL 隧道和 DTLS 隧道。

注　父会话表示客户端何时未主动连接。它不表示加密隧道。如果客户端关闭或休眠，则 IPsec、IKE、TLS 和 DLTLS 隧道关闭，但是，父会话保留到空闲时间或达到最大连接时间限制为止。这让用户重新连接而无需重新进行验证。

本示例中，即使只有一位用户登录，您也会看到设备上分配了三个隧道。IPsec LAN-to-LAN 隧道算作一个会话，它允许通过隧道建立主机之间的多个连接。IPsec 远程访问会话是支持一个用户连接的一个远程访问隧道。

从输出中，可以看到哪些会话处于活动状态。如果会话没有关联的基础隧道，则状态为 *waiting to resume* 模式（在会话输出中显示为无客户端）。此模式意味着开始从头端设备进行失效对等设备检测，而头端设备不再可以与客户端通信。遇到此情况时，您可以保留会话从而让用户漫游网络、进入休眠状态、恢复会话等。这些会话计入主动连接的会话（从许可证角度）并在用户空闲超时、用户注销或原始会话恢复时被清除。

“Active SSL VPN With Client” 列显示传递数据的活动连接数。“Cumulative SSL VPN With Client” 列显示已建立的活动会话数。它包括非活动的会话且仅在添加新会话时递增。“Peak Concurrent SSL VPN With Client” 列显示传递数据的并发活动会话的最大数量。“Inactive SSL VPN With Client” 列显示 AnyConnect 客户端断开连接的时间长度。您可以使用此非活动超时值来确定许可证何时到期。这样 ASA 可以确定是否可以重新连接。没有与之关联的活动 SSL 隧道的 AnyConnect 会话。

表 14-3 说明活动会话表和会话信息表中的字段。

表 14-3　show vpn-sessiondb summary 命令：活动会话和会话信息字段

字段	说明
Concurrent Limit	此 ASA 上允许的并发活动会话的最大数量。
Cumulative Sessions	自上次启动或重置 ASA 以来所有类型的会话数。
LAN-to-LAN	当前处于活动状态的 IPsec LAN-to-LAN 会话数。
Peak Concurrent	自上次启动或重置 ASA 以来并发活动的所有类型会话的最大数量。
Percent Session Load	使用中的 VPN 会话分配的百分比。此值等于活动会话总数除以可用会话的最大数量（以百分比形式显示）。可用会话的最大数量可以是以下项之一： • 许可的 IPsec 和 SSL VPN 会话的最大数量 • **vpn-sessiondb ?**（已配置会话的最大数量） • **max-anyconnect-premium-or-essentials-limit** （AnyConnect Premium 或 Essentials 会话上限） • **max-other-vpn-limit**（其他 VPN 会话上限）
Remote Access	ra-ikev1-ipsec - IKEv1 IPsec 远程访问用户数、L2TP over IPsec 以及通过当前活动的 NAT 会话的 IPsec。
Total Active Sessions	当前处于活动状态的所有类型会话的数量。

活动 NAC 会话表显示有关接受状态验证的远程对等设备的一般统计信息。

累计 NAC 会话表显示有关将要或已接受状态验证的远程对等设备的一般统计信息。

表 14-4 说明活动 NAC 会话表和总累计 NAC 会话表中的字段。

表 14-4　show vpn-sessiondb summary 命令：活动 NAC 会话和总累计 NAC 会话的字段

字段	说明
Accepted	通过状态验证以及由访问控制服务器授予访问策略的对等设备数量。
Exempted	由于匹配 ASA 上配置的状态验证例外列表中的某个条目而未接受状态验证的对等设备数量。
Hold-off	在状态验证成功后 ASA 失去其 EAPoUDP 通信的对等设备数量。NAC 保留计时器属性（Configuration（配置）> VPN > NAC）确定每个对等设备的此类型事件与下一次状态验证尝试之间的延迟。
N/A	根据 VPN NAC 组策略为其禁用 NAC 的对等设备数量。
Non-responsive	未响应基于 UDP 的可扩展身份验证协议 (EAP) 状态验证请求的对等设备数量。没有 CTA 在其中运行的对等设备不响应这些请求。如果 ASA 配置支持无客户端主机，则访问控制服务器将与无客户端主机关联的访问策略下载到这些对等设备的 ASA。否则，ASA 将分配 NAC 默认策略。
Rejected	未能通过状态验证以及未被访问控制服务器授予访问策略的对等设备数量。

活动 VLAN 映射会话表显示有关接受状态验证的远程对等设备的一般统计信息。

累计 VLAN 映射会话表显示有关将要或已接受状态验证的远程对等设备的一般统计信息。

表 14-5 说明活动 VLAN 映射会话表和累计 VLAN 映射会话表中的字段。

表 14-5　show vpn-sessiondb summary 命令：活动 VLAN 映射会话和累计活动 VLAN 映射会话的字段

字段	说明
Access	已保留供将来使用。
Auth	已保留供将来使用。
Guest	已保留供将来使用。
N/A	已保留供将来使用。
Quarantine	已保留供将来使用。
Static	此字段显示分配给预配置的 VLAN 的 VPN 会话数量。

相关命令

命令	说明
show vpn-sessiondb	显示按您指定的标准过滤和排序（可选）的会话（具有或没有扩展的详细信息）。
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。

show wccp

要显示关于 Web 缓存通信协议 (WCCP) 的全局统计信息，请在特权 EXEC 模式下使用 **show wccp** 命令。

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

语法说明

detail	（可选）显示关于路由器和所有 Web 缓存的信息。
service-number	（可选）缓存所控制的 Web 缓存服务组的标识号。号码可在 0 到 256 之间。对于使用 Cisco Cache Engine 的 Web 缓存，以值 99 指示反向代理服务。
view	（可选）显示已检测或尚未检测特定服务组的其他成员。
web-cache	指定 Web 缓存服务的统计信息。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何显示 WCCP 信息：

```
ciscoasa(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
ciscoasa(config)#
```

相关命令

命令	说明
wccp	对服务组启用 WCCP 支持。
wccp redirect	启用 WCCP 重定向支持。

show webvpn csd

要确定 CSD 是否已启用、显示运行的配置中的 CSD 版本、确定哪个映像在提供 Host Scan 软件包以及测试一个文件以查看该文件是不是有效的 CSD 分发软件包，请在特权 EXEC 模式下使用 **show webvpn csd** 命令。

show webvpn csd [**image** *filename*]

语法说明

filename	指定一个文件的名称以测试该文件是否为有效的 CSD 分发软件包。它必须采用 **csd_n.n.n-k9.pkg** 形式。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC 模式	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

示例

使用 **show webvpn csd** 命令检查 CSD 的运行状态。CLI 做出响应而显示一条消息，指出 CSD 是否已安装以及是否已启用，Host Scan 是否已安装以及是否已启用，以及哪个映像在提供 Host Scan 软件包（如果安装了 CSD 软件包和 Host Scan 软件包）。

```
ciscoasa# show webvpn csd
```

以下是您可能收到的消息：

- `Secure Desktop is not installed`

  `Hostscan is not installed`

- `Secure Desktop version n.n.n.n is currently installed but not enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)`

- `Secure Desktop version n.n.n.n is currently installed and enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed and enabled via the CSD package)`

  消息“`Secure Desktop version n.n.n.n is currently installed...`”意味着在 ASA 和运行的配置中加载了此映像。镜像可能**已启用**或**未启用**。 您可以转到 WebVPN 配置模式并输入 **csd enable** 命令以启用 CSD。

消息 “(Hostscan is currently installed and enabled via the CSD package)” 意味着 CSD 软件包随附的 Host Scan 软件包是使用的 Host Scan 软件包。

- `Secure Desktop version n.n.n.n is currently installed and enabled`
  `Hostscan version n.n.n.n is currently installed and enabled`

  消息 “Secure Desktop version *n.n.n.n* is currently installed and enabled Hostscan version *n.n.n.n* is currently installed and enabled” 意味着已安装作为单独软件包或者作为 AnyConnect 映像的一部分而提供的 CSD 和 Host Scan 软件包。如果 Host Scan 已启用且安装并启用了 CSD 和具有 Host Scan 的 AnyConnect 映像或者独立 Host Scan 软件包，则作为单独软件包或者作为 AnyConnect 映像的一部分而提供的 Host Scan 软件包优先于 CSD 软件包随附的软件包。

- `Secure Desktop version n.n.n.n is currently installed but not enabled`
  `Hostscan version n.n.n.n is currently installed but not enabled`

使用 **show webvpn csd image** *filename* 命令测试文件以确定 CSD 分发软件包是否有效。

ciscoasa# **show webvpn csd image csd_n.n.n-k9.pkg**

输入以下命令时，CLI 以如下某个消息做出响应：

- `ERROR: This is not a valid Secure Desktop image file.`

  确保文件名格式为 **csd_n.n.n_k9.pkg**。如果 CSD 软件包没有此命名约定，请用从以下网站获得的文件替换该文件：

  http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

  然后，重新输入 **show webvpn csd image** 命令。如果镜像有效，请在 webvpn 配置模式下使用 **csd image** 和 **csd enable** 命令安装和启用 CSD。

- `This is a valid Cisco Secure Desktop image:`
  `Version  : 3.6.172.0`
  `Hostscan Version  : 3.6.172.0`
  `Built on : Wed Feb 23 15:46:44 MST 2011`

  注意，如果文件有效，CLI 提供版本和日期戳。

相关命令

命令	说明
csd enable	为管理和远程用户访问启用 CSD。
csd image	从运行配置路径中的指定的闪存驱动器中复制命令中指定的 CSD 映像。

show webvpn group-alias

要显示特定隧道组或所有隧道组的别名，请在特权 EXEC 模式下使用 **group-alias** 命令。

show webvpn group-alias [*tunnel-group*]

语法说明

tunnel-group	（可选）指定显示其组别名的特定隧道组。

默认值

如果没有输入隧道组名称，此命令显示所有隧道组的所有别名。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.1	引入了此命令。

使用指南

输入 **show webvpn group-alias** 命令时，WebVPN 必须处于运行状态。

每个隧道组不能有多个别名，也不能没有别名。

示例

以下示例展示 **show webvpn group-alias** 命令，该命令显示隧道组 “devtest” 的别名以及该命令的输出：

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

相关命令

命令	说明
group-alias	为该组指定一个或多个 URL。
tunnel-group webvpn-attributes	进入用于配置 WebVPN 隧道组属性的 config-webvpn 模式。

show webvpn group-url

要显示特定隧道组或所有隧道组的 URL，请在特权 EXEC 模式下使用 **group-url** 命令。

show webvpn group-url [*tunnel-group*]

语法说明

tunnel-group	（可选）指定要显示其 URL 的特定隧道组。

默认值

如果没有输入隧道组名称，此命令显示所有隧道组的所有 URL。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

输入 **show webvpn group-url** 命令时，WebVPN 必须处于运行状态。每个组可以有多个 URL 或没有 URL。

示例

以下示例展示 **show webvpn group-url** 命令，该命令显示隧道组 “frn-eng1” 的 URL 以及该命令的输出：

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

相关命令

命令	说明
group-url	为该组指定一个或多个 URL。
tunnel-group webvpn-attributes	进入用于配置 WebVPN 隧道组属性的 config-webvpn 模式。

show webvpn kcd

在 webvpn 配置模式下使用 **show webvpn kcd** 命令在 ASA 上显示域控制器信息和域加入状态。

show webvpn kcd

语法说明

无。

默认值

没有此命令的默认值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

webvpn 配置模式中的 **show webvpn kcd** 命令在 ASA 上显示域控制器信息和域加入状态。

示例

以下示例展示来自 **show webvpn kcd** 命令的要注意的重要详细信息以及对状态消息的解释。

此示例显示注册正在进行尚未完成：

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: In-Progress
```

此示例显示注册已成功并且 ASA 已加入域：

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: Complete
```

相关命令

命令	说明
clear aaa kerberos	清除 ASA 上缓存的所有 Kerberos 票证。
kcd-server	允许 ASA 加入 Active Directory 域。
show aaa kerberos	显示 ASA 上缓存的所有 Kerberos 票证。

show webvpn sso-server

要显示 WebVPN 单点登录服务器的运行统计信息，请在特权 EXEC 模式下使用 **show webvpn sso-server** 命令。

show webvpn sso-server [*name***]**

语法说明

name	（可选）指定 SSO 服务器的名称。服务器名称长度必须在 4 到 31 个字符之间。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Config-webvpn-sso-saml	• 是	—	• 是	—	—
Config-webvpn-sso-siteminder	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。**show webvpn sso-server** 命令显示在安全设备上配置的所有 SSO 服务器的运行统计信息。

如果没有输入 SSO 服务器名称参数，将显示所有 SSO 服务器的统计信息。

示例

以下示例（在特权 EXEC 模式中输入）显示 SiteMinder 类型 SSO 服务器指定示例的统计信息：

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa#
```

以下示例是在没有特定 SSO 服务器名称的情况下发出的命令，它显示 ASA 上所有配置的 SSO 服务器的统计信息：

```
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
max-retry-attempts	配置 ASA SSO 身份验证尝试失败后的重试次数。
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder-type SSO 服务器。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
sso-server	创建单点登录服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

show webvpn anyconnect

要查看安装在 ASA 上且加载到缓存内存中的 SSL VPN 客户端映像的相关信息，或者测试某个文件以查看其是否为有效的客户端映像，请在特权 EXEC 模式下使用 **show webvpn anyconnect** 命令。

show webvpn anyconnect [**image** *filename*]

语法说明

image *filename*	指定要作为 SSL VPN 客户端映像文件测试的文件的名称。

默认值

此命令没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。
8.4(1)	此命令的 **show webvpn anyconnect** 形式取代了 **show webvpn svc**。

使用指南

使用 **show webvpn anyconnect** 命令来查看在缓存内存中加载且可供下载到远程 PC 的 SSL VPN 客户端映像的相关信息。使用 **image** *filename* 关键字和参数测试某个文件以查看其是否为有效映像。如果该文件不是有效映像，则会显示如下消息：

```
ERROR: This is not a valid SSL VPN Client image file.
```

示例

以下示例展示当前安装的映像的 **show webvpn anyconnect** 命令的输出：

```
ciscoasa# show webvpn anyconnect
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

以下示例展示针对某个有效映像的 **show webvpn anyconnect image** *filename* 命令的输出：

```
ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg
```

```
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

相关命令

命令	说明
anyconnect enable	使 ASA 可以将 SSL VPN 客户端下载到远程 PC。
anyconnect image	使安全设备将 SSL VPN 客户端文件从闪存内存加载到缓存内存，并指定安全设备尝试将客户端映像与操作系统相匹配时将客户端映像的各个部分下载到远程 PC 的顺序。
vpn-tunnel-protocol	为远程 VPN 用户启用特定的 VPN 隧道协议（包括 SSL VPN 客户端使用的 SSL）。

show xlate

要显示有关 NAT 会话 (xlates) 的信息，请在特权 EXEC 模式下使用 **show xlate** 命令。

show xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]] [**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**type** *type*]

show xlate count

语法说明

count	显示转换计数。
global *ip1*[**-***ip2*]	（可选）按映射 IP 地址或地址范围显示活动的转换。
gport *port1*[**-***port2*]	按映射端口或端口范围显示活动的转换。
interface *if_name*	（可选）按接口显示活动转换。
local *ip1*[**-***ip2*]	（可选）按实际 IP 地址或地址范围显示活动的转换。
lport *port1*[**-***port2*]	按实际端口或端口范围显示活动的转换。
netmask *mask*	（可选）指定用于限定映射的或实际 IP 地址的网络掩码。
type *type*	（可选）按类型显示活动的转换。您可以输入以下一个或多个类型： • **static** • **portmap** • **dynamic** • **twice-nat** 指定多个类型时，请用空格来分隔类型。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	此命令已修改以支持新的 NAT 实施。
8.4(3)	添加了 **e** 标志以显示扩展 PAT 的使用。此外，将显示 xlate 扩展到的目标地址。
9.0(1)	此命令已修改以支持 IPv6。

使用指南

show xlate 命令显示转换槽的内容。

当 **vpnclient** 配置已启用且内部主机发出 DNS 请求时，**show xlate** 命令可以为静态转换列出多个 xlate。

在 ASA 集群环境中，可将最多三个 xlate 复制到集群中的不同节点以处理 PAT 会话。在拥有该连接的设备上创建了一个 xlate。在其他设备上创建一个 xlate 以备份 PAT 地址。最后，导向器上存在一个可复制该流的 xlate。在备用和导向器是同一设备的情况下，可能创建两个（而不是三个）xlate。

示例

以下是 **show xlate** 命令的输出示例。

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
    10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
    10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:5:14 timeout 0:00:00
```

以下是来自 **show xlate** 命令的输出示例，显示 **e - extended** 标记以及 xlate 扩展到的目标地址的用法。

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
    flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
    flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
    flags idle 0:00:10 timeout 0:00:30
```

以下是来自 **show xlate** 命令的输出示例，其中显示从 IPv4 到 IPv6 的转换。

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
flags sT idle 0:16:16 timeout 0:00:00
```

相关命令

命令	说明
clear xlate	清除当前转换和连接信息。
show conn	显示所有活动连接。
show local-host	显示本地主机网络信息。
show uauth	显示当前已验证的用户。

show zone

要显示分区 ID、情景、安全级别和成员，请在特权 EXEC 模式下使用 **show zone** 命令。

show zone [*name*]

语法说明

name	（可选）通过 **zone** 命令标识分区名称集。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.3(2)	我们引入了此命令。

使用指南

要查看分区配置，请使用 **show running-config zone** 命令。

示例

请参阅 **show zone** 命令的以下输出：

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

相关命令

命令	说明
clear configure zone	清除区域配置。
clear conn zone	清除区域连接。
clear local-host zone	清除区域主机。
show asp table routing	显示用于调试的加速安全路径表，并显示与每个路由关联的区域。
show asp table zone	显示用于调试的加速安全路径表。

命令	说明
show conn long	显示区域的连接信息。
show local-host zone	显示区域内本地主机的网络状态。
show nameif zone	显示接口名称和区域名称。
show route zone	显示区域接口的路由。
show running-config zone	显示区域配置。
zone	配置流量区域。
zone-member	将接口分配给流量区域。

第 15 章

shun 至 snmp-server user-list 命令

shun

要阻止来自攻击主机的连接，请在特权 EXEC 模式下使用 **shun** 命令。要禁用回避，请使用此命令的 **no** 形式。

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

语法说明

dest_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标端口。
dest_ip	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标地址。
protocol	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的 IP 协议，例如 UDP 或 TCP。默认情况下，protocol 为 0（任何协议）。
source_ip	指定攻击主机的地址。如果仅指定源 IP 地址，则以后来自此地址的所有连接都将被丢弃；当前连接保持不变。要丢弃当前连接并同时放置 shun，请指定连接的其他参数。请注意，shun 适用于后面所有来自源 IP 地址的连接，无论目标参数为何。
source_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的源端口。
vlan_id	（可选）指定源主机所在的 VLAN ID。

默认值

默认 protocol 是 0（任何协议）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

shun 命令可以阻止来自攻击主机的连接。后面来自源 IP 地址的所有连接都将被丢弃并记录，直到手动或被思科 IPS 传感器取消阻止功能。无论使用指定主机地址的连接当前是否为活动状态，**shun** 命令的阻止功能都适用。

如果您指定目标地址、来源和目标端口以及协议，则会丢弃匹配的连接以及在后面所有来自源 IP 地址的连接上放置 shun；将会避开后面所有的连接，而不只是与这些特定连接参数匹配的连接。

对每个源 IP 地址只能使用一个 **shun** 命令。

由于 **shun** 命令用于动态阻止攻击，因此不会显示在 ASA 配置中。

只要删除接口配置，所有附加到该接口的 shun 也会一同删除。如果新增接口或更换同一接口（使用同一名称），要想 IPS 传感器监控该接口，必须将该接口到 IPS 传感器。

示例

以下示例展示攻击主机 (10.1.1.27) 使用 TCP 与受攻击主机 (10.2.2.89) 建立连接。ASA 连接表中的连接如下所示：

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

使用以下选项应用 **shun** 命令：

```
ciscoasa# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

此命令将从 ASA 连接表删除特定的当前接通，同时禁止来自 10.1.1.27 的所有后续数据包通过 ASA。

相关命令

命令	说明
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
show conn	显示所有活动的连接。
show shun	显示规避信息。

shutdown

要禁用某个接口，在接口配置模式下使用 **shutdown** 命令。要启用接口，请使用此命令的 **no** 形式。

shutdown

no shutdown

语法说明

此命令没有任何参数或关键字。

默认值

所有物理接口默认关闭。在安全情景下分配的接口在配置中未关闭。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	此命令已从 **interface** 命令的关键字转变为接口配置模式命令。

使用指南

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不管接口在系统执行空间中的状态为何。但是，要通过该接口传递流量，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- 冗余接口 - 已启用。但是，要通过该冗余接口传递流量，还必须启用该成员物理接口。
- 子接口 - 已启用。但是，要通过该子接口传递流量，还必须启用该物理接口。

注　此命令只禁用软件接口。物理链路保持运行，直接连接的设备即使其相应接口已使用 **shutdown** 命令配置，也会被标识为运行。

示例

以下示例启用主接口：

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

以下示例启用子接口：

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

以下示例关闭子接口：

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# shutdown
```

相关命令

命令	说明
clear xlate	重置现有连接的所有转换，从而导致重置这些连接。
interface	配置接口并进入接口配置模式。

shutdown (ca-server mode)

要禁用本地证书颁发机构 (CA) 服务器并让用户不可访问注册接口，请在 CA 服务器配置模式下使用 **shutdown** 命令。要启用 CA 服务器，锁定配置使其无法被更改，并且使注册接口可供访问，请使用此命令的 **no** 形式。

[no] shutdown

语法说明

此命令没有任何参数或关键字。

默认值

最初，CA 服务器默认关闭。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

CA 服务器模式下的此命令类似于接口模式下的 **shutdown** 命令。在设置时，本地 CA 服务器默认关闭，必须使用 **no shutdown** 命令启用。第一次使用 **no shutdown** 命令时，启用 CA 服务器并生成 CA 服务器证书和密钥对。

注　CA 配置在锁定后无法更改，通过发出 **no shutdown** 命令可生成 CA 证书。

要使用 **no shutdown** 命令启用 CA 服务器并锁定当前配置，需要使用一个 7 字符的密码来编码和存档包含要生成的 CA 证书和密钥对的 PKCS12 文件。该文件存储到之前指定的 **database path** 命令所标识的存储位置。

示例

以下示例禁用本地 CA 服务器并使注册接口无法被访问：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# shutdown
ciscoasa(config-ca-server)#
```

以下示例启用本地 CA 服务器并使注册接口可供访问：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown
ciscoasa(config-ca-server)#
```

```
ciscoasa(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin.Please wait...

ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问，可让您配置和管理本地 CA。
show crypto ca server	显示 CA 配置的状态。

sla monitor

要创建 SLA 操作，请在全局配置模式下使用 **sla monitor** 命令。要删除 SLA 操作，则使用此命令的 **no** 形式。

sla monitor *sla_id*

no sla monitor *sla_id*

语法说明

sla_id	指定所配置的 SLA 的 ID。如果 SLA 不存在，则会创建。有效值为从 1 到 2147483647。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

sla monitor 命令用于创建 SLA 操作并进入 SLA Monitor 配置模式。输入此命令后，命令提示将变为 `ciscoasa(config-sla-monitor)#`，以表示您在 SLA Monitor 配置模式下。如果 SLA 操作已存在，并且已为其定义类型，则提示显示为 `ciscoasa(config-sla-monitor-echo)#`。最多可以创建于 2000 个 SLA 操作。在任何时间只能调试 32 个 SLA 操作。

no sla monitor 命令用于删除指定的 SLA 操作，这些命令用于配置该操作。

在配置 SLA 操作后，必须使用 **sla monitor schedule** 命令计划操作。SLA 操作在计划后，无法修改其配置。要修改已计划 SLA 操作的配置，必须使用 **sla monitor** 命令完全删除所选的 SLA 操作。删除 SLA 操作也会删除关联的 **sla monitor schedule** 命令。然后可以重新输入 SLA 操作配置。

要显示操作的当前配置设置，请使用 **show sla monitor configuration** 命令。要显示 SLA 操作的运行统计信息，请使用 **show sla monitor operation-state** 命令。要查看配置中的 SLA 命令，请使用 **show running-config sla monitor** 命令。

示例

以下示例配置 ID 为 123 的 SLA 操作，并且创建 ID 为 1 的跟踪条目来跟踪 SLA 的可访问性：

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
```

```
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

相关命令

命令	说明
frequency	指定 SLA 操作重复的速率。
show sla monitor configuration	显示 SLA 配置设置。
sla monitor schedule	计划 SLA 操作。
timeout	设置 SLA 操作等待响应的时间。
track rtr	创建用于轮询 SLA 的跟踪条目。

sla monitor schedule

要计划 SLA 操作，请在全局配置模式下使用 **sla monitor schedule** 命令。要删除 SLA 操作计划并将操作置于挂起状态，请使用此命令的 **no** 形式。

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

语法说明

after *hh*:*mm*:*ss*	表示操作应在命令输入后指定的时、分、秒开始。
ageout *seconds*	（可选）指定当操作未主动收集信息时在内存中保持的秒数。在 SLA 操作过时后，它将从运行配置中删除。
day	操作开始的日期。有效值为从 1 到 31。如果未指定日期，则使用当天。如果指定了日期，还必须指定月份。
hh:*mm*[:*ss*]	指定 24 小时制的绝对开始时间。秒可选。除非指定 *month* 和 *day*，否则下次默认使用指定的时间。
life forever	（可选）计划操作无限期运行。
life *seconds*	（可选）设置操作主动收集信息的秒数。
month	（可选）操作开始的月份。如果未指定月份，则会使用当前月份。如果指定了月份，还必须指定日期。 可以输入月份的完整英文名或只输入前三个字母。
now	表示操作应在命令输入后立即开始。
pending	表示不收集信息。这是默认状态。
recurring	（可选）表示操作将在指定的时间自动开始，并且每天运行指定的时长。
sla-id	计划的 SLA 操作的 ID。
start-time	设置 SLA 操作开始的时间。

默认值

默认值如下：

- SLA 操作在到达计划的时间之前处于 **pending** 状态。在此状态下，操作已启用，但不主动收集数据。
- 默认 **ageout** 时间是 0 秒（永不过期）。
- 默认 **life** 是 3600 秒（一个小时）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

当 SLA 操作处于活动状态时，它会立即开始收集信息。以下时间线展示了操作的老化过程：

```
W--------------------X--------------------Y--------------------Z
```

- W 是使用 **sla monitor** 命令配置的 SLA 操作时间。
- X 是 SLA 操作的开始时间。这是操作 “ 激活 ” 的时间。
- Y 是使用 **sla monitor schedule** 命令配置的寿命结束时间（**life** 秒数递减计数至零）。
- Z 是操作到期。

到期过程（如有使用）在 W 时开始递减计数，在 X 和 Y 之间暂停，然后重置为其配置的大小，在 Y 时又开始递减计数。当 SLA 操作到期时，SLA 操作配置将从运行配置中删除。操作可在其执行前到期（也就是说，Z 可以发行在 X 之前）。为确保不会发生这种情况，操作配置时间与开始时间（X 与 W）之间的差必须小于 age-out seconds。

recurring 关键字仅可用于计划单一 SLA 操作。使用单一 **sla monitor schedule** 命令无法计划多个 SLA 操作。循环 SLA 操作的 **life** 值应小于一天。循环操作的 **ageout** 值必须为 “never”（使用 0 值指定），或者 **life** 和 **ageout** 值的和必须超过一天。如果未指定循环选项，操作将在现有正常计划模式下开始。

SLA 操作在计划后，无法修改其配置。要修改已计划 SLA 操作的配置，必须使用 **sla monitor** 命令完全删除所选的 SLA 操作。删除 SLA 操作也会删除关联的 **sla monitor schedule** 命令。然后可以重新输入 SLA 操作配置。

示例

以下示例展示了计划在 4 月 5 日下午 3:00 开始主动收集数据 的 SLA 操作 25。此操作在 12 小时无活动后过期。当此 SLA 操作过期时，SLA 操作的所有配置信息将从运行配置中删除。

```
ciscoasa(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

以下示例展示了计划在 5 分钟延迟后开始收集数据的 SLA 操作 1。适用一小时的默认寿命。

```
ciscoasa(config)# sla monitor schedule 1 start after 00:05:00
```

以下示例展示了计划立即开始收集数据并且无限期运行的 SLA 操作 3：

```
ciscoasa(config)# sla monitor schedule 3 life forever start-time now
```

以下示例展示了计划在每天凌晨 1:30 自动开始收集数据的 SLA 操作 15：

```
ciscoasa(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

相关命令

命令	说明
show sla monitor configuration	显示 SLA 配置设置。
sla monitor	定义 SLA 监控操作。

smart-tunnel auto-signon enable

要在无客户端（基于浏览器）SSL VPN 会话中启用智能隧道自动登录，请在组策略 webvpn 配置模式下或用户名 webvpn 配置模式下使用 **smart-tunnel auto-signon enable** 命令。

要从组策略或用户名中删除 **smart-tunnel auto-signon enable** 命令而从默认组策略继承，请使用此命令的 **no** 形式。

no smart-tunnel auto-signon enable *list* [**domain** *domain*] [port *port*] [realm *realm string*]

语法说明

domain *domain*	（可选）。在身份验证时要添加到用户名的域名称。如果输入域名，请在列表条目中输入 **use-domain** 关键字。
list	智能隧道自动登录列表的名称已在 ASA webvpn 配置中。 要查看 SSL VPN 配置中的智能隧道自动登录列表条目，请在特权 EXEC 模式下输入 **show running-config webvpn smart-tunnel** 命令。
port	指定哪个端口执行自动登录。
realm	配置身份验证的领域。

默认值

此命令不存在默认值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。
8.4(1)	引入了可选参数 *realm* 和 *port*。

使用指南

智能隧道自动登录功能只支持使用 Microsoft WININET 库进行 HTTP 和 HTTPS 通信的应用。例如，Microsoft Internet Explorer 使用 WININET 动态链接库与网络服务器通信。

必须先使用 **smart-tunnel auto-signon** *list* 命令创建服务器的列表。只能将一个列表分配到组策略或用户名。

领域字符串与网站的受保护区域关联，并且在身份验证过程中通过身份验证提示或 HTTP 报头传回浏览器。如果管理员不知道相应的领域，应执行一次登录，从提示对话中获取领域字符串。

管理员现在可以选择性指定相应主机的端口号。对于 Firefox，如果未指定端口号，将在 HTTP 和 HTTPS（分别通过默认端口号 80 和 443 访问）上执行自动登录。

示例

以下命令启用名为 HR 的智能隧道自动登录列表：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR
ciscoasa(config-group-webvpn)
```

以下命令启用名为 HR 的智能隧道自动登录列表，并且在身份验证过程中将名为 CISCO 的域添加到用户名。

```
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

以下命令从组策略中删除名为 HR 的智能隧道自动登录列表，并且从默认组策略继承智能隧道自动登录列表命令。

```
ciscoasa(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

相关命令

命令	说明
smart-tunnel auto-signon *list*	创建在智能隧道连接中自动提交凭证的服务器列表。
show running-config webvpn smart-tunnel	显示 ASA 上的智能隧道配置。
smart-tunnel auto-start	在用户登录后自动开始智能隧道访问。
smart-tunnel disable	禁止智能隧道访问。
smart-tunnel *list*	将条目添加到能够使用无客户端 SSL VPN 会话连接私有站点的应用列表。

smart-tunnel auto-signon list

在 webvpn 配置模式下使用 **smart-tunnel auto-signon list** 命令创建在智能隧道连接中自动提交凭证的服务器列表。请对要添加到列表的每一台服务器使用此命令。

要从列表中删除条目，请使用此命令的 **no** 形式，指定在 ASA 配置中显示的列表和 IP 地址或主机名。

no smart-tunnel auto-signon *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

要显示智能隧道自动登录列表条目，请在特权 EXEC 模式下输入 **show running-config webvpn smart-tunnel** 命令。

要从 ASA 配置中删除服务器的整个列表，请使用此命令的 **no** 形式，并且仅指定列表。

no smart-tunnel auto-signon *list*

语法说明

host	按其主机名或通配符掩码标识的服务器。
hostname-mask	自动进行身份验证的主机名或通配符掩码。
ip	用其 IP 地址和子网掩码标识的服务器。
ip-address [*netmask*]	自动进行身份验证的主机的子网。
list	远程服务器列表的名称。如果它包含空格，请用引号括住名称。字符串最多可以包含 64 个字符。如果配置中没有列表，ASA 将会创建列表。或者将条目添加到列表。
use-domain	（可选）如果身份验证需要，将 Windows 域添加到用户名。如果输入此关键字，请确保在将智能隧道列表分配到一个或多个组策略或用户名时指定域名。

默认值

此命令不存在默认值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

智能隧道自动登录功能只支持使用 Microsoft WININET 库进行 HTTP 和 HTTPS 通信的应用。例如，Microsoft Internet Explorer 使用 WININET 动态链接库与网络服务器通信。

填充智能隧道自动登录列表后，在组策略 webvpn 或用户名 webvpn 模式下使用 **smart-tunnel auto-signon enable** *list* 命令分配列表。

示例

如果身份验证需要，以下命令将子网中的所有主机添加到用户名，如果身份验证需要，还会添加 Windows 域：

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

以下命令从列表中删除该条目：

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

如果删除的条目是列表中的唯一条目，上面所示的命令还会删除名为 HR 的列表。否则，以下命令将从 ASA 配置中删除整个列表：

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR
```

以下命令将域中的所有主机添加到名为 intranet 的智能隧道自动登录列表中：

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

以下命令从列表中删除该条目：

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

相关命令

命令	说明
smart-tunnel auto-signon enable	为命令模式中指定的组策略或用户名启用智能隧道自动登录。
smart-tunnel auto-signon enable *list*	将智能隧道自动登录列表分配到组策略或用户名
show running-config webvpn smart-tunnel	显示智能隧道配置。
smart-tunnel auto-start	在用户登录后自动开始智能隧道访问。
smart-tunnel enable	允许用户登录后进行智能隧道访问，但要求用户在 SSL VPN 门户网站页面上使用 **Application Access**（应用访问）> **Start Smart Tunnels**（启动智能隧道）按钮手动启动智能隧道访问。

smart-tunnel auto-start

要使用户在无客户端（基于浏览器）SSL VPN 会话中登录时自动启动智能隧道访问，请在组策略 webvpn 配置模式下或用户名 webvpn 配置模式下使用 **smart-tunnel auto-start** 命令。

smart-tunnel auto-start *list*

要从组策略或用户名删除 **smart-tunnel** 命令并且从默认组策略继承 [**no**] **smart-tunnel** 命令，请使用此命令的 **no** 形式。

no smart-tunnel

语法说明

list	*list* 是 ASA webvpn 配置中已存在的智能隧道列表的名称。 要查看 SSL VPN 配置中已存在的任何智能隧道列表条目，请在特权 EXEC 模式下输入 **show running-config webvpn** 命令。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 WebVPN 配置模式	• 是	—	• 是	—	—
用户名 webvpn 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

此命令需要您先使用 **smart-tunnel list** 命令创建应用列表。

此选项在用户登录时启动智能隧道访问，它仅适用于 Windows。

示例

以下命令对名为 apps1 的应用列表启动智能隧道访问：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1
ciscoasa(config-group-webvpn)
```

以下命令从组策略中删除名为 apps1 的列表，并且从默认组策略继承智能隧道命令：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

相关命令

命令	说明
show running-config webvpn	显示无客户端 SSL VPN 配置，包括所有智能隧道列表条目。
smart-tunnel disable	禁止智能隧道访问。
smart-tunnel enable	允许用户登录后进行智能隧道访问，但要求用户在 SSL VPN 门户网站页面上使用 **Application Access**（应用访问）> **Start Smart Tunnels**（启动智能隧道）按钮手动启动智能隧道访问。
smart-tunnel list	将条目添加到能够使用无客户端 SSL VPN 会话连接私有站点的应用列表。

smart-tunnel disable

要禁止通过无客户端（基于浏览器）SSL VPN 会话的智能隧道访问，请在组策略 webvpn 配置模式或用户名 webvpn 配置模式下使用 **smart-tunnel disable** 命令。

smart-tunnel disable

要从组策略或用户名删除 **smart-tunnel** 命令并且从默认组策略继承 [**no**] **smart-tunnel** 命令，请使用此命令的 **no** 形式。

no smart-tunnel

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略 WebVPN 配置模式	• 是	—	• 是	—	—
用户名 webvpn 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

默认情况下，智能隧道未启用，因此仅当（默认）组策略或用户名配置包含您不想用于相关组策略或用户名的 **smart-tunnel auto-start** 或 **smart-tunnel enable** 命令时，才需要使用 **smart-tunnel disable** 命令。

示例

以下命令禁止智能隧道访问：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel disable
ciscoasa(config-group-webvpn)
```

相关命令

命令	说明
smart-tunnel auto-start	在用户登录后自动开始智能隧道访问。
smart-tunnel enable	允许用户登录后进行智能隧道访问，但要求用户在 SSL VPN 门户网站页面上使用 **Application Access**（应用访问）> **Start Smart Tunnels**（启动智能隧道）按钮手动启动智能隧道访问。
smart-tunnel list	将条目添加到能够使用无客户端 SSL VPN 会话连接私有站点的应用列表。

smart-tunnel enable

要启用通过无客户端（基于浏览器）SSL VPN 会话的智能隧道访问，请在组策略 webvpn 配置模式或用户名 webvpn 配置模式下使用 **smart-tunnel enable** 命令。

smart-tunnel enable *list*

要从组策略或用户名删除 **smart-tunnel** 命令并且从默认组策略继承 [**no**] **smart-tunnel** 命令，请使用此命令的 **no** 形式。

no smart-tunnel

语法说明

list	*list* 是 ASA webvpn 配置中已存在的智能隧道列表的名称。 要查看 SSL VPN 配置中的智能隧道列表条目，请在特权 EXEC 模式下输入 **show running-config webvpn** 命令。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 WebVPN 配置模式	• 是	—	• 是	—	—
用户名 webvpn 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

smart-tunnel enable 命令将符合智能隧道访问条件的应用列表分配到组策略或用户名。它要求用户在无客户端 SSL VPN 门户网站页面上使用 **Application Access**（应用访问）> **Start Smart Tunnels**（启动智能隧道）按钮手动启动智能隧道访问。也可以使用 **smart-tunnel auto-start** 命令在用户登录时自动启动智能隧道访问。

这两个命令都需要您先使用 **smart-tunnel list** 命令创建应用列表。

示例

以下命令启用名为 apps1 的智能隧道列表：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel enable apps1
ciscoasa(config-group-webvpn)
```

以下命令从组策略中删除名为 apps1 的列表，并且从默认组策略继承智能隧道列表：

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

相关命令

命令	说明
show running-config webvpn	显示无客户端 SSL VPN 配置，包括所有智能隧道列表条目。
smart-tunnel auto-start	在用户登录后自动开始智能隧道访问。
smart-tunnel disable	禁止智能隧道访问。
smart-tunnel list	将条目添加到能够使用无客户端 SSL VPN 会话连接私有站点的应用列表。

smart-tunnel list

要填写可以使用无客户端（基于浏览器）SSL VPN 会话来连接私有站点的应用列表，请在 webvpn 配置模式下使用 **smart-tunnel list** 命令。要从列表中删除应用，请使用此命令的 **no** 形式并指定条目。要从 ASA 配置中删除应用的整个列表，请使用此命令的 **no** 形式，并且仅指定列表。

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

no smart-tunnel list *list*

语法说明

application	要授予智能隧道访问权限的应用名称。字符串最多可以包含 64 个字符。
hash	（可选且仅适用于 Windows）要获取此值，请在使用 SHA-1 算法计算哈希的实用程序中输入应用的校验和（即可执行文件的校验和）。此类实用程序的一个典型示例是 Microsoft File Checksum Integrity Verifier (FCIV)，可从 http://support.microsoft.com/kb/841290/ 下载。安装 FCIV 后，将要进行哈希计算的应用的临时副本放到不含空格的路径上（例如 c:/fciv.exe），然后在命令行中输入 **fciv.exe -sha1** *application*（例如 **fciv.exe -sha1 c:\msimn.exe**）以显示 SHA-1 哈希。 SHA-1 哈希始终为 40 个十六进制字符。
list	应用或程序列表的名称。如果它包含空格，请用引号括住名称。如果配置中没有列表，CLI 将会创建列表。或者将条目添加到列表。
path	对于 Mac OS，是指应用的完整路径。对于 Windows，是指应用的文件名；或者应用的完整或部分路径，包括其文件名。字符串最多可以包含 128 个字符。
platform *OS*	（操作系统是 Microsoft Windows 时可选）输入 **windows** 或 **mac** 以指定应用的主机。

默认值

Windows 是默认平台。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.0(4)	添加了 **platform** *OS*。

使用指南

您可以在 ASA 上配置多个智能隧道列表，但不能将多个智能隧道列表分配到一个指定的组策略或用户名。要填充智能隧道列表，请为每个应用输入一次 **smart-tunnel list** 命令，输入相同的 *list* 字符串，但指定各操作系统唯一的 *application* 和 *path*。为您希望列表支持的每个 *OS* 输入一次该命令。

如果 OS 与条目中指定的操作系统不匹配，会话将忽略列表条目。如果应用的路径不存在，它也会忽略条目。

要查看 SSL VPN 配置中的智能隧道列表条目，请在特权 EXEC 模式下输入 **show running-config webvpn smart-tunnel** 命令。

path 必须与计算机上的路径匹配，但不一定要完整。例如，*path* 可以只包含可执行文件及其扩展名。

智能隧道有以下要求：

- 生成智能隧道连接的远程主机必须运行 Microsoft Windows Vista、Windows XP 或 Windows 2000 的 32 位版本；或者 Mac OS 10.4 或 10.5。
- 使用智能隧道或端口转发的 Microsoft Windows Vista 的用户必须将 ASA 的 URL 添加到 “ 受信任的站点 ” 区域。要访问 “ 受信任的站点 ” 区域，他们必须启动 Internet Explorer 并选择 “ 工具 ”>“Internet 选项 ”>“ 安全 ” 选项卡。Vista 用户也可以禁用受保护模式，以简化智能隧道访问；但我们不建议这种方法，因为它会增大计算机受到攻击的风险。
- 必须为浏览器启用 Java、Microsoft ActiveX 或两者。
- Mac OS 需要 Safari 3.1.1 或更高版本才可支持智能隧道。

在 Microsoft Windows 上，仅 Winsock 2、基于 TCP 的应用可用于智能隧道访问。

在 Mac OS 上，使用 TCP、动态链接到 SSL 库的应用可在智能隧道上运行。以下类型的应用无法在智能隧道上运行：

- 使用 dlopen 或 dlsym 查找 libsocket 调用的应用
- 查找 libsocket 调用的静态链接应用
- 使用两级名称空间的 Mac OS 应用。
- Mac OS 基于控制台的应用，如 Telnet、SSH 和 cURL。
- Mac OS PowerPC 类型的应用。要确定 Mac OS 应用的类型，请右键点击其图标并选择 Get Info（获取信息）。

在 Mac OS 上，只有从门户网站页面启动的应用才可建立智能隧道会话。此要求包括 Firefox 对智能隧道的支持。第一次使用智能隧道时使用 Firefox 启动另一个 Firefox 实例需要名为 csco_st 的用户配置文件。如果此用户配置文件不存在，会话将提示用户创建一个。

以下限制适用于智能隧道：

- 如果远程计算机需要代理服务器来连接 ASA，连接终端的 URL 必须在代理服务排除的 URL 列表中。在此配置中，智能隧道仅支持基本身份验证。
- 智能隧道自动登录功能仅支持在 Microsoft Windows 操作系统上使用 Microsoft WININET 库进行 HTTP 和 HTTPS 通信的应用。例如，Microsoft Internet Explorer 使用 WININET 动态链接库与网络服务器通信。
- 组策略或本地用户政策支持不超过一个适合智能隧道访问的应用列表和一个智能隧道自动登录服务器列表。
- 状态故障切换不保留智能隧道连接。用户在故障切换后必须重新连接。

注　智能隧道访问突发问题可能表示：由于应用升级，*path* 值不是最新的。例如，在生产应用的公司被收购和应用升级后，应用的默认路径通常会改变。

输入 hash 可以合理保证无客户端 SSL VPN 不会允许与 *path* 中指定的字符串匹配的非法文件。由于应用的每个版本或补丁具有不同的校验和，因此您输入的 *hash* 只能与远程主机上的一个版本或补丁匹配。要为应用的多个版本指定 *hash*，请为每个版本输入一次 **smart-tunnel list** 命令，并且输入相同的 *list* 字符串，但在每个命令中指定唯一的 *application* 字符串和唯一的 *hash* 值。

注　如果您输入 *hash* 值并且希望应用的未来版本或补丁支持智能隧道访问，则必须维护智能隧道列表。智能隧道访问突发问题可能表示：由于应用升级，包含 *hash* 值的应用列表不是最新的。不输入 *hash* 即可避免此问题。

在配置智能隧道列表后，使用 **smart-tunnel auto-start** 或 **smart-tunnel enable** 命令将列表分配到组策略或用户名。

示例

以下命令将 Microsoft Windows 应用 Connect 添加到名为 apps1 的智能隧道列表：

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

以下命令将添加 Windows 应用 msimn.exe，并且要求远程主机上应用的哈希值与输入的最后一个字符串匹配才支持智能隧道访问：

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

以下命令为 Mac OS 的浏览器 Safari 提供智能隧道支持：

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

相关命令

命令	说明
show running-config webvpn smart-tunnel	显示 ASA 上的智能隧道配置。
smart-tunnel auto-start	在用户登录后自动开始智能隧道访问。
smart-tunnel disable	禁止智能隧道访问。
smart-tunnel enable	允许用户登录后进行智能隧道访问，但要求用户在 SSL VPN 门户网站页面上使用 **Application Access**（应用访问）> **Start Smart Tunnels**（启动智能隧道）按钮手动启动智能隧道访问。

smart-tunnel network

要创建主机列表以用于配置智能隧道策略，请在 webvpn 配置模式下使用 **smart-tunnel network** 命令。要对智能隧道策略禁止主机列表，请使用此命令的 **no** 形式。

smart-tunnel network

no smart-tunnel network

语法说明

host *host mask*	主机名掩码，例如 *.cisco.com。
ip *ip address*	网络的 IP 地址。
netmask	网络的子网掩码。
network name	要应用到隧道策略的网络名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	• 是	• 是	—	—

命令历史

版本	**修改**
8.3(1)	引入了此命令。

使用指南

当智能隧道打开后，您可以通过 **smart-tunnel network** 命令（配置网络 [一组主机]）和 **smart-tunnel tunnel-policy** 命令（使用指定的智能隧道网络对用户执行策略）允许隧道外部的流量。

示例

以下是说明如何使用 **smart-tunnel network** 命令的示例：

```
ciscoasa(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

相关命令

命令	**说明**
smart-tunnel tunnel-policy	使用指定的智能隧道网络对用户执行策略。

smart-tunnel tunnel-policy

要将智能隧道策略应用到特定组或用户策略，请在 webvpn 配置模式下使用 **smart-tunnel tunnel-policy** 命令。要取消将智能隧道应用到特定组，请使用此命令的 [no] 形式。

smart-tunnel tunnel-policy

no smart-tunnel tunnel-policy

语法说明

excludespecified	只允许网络名称指定的网络外部的网络通过隧道传输。
network name	列出要通过隧道传输的网络。
tunnelall	使一切内容通过隧道传输（加密）。
tunnelspecified	只允许网络名称指定的网络通过隧道传输。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.3.1	引入了此命令。

使用指南

当智能隧道打开后，您可以通过 **smart-tunnel network** 命令（配置网络 [一组主机]）和 **smart-tunnel tunnel-policy** 命令（使用指定的智能隧道网络对用户执行策略）允许隧道外部的流量。

示例

以下是如何使用 **smart-tunnel tunnel-policy** 命令的示例：

```
ciscoasa(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

相关命令

命令	说明
smart-tunnel network	创建用于配置智能隧道策略的主机列表。

smtp from-address

要为本地 CA 服务器生成的所有邮件（例如分发一次性密码）指定在邮件 From:（发件人：）字段中使用的邮件地址，请在 CA 服务器配置模式下使用 **smtp from-address** 命令。要将邮件地址重置为默认值，请使用此命令的 **no** 形式。

smtp from-address *e-mail_address*

no smtp from-address

语法说明

e-mail_address	指定在 CA 服务器生成的所有邮件的 From:（发件人：）字段中出现的邮件地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例指定来自本地 CA 服务器的所有邮件的 From:（发件人：）字段都包含 ca-admin@asa1-ca.example.com：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

以下示例将来自本地 CA 服务器的所有邮件的 From:（发件人：）字段重置为默认地址 admin@asa1-ca.example.com：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问权限，从而允许配置和管理本地 CA。
smtp subject	定制要在本地 CA 服务器生成的所有邮件主题字段中显示的文本。

smtp subject

要定制在本地证书颁发机构 (CA) 服务器生成的所有邮件（例如分发一次性密码）主题字段中显示的文本，请在 CA 服务器配置模式下使用 **smtp subject** 命令。要将文本重置为默认值，请使用此命令的 **no** 形式。

smtp subject *subject-line*

no smtp subject

语法说明

subject-line	指定从 CA 服务器发送的所有邮件 Subj:（主题：）字段中出现的文本。最大字符数为 127。

默认值

默认情况下，Subj:（主题：）字段中的文本为 “Certificate Enrollment Invitation”（证书注册邀请）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例指定发自 CA 服务器的所有邮件的 Subj:（主题：）字段中出现文本 *Action: Enroll for a certificate*：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp subject Action: Enroll for a certificate
ciscoasa(config-ca-server)#
```

以下示例将发自 CA 服务器的所有邮件的 Subj:（主题：）字段文本重置为默认文本 “Certificate Enrollment Invitation”（证书注册邀请）：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no smtp subject
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问权限，从而允许配置和管理本地 CA。
smtp from-address	指定要在本地 CA 服务器生成的所有邮件的 From:（收件人：）字段中使用的邮件地址。

smtps

要进入 SMTPS 配置模式，请在全局配置模式下使用 **smtps** 命令。要删除在 SMTPS 命令模式中输入的任何命令，请使用此命令的 **no** 版本。SMTPS 是用于通过 SSL 连接发送邮件的 TCP/IP 协议。

smtps

no smtps

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例显示如何进入 SMTPS 配置模式：

```
ciscoasa(config)# smtps
ciscoasa(config-smtps)#
```

相关命令

命令	说明
clear configure smtps	删除 SMTPS 配置。
show running-config smtps	显示 SMTPS 的运行配置。

smtp-server

要配置 SMTP 服务器，请在全局配置模式下使用 **smtp-server** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

语法说明

backup_server	标识当主要 SMTP 服务器不可用时转发事件消息的备用 SMTP 服务器。使用 IP 地址或主机名（使用 **name** 命令配置）。
primary_server	标识主要 SMTP 服务器。使用 IP 地址或主机名（使用 **name** 命令配置）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 包括事件系统可用以向外部实体通知已发生特定事件的内部 SMTP 客户端。您可以配置 SMTP 服务器接收这些事件通知，然后将其转发到指定的邮件地址。SMTP 工具仅当您启用以邮件发送活动到 ASA 时才会激活。

示例

以下示例展示如何设置 IP 地址为 10.1.1.24 的 SMTP 服务器和 IP 地址为 10.1.1.34 的备用 SMTP 服务器：

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp cpu threshold rising

要配置 CPU 使用上限阈值和阈值监控期，请在全局配置模式下使用 **snmp cpu threshold rising** 命令。若要不配置阈值和阈值监控期，请使用此命令的 **no** 形式。

snmp cpu threshold rising *threshold_value monitoring_period*

no snmp cpu threshold rising *threshold_value monitoring_period*

语法说明

monitoring_period	定义监控期（分钟）。
threshold_value	以 CPU 占用百分比定义阈值级别。

默认值

如果未配置 **snmp cpu threshold rising** 命令，CPU 使用上限阈值级别的默认值设为 70%，临界阈值级别的默认值设为 95%。默认监控期设置为一分钟。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(1)	引入了此命令。不适用于 ASA 服务模块。

使用指南

临界 CPU 阈值级别始终保持在 95%，无法配置。CPU 使用阈值的有效范围从 10% 到 94%。监控期的有效值范围为 1-60 分钟。

示例

以下示例展示如何将 SNMP CPU 阈值配置为 75% 的 CPU 占用率和 30 分钟的监控期：

```
ciscoasa(config)# snmp cpu threshold 75% 30
```

相关命令

命令	说明
snmp-server enable traps	启用 SNMP 相关的陷阱。
snmp link threshold	定义 SNMP 接口阈值。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp link threshold

要配置 SNMP 物理接口阀值和系统内存占用阈值，请在全局配置模式下使用 **snmp link threshold** 命令。要清除 SNMP 物理接口阀值和系统内存占用阈值，请使用此命令的 **no** 形式。

snmp link threshold *threshold_value*

no snmp link threshold *threshold_value*

语法说明

threshold_value	以 CPU 占用百分比定义阈值。

默认值

如果不配置 **snmp link threshold** 命令，默认阈值为 70% 的 CPU 占用率和系统内存占用率。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

物理接口阈值的有效范围从 30% 到 99%。**snmp link threshold** 命令仅适用于管理员情景。

示例

以下示例展示如何将所有物理接口的 SNMP 接口阈值配置为 75%：

```
ciscoasa(config)# snmp link threshold 75%
```

相关命令

命令	说明
snmp-server enable traps	启用 SNMP 相关的陷阱。
snmp cpu threshold rising	定义 SNMP CPU 阈值。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-map

要标识用于为 SNMP 检查定义参数的特定映射，请在全局配置模式下使用 **snmp-map** 命令。要删除映射，请使用此命令的 **no** 形式。

snmp-map *map_name*

no snmp-map *map_name*

语法说明

map_name	SNMP 映射的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **snmp-map** 命令标识用于为 SNMP 检查定义参数的特定映射。输入此命令后，系统将进入 SNMP 映射配置模式，在该模式中可输入用于定义特定映射的不同命令。在定义 SNMP 映射后，可使用 **inspect snmp** 命令启用映射。然后，您可以使用 **class-map**、**policy-map** 和 **service-policy** 命令定义一个流量类，将 **inspect** 命令应用到该类中，并将策略应用到一个或多个接口上。

示例

以下示例展示如何标识 SNMP 流量、定义 SNMP 映射、定义策略以及将该策略应用到外部接口。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
deny version	不允许使用特定版本的 SNMP 的流量。
inspect snmp	启用 SNMP 应用检查。
policy-map	将类映射与特定安全操作关联。

snmp-server community

要设置 SNMP 社区字符串，请在全局配置模式下使用 **snmp-server community** 命令。要删除 SNMP 社区字符串，请使用此命令的 **no** 形式。

snmp-server community [*0* | *8*] *community-string*

no snmp-server community [*0* | *8*] *community-string*

语法说明

0	（可选）指定后接未加密的（明文）社区字符串。
8	指定后接加密的社区字符串。
community-string	设置 SNMP 社区字符串，即已加密或未加密（明文）形式的密码。社区字符串最多可以包含 32 个字符。

默认值

默认社区字符串是 “public”。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	*text* 参数已改为 *community-string* 参数。
8.3(1)	添加了对已加密密码的支持。

使用指南

SNMP 社区字符串是 SNMP 管理站与管理的网络节点之间的共享密钥。它只用于管理站与设备之间的版本 1 和 2c 通信。ASA 使用密钥确定传入的 SNMP 请求是否有效。

例如，您可以使用社区字符串指定站点，然后使用同一字符串配置路由器、ASA 和管理站。ASA 使用此字符串，不响应包含无效社区字符串的请求。

在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。

加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

注　如果从版本 8.3(1) 降级到 ASA 软件的更低版本并且已配置加密密码，必须先使用 **no key config-key password encryption** 命令将加密的密码恢复为明文，然后保存结果。

示例

以下示例将社区字符串设置为“onceuponatime”：

```
ciscoasa(config)# snmp-server community onceuponatime
```

以下示例设置加密的社区字符串：

```
ciscoasa(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

以下示例为未加密的社区字符串：

```
ciscoasa(config)# snmp-server community 0 cisco
```

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 计数器。
snmp-server contact	设置 SNMP 联系人姓名。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-server contact

要设置 SNMP 服务器联系人姓名，请在全局配置模式下使用 **snmp-server contact** 命令。要删除 SNMP 联系人姓名，请使用此命令的 **no** 形式。

snmp-server contact *text*

no snmp-server contact [*text*]

语法说明

text	指定联系人或 ASA 系统管理员的姓名。姓名区分大小写，最多可包含 127 个字符。接受空格，但多个空间缩为一个空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例将 SNMP 服务器联系人设为 EmployeeA：

```
ciscoasa(config)# snmp-server contact EmployeeA
```

相关命令

命令	说明
snmp-server community	设置 SNMP 社区字符串。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server enable traps	启用 SNMP 陷阱。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-server enable

要在 ASA 上启用 SNMP 服务器，请在全局配置模式下使用 **snmp-server enable** 命令。要禁用 SNMP 服务器，请使用此命令的 **no** 形式。

snmp-server enable

no snmp-server enable

语法说明

此命令没有任何参数或关键字。

默认值

启用 SNMP 服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以轻松启用和禁用 SNMP，而无需配置和重新配置 SNMP 陷阱或其他配置。

示例

以下示例启用 SNMP、配置 SNMP 主机和陷阱，然后将陷阱作为系统日志消息发送。

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

相关命令

命令	说明
snmp-server community	设置 SNMP 社区字符串。
snmp-server contact	设置 SNMP 联系人姓名。
snmp-server enable traps	启用 SNMP 陷阱。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-server enable traps

要让 ASA 将陷阱发送到 NMS，请在全局配置模式下使用 **snmp-server enable traps** 命令。要禁用陷阱，请使用此命令的 **no** 形式。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **config** | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **ikev2** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [**...**] | **config** | **entity** [*trap*] [**...**] | **ipsec** [*trap*] [**...**] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

语法说明

all	启用所有陷阱。
config	启用配置陷阱。
connection-limit-reached	启用达到连接限制陷阱。
cpu threshold rising	启用接近 CPU 阈值陷阱。
entity [*trap*]	启用实体陷阱。**entity** 的陷阱包括： • **accelerator-temperature** • **chassis-fan-failure** • **chassis-temperature** • **config-change** • **cpu-temperature** • **fan-failure** • **fru-insert** • **fru-remove** • **power-supply** • **power-supply-failure** • **power-supply-presence** • **power-supply-temperature**
ipsec [*trap*]	启用 IPsec 陷阱。**ipsec** 的陷阱包括： • **start** • **stop**
ikev2 [*trap*]	启用 IKEv2 IPsec 陷阱。**ikev2** 的陷阱包括： • **start** • **stop**
link-threshold	启用达到链路阈值陷阱。
memory-threshold	启用达到内存阈值陷阱。
nat [*trap*]	启用 NAT 相关的陷阱。**nat** 的陷阱包括： • **packet-discard**

remote-access [*trap*]	启用远程访问陷阱。**remote-access** 的陷阱包括： • **session-threshold-exceeded**
snmp [*trap*]	启用 SNMP 陷阱。默认启用所有 SNMP 陷阱。**snmp** 的陷阱包括： • **authentication** • **linkup** • **linkdown** • **coldstart** • **warmstart**
syslog	启用系统日志消息陷阱。

默认值

默认配置启用了以下 **snmp** 陷阱 (**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**)。如果输入此命令而不指定陷阱类型，则默认值为 **syslog**。（默认 **snmp** 陷阱仍然随 **syslog** 陷阱一起启用。）默认情况下禁用所有其他陷阱。

使用此命令的 **no** 形式及 **snmp** 关键字可以禁用这些陷阱。**clear configure snmp-server** 命令将恢复默认启用 SNMP 陷阱。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	添加了以下陷阱：**snmp warmstart**、**nat packet-discard**、**link-threshold**、**memory-threshold**、**entity power-supply**、**entity fan-failure**、**entity cpu-temperature**、**cpu threshold rising** 和 **connection-limit-reached**。这些陷阱不适用于 ASASM。
8.6(1)	添加了以下陷阱，以支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X：**entity power-supply-failure**、**entity chassis-fan-failure**、**entity power-supply-presence**、**entity chassis-temperature** 和 **entity power-supply-temperature**。
9.0(1)	为 IKEv2 和 IPsec 添加了对多情景模式的支持。
9.3(2)	添加了对以下陷阱的支持：**config** 和 **entity accelerator-temperature**。

使用指南

要启用个别陷阱或一组陷阱，请对每种功能类型输入此命令。要启用所有陷阱，请输入 **all** 关键字。

要将陷阱发送到 NMS，请输入 **logging history** 命令，然后使用 **logging enable** 命令启用日志记录。

在管理员情景中生成的陷阱只包括：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

对系统情景中物理连接的接口，仅通过管理员情景生成的陷阱包括：

- **interface-threshold**

所有其他陷阱适用于管理员和用户情景。

accelerator-temperature 阈值陷阱仅适用于 ASA 5506-X 和 ASA 5508-X。

chassis-fan-failure 陷阱不适用于 ASA 5506-X。

config 陷阱启用 ciscoConfigManEvent 通知和 ccmCLIRunningConfigChanged 通知，在退出配置模式后生成。

以下陷阱不适用于 ASA 5506-X 和 ASA 5508-X：**fan-failure**、**fru-insert**、**fru-remove**、**power-supply**、**power-supply-failure**、**power-supply-presence** 和 **power-supply-temperature**。

多情景模式指南

- 在多情景模式下，**fan-failure** 陷阱、**power-supply-failure** 陷阱和 **cpu-temperature** 陷阱仅从管理员情景生成，而不从用户情景生成。这些陷阱仅适用于 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X；它们不适用于 ASA 5505。
- 多情景模式下不支持 **snmp-server enable traps remote-access session-threshold-exceeded** 命令。

如果 CPU 占用率超过为配置的监控期配置的阈值，将生成 **cpu threshold rising** 陷阱。

当使用的系统内存达到 80% 时，将生成 **memory-threshold** 陷阱。

注　SNMP 不监控电压传感器。

示例

以下示例启用 SNMP、配置 SNMP 主机和陷阱，然后将陷阱作为系统日志消息发送：

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

相关命令

命令	说明
snmp-server community	设置 SNMP 社区字符串。
snmp-server contact	设置 SNMP 联系人姓名。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server host	设置 SNMP 主机地址。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-server group

要配置新 SNMP 组，请在全局配置模式下使用 **snmp-server group** 命令。要移除指定的 SNMP 组，请使用此命令的 **no** 形式。

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

语法说明

auth	指定不加密的数据包身份验证。
group-name	指定组的名称。
noauth	不指定数据包身份验证。
priv	指定加密的数据包身份验证。
v3	指定组使用 SNMP 版本 3 安全模型，这在支持的安全模型中是最安全的。此版本允许您明确配置身份验证特性。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。
8.3(1)	添加了对密码加密的支持。

使用指南

要使用版本 3 安全模型，必须先配置 SNMP 组，然后配置 SNMP 用户，再配置 SNMP 主机。您还必须指定版本 3 和安全级别。在内部配置社区字符串时，会自动创建两个名为 “public” 的组 - 一个用于版本 1 安全模型，一个用于版本 2c 安全模型。在删除社区字符串时，会自动删除两个配置的组。

注　配置为属于特定组的用户应与该组具有相同的安全模型。

在引导或升级 ASA 时，不再支持单位数密码以及开头为数字后接空格的密码。例如，0 pass 和 1 均为无效密码。

注　如果从版本 8.3(1) 降级到 ASA 软件的更低版本并且已配置加密密码，必须先使用 **no key config-key password encryption** 命令将加密的密码恢复为明文，然后保存结果。

示例

以下示例展示 ASA 如何使用 SNMP 版本 3 安全模型接收 SNMP 请求，包括创建组、创建用户和创建主机：

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

相关命令

命令	说明
clear configure snmp-server	清除配置 SNMP 计数器。
snmp-server host	设置 SNMP 主机地址。
snmp-server user	创建新的 SNMP 用户。

snmp-server host

要在 ASA 上指定可以使用 SNMP 的 NMS，请在全局配置模式下使用 **snmp-server host** 命令。要禁用 NMS，请使用此命令的 **no** 形式。

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

语法说明

0	（可选）指定后接未加密的（明文）社区字符串。
8	指定后接加密的社区字符串。
community	指定从 NMS 发出的请求需要非默认字符串，或者在生成发送到 NMS 的陷阱时需要非默认字符串。仅适用于 SNMP 版本 1 或 2c。
community-string	指定与通知一起发送或者在 NMS 产生的请求中发送的密码式社区字符串。社区字符串最多可以包含 32 个字符。可以是加密或未加密（明文）格式。
hostname	指定 SNMP 通知主机，通常是 NMS 或 SNMP 管理器。
interface	指定 NMS 用于与 ASA 通信的接口名称。
ip_address	指定 SNMP 陷阱应发送到或从中发出 SNMP 请求的 NMS 的 IP 地址。*仅*支持 IPv4 地址。
poll	（可选）指定主机可以浏览（轮询），但不能发送陷阱。
port	设置 NMS 主机的 UDP 端口号。
trap	（可选）指定只能发送陷阱，并且此主机不可浏览（轮询）。
udp-port	（可选）指定 SNMP 陷阱必须发送到 NMS 主机的非默认端口。
username	在发送到主机的陷阱 PDU 中嵌入用户名。仅适用于 SNMP 版本 3。
version {**1** | **2c** | **3**}	（可选）指定 SNMP 陷阱版本。ASA 不支持基于 SNMP 请求的过滤（轮询）。

默认值

默认 UDP 端口为 162。

默认版本为 1。

默认启用 SNMP 陷阱。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	• 支持 SNMP 版本 3。 • 引入了 *username* 参数。 • *text* 参数已改为 *community-string* 参数。 • *interface_name* 参数已更改为 *interface* 参数。
8.3(1)	添加了对已加密密码的支持。

使用指南

如果在当前使用的端口上配置 **snmp-server host** 命令，将显示以下消息：

警告 **The UDP port *port* is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用时，将发出系统日志消息 %ASA-1-212001。

要使用版本 3 安全模型，必须先配置 SNMP 组，然后依次配置 SNMP 用户和 SNMP 主机。设备上必须已经配置用户名。在将设备配置为故障切换队的备用设备时，将从活动的设备复制 SNMP 引擎 ID 和用户配置。此操作允许从 SNMP 版本 3 查询的角度透明切换。无需在 NMS 中做任何配置更改即可适应切换事件。

在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。

加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

在引导或升级 ASA 时，不再支持单位数密码以及开头为数字后接空格的密码。例如，0 pass 和 1 均为无效密码。

注 如果从版本 8.3(1) 降级到 ASA 软件的更低版本并且已配置加密密码，必须先使用 **no key config-key password encryption** 命令将加密的密码恢复为明文，然后保存结果。

示例

以下示例将主机设置为 192.0.2.5（连接至内部接口）：

```
ciscoasa(config)# snmp-server host inside 192.0.2.5
ciscoasa(config)# snmp-server host inside 192.0.2.5 version 3 username user1 password
cisco123 mschap md5aes128 udp-port 190
```

以下示例展示 ASA 如何使用 SNMP 版本 3 安全模型接收 SNMP 请求，包括创建组、创建用户和创建主机：

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 username user1 password
cisco123 mschap priv admin
```

以下示例设置主机使用加密的社区字符串：

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
username user1 password cisco123 mschap
```

以下示例设置主机使用未加密的社区字符串：

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco username user1 password
cisco123 mschap
```

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 配置计数器。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server group	配置新的 SNMP 组。
snmp-server user	配置新的 SNMP 用户。

snmp-server host-group

要将用户列表中的单一用户或一组用户与网络对象关联，请在全局配置模式下使用 **snmp-server host-group** 命令。要删除关联，请使用此命令的 **no** 形式。

snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

no snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

语法说明

community	指定从 NMS 发出的请求需要非默认字符串，或者在生成发送到 NMS 的陷阱时需要非默认字符串。仅适用于 SNMP 版本 1 或 2c。
community-string	指定与通知一起发送或者在 NMS 产生的请求中发送的密码式社区字符串。社区字符串最多可以包含 32 个字符。
interface-network-object-name	指定用户或用户组关联的接口网络对象名称。
poll	（可选）指定主机可以浏览（轮询），但不能发送陷阱。
udp-port *port*	（可选）指定必须将 SNMP 陷阱发送到 NMS 主机的非默认端口，并且设置 NMS 主机的 UDP 端口号。
user-list *list_name*	指定用户列表的名称。
username	指定用户的名称。
version {**1** | **2c** | **3**}	（可选）将 SNMP 通知版本设置为版本 1、2c、3 以用于发送陷阱。

默认值

默认 UDP 端口为 162。

默认版本为 1。

默认启用 SNMP 陷阱。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

现在最多可以增加到 4000 台主机。支持的活动轮询目标数是 128。您可以使用主机名或 IP 地址范围定义主机。可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。

如果您使用 SNMP 通知版本 1 或 2c 来发送陷阱，可以将单个用户与网络对象关联。如果您使用 SNMP 版本 3 来发送陷阱，可以将单个用户或用户组与网络对象关联。使用 **snmp-server user-list** 命令创建用户组。用户可以属于任何组配置。

如果使用的是 SNMP 版本 3，则必须将用户名与 SNMP 主机关联。

示例

以下示例使用 SNMP 通知版本 1 将单个用户与网络对象关联：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
```

以下示例使用 SNMP 通知版本 2c 将单个用户与网络对象关联：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

以下示例使用 SNMP 通知版本 3 将单个用户与网络对象关联：

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
```

以下示例使用 SNMP 通知版本 3 将用户列表与网络对象关联：

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

相关命令

命令	说明
clear configure snmp-server host-group	清除所有 SNMP 主机组配置。
show running-config snmp-server host-group	从运行配置过滤 SNMP 服务器主机组配置。

snmp-server listen-port

要设置 SNMP 请求的侦听端口，请在全局配置模式下使用 **snmp-server listen-port** 命令。要恢复默认端口，请使用此命令的 **no** 形式。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

语法说明

lport	接受传入请求的端口[1]。

1. **snmp-server listen-port** 命令只适用于管理情景，不适用于系统情景。

默认值

默认端口为 161。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果在目前使用中的端口上配置 **snmp-server listen-port** 命令，将显示以下消息：

警告 **The UDP port *port* is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用时，将发出系统日志消息 %ASA-1-212001。

示例

以下示例将侦听端口设置为 192：

```
ciscoasa(config)# snmp-server listen-port 192
```

相关命令

命令	说明
snmp-server community	设置 SNMP 社区字符串。
snmp-server contact	设置 SNMP 联系人姓名。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server enable traps	启用 SNMP 陷阱。
snmp-server location	设置 SNMP 服务器位置字符串。

snmp-server location

要设置 SNMP 的 ASA 位置，请在全局配置模式下使用 **snmp-server location** 命令。要删除该位置，请使用此命令的 **no** 形式。

snmp-server location *text*

no snmp-server location [*text*]

语法说明

location *text*	指定安全设备位置。**location** *text* 区分大小写，最多可包含 127 个字符。接受空格，但多个空间缩为一个空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例将 SNMP 的 ASA 位置设置为 Building 42, Sector 54：

```
ciscoasa(config)# snmp-server location Building 42, Sector 54
```

相关命令

命令	说明
snmp-server community	设置 SNMP 社区字符串。
snmp-server contact	设置 SNMP 联系人姓名。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server enable traps	启用 SNMP 陷阱。
snmp-server host	设置 SNMP 主机地址。

snmp-server user

要配置新的 SNMP 用户，请在全局配置模式下使用 **snmp-server user** 命令。要删除指定的 SNMP 用户，请使用此命令的 **no** 形式。

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password*]} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password*]} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

语法说明

128	（可选）指定对加密使用 128 位 AES 算法。
192	（可选）指定对加密使用 192 位 AES 算法。
256	（可选）指定对加密使用 256 位 AES 算法。
3des	（可选）指定对加密使用 168 位 3DES 算法。
aes	（可选）指定对加密使用 AES 算法。
auth	（可选）指定应使用的身份验证级别。
auth-password	（可选）指定可让代理从主机接收数据包的字符串。最小长度为一个字符；建议长度至少为八个字符，并且应包含字母和数字。最大长度是 64 个字符。您可以指定纯文本密码或本地化的 MD5 摘要。如果您有本地化的 MD5 或 SHA 摘要，便可指定该字符串而不是纯文本密码。摘要应格式化为 aa:bb:cc:dd，其中 aa、bb 和 cc 是十六进制值。摘要长度应正好是 16 个二进制八位数。
des	（可选）指定对加密使用 56 位 DES 算法。
encrypted	（可选）指定密码是否以加密形式显示。加密密码必须为十六进制形式。
group-name	指定用户所属组的名称。
md5	（可选）指定 HMAC-MD5-96 身份验证级别。
priv	指定加密的数据包身份验证。
priv-password	（可选）指定用于表示隐私用户密码的字符串。最小长度为一个字符；建议长度至少为八个字符，并且应包含字母和数字。最大长度是 64 个字符。您可以指定纯文本密码或本地化的 MD5 摘要。如果您有本地化的 MD5 或 SHA 摘要，便可指定该字符串而不是纯文本密码。摘要应格式化为 aa:bb:cc:dd，其中 aa、bb 和 cc 是十六进制值。摘要长度应正好是 16 个二进制八位数。
sha	（可选）指定 HMAC-SHA-96 身份验证级别。
username	指定在连接到代理的主机上使用的用户名。
v3	指定应使用 SNMP 版本 3 安全模型。允许使用 **encrypted**、**priv** 或 **auth** 关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

SNMP 用户必须是 SNMP 组的一部分。要使用版本 3 安全模型，必须先配置 SNMP 组，然后配置 SNMP 用户，再配置 SNMP 主机。

注　如果忘记了密码，将无法恢复，而必须重新配置用户。

当 snmp 服务器用户配置显示在控制台上或写入文件（例如，启动配置文件）时，始终出现本地化身份验证和隐私摘要，而不是纯文本密码。这种使用方式是 RFC 3414 第 11.2 章规定的。

注　您必须拥有 3DES 或 AES 功能许可证才可使用 3DES 或 AES 算法配置用户。

在引导或升级 ASA 时，不再支持单位数密码以及开头为数字后接空格的密码。例如，0 pass 和 1 均为无效密码。

在集群中，必须手动为 SNMPv3 用户更新每个集群的 ASA。可在主设备上输入 **snmp-server user** *username group-name* **v3** 命令并且使用非本地化形式的 *priv-password* 选项和 *auth-password* 选项来完成此操作。

将会出现一则错误消息，通知您在集群复制或配置时不会复制 SNMPv3 用户命令。您可以单独在从 ASA 上配置 SNMPv3 用户和组命令。这也意味着现有 SNMPv3 用户和组命令在复制时不会清除，您可以在集群的所有从设备上输入 SNMPv3 用户和组命令。例如：

在使用以本地化按键输入的命令的主设备上：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:
da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

在集群复制期间的从设备上（仅当配置中存在 **snmp-server user** 命令时才会出现）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

示例

以下示例展示 ASA 如何使用 SNMP 版本 3 安全模型接收 SNMP 请求：

```
ciscoasa(config)# snmp-server group engineering v3 auth
ciscoasa(config)# snmp-server user engineering v3 auth sha mypassword
```

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
snmp-server enable	在 ASA 上启用 SNMP。
snmp-server group	创建新的 SNMP 组。
snmp-server host	设置 SNMP 主机地址。

snmp-server user-list

要使用指定用户所在的组配置 SNMP 用户列表，请在全局配置模式下使用 **snmp-server user-list** 命令。要删除指定的 SNMP 用户列表，请使用此命令的 **no** 形式。

snmp-server user-list *list_name* **username** *user_name*

no snmp-server user-list *list_name* **username** *user_name*

语法说明

list_name	指定用户列表的名称，最长可达 33 个字符。
username *user_name*	指定可在用户列表中配置的用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **snmp-server user** *username* 命令可配置用户列表中的用户。用户列表必须具有多个用户，并且能与主机名或 IP 地址范围关联。

示例

以下示例展示如何为名为 engineering 的用户列表创建用户组：

```
ciscoasa(config)# snmp-server user-list engineering username user1
ciscoasa(config)# snmp-server user-list engineering username user2
ciscoasa(config)# snmp-server user-list engineering username user3
```

命令	说明
show running-config snmp-server user-list	从运行配置过滤 SNMP 用户列表配置。
clear snmp-server user-list	清除 SNMP 用户列表配置。

至 storage-objects 命令

disable	禁止加载带开发密钥签名的映像。
enable	允许加载带开发密钥签名的映像。

software-version

要标识 Server（服务器）和 User-Agent（用户代理）报头字段（显示服务器或终端的软件版本），请在参数配置模式下使用 **software-version** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

software-version action {mask | log} [log]

no software-version action {mask | log} [log]

语法说明

log	指定违规情况下的独立或附加日志。
mask	在 SIP 消息中屏蔽软件版本。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何在 SIP 检查策略映射中标识软件版本：

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# software-version action log
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

speed

要设置铜缆 (RJ-45) 以太网接口的速度，请在接口配置模式下使用 **speed** 命令。要将速度设置恢复为默认值，请使用此命令的 **no** 形式。

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

语法说明

10	将速度设置为 10BASE-T。
100	将速度设置为 100BASE-T。
1000	将速度设置为 1000BASE-T。仅适用于铜缆千兆以太网。
auto	自动检测速度。
nonegotiate	对于光纤接口，将速度设置为 1000 Mbps，并且不协商链路参数。此命令和此命令的 **no** 形式是仅有的可用于光纤接口的设置。将该值设置为 **no speed nonegotiate**（默认值）时，接口启用链路协商，以交换流控制参数和远程故障信息。

默认值

对于铜缆接口，默认值为 **speed auto**。

对于光纤接口，默认值为 **no speed nonegotiate**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
接口配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	此命令已从 **interface** 命令的关键字转变为接口配置模式命令。

使用指南

仅设置物理接口上的速度。

如果网络不支持自动检测，则将速度设置为特定值。

对于 ASA 5500 系列上的 RJ-45 接口，默认自动协商设置还包括自动 MDI/MDIX 功能。在自动协商阶段检测到直通电缆时，自动 MDI/MDIX 通过执行内部交叉消除对交叉电缆的需求。必须将速度或双工设置为自动协商以对接口启用自动 MDI/MDIX。如果同时将速度和双工明确设置为固定值，然后禁用这两种设置的自动协商，则也会禁用自动 MDI/MDIX。

如果将 PoE 端口（若可用）上的速度设置为除 **auto** 以外的任何值，则不支持 IEEE 802.3af 的思科 IP 电话和思科无线接入点不会被检测到，也不会被供电。

注　请勿对具有光纤接口的 ASA 5500x 系列或 ASA 5585 设置 **speed** 命令。这样做会导致链路故障。

示例

以下示例将速度设置为 1000BASE-T：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

相关命令

命令	说明
clear configure interface	清除接口的所有配置。
duplex	设置双工模式。
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。
show running-config interface	显示接口配置。

split-dns

要输入将通过拆分隧道解析的域的列表，请在组策略配置模式下使用 **split-dns** 命令。要删除列表，请使用此命令的 **no** 形式。

要删除所有拆分隧道域列表，请使用 **no split-dns** 命令且不带参数。这将删除所有已配置的拆分隧道域列表，包括通过发出 **split-dns none** 命令创建的空列表。

当不存在拆分隧道域列表时，用户将继承默认组策略中存在的任意域列表。要阻止用户继承此类拆分隧道域列表，请使用 **split-dns none** 命令。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

语法说明

value *domain-name*	提供 ASA 通过拆分隧道解析的域名。
none	指示不存在拆分 DNS 列表。设置具有空值的拆分 DNS 列表，从而禁止拆分 DNS 列表。阻止从默认或指定的组策略继承拆分 DNS 列表。

默认值

禁用拆分 DNS。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用单个空格分隔域列表中的各个条目。条目的数量没有限制，但整个字符串不能超过 255 个字符。只能使用字母数字字符、连字符 (-) 和句点 (.)。

使用 **no split-dns** 命令且不带参数时，将删除所有当前值，包括通过发出 **split-dns none** 命令创建的空值。

从版本 3.0.4235 开始，用于 Windows 平台的 AnyConnect 安全移动客户端支持真实拆分 DNS 功能。

示例

以下示例展示如何配置将通过名为 FirstGroup 的组策略的拆分隧道解析的 Domain1、Domain2、Domain3 和 Domain4 域：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

相关命令

命令	说明
default-domain	指定 IPsec 客户端用来进行 DNS 查询的默认域名，这些查询将忽略域字段。
split-dns	提供要通过拆分隧道解析的域列表。
split-tunnel-network-list	标识 ASA 用来区分哪些网络需要隧道化的访问列表。
split-tunnel-policy	让 IPsec 客户端有条件地通过 IPsec 隧道以加密形式传输数据包，或以明文形式将数据包传输到网络接口。

split-horizon

要重新启用 EIGRP 水平拆分，请在接口配置模式下使用 **split-horizon** 命令。要禁用 EIGRP 水平拆分，请使用此命令的 **no** 形式。

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

语法说明

as-number	EIGRP 路由进程的自主系统编号。

默认值

启用 **split-horizon** 命令。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果网络包括 X.25 分组交换网络上的链路，可以使用 **neighbor** 命令使水平拆分功能失效。或者，可以在配置中显式指定 **no split-horizon eigrp** 命令。但如果这样做，必须同样禁用所有路由器的水平拆分，并访问该网络上的任意相关组播组中的服务器。

一般来说，最好不要更改水平拆分的默认状态，除非您确定您的应用需要更改才能正常通告路由。如果在串行接口上禁用水平拆分，并且该接口连接到分组交换网络，则必须禁用所有路由器的水平拆分，并访问该网络上的任意相关组播组中的服务器。

示例

以下示例禁用接口 Ethernet0/0 上的 EIGRP 水平拆分：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no split-horizon eigrp 100
```

相关命令

命令	说明
router eigrp	创建 EIGRP 路由进程并进入配置模式下为此过程。

split-tunnel-all-dns

要使 AnyConnect 安全移动客户端通过 VPN 隧道解析所有 DNS 地址，请在组策略配置模式下使用 **split-tunnel-all-dns** 命令。

要从运行配置中删除该命令，请使用此命令的 **no** 形式。这样可继承其他组策略中的值。

split-tunnel-all-dns {disable | enable}

no split-tunnel-all-dns [{disable | enable}]

语法说明

disable （默认）	AnyConnect 客户端根据拆分隧道策略（隧道化所有网络、隧道化网络列表中指定的网络或排除网络列表中指定的网络）通过隧道发送 DNS 查询。
enable	AnyConnect 客户端通过 VPN 隧道解析所有 DNS 地址。

默认值

默认设置为禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(5)	引入了此命令。

使用指南

split-tunnel-all-dns enable 命令适用于使用 SSL 或 IPsec/IKEv2 协议的 VPN 连接，并指示 AnyConnect 客户端通过 VPN 隧道解析所有 DNS 地址。如果 DNS 解析失败，地址将保持未解析状态，并且 AnyConnect 客户端不会尝试通过公共 DNS 服务器解析该地址。

默认情况下，此功能已禁用。客户端根据拆分隧道策略（隧道化所有网络、隧道化网络列表中指定的网络或排除网络列表中指定的网络）通过隧道发送 DNS 查询。

示例

以下示例将 ASA 配置为使 AnyConnect 客户端通过 VPN 隧道解析所有 DNS 查询：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-all-dns enable
```

相关命令

命令	说明
default-domain	指定传统 IPsec (IKEv1) VPN 客户端或 AnyConnect VPN 客户端 (SSL) 用来进行 DNS 查询的默认域名，这些查询将忽略域字段。
split-dns	提供要通过拆分隧道解析的域列表。
split-tunnel-network-list	确定 ASA 用来区分需要和不需要隧道的网络的访问列表。
split-tunnel-policy	让传统 VPN 客户端 (IPsec/IKEv1) 或 AnyConnect VPN 客户端 (SSL) 有条件地通过隧道以加密形式传输数据包，或以明文形式将数据包传输到网络接口

split-tunnel-network-list

要创建用于拆分隧道的网络列表，请在组策略配置模式下使用 **split-tunnel-network-list** 命令。要删除网络列表，请使用此命令的 **no** 形式。

要删除所有拆分隧道网络列表，请使用 **no split-tunnel-network-list** 命令且不带参数。这将删除所有已配置的网络列表，包括通过发出 **split-tunnel-network-list none** 命令创建的空列表。

当不存在拆分隧道网络列表时，用户将继承默认或指定组策略中存在的任意网络列表。要阻止用户继承此类网络列表，请使用 **split-tunnel-network-list none** 命令。

拆分隧道网络列表会将需要流量通过隧道的网络与不需要隧道化的网络区分开。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

语法说明

none	指示不存在用于拆分隧道的网络列表； ASA 隧道化所有流量。 设置具有空值的拆分隧道网络列表，从而禁止拆分隧道。阻止从默认或指定的组策略继承默认拆分隧道网络列表。
value *access-list name*	标识枚举了要隧道化或不隧道化的网络的访问列表。

默认值

默认情况下，不存在拆分隧道网络列表。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 根据网络列表做出拆分隧道决策，该网络列表是包含专用网络地址列表的标准 ACL。

使用 **no split-tunnel-network-list** 命令且不带参数时，将删除所有当前网络列表，包括通过发出 **split-tunnel-network-list none** 命令创建的空值。

注　ASA 提供对 200 个拆分网络的支持。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置名为 FirstList 的网络列表：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-network-list FirstList
```

相关命令

命令	说明
access-list	创建访问列表，或使用可下载访问列表。
default-domain	指定 IPsec 客户端用来进行 DNS 查询的默认域名，这些查询将忽略域字段。
split-dns	提供要通过拆分隧道解析的域列表。
split-tunnel-policy	让 IPsec 客户端有条件地通过 IPsec 隧道以加密形式传输数据包，或以明文形式将数据包传输到网络接口。

split-tunnel-policy

要设置拆分隧道策略，请在组策略配置模式下使用 **split-tunnel-policy** 命令。要从运行配置中删除 split-tunnel-policy 属性，请使用此命令的 **no** 形式。

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

语法说明

excludespecified	定义流量可不受阻碍进入的网络的列表。对于想要访问本地网络上的设备（如打印机），而通过隧道连接到公司网络的用户来说，此功能非常有用。
split-tunnel-policy	指示您正在设置隧道流量的规则。
tunnelall	指定没有流量可以不受阻碍地进入或到达 ASA 以外的任何其他目的地。远程用户通过公司网络访问互联网，没有访问本地网络的权限。
tunnelspecified	将所有来自或流向指定网络的流量隧道化。此选项启用分割隧道。可以让您创建要隧道化的地址的网络列表。数据不受阻碍地传送到所有其他地址，并由远程用户的互联网运营商进行路由。

默认值

默认情况下禁用拆分隧道，即 **tunnelall**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

拆分隧道主要是一个流量管理功能，而不是安全功能。事实上，为获得最优安全性，建议不要启用拆分隧道。

这允许从其他组策略继承拆分隧道的值。

拆分隧道可以让远程访问 VPN 客户端有条件地通过 IPsec 或 SSL 隧道以加密形式传输数据包，或以明文形式将数据包传输到网络接口。启用拆分隧道时，若数据包不以另一侧 IPsec 或 SSL VPN 隧道终端为目的地，则不必加密、通过隧道发送、解密以及路由到最终目的地。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置仅指定隧道的网络的分割隧道策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
```

相关命令

命令	说明
default-domain	指定 IPsec 客户端用来进行 DNS 查询的默认域名，这些查询将忽略域字段。
split-dns	提供要通过拆分隧道解析的域列表。
split-tunnel-network-list none	指示不存在用于分割隧道的访问列表。所有流量均通过隧道传输。
split-tunnel-network-list value	确定 ASA 用来区分需要和不需要隧道的网络的访问列表。

spoof-server

要替代 HTTP 协议检查的服务器报头字段的字符串，请在参数配置模式下使用 **spoof-server** 命令。要禁用此功能，请使用此命令的 **no** 形式。

spoof-server *string*

no spoof-server *string*

语法说明

string	用于替代服务器报头字段的字符串。最多 82 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

WebVPN 流不受 **spoof-server** 命令影响。

示例

以下示例展示如何替代 HTTP 检查策略映射中的服务器报头字段的字符串：

```
ciscoasa(config-pmap-p)# spoof-server string
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

sq-period

要指定 NAC 框架会话中每个成功的安全状态验证与下次查询主机状态更改的间隔时间，请在 nac-policy-nac-framework 配置模式下使用 **sq-period** 命令。要从 NAC 策略中删除该命令，请使用此命令的 **no** 形式。

sq-period *seconds*

no sq-period [*seconds*]

语法说明

seconds	每个成功安全状态验证之间的秒数。范围是 30 到 1800。

默认值

默认值为 300。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Nac-policy-nac-framework 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.3(0)	“nac-” 从命令名称中删除。命令在组策略配置模式下移到 nac- 策略 -nac- 框架配置模式。
7.2(1)	引入了此命令。

使用指南

在每个成功的安全状态验证和状态查询响应后，ASA 会启动状态查询计时器。此计时器到期将触发对主机状态变化的查询，称为*状态查询*。

示例

以下示例将状态查询计时器的值更改为 1800 秒：

```
ciscoasa(config-nac-policy-nac-framework)# sq-period 1800
ciscoasa(config-nac-policy-nac-framework)
```

以下示例从 NAC 框架策略中删除状态查询计时器：

```
ciscoasa(config-nac-policy-nac-framework)# no sq-period
ciscoasa(config-nac-policy-nac-framework)
```

相关命令

命令	说明
nac-policy	创建和访问 Cisco NAC 策略，并指定其类型。
nac-settings	将 NAC 策略分配到组策略。
eou timeout	更改将 EAP 通过 UDP 消息发送到 NAC 框架配置中的远程主机后等待秒的数。
reval-period	指定 NAC 框架会话中每次成功安全状态验证之间的时间间隔。
debug eap	启用对可扩展身份验证协议事件的记录以调试 NAC 框架消息。

ssh

要添加对 ASA 的 SSH 访问权限，请在全局配置模式下使用 **ssh** 命令。要禁止对 ASA 的 SSH 访问，请使用此命令的 **no** 形式。

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

语法说明

interface	启用 SSH 的 ASA 接口。如果未指定，将在除外部接口之外的所有接口上启用 SSH。
ip_address	已被授权向 ASA 发起 SSH 连接的主机或网络的 IPv4 地址。对于主机，也可以输入主机名。
ipv6_address/*prefix*	已被授权向 ASA 发起 SSH 连接的主机或网络的 IPv6 地址和前缀。
mask	*ip_address* 的网络掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令支持 IPv4 和 IPv6 地址。**ssh** *ip_address* 命令指定已被授权向 ASA 发起 SSH 连接的主机或网络。配置中可以有多个 ssh 命令。该命令的 **no** 形式可从配置中删除特定 SSH 命令。使用 **clear configure ssh** 命令可删除所有 SSH 命令。

在可以开始使用 SSH 连接到 ASA 之前，必须使用 **crypto key generate rsa** 命令生成默认 RSA 密钥。

ASA 支持以下安全算法和密码：

- 3DES 和 AES 密码，用于数据加密
- HMAC-SHA 和 HMAC-MD5 算法，用于确保数据包完整性
- RSA 公共密钥算法，用于主机身份验证

ASA 不支持以下 SSH 版本 2 功能：

- X11 转发
- 端口转发

- SFTP 支持
- Kerberos 和 AFS 票证传递
- 数据压缩

示例

以下示例展示如何将内部接口配置为接受来自 IP 地址为 10.1.1.1 的管理控制台的 SSH 版本 2 连接。空闲会话超时设置为 60 分钟，并启用 SCP。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
crypto key generate rsa	生成身份证书的 RSA 密钥对。
debug ssh	显示 SSH 命令的调试信息和错误消息。
show running-config ssh	显示运行配置中的当前 SSH 命令。
ssh scopy enable	在 ASA 上启用安全复制服务器。
ssh version	限制 ASA 使用 SSH 版本 1 或 SSH 版本 2。

ssh authentication

要启用每个用户的公共密钥身份验证，请在用户名属性模式下使用 **ssh authentication** 命令。要禁用每个用户的公共密钥身份验证，请使用此命令的 **no** 形式。

ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

no ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

语法说明

hashed	通过 SHA-256 进行哈希处理，32 字节长，各个字节间用冒号分隔（用于解析目的）。
key	*key* 参数的值可以是以下值之一： • 当提供 *key* 参数并且未指定哈希标记时，密钥的值必须是由可生成 SSH-RSA 原始密钥（即，不带证书）的 SSH 密钥生成软件所生成的 Base64 编码公共密钥。在提交 Base64 编码的公共密钥之后，该密钥通过 SHA-256 进行哈希处理，相应的 32 字节哈希用于所有进一步比较。 • 当提供 *key* 参数并且指定哈希标记时，密钥的值必须先前已通过 SHA-256 进行哈希处理并且为 32 字节长，各个字节间用冒号分隔（用于解析目的）。
nointeractive	**nointeractive** 选项用于抑制当导入 SSH 公共密钥文件格式的密钥时出现的所有提示。此非交互式数据输入模式仅供 ASDM 使用。
pkf	对于 **pkf** 密钥，系统将提示您粘贴 PKF 格式的密钥，最长 4096 位。此格式用于由于过大而无法以 Base64 格式内嵌粘贴的密钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF，并使用 **pkf** 关键字作为密钥提示。 **注**　可以将 **pkf** 选项与故障切换一起使用，但 PKF 密钥不会自动复制到备用系统。必须输入 **write standby** 命令才能同步 PKF 密钥。
publickey	对于 **publickey**，*key* 是 Base64 编码的公共密钥。可以使用任何可生成 SSH-RSA 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成密钥。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户名属性	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

可以指定公共密钥文件 (PKF) 格式的密钥（**pkf** 关键字）或 Base64 密钥（**publickey** 关键字）。

key 字段和 **hashed** 关键字仅对 **publickey** 选项可用，而 **nointeractive** 关键字仅对 **pkf** 选项可用。

当保存配置后，哈希密钥值将保存到配置，ASA 重新启动时将使用该值。

当在 ASA 上使用 **show running-config username** 命令查看密钥时，密钥使用 SHA-256 哈希加密。即使您输入 **pkf** 形式的密钥，ASA 也会对密钥进行哈希处理，并将其显示为哈希的 **publickey**。如果您需要从 **show** 输出复制密钥，请使用 **hashed** 关键字指定 **publickey** 类型。

示例

以下示例展示如何使用 PKF 格式的密钥进行身份验证：

```
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
debug ssh	显示 SSH 命令的调试信息和错误消息。
show running-config ssh	显示运行配置中的当前 SSH 命令。
ssh version	限制 ASA 使用 SSH 版本 1 或 SSH 版本 2。

ssh disconnect

要断开活动 SSH 会话，请在特权 EXEC 模式下使用 **ssh disconnect** 命令。

ssh disconnect *session_id*

语法说明

session_id	断开通过 ID 编号指定的 SSH 会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须指定会话 ID。使用 **show ssh sessions** 命令可获取要断开的 SSH 会话的 ID。

示例

以下示例展示要断开的 SSH 的会话：

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
ciscoasa# ssh disconnect 2
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

相关命令

命令	说明
show ssh sessions	显示有关 ASA 的活动 SSH 会话的信息。
ssh timeout	设置空闲 SSH 会话的超时值。

ssh key-exchange

要使用 Diffie-Hellman (DH) 组 1 或 DH 组 14 密钥交换方法交换密钥，请在全局配置模式下使用 **ssh key-exchange** 命令。要禁止使用 DH 组 1 或 DH 组 14 密钥交换方法进行密钥交换，请使用此命令的 **no** 形式。

ssh key-exchange group {dh-group1 | dh-group14} sha1

no ssh key-exchange group {dh-group1 | dh-group14} sha1

语法说明

dh-group1	指示将遵循 DH 组 1 密钥交换方法并应在交换密钥时使用该方法。由于历史遗留原因，DH 组 2 称为 DH 组 1。
dh-group14	指示将遵循 DH 组 14 密钥交换方法并应在交换密钥时使用该方法。
group	指示将遵循 DH 组 1 密钥交换方法或 DH 组 14 密钥交换方法并应在交换密钥时使用该方法。
key-exchange	指示将遵循 DH 组 1 或 DH 组 14 密钥交换方法并应在交换密钥时使用该方法。
sha-1	指定应使用 SHA-1 加密算法。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(4)	引入了此命令。
9.1(2)	此命令更改为 **ssh key-exchange group dh-group1-sha1**。

使用指南

在可以开始使用 SSH 连接到 ASA 之前，必须使用 **crypto key generate rsa** 命令生成默认 RSA 密钥。

ASA 支持使用 DH 组 1 和组 14 密钥交换方法进行密钥交换。如果未指定 DH 组密钥交换方法，则使用 DH 组 1 密钥交换方法。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

注　此命令在 9.1(1) 或 9.1.1(2) 版本中不可用。

示例

以下示例展示如何使用 DH 组 14 密钥交换方法交换密钥：

```
ciscoasa(config)# ssh key-exchange dh-group-1-sha1
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
crypto key generate rsa	生成身份证书的 RSA 密钥对。
debug ssh	显示 SSH 命令的调试信息和错误消息。
show running-config ssh	显示运行配置中的当前 SSH 命令。
ssh scopy enable	在 ASA 上启用安全复制服务器。
ssh version	限制 ASA 使用 SSH 版本 1 或 SSH 版本 2。

ssh pubkey-chain

要在 ASA 数据库中手动添加或删除自注册安全复制 (SCP) 客户端的 SSH 服务器及其密钥，请在全局配置模式下使用 **ssh pubkey-chain** 命令。要删除所有主机密钥，请使用此命令的 **no** 形式。要仅删除单个服务器密钥，请参阅 **server** 命令。

ssh pubkey-chain

no ssh pubkey-chain

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.1(5)	我们引入了此命令。

使用指南

可以使用自注册 SCP 客户端将文件复制到 ASA 或者从其中复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如有需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器（请参阅 **server** 命令），都可以指定 SSH 主机的 **key-string**（公共密钥）或 **key-hash**（哈希值）。

示例

以下示例为 10.86.94.170 上的服务器添加经过哈希处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

相关命令

命令	说明
copy	将文件复制到 ASA 或者从其中复制文件。
key-hash	输入哈希 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
server	向 ASA 数据库添加 SSH 服务器和主机密钥。
ssh stricthostkeycheck	为自注册安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

ssh scopy enable

要在 ASA 上启用安全复制 (SCP)，请在全局配置模式下使用 **ssh scopy enable** 命令。要禁用 SCP，请使用此命令的 **no** 形式。

ssh scopy enable

no ssh scopy enable

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

SCP 仅在服务器进行实施；它能够接受和终止 SCP 的连接，但不能发起连接。ASA 具有以下限制：

- 此 SCP 实施中不提供目录支持，因而限制了对 ASA 内部文件的远程客户端访问。
- 使用 SCP 时没有标语支持。
- SCP 不支持通配符。
- ASA 许可证必须具有 VPN-3DES-AES 功能才能支持 SSH 版本 2 连接。

在启动文件传输之前，ASA 会检查可用闪存。如果没有足够的可用空间，ASA 将终止 SCP 连接。如果要覆盖闪存中的文件，您仍需要有足够的可用空间以保存将复制到 ASA 的文件。SCP 过程会先将文件复制到临时文件，然后用临时文件覆盖要替换的文件。如果闪存中没有足够的空间保存要复制的文件和要覆盖的文件，ASA 将终止 SCP 连接。

示例

以下示例展示如何将内部接口配置为接受来自 IP 地址为 10.1.1.1 的管理控制台的 SSH 版本 2 连接。空闲会话超时设置为 60 分钟，并启用 SCP。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
debug ssh	显示 SSH 命令的调试信息和错误消息。
show running-config ssh	显示运行配置中的当前 SSH 命令。
ssh	允许从指定的客户端或网络到 ASA 的 SSH 连接。
ssh version	限制 ASA 使用 SSH 版本 1 或 SSH 版本 2。

ssh stricthostkeycheck

要启用自注册安全复制 (SCP) 客户端的 SSH 主机密钥检查，请在全局配置模式下使用 **ssh stricthostkeycheck** 命令。要禁用主机密钥检查，请使用此命令的 **no** 形式。

ssh stricthostkeycheck

no ssh stricthostkeycheck

语法说明

此命令没有任何参数或关键字。

命令默认

默认情况下，此命令已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.1(5)	我们引入了此命令。

使用指南

可以使用自注册 SCP 客户端将文件复制到 ASA 或者从其中复制文件。当启用此选项时，如果 ASA 中尚未存储主机密钥，系统会提示您接受或拒绝主机密钥。当禁用此选项时，如果以前未存储过主机密钥，ASA 会自动接受主机密钥。

示例

以下示例启用 SSH 主机密钥检查：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)?yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []?cisco123

Destination filename [x]?
```

相关命令

命令	说明
copy	将文件复制到 ASA 或者从其中复制文件。
key-hash	输入哈希 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
server	向 ASA 数据库添加 SSH 服务器和主机密钥。
ssh pubkey-chain	在 ASA 数据库中手动添加或删除服务器及其密钥。

ssh timeout

要更改默认 SSH 会话空闲超时值，请在全局配置模式下使用 **ssh timeout** 命令。要恢复默认超时值，请使用此命令的 **no** 形式。

ssh timeout *number*

no ssh timeout

语法说明

number	指定 SSH 会话在断开前可以保持非活动状态的持续时间（以分钟为单位）。有效值为 1 到 60 分钟。

默认值

默认会话超时值为 5 分钟。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ssh timeout 命令指定会话在断开前可以保持空闲状态的持续时间（以分钟为单位）。默认持续时间为 5 分钟。

示例

以下示例展示如何将内部接口配置为仅接受来自 IP 地址为 10.1.1.1 的管理控制台的 SSH 版本 2 连接。空闲会话超时设置为 60 分钟，并启用 SCP。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
show running-config ssh	显示运行配置中的当前 SSH 命令。
show ssh sessions	显示有关 ASA 的活动 SSH 会话的信息。
ssh disconnect	断开活动的 SSH 会话。

ssh version

要限制 ASA 接受的 SSH 版本，请在全局配置模式下使用 **ssh version** 命令。要恢复默认值，请使用此命令的 **no** 形式。默认值允许与 ASA 建立 SSH 版本 1 和 SSH 版本 2 连接。

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

语法说明

1	指定仅支持 SSH 版本 1 连接。
2	指定仅支持 SSH 版本 2 连接。

默认值

默认情况下，SSH 版本 1 和 SSH 版本 2 均受支持。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

1 和 2 指定限制 ASA 使用 SSH 的哪个版本。该命令的 **no** 形式会将 ASA 恢复为默认状态，即兼容模式（两个版本均可使用）。

示例

以下示例展示如何将内部接口配置为接受来自 IP 地址为 10.1.1.1 的管理控制台的 SSH 版本 2 连接。空闲会话超时设置为 60 分钟，并启用 SCP。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

相关命令

命令	说明
clear configure ssh	清除运行配置中的所有 SSH 命令。
debug ssh	显示 SSH 命令的调试信息和错误消息。
show running-config ssh	显示运行配置中的当前 SSH 命令。
ssh	允许从指定的客户端或网络到 ASA 的 SSH 连接。

ssl certificate-authentication

要启用客户端证书身份验证以向后兼容 8.2(1) 之前的版本，请在全局配置模式下使用 **ssl certificate-authentication** 命令。要禁用 ssl 证书身份验证，请使用此命令的 **no** 形式。

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-number*

语法说明

interface-name	所选接口的名称，如 inside、management 和 outside。
port-number	TCP 端口号，在 1 到 65535 范围内的整数。

默认值

默认禁用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
8.0(3)	引入了此命令。
8.2(1)	此命令不再需要，但 ASA 会保留该命令以便降级到以前的版本。

使用指南

此命令替换已废弃的 **http authentication-certificate** 命令。

示例

以下示例展示如何将 ASA 配置为使用 SSL 证书身份验证功能：

```
ciscoasa(config)# ssl certificate-authentication interface inside port 330
```

相关命令

命令	说明
show running-config ssl	显示当前配置的 SSL 命令集。

ssl cipher

要指定 SSL、DTLS 和 TLS 协议的加密算法，请在全局配置模式下使用 **ssl cipher** 命令。要恢复默认设置（即一组完整的加密算法），请使用此命令的 **no** 形式。

ssl cipher *version* [*level* | **custom** "*string*"]

no ssl cipher *version* [*level* | **custom** "*string*"]

语法说明

custom *string*	允许使用 OpenSSL 密码定义字符串完全控制密码套件。
level	指定密码的强度并指示所支持的最低密码级别。有效值（按强度的升序排列）如下： • **all** - 包括所有密码，其中包括 NULL-SHA。 • **low** - 包括除 NULL-SHA 以外的所有密码。 • **medium** - 包括除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 以外的所有密码。 • **fips** - 包括所有符合 FIPS 的密码（不包括 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA）。 • **high**（仅适用于 TLSv1.2 ）- 仅包括使用 SHA-2 密码的 AES-256。
version	指定 SSL、DTLS 或 TLS 协议版本。支持的版本包括： • **default** - 用于出站连接的密码集。 • **dtlsv1** - 用于 DTLSv1 入站连接的密码。 • **sslv3** - 用于 SSLv3 入站连接的密码。 • **tlsv1** - 用于 TLSv1 入站连接的密码。 • **tlsv1.1** - 用于 TLSv1.1 入站连接的密码。 • **tlsv1.2** - 用于 TLSv1.2 入站连接的密码。

默认值

所有协议版本的默认值均为 **medium**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

从 ASA 版本 9.3(2) 开始，此命令替换了 **ssl encryption** 命令。

建议的设置为 **medium**。使用 **high** 可能会限制连接。如果仅配置了几个密码，使用 **custom** 可能会限制功能。限制默认定制值会限制出站连接，包括集群。

有关使用 OpenSSL 的密码的详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html。

使用 **show ssl ciphers all** 命令可查看哪些密码支持哪些版本的列表。例如：

```
These are the ciphers for the given cipher level; not all ciphers are supported by all
versions of SSL/TLS.
These names can be used to create a custom cipher list:
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (sslv3, tlsv1)
  RC4-MD5 (sslv3, tlsv1)
  DES-CBC-SHA (sslv3, tlsv1)
  NULL-SHA (sslv3, tlsv1)
```

ASA 将支持的密码的优先级顺序指定为：

TLSv1.2 (1-9) 支持的密码

1. DHE-RSA-AES256-SHA256
2. AES256-SHA256
3. DHE-RSA-AES128-SHA256
4. AES128-SHA256
5. DHE-RSA-AES256-SHA
6. AES256-SHA
7. DHE-RSA-AES128-SHA
8. AES128-SHA
9. DES-CBC3-SHA

TLSv1.1 或 TLSv1.2 (10-13) 不支持的密码

10. RC4-SHA
11. RC4-MD5
12. DES-CBC-SHA
13. NULL-SHA

示例

以下示例展示如何将 ASA 配置为使用符合 FIPS 的 TLSv1.1 密码：

```
ciscoasa(config)# ssl cipher tlsv1.1 fips
```

以下示例展示如何将 ASA 配置为使用 SSLv3 定制密码：

```
ciscoasa(config)# ssl cipher sslv3 custom "RC4:ALL:!DH"
```

以下示例展示如何将 ASA 配置为使用 TLSv1 定制密码：

```
ciscoasa(config)# ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

相关命令

命令	说明
show running-config ssl	显示当前配置的 SSL 命令集。
show ssl ciphers	显示所支持密码的列表。

ssl client-version

要指定 ASA 在用作客户端时所使用的 SSL/TLS 协议版本，请在全局配置模式下使用 **ssl client-version** 命令。要恢复为默认值，请使用此命令的 **no** 形式。

ssl client-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]

no ssl client-version

语法说明

any	发送 SSLv3 客户端问候并协商 SSLv3 （或更高版本）。
sslv3	发送 SSLv3 客户端问候并协商 SSLv3 （或更高版本）。
sslv3-only	发送 SSLv3 客户端问候并协商 SSLv3 （或更高版本）。 **注**　此选项自版本 9.3(2) 起已废弃。
tlsv1	发送 TLSv1 客户端问候并协商 TLSv1 （或更高版本）。
tlsv1.1	发送 TLSv1.1 客户端问候并协商 TLSv1.1 （或更高版本）。
tlsv1.2	发送 TLSv1.2 客户端问候并协商 TLSv1.2 （或更高版本）。
tlsv1-only	发送 TLSv1 客户端问候并协商 TLSv1 （或更高版本）。 **注**　此选项自版本 9.3(2) 起已废弃。

默认值

默认值为 **tlsv1**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(2)	SSLv3 已废弃。默认值现在为 **tlsv1** 而不是 **any**。**any** 关键字已废弃。

使用指南

如果使用 **any**、**sslv3** 或 **sslv3-only** 关键字，命令会被接受，但会显示以下警告。

```
WARNING: SSLv3 is deprecated.Use of TLSv1 or greater is recommended.
```

在下一个主要 ASA 版本中，这些关键字将从 ASA 中删除。

示例

以下示例展示如何将 ASA 配置为在用作 SSL 客户端时指定 SSLv3 协议版本：

```
ciscoasa(config)# ssl client-version any
```

相关命令

命令	说明
clear config ssl	从配置中删除所有 SSL 命令，从而恢复为默认值。
ssl encryption	指定 SSL/TLS 协议使用的加密算法。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl server-version	指定 ASA 将协商 SSL/TLS 连接的最低协议版本。
ssl trust-point	指定表示接口的 SSL 证书的证书信任点。

ssl dh-group

要指定将与 TLS 所使用的 DHE-RSA 密码一起使用的 Diffie-Hellmann (DH) 组，请在全局配置模式下使用 **ssl dh-group** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

no ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

语法说明

group1	配置 DH 组 1（768 位模数）。
group2	配置 DH 组 2（1024 位模数）。
group5	配置 DH 组 5（1536 位模数）。
group14	配置 DH 组 14（2048 位模数，224 位素数阶子组）。
group24	配置 DH 组 24（2048 位模数，256 位素数阶子组）。

默认值

默认值为 DH 组 2。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

组 1 和 2 与 Java 7 及更早版本兼容。组 5、14 和 24 与 Java 7 不兼容。所有组均与 Java 8 兼容。组 14 和 24 符合 FIPS。

示例

以下示例展示如何将 ASA 配置为使用特定 DH 组：

```
ciscoasa(config)# ssl dh-group group14
```

相关命令

命令	说明
show running-config ssl	显示当前配置的 SSL 命令集。

ssl encryption（已废弃）

注　支持此命令的最后一个版本是版本 9.3(1)。

要为 SSL、DTLS 和 TLS 协议指定加密算法，请在全局配置模式下使用 **ssl encryption** 命令。要恢复默认设置（即一组完整的加密算法），请使用此命令的 **no** 形式。

ssl encryption [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] [**dhe-aes256-sha1**] [**dhe-aes128-sha1**]

no ssl encryption

语法说明

3des-sha1	指定采用安全哈希算法 1 的三重 DES 168 位加密（符合 FIPS）。
aes128-sha1	指定使用 安全哈希算法 1（符合 FIPS）的三重 AES 128 位加密。
aes256-sha1	指定使用 安全哈希算法 1（符合 FIPS）的三重 AES 256 位加密。
dhe-aes128-sha1	指定用于传输层安全 (TLS) 的 AES 128 位加密密码套件（符合 FIPS）。
dhe-aes256-sha1	指定用于传输层安全 (TLS) 的 AES 256 位加密密码套件（符合 FIPS）。
des-sha1	指定采用安全哈希算法 1 的 DES 56 位加密。
null-sha1	指定采用安全哈希算法 1 的空加密。此设置实施消息完整性，不实施机密性。 **注意事项**　如果指定 **null-sha1**，则数据不加密。
rc4-md5	指定具有 MD5 哈希功能的 RC4 128 位加密。
rc4-sha1	指定采用安全哈希算法 1 的 RC4 128 位加密。

默认值

默认情况下，ASA 上的 SSL 加密列表包含按以下顺序排列的算法：

1. RC4-SHA1
2. AES128-SHA1（符合 FIPS）
3. AES256-SHA1（符合 FIPS）
4. 3DES-SHA1（符合 FIPS）
5. DHE-AES256-SHA1（符合 FIPS）
6. DHE-AES128-SHA1（符合 FIPS）

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.1(2)	增加了对使用 DHE-AES128-SHA1 和 DHE-AES256-SHA1 算法的 SSL 加密的支持。
9.3(2)	此命令已废弃并已被 **ssl cipher** 命令取代。

使用指南

再次发出该命令将覆盖以前的设置。ASDM License（ASDM 许可证）选项卡反映了许可证支持的最大加密，而不是您配置的值。

算法的排序决定了它们的使用优先权。您可以添加或删除算法以满足您的环境的需求。

对于符合 FIPS 的 AnyConnect 客户端 SSL 连接，必须确保符合 FIPS 的密码是 SSL 加密列表中指定的第一个密码。

一些应用不支持 DHE，因此请包括至少一种其他 SSL 加密方法以确保密码套件在两种情况下均可使用。

加密操作使用了对称密钥算法，请参阅 http://en.wikipedia.org/wiki/Symmetric-key_algorithm。

示例

以下示例展示如何将 ASA 配置为使用 3des-sha1 和 des-sha1 加密算法：

```
ciscoasa(config)# ssl encryption 3des-sha1 des-sha1
```

从 ASA 版本 9.3(2) 开始

以下示例展示此命令已废弃并已被 **ssl cipher** 命令取代：

```
ciscoasa(config)# ssl encryption ?

configure mode commands/options:
This command is DEPRECATED, use 'ssl cipher' instead.

  3des-sha1         Indicate use of 3des-sha1 for ssl encryption
  aes128-sha1       Indicate use of aes128-sha1 for ssl encryption
  aes256-sha1       Indicate use of aes256-sha1 for ssl encryption
  des-sha1          Indicate use of des-sha1 for ssl encryption
  dhe-aes128-sha1   Indicate use of dhe-aes128-sha1 for ssl encryption
  dhe-aes256-sha1   Indicate use of dhe-aes256-sha1 for ssl encryption
  null-sha1         Indicate use of null-sha1 for ssl encryption (NOTE: Data is
                    NOT encrypted if this cipher is chosen)
  rc4-md5           Indicate use of rc4-md5 for ssl encryption
  rc4-sha1          Indicate use of rc4-sha1 for ssl encryption

ciscoasa(config)# ssl encryption rc4-sha1 aes256-sha1 aes128-sha1

WARNING: This command has been deprecated; use 'ssl cipher' instead.
INFO: Converting to: ssl cipher default custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher sslv3 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher tlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher dtlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
```

相关命令

命令	说明
clear config ssl	从配置中删除所有 SSL 命令，从而恢复为默认值。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl client-version	指定 ASA 用作客户端时所使用的 SSL/TLS 协议版本。
ssl server-version	指定 ASA 将协商 SSL/TLS 连接的最低协议版本。
ssl trust-point	指定表示接口的 SSL 证书的证书信任点。
ssl cipher	指定 SSL、DTLS 和 TLS 协议的加密算法。 **注**　自 9.3(2) 版本起可用。

ssl server-version

要设置 ASA 将协商 SSL/TLS 连接的最低协议版本，请在全局配置模式下使用 **ssl server-version** 命令。要恢复为默认值 any，请使用此命令的 **no** 形式。

ssl server-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]

no ssl server-version

语法说明

any	接受 SSLv2 客户端问候并协商最高通用版本。
sslv3	接受 SSLv2 客户端问候并协商 SSLv3（或更高版本）。
sslv3-only	接受 SSLv2 客户端问候并协商 SSLv3（或更高版本）。 **注**　此选项自版本 9.3(2) 起已废弃。
tlsv1	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。
tlsv1.1	接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。
tlsv1.2	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。
tlsv1-only	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。 **注**　此选项自版本 9.3(2) 起已废弃。

默认值

默认值为 **tlsv1**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(2)	SSLv3 已废弃。默认值现在为 **tlsv1** 而不是 **any**。**any** 关键字已废弃。

使用指南

如果使用 **any**、**sslv3** 或 **sslv3-only** 关键字，命令会被接受，但会显示以下警告。

```
WARNING: SSLv3 is deprecated.Use of TLSv1 or greater is recommended.
```

在下一个主要 ASA 版本中，这些关键字将从 ASA 中删除。

示例

以下示例展示如何将 ASA 配置为协商 SSL/TLS 连接：

```
ciscoasa(config)# ssl server-version tlsv1
```

相关命令

命令	说明
clear config ssl	从配置中删除所有 SSL 命令，从而恢复为默认值。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl client-version	指定 ASA 用作客户端时所使用的 SSL/TLS 协议版本。
ssl encryption	指定 SSL/TLS 协议使用的加密算法。
ssl trust-point	指定表示接口的 SSL 证书的证书信任点。

ssl trust-point

要指定表示接口的 SSL 证书的证书信任点，请在全局配置模式下使用带 *interface* 参数的 **ssl trust-point** 命令。要从未指定接口的配置中删除 SSL 信任点，请使用此命令的 **no** 形式。要删除指定了接口的条目，请使用此命令的 **no ssl trust-point** *name* [*interface*] 形式。

ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

no ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

语法说明

domain *domain-name*	将此信任点与用于访问此接口的特定域名（例如，www.cisco.com）相关联。
interface	指定信任点应用到的接口的名称。**nameif** 命令定义接口的名称。
name	根据 **crypto ca trustpoint** *name* 命令中的配置指定 CA 信任点的名称。
vpnlb-ip	将此信任点与此接口上的 VPN 负载平衡集群 IP 地址相关联。仅应用于接口。

默认值

默认情况下没有信任点关联。ASA 使用默认的自生成 RSA 密钥对证书。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(2)	增加了 **domain** *domain-name* 关键字参数对。

使用指南

如果不指定接口或域，则此条目将表示所有未与各自信任点关联的接口上使用的回退信任点。

如果输入 **ssl trustpoint ?** 命令，则显示可用的已配置信任点。如果输入 **ssl trust-point** *name* **?** 命令（例如，**ssl trust-point mysslcert ?**），则显示信任点 SSL 证书关联的可用已配置接口。

最多可为每个接口配置 16 个信任点。

使用此命令时请遵守以下准则：

- *trustpoint* 的值必须是 **crypto ca trustpoint** *name* 命令中配置的 CA 信任点的名称。
- *interface* 的值必须是之前配置的接口的 *nameif* 名称。
- 删除信任点也会删除引用该信任点的任何 **ssl trust-point** 条目。
- 您可以为每个接口指定一个 **ssl trust-point** 条目，还可以指定一个不指定接口的条目。
- 一个配置了 **domain** 关键字的信任点可应用于多个接口（取决于连接方式）。

- 每个 *domain-name* 值只能有一个 **ssl trust-point**。
- 可以将同一信任点重复用于多个条目。
- 如果在输入此命令后显示以下错误：

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

  表示用户已配置新证书来替换先前配置的证书。No action is required.

- 证书按以下顺序选择：
  - 如果连接与 **domain** 关键字的值匹配，则首选该证书。（**ssl trust-point** *name* **domain** *domain-name* 命令）
  - 如果与负载平衡地址建立连接，则选择 vpnlb-ip 证书。（**ssl trust-point** *name* **interface vpnlb-ip** 命令）
  - 为接口配置的证书。（**ssl trust-point** *name* **interface** 命令）
  - 未与接口关联的默认证书。（**ssl trust-point** *name* 命令）
  - ASA 的自签、自生成证书。

示例

以下示例展示如何为内部接口配置一个名为 FirstTrust 的 SSL 信任点，以及如何配置一个名为 DefaultTrust 且未关联任何接口的信任点。

```
ciscoasa(config)# ssl trust-point FirstTrust inside
ciscoasa(config)# ssl trust-point DefaultTrust
```

以下示例展示如何使用该命令的 **no** 形式删除未关联任何接口的信任点：

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

以下示例展示如何删除已关联接口的信任点：

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point FirstTrust inside
ciscoasa(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

以下示例展示如何为已配置的信任点分配特定域名：

```
ciscoasa(config)# ssl trust-point www-cert domain www.example.com
```

相关命令

命令	说明
clear config ssl	从配置中删除所有 SSL 命令，从而恢复为默认值。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl client-version	指定 ASA 用作客户端时所使用的 SSL/TLS 协议版本。
ssl encryption	指定 SSL/TLS 协议使用的加密算法。

命令	说明
ssl server-version	指定 ASA 将协商 SSL/TLS 连接的最低协议版本。
show ssl	显示 SSL 配置统计信息。

sso-server

要创建用于 ASA 用户身份验证的单点登录 (SSO) 服务器，请在 webvpn 配置模式下使用 **sso-server** 命令 。使用此命令时，必须指定 SSO 服务器类型。

要删除 SSO 服务器，请使用此命令的 **no** 形式。

sso-server *name* **type [***siteminder* | *saml-v1.1-post* **]**

no sso-server *name*

注　SSO 身份验证需要此命令。

语法说明

name	指定 SSO 服务器的名称。最少 4 个字符，最多 31 个字符。
saml-v1.1-post	指定要配置的 ASA SSO 服务器是 SAML、版本 1.1、POST 类型的 SSO 服务器。
siteminder	指定要配置的 ASA SSO 服务器是 Computer Associates SiteMinder SSO 服务器。
type	指定 SSO 服务器的类型。SiteMinder 和 SAML-V1.1-POST 是仅有的可用类型。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。**sso-server** 命令可用于创建 SSO 服务器。

在身份验证中，ASA 充当 WebVPN 用户登录 SSO 服务器的代理。ASA 当前支持 SiteMinder SSO 服务器（以前称为 Netegrity SiteMinder ）和 SAML POST 类型 SSO 服务器。当前，类型选项的可用参数限制为 *siteminder* 或 *saml-V1.1-post*。

示例

以下示例在 webvpn 配置模式下输入，创建一个名为 “example1” 的 SiteMinder 类型的 SSO 服务器：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example1 type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
```

以下示例在 webvpn 配置模式下输入，创建一个名为 “example2” 的 SAML、版本 1.1、POST 类型的 SSO 服务器：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example2 type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml)#
```

相关命令

命令	说明
assertion-consumer-url	标识 SAML 类型 SSO 声明消费者服务的 URL。
issuer	指定 SAML 类型 SSO 服务器的安全设备名称。
max-retry-attempts	配置 ASA SSO 身份验证尝试失败后的重试次数。
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示 SSO 服务器的运行统计信息。
test sso-server	测试与试用身份验证请求 SSO 服务器。
trustpoint	指定包含要用于签署 SAML 类型浏览器声明的证书的信任点名称。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

sso-server value (group-policy webvpn)

要为组策略分配 SSO 服务器，请在组策略配置模式中可用的 webvpn 配置模式下使用 **sso-server value** 命令。

要删除分配并使用默认策略，请使用此命令的 **no** 形式。

要防止继承默认策略，请使用 **sso-server none** 命令。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

语法说明

name	指定将分配给组策略的 SSO 服务器的名称。

默认值

分配给组的默认策略为 DfltGrpPolicy。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

在组策略 webvpn 模式下输入 **sso-server value** 命令可为组策略分配 SSO 服务器。

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。ASA 当前支持 SiteMinder 类型的 SSO 服务器和 SAML POST 类型的 SSO 服务器。此命令适用于这两种类型的 SSO 服务器。

注　在用户名 webvpn 配置模式下输入同一命令 **sso-server value** 可为用户策略分配 SSO 服务器。

示例

以下示例命令创建组策略 my-sso-grp-pol 并将其分配到名为 example 的 SSO 服务器：

```
ciscoasa(config)# group-policy my-sso-grp-pol internal
ciscoasa(config)# group-policy my-sso-grp-pol attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# sso-server value example
ciscoasa(config-group-webvpn)#
```

相关命令

命令	说明
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
sso-server value (username webvpn)	为用户策略分配 SSO 服务器。
web-agent-url	指定的 SSO 服务器 URLASA 使 SiteMinder-type SSO 身份验证请求。

sso-server value (username webvpn)

要为用户策略分配 SSO 服务器，请在用户名配置模式中可用的 webvpn 配置模式下使用 **sso-server value** 命令。

要删除用户的 SSO 服务器分配，请使用此命令的 **no** 形式。

当用户策略从组策略继承了不需要的 SSO 服务器分配时，使用 **sso-server none** 命令可删除该分配。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

语法说明

name	指定将分配给用户策略的 SSO 服务器的名称。

默认值

用户策略的默认设置是使用组策略中的 SSO 服务器分配。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。ASA 当前支持 SiteMinder 类型的 SSO 服务器和 SAML POST 类型的 SSO 服务器。

此命令适用于这两种类型的 SSO 服务器。

sso-server value 命令可为用户策略分配 SSO 服务器。

注　在组 webvpn 配置模式下输入同一命令 **sso-server value** 可为组策略分配 SSO 服务器。

示例

以下示例命令将名为 my-sso-server 的 SSO 服务器分配到名为 Anyuser 的 WebVPN 用户的用户策略：

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# sso-server value my-sso-server
ciscoasa(config-username-webvpn)#
```

相关命令

命令	说明
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
sso-server value (config-group-webvpn)	为组策略分配 SSO 服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

start-url

要输入用于获取可选登录前 Cookie 的 URL，请在 aaa-server-host 配置模式下使用 **start-url** 命令。这是带有 HTTP Forms 命令的 SSO。

start-url *string*

注　要正确配置带有 HTTP 协议的 SSO，您必须透彻地了解身份验证和 HTTP 协议交换的工作原理。

语法说明

string	SSO 服务器的 URL。最大 URL 长度为 1024 个字符。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server-host 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

ASA 的 WebVPN 服务器可以使用 HTTP POST 请求将单点登录身份验证请求提交到身份验证 Web 服务器。身份验证 Web 服务器可通过将 Set-Cookie 报头与登录页面内容一起发送来执行登录前序列。您可以使用浏览器直接连接到身份验证 Web 服务器的登录页面来查看此操作。如果 Web 服务器在登录页面加载时设置 Cookie，并且此 Cookie 与接下来的登录会话相关，则必须使用 **start-url** 命令输入用于获取 Cookie 的 URL。在登录前 Cookie 序列随表单提交到身份验证 Web 服务器之后，实际登录序列启动。

注　仅当进行登录前 Cookie 交换时才需要 **start-url** 命令。

示例

以下示例在 aaa-server 主机配置模式下输入，指定用于获取 https://example.com/east/Area.do?Page-Grp1 的登录前 Cookie 的 URL：

```
ciscoasa(config)# aaa-server testgrp1 (inside) host example.com
ciscoasa(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	说明
action-uri	指定要接收用于单点登录身份验证的用户名和密码的 Web 服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建用于与身份验证 Web 服务器交换的隐藏参数。
password-parameter	指定 HTTP POST 请求参数（其中必须提交用户密码以供 SSO 身份验证）的名称。
user-parameter	在必须提交用户名以供 SSO 身份验证时指定 HTTP POST 请求参数的名称。

state-checking

要对 H.323 实施状态检查，请在参数配置模式下使用 **state-checking** 命令。要禁用此功能，请使用此命令的 **no** 形式。

state-checking [h225 | ras]

no state-checking [h225 | ras]

语法说明

h225	对 H.225 实施状态检查。
ras	对 RAS 实施状态检查。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	**修改**
7.2(1)	引入了此命令。

示例

以下示例展示如何对 H.323 呼叫上的 RAS 实施状态检查：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# state-checking ras
```

相关命令

命令	**说明**
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

strict-header-validation

要按照 RFC 3261 对 SIP 消息中的报头字段启用严格验证，请在参数配置模式下使用 **strict-header-validation** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

strict-header-validation action {drop | drop-connection | reset | log} [log]

no strict-header-validation action {drop | drop-connection | reset | log} [log]

语法说明

drop	如果发生违规，则丢弃数据包。
drop-connection	丢弃违规的连接。
reset	重置违规的连接。
log	指定违规情况下的独立或附加日志。它可以关联到任何操作。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何对 SIP 检查策略映射中的 SIP 报头字段启用严格验证：

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-header-validation action log
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

strict-http

要允许转发不合规的 HTTP 流量，请在 HTTP 映射配置模式下使用 **strict-http** 命令，该模式可通过 **http-map** 命令访问。要将此功能重置为默认行为，请使用该命令的 **no** 形式。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

语法说明

action	消息未通过此命令检查时执行的操作。
allow	允许消息。
drop	关闭连接。
log	（可选）生成系统日志。
reset	关闭连接，并向客户端和服务器发送一条 TCP 重置消息。

默认值

此命令默认已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
HTTP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

虽然无法禁用严格 HTTP 检查，但 **strict-http action allow** 命令会使 ASA 允许转发不合规的 HTTP 流量。此命令会覆盖默认行为（即拒绝转发不合规的 HTTP 流量）。

示例

以下示例允许转发不合规的 HTTP 流量：

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# strict-http allow
ciscoasa(config-http-map)#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug appfw	显示与增强型 HTTP 检查关联的流量详细信息。
http-map	为配置增强型 HTTP 检查定义 HTTP 映射。
inspect http	应用要用于应用检查的特定 HTTP 映射。
policy-map	将类映射与特定安全操作关联。

strip-group

此命令仅适用于接收到的 “ 用户 @ 领域 ” 形式的用户名。领域是通过 “@” 分隔符附加到用户名的管理域 (juser@abc)。

要启用或禁用剥离组处理，请在隧道组常规属性配置模式下使用 **strip-group** 命令。ASA 通过从 VPN 客户端提交的用户名获取组名称来选择 IPsec 连接的隧道组。当启用剥离组处理时，ASA 仅发送用户名的用户部分进行授权 / 身份验证。否则（如果禁用），ASA 将发送整个用户名，包括领域。

要禁用剥离组处理，请使用此命令的 **no** 形式。

strip-group

no strip-group

语法说明

此命令没有任何参数或关键字。

默认值

此命令的默认设置禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

只能将此属性应用于 IPsec 远程访问隧道类型。

注　由于 MSCHAPv2 的限制，当 MSCHAPv2 用于 PPP 身份验证时，您不能执行隧道组交换。MSCHAPv2 期间的哈希计算绑定到用户名字符串（如用户 + 分隔符 + 组）。

示例

以下示例为 IPsec 型远程访问配置名为 “remotegrp” 的远程访问隧道组，然后进入常规配置模式，将名为 “remotegrp” 的隧道组设置为默认组策略，再为该隧道组启用剥离组：

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-group
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
group-delimiter	启用组名称解析，并指定要在根据用户名解析组名称时使用的分隔符，这些用户名是在协商隧道时收到的。
show running-config tunnel group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group general-attributes	指定命名的隧道组的常规属性。

strip-realm

要启用或禁用剥离领域处理，请在隧道组常规属性配置模式下使用 **strip-realm** 命令。剥离领域处理会在向身份验证或授权服务器发送用户名时从用户名中删除领域。领域是通过 “@” 分隔符附加到用户名的管理域 (username@realm)。如果启用该命令，ASA 仅发送用户名的用户部分进行授权 / 身份验证。否则，ASA 将发送整个用户名。

要禁用剥离领域处理，请使用此命令的 **no** 形式。

strip-realm

no strip-realm

语法说明

此命令没有任何参数或关键字。

默认值

此命令的默认设置禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0.1	引入了此命令。

使用指南

只能将此属性应用于 IPsec 远程访问隧道类型。

示例

以下示例为 IPsec 型远程访问配置名为 “remotegrp” 的远程访问隧道组，然后进入常规配置模式，将名为 “remotegrp” 的隧道组设置为默认组策略，再为该隧道组启用剥离领域：

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-real
```

storage-key

要指定存储密钥以保护在会话间存储的数据，请在组策略 webvpn 配置模式下使用 **storage-key** 命令。要从配置中删除此命令，请使用此命令的 **no** 版本。

storage- key {**none** | **value** *string*}

no storage-key

语法说明

string	指定要用作存储密钥值的字符串。此字符串最长可为 64 个字符。

默认值

默认值为 **none**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略 WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

虽然可以在存储密钥值中使用除空格外的任意字符，但我们建议仅使用标准字母数字字符集：0 到 9 和 a 到 z。

示例

以下示例将存储密钥设置为值 abc123：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-key value abc123
```

相关命令

命令	说明
storage-objects	配置会话之间所存储数据的存储对象。

storage-objects

要指定将哪些存储对象用于会话间存储的数据，请在组策略 webvpn 配置模式下使用 **storage-objects** 命令。要从配置中删除此命令，请使用此命令的 **no** 版本。

storage- objects {**none** | **value** *string*}

no storage-objects

语法说明

string	指定存储对象的名称。此字符串最长可为 64 个字符。

默认值

默认值为 **none**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略 WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

虽然可以在存储对象名称中使用除空格和逗号以外的任意字符，但我们建议仅使用标准字母数字字符集：0 到 9 和 a 到 z。在字符串中使用逗号（无空格）分隔存储对象的名称。

示例

以下示例将存储对象名称设置为 cookies 和 xyz456：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-object value cookies,xyz456
```

相关命令

命令	说明
storage-key	配置要用于会话间存储的数据的存储密钥。
user-storage	配置用于存储会话间用户数据的位置

第 17 章

subject-name 至 sysopt radius ignore-secret 命令

subject-name（加密 CA 证书映射）

要指示规则条目应该应用于 IPsec 对等设备证书的使用者 DN，请在加密 CA 证书映射配置模式下使用 **subject-name** 命令。要删除使用者名称，请使用此命令的 **no** 形式。

subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

语法说明

attr *tag*	指示仅将来自证书 DN 的指定属性值与规则条目字符串作比较。标记值如下所示： DNQ = DN 限定符 GENQ = 辈分限定符 I = 姓名首字母缩写 GN = 名 N = 名字 SN = 姓 IP = IP 地址 SER = 序列号 UNAME = 非结构化名称 EA = 邮件地址 T = 职位 O = 组织名称 L = 地区 SP = 州 / 省 C = 国家 / 地区 OU = 组织单位 CN= 公用名称
co	指定规则条目字符串必须是 DN 字符串或指示的属性中的子字符串。
eq	指定 DN 字符串或指示的属性必须与整个规则字符串匹配。
nc	指定规则条目字符串不得是 DN 字符串或指示的属性中的子字符串。
ne	指定 DN 字符串或指示的属性不得与整个规则字符串匹配。
string	指定要匹配的值。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
加密 CA 证书映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入证书映射 1 的 CA 证书映射配置模式，并创建一个规则条目来指示证书使用者的 Organization 属性必须等于 Central：

```
ciscoasa(config)# crypto ca certificate map 1
ciscoasa(ca-certificate-map)# subject-name attr o eq central
ciscoasa(ca-certificate-map)# exit
```

相关命令

命令	说明
crypto ca certificate map	进入 CA 证书映射配置模式。
issuer-name	标识 CA 证书中要与规则条目字符串进行比较的 DN。
tunnel-group-map	将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联起来。

subject-name (crypto ca trustpoint)

要在注册时将指示的使用者 DN 包括在证书中，请在 crypto ca trustpoint 配置模式下使用 **subject-name** 命令。此命令指明使用证书的个人或系统。要恢复默认设置，请使用此命令的 **no** 形式。

subject-name *X.500_name*

no subject-name

语法说明

X.500_name	定义 X.500 可分辨名称。使用逗号分隔属性值对。用引号将包含逗号或空格的任何值引起来。例如：**cn=crl,ou=certs,o="cisco systems, inc.",c=US**。最大长度是 500 个字符。

默认值

默认设置是不包含使用者名称。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，在 URL https//:frog.example.com 上设置自动注册，并将使用者 DN OU“certs” 包含在中心信任点的注册请求中：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url http://frog.example.com/
ciscoasa(ca-trustpoint)# subject-name ou=certs
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment url	指定用于向 CA 注册的 URL。

subject-name-default

要指定要在本地 CA 服务器签发的所有用户证书中附加到用户名后面的通用使用者名称可分辨名称 (DN)，请在 CA 服务器配置模式下使用 **subject-name-default** 命令。要将 subject-name DN 重置为默认值，请使用此命令的 **no** 形式。

subject-name-default *dn*

no subject-name-default

语法说明

dn	指定与用户名一起包含在本地 CA 服务器签发的所有用户证书中的通用使用者名称 DN。支持的 DN 属性包括 cn（公用名称）、ou（组织单位）、ol（组织地区）、st（州）、ea（邮件地址）、c（公司）、t（职位）和 sn（姓）。使用逗号分隔属性值对。插入引号括起任何包含逗号的值。*dn* 最多可包含 500 个字符。

默认值

此命令不是默认配置的一部分。此命令指定证书中的默认 DN。如果用户输入中有 DN，ASA 会忽略此命令。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

subject-name-default 命令指定要与用户名一起使用的常见通用 DN，以形成签发的证书的使用者名称。为此，只需将 *dn* 值指定为 cn=username。此命令使得无需专门为每个用户定义使用者名称 DN。如果是使用 **crypto ca server user-db add** dn *dn* 命令添加用户，DN 字段是可选的。

如果用户输入中未指定 DN，ASA 只会在签发证书时使用此命令。

示例

以下示例指定 DN：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问权限，从而允许配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
keysize	指定在用户证书注册时生成的公共密钥和专用密钥的大小。
lifetime	指定 CA 证书、签发的证书或 CRL 的生命期。

subnet

要配置网络对象的网络，请在对象配置模式下使用 **subnet** 命令。使用此命令的 **no** 形式可从配置中删除对象。

subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

no subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

语法说明

IPv4_address IPv4_mask	指定 IPv4 网络地址和子网掩码，用空格分隔。
IPv6_address/*IPv6_prefix*	指定 IPv6 网络地址和前缀长度，用 / 字符分隔，不得包含空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
对象网络配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

如果您使用不同 IP 地址配置现有网络对象，新配置将会替换现有配置。

示例

以下示例展示如何创建子网网络对象：

```
ciscoasa (config)# object network OBJECT_SUBNET
ciscoasa (config-network-object)# subnet 10.1.1.0 255.255.255.0
```

相关命令

命令	说明
clear configure object	清除所有已创建对象。
description	将添加到网络对象的说明。
fqdn	指定完全限定域名网络对象。
host	指定主机的网络对象。
nat	实现网络对象的 NAT。
object network	创建网络对象。

命令	说明
object-group network	创建网络对象组。
range	指定网络对象的地址范围。
show running-config object network	显示网络对象的配置。

summary-address (EIGRP)

要在特定接口上配置 EIGRP 的摘要，请在接口配置模式下使用 **summary-address** 命令。要删除摘要地址，请使用此命令的 **no** 形式。

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

语法说明

as-number	自主系统编号。此编号必须与 EIGRP 路由进程的自主系统编号相同。
addr	摘要 IP 地址。
mask	要应用于 IP 地址的子网掩码。
admin-distance	（可选）摘要路由的管理距离。有效值为从 0 到 255。如果未指定，则默认值为 5。

默认值

默认值如下：

- EIGRP 会自动将路由汇总到网络级别，对于单个主机路由也是如此。
- EIGRP 摘要路由的管理距离是 5。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

默认情况下，EIGRP 会将子网路由汇总到网络级别。使用 **no auto-summary** 命令可禁用自动路由摘要。使用 **summary-address** 命令可手动定义每个接口的子网路由摘要。

示例

以下示例配置 **tag** 设置为 3 的路由摘要：

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

以下示例展示如何使用 **summary-address** 命令的 **no** 形式将某个选项重新设置为默认值。在此示例中，**tag** 值（在上一示例中设置为 3）从 **summary-address** 命令中被删除。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

以下示例从配置中删除 **summary-address** 命令：

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

相关命令

命令	说明
auto-summary	自动为 EIGRP 路由进程创建摘要地址。

summary-address (OSPFv2)

要为 OSPF 创建汇聚地址，请在路由器配置模式下使用 **summary-address** 命令。要删除摘要地址或特定摘要地址选项，请使用此命令的 **no** 形式。

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

语法说明

addr	为地址范围指定的摘要地址的值。
mask	用于摘要路由的 IP 子网掩码。
not-advertise	（可选）抑制与指定前缀 / 掩码对匹配的路由。
tag *tag_value*	（可选）连接到每个外部路由的 32 位十进制值。此值不使用 OSPF 本身。它可以用于 Asbr 之间传递信息。如果未指定，则远程的自主系统编号将使用于自 BGP 和 EGP ；路由对于其他协议，使用零 (0)。有效值范围为 0 到 4294967295。

默认值

默认值如下：

- *tag_value* 为 0。
- 不抑制与指定前缀 / 掩码对匹配的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
路由器配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

可以汇总从其他路由协议获知的路由。对 OSPF 使用此命令会导致 OSPF 自主系统边界路由器 (ASBR) 将一个外部路由通告为指定地址涵盖的所有重分布路由的汇聚路由。此命令仅汇总来自其他路由协议且正被重分布到 OSPF 的路由。使用 **area range** 命令可在各 OSPF 区域之间进行路由汇总。

要从配置中删除 **summary-address** 命令，请使用此命令的 no 形式且不指定任何可选关键字或参数。要从配置中的摘要命令删除选项，请对要删除的选项使用此命令的 **no** 形式。有关详细信息，请参阅 “ 示例 ” 部分。

示例

以下示例配置 **tag** 设置为 3 的路由摘要：

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

以下示例展示如何使用 **summary-address** 命令的 **no** 形式将某个选项重新设置为默认值。在此示例中，**tag** 值（在上一示例中设置为 3）从 **summary-address** 命令中被删除。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

以下示例从配置中删除 **summary-address** 命令：

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

相关命令

命令	说明
area range	在区域边界对路由进行整合和汇总。
router ospf	进入路由器配置模式。
show ospf summary-address	显示每个 OSPF 路由进程的摘要地址设置。

summary-prefix (OSPFv3)

要配置 IPv6 摘要前缀，请在 IPv6 路由器配置模式下使用 **summary-prefix** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

语法说明

not-advertise	（可选）抑制与指定前缀 / 掩码对匹配的路由。此关键字仅适用于 OSPFv3。
prefix	指定目标的 IPv6 前缀。
tag *tag_value*	（可选）指定可用作匹配值的标记值，用于通过路由映射来控制重分布。此关键字仅适用于 OSPFv3。

默认值

默认值如下：

- *tag_value* 为 0。
- 不抑制与指定前缀 / 掩码对匹配的路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
IPv6 路由器配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可配置 IPv6 摘要前缀。

示例

在以下示例中，摘要前缀 FECO::/24 包含地址 FECO::/1 至 FECO::/24。只有地址 FECO::/24 在外部 LSA 中通告：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 172.16.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

相关命令

命令	说明
ipv6 router ospf	进入 OSPFv3 的路由器配置模式。
redistribute	将来自一个 OSPFv3 路由域的 IPv6 路由重分布到另一个 OSPFv3 路由域。

sunrpc-server

要在 SunRPC 服务表中创建条目，请在全局配置模式下使用 **sunrpc-server** 命令。要从配置中删除 SunRPC 服务表条目，请使用此命令的 **no** 形式。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol [tcp | udp] port** *port* [- *port*] **timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol [tcp | udp] port** *port* [- *port*] **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

语法说明

ifc_name	服务器接口名称。
ip_addr	SunRPC 服务器的 IP 地址。
mask	网络掩码。
port *port* [- *port*]	指定 SunRPC 协议端口范围。
port- *port*	（可选）指定 SunRPC 协议端口范围。
protocol tcp	指定 SunRPC 传输协议。
protocol udp	指定 SunRPC 传输协议。
service	指定服务。
service_type	设置 SunRPC 服务计划编号（如在 **sunrpcinfo** 命令中所指定）。
timeout *hh:mm:ss*	指定关闭对 SunRPC 服务流量的访问前的超时空闲时间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

SunRPC 服务表用于允许 SunRPC 流量在超时指定的持续时间内根据建立的 SunRPC 会话通过 ASA。

示例

以下示例展示如何创建 SunRPC 服务表：

```
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

相关命令

命令	说明
clear configure sunrpc-server	从 ASA 清除 Sun 远程处理器调用服务。
show running-config sunrpc-server	显示有关 SunRPC 配置的信息。

support-user-cert-validation

要根据当前信任点验证远程用户证书（假设已向签发远程证书的 CA 对该信任点进行了身份验证），请在 crypto ca trustpoint 配置模式下使用 **support-user-cert-validation** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

support-user-cert-validation

no support-user-cert-validation

语法说明

此命令没有任何参数或关键字。

默认值

默认设置是支持用户证书验证。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 可以有使用同一 CA 的两个信任点，这会导致有两个不同的身份证书来自同一 CA。如果信任点已经向 CA 进行了身份验证，且该 CA 与已启用此功能的另一个信任点相关联，则会自动禁用此选项。这样可防止在选择路径验证参数时产生混淆。如果用户尝试在已向与另一个信任点关联的 CA 进行过身份验证且启用了此功能的信任点上激活此功能，则不允许进行该操作。不能有两个信任点都启用此设置并向同一 CA 进行身份验证。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并允许中心信任点接受用户验证：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# support-user-cert-validation
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。

sw-module module password-reset

要将软件模块上的密码重置为默认值，请在特权 EXEC 模式下使用 **sw-module module password-reset** 命令。

sw-module module *id* **password-reset**

语法说明

id	指定模块 ID（**cxsc** 或 **ips**）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
				多个	
	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。

使用指南

在重置密码后，您应该使用模块应用将密码更改为唯一值。重置模块密码会导致模块重启。在模块重启时服务不可用，重启可能需要几分钟。您可以运行 **show module** 命令来监控模块状态。

此命令始终提示予以确认。如果命令成功，则不会出现其他输出。如果命令失败，则会出现错误消息，说明失败原因。

此命令仅在模块处于开启状态时才有效。

默认密码取决于模块：

- ASA IPS - 用户 cisco 的默认密码是 **cisco**。
- ASA CX - 用户 admin 的默认密码是 **Admin123**。

示例

以下示例重置 IPS 模块上的密码：

```
ciscoasa# sw-module module ips password-reset
Reset the password on module ips?[confirm] y
```

相关命令

命令	说明
sw-module module recover	通过从磁盘加载恢复映像来恢复模块。
sw-module module reload	重新加载模块软件。
sw-module module reset	关闭并重新加载模块。
sw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

sw-module module recover

要为软件模块从磁盘加载恢复软件映像或者要配置映像位置，请在特权 EXEC 模式下使用 **sw-module module recover** 命令。在某些情况下（例如，模块无法加载当前映像）可能需要使用此命令来恢复模块。

sw-module module *id* **recover** {**boot | stop | configure image** *path*}

语法说明

id	指定模块 ID，可以是以下项之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块
boot	根据 **configure** 设置开始恢复模块并下载恢复映像。之后从新映像重启模块。
configure image *path*	在本地磁盘上配置新的映像位置，例如 disk0:image2。
stop	停止恢复操作。模块从原始映像启动。必须在使用 **sw-module module** *id* **recover boot** 命令开始恢复后 30 秒内输入此命令。如果在此期间过后发出 **stop** 命令，则可能会导致意外结果，例如模块变为无响应。 但是，如果模块无响应，则可能需要先停止模块，再重新启动模块或应用新映像。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。
9.2(1)	通过增加 **sfr** 关键字，增加了对 ASA FirePOWER 模块的支持。

使用指南

使用此命令可安装软件模块。使用此命令安装的软件模块可以是尚未在设备上配置的新模块，也可以是出现了故障并需要重新安装的现有模块。

安装映像时，请使用以下命令序列：

- **sw-module module** *id* **configure image** *path*，以标识软件模块映像在 disk0 上的位置。
- **sw-module module** *id* **boot**，以启动该映像。

仅在模块处于 “ 开启 ”、“ 关闭 ”、“ 无响应 ” 或 “ 恢复 ” 状态时才可以启动映像。有关状态信息，请参阅 **show module** 命令。如果模块不是处于开启状态，ASA 会强制关闭模块。强制关闭会破坏旧模块磁盘映像（包括任何配置），因此，这种做法应仅作为一种灾难恢复机制。

可以使用 **show module** *id* **recover** 命令查看恢复配置。

注意　对于 IPS 模块，请勿在模块软件中使用 **upgrade** 命令来安装映像。请参阅《CLI 配置指南》中有关每个软件模块的章节，了解如何完成模块安装和初始配置。

示例

以下示例将模块设置为从 disk0:image2 下载映像：

```
ciscoasa# sw-module module ips recover configure image disk0:image2
```

以下示例恢复模块：

```
ciscoasa# sw-module module ips recover boot
The module in slot ips will be recovered.This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips?[confirm]
```

相关命令

命令	说明
debug module-boot	显示关于模块引导进程的调试消息。
sw-module module reset	关闭模块并执行重置。
sw-module module reload	重新加载模块软件。
sw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

sw-module module reload

要为软件模块重新加载模块软件，请在特权 EXEC 模式下使用 **sw-module module reload** 命令。

sw-module module *id* **reload**

语法说明

id	指定模块 ID，可以是以下项之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。
9.2(1)	通过增加 **sfr** 关键字，增加了对 ASA FirePOWER 模块的支持。

使用指南

此命令不同于 **sw-module module reset** 命令，后者也会在重新加载模块之前执行重置。

仅在模块处于启用状态时此命令才有效。有关状态信息，请参阅 **show module** 命令。

示例

以下示例重新加载 IPS 模块：

```
ciscoasa# sw-module module ips reload
Reload module in slot ips?[confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导进程的调试消息。
sw-module module recover	通过从磁盘加载恢复映像来恢复模块。

命令	说明
sw-module module reset	关闭模块并执行重置。
sw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

sw-module module reset

要重置模块然后重新加载模块软件，请在特权 EXEC 模式下使用 **sw-module module reset** 命令。

sw-module module *id* **reset**

语法说明

id	指定模块 ID，可以是以下项之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。
9.2(1)	通过增加 **sfr** 关键字，增加了对 ASA FirePOWER 模块的支持。

使用指南

当模块处于开启状态时，**sw-module module reset** 命令会提示您先关闭软件再执行重置。

可以使用 **sw-module module recover** 命令恢复模块。如果在模块处于恢复状态时输入 **sw-module module reset** 命令，模块不会中断恢复过程。**sw-module module reset** 命令执行模块重置，重置后模块恢复过程会继续进行。如果模块挂起，可能需要在恢复过程中重置模块；重置或许能够解决这个问题。

此命令不同于 **sw-module module reload** 命令，后者仅重新加载软件而不执行重置。

此命令仅在模块状态为启用、关闭、无响应或恢复时才可用。有关状态信息，请参阅 **show module** 命令。

示例

以下示例重置处于开启状态的 IPS 模块：

```
ciscoasa# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips?[confirm] y
```

```
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导进程的调试消息。
sw-module module recover	通过从磁盘加载恢复映像来恢复模块。
sw-module module reload	重新加载模块软件。
sw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

sw-module module shutdown

要关闭模块软件，请在特权 EXEC 模式下使用 **sw-module module shutdown** 命令。

sw-module module *id* **shutdown**

语法说明

id	指定模块 ID，可以是以下项之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。
9.2(1)	通过增加 **sfr** 关键字，增加了对 ASA FirePOWER 模块的支持。

使用指南

关闭模块软件使得模块可以安全断电而不会丢失配置数据。

仅在模块状态为启用或无响应时此命令才有效。有关状态信息，请参阅 **show module** 命令。

示例

以下示例关闭 IPS 模块：

```
ciscoasa# sw-module module ips shutdown
Shutdown module in slot ips?[confirm] y
Shutdown issued for module in slot ips
ciscoasa#
%XXX-5-505001: Module in slot ips is shutting down.Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
sw-module module recover	通过从磁盘加载恢复映像来恢复模块。
sw-module module reload	重新加载模块软件。
sw-module module reset	关闭模块并执行重置。
show module	显示模块信息。

sw-module module uninstall

要卸载软件模块映像及关联的配置，请在特权 EXEC 模式下使用 **sw-module module uninstall** 命令。

sw-module module *id* **uninstall**

语法说明

id	指定模块 ID，可以是以下项之一： • **sfr** - ASA FirePOWER 模块。 • **ips** - IPS 模块 • **cxsc** - ASA CX 模块

命令默认

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.6(1)	我们引入了此命令。
9.1(1)	通过增加 **cxsc** 关键字，增加了对 ASA CX 软件模块的支持。
9.2(1)	通过增加 **sfr** 关键字，增加了对 ASA FirePOWER 模块的支持。

使用指南

此命令永久卸载软件模块映像及关联的配置。

示例

以下示例卸载 IPS 模块映像和配置：

```
ciscoasa# sw-module module ips uninstall
Module ips will be uninstalled.This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.

Uninstall module <id>?[confirm]
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
sw-module module recover	通过从磁盘加载恢复映像来恢复模块。
sw-module module reload	重新加载模块软件。
sw-module module reset	关闭模块并执行重置。
show module	显示模块信息。

switchport access vlan

对于带有内置交换机的型号（例如 ASA 5505 自适应安全设备），可在接口配置模式下使用 **switchport access vlan** 命令向 VLAN 分配交换机端口。

switchport access vlan *number*

no switchport access vlan *number*

语法说明

vlan *number*	指定要向其分配交换机端口的 VLAN ID。VLAN ID 为 1 至 4090。

默认值

默认情况下，所有交换机端口都分配给 VLAN 1。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在透明防火墙模式下，在 ASA 5505 自适应安全设备基础许可证中可以配置 2 个活动 VLAN，在增强型安全许可证中可以配置 3 个活动 VLAN（其中一个 VLAN 必须用于故障切换）。

在路由模式下，在 ASA 5505 自适应安全设备基础许可证中最多可以配置 3 个活动 VLAN，在增强型安全许可证中最多可以配置 20 个活动 VLAN。

活动 VLAN 是一个已经配置 **nameif** 命令的 VLAN。

可以使用 **switchport access vlan** 命令向每个 VLAN 分配一个或多个物理接口。默认情况下，接口的 VLAN 模式是接入端口（一个 VLAN 与接口关联）。如果想创建中继端口以允许多个 VLAN 通过接口，可使用 **switchport mode access trunk** 命令将模式更改为中继模式，然后使用 **switchport trunk allowed vlan** 命令。

示例

以下示例将 5 个物理接口分配给 3 个 VLAN 接口：

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

...
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show running-config interface	显示运行配置中的接口配置。
switchport mode	将 VLAN 模式设置为接入模式或中继模式。
switchport protected	防止一个交换机端口与相同 VLAN 上的其他交换机端口进行通信，以提高安全性。
switchport trunk allowed vlan	将 VLAN 分配给中继端口。

switchport mode

对于带有内置交换机的型号（例如 ASA 5505 自适应安全设备），可在接口配置模式下使用 **switchport mode** 命令将 VLAN 模式设置为接入模式（默认设置）或中继模式。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

语法说明

access	将交换机端口设置为接入模式，这样，交换机端口仅允许一个 VLAN 的流量通过。数据包在不带 802.1Q VLAN 标记的情况下退出交换机端口。如果数据包在带有标记的情况下进入交换机端口，数据包将被丢弃。
trunk	将交换机端口设置为中继模式，这样，交换机端口可以有多个 VLAN 的流量通过。数据包在带有 802.1Q VLAN 标记的情况下退出交换机端口。如果数据包在不带标记的情况下进入交换机端口，数据包将被丢弃。

默认值

默认模式是接入模式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
7.2(2)	现在可以配置多个中继端口，而不仅限于一个中继。

使用指南

默认情况下，交换机端口的 VLAN 模式是接入端口（一个 VLAN 与交换机端口关联）。在接入模式下，可使用 **switchport access vlan** 命令向 VLAN 分配交换机端口。如果想创建中继端口以允许多个 VLAN 通过交换机端口，可将模式设置为中继模式，然后使用 **switchport trunk allowed vlan** 命令向中继分配多个 VLAN。如果将模式设置为中继模式但未配置 **switchport trunk allowed vlan** 命令，交换机端口将会保持 “ 线路协议关闭 ” 状态，且不能参与流量转发。中继模式仅适用于增强型安全许可证。

switchport vlan access 命令在接入模式下才会生效。**switchport trunk allowed vlan** 命令在中继模式下才会生效。

示例

以下示例配置分配给 VLAN 100 的接入模式交换机端口，并配置分配给 VLAN 200 和 VLAN 300 的中继模式交换机端口：

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200,300
ciscoasa(config-if)# no shutdown

...
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show running-config interface	显示运行配置中的接口配置。
switchport access vlan	将交换机端口分配给 VLAN。
switchport protected	防止一个交换机端口与相同 VLAN 上的其他交换机端口进行通信，以提高安全性。
switchport trunk allowed vlan	将 VLAN 分配给中继端口。

switchport monitor

对于带有内置交换机的型号（例如 ASA 5505 自适应安全设备），可在接口配置模式下使用 **switchport monitor** 命令启用 SPAN（又称为交换机端口监控）。为其输入此命令的端口（称为目标端口）接收在指定源端口上传输或接收到的每个数据包的副本。使用 SPAN 功能，可以将嗅探器连接到目标端口，以便监控流量。可以通过多次输入此命令来指定多个源端口。只能为一个目标端口启用 SPAN。要禁用源端口监控，请使用此命令的 **no** 形式。

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

语法说明

both	（可选）指定监控传输的流量和接收的流量。**both** 是默认设置。
rx	（可选）指定仅监控接收的流量。
source_port	指定要监控的端口。可以指定任何以太网端口和 Internal-Data0/1 背板端口（该端口在各 VLAN 接口之间传递流量）。由于 Internal-Data0/1 端口是千兆以太网端口，因此，快速以太网目标端口可能出现流量过载。应密切监控 Internal-Data0/1 端口。
tx	（可选）指定仅监控传输的流量。

默认值

要监控的默认流量类型是 **both**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

如果不启用 SPAN，将嗅探器连接到其中一个交换机端口只会捕获流向或来自该端口的流量。要捕获流向或来自多个端口的流量，需要启用 SPAN 并标识要监控的端口。

将 SPAN 目标端口连接到另一台交换机时须小心，因为可能会导致网络环路。

示例

以下示例将以太网 0/1 端口配置为目标端口，并使用该端口监控以太网 0/0 端口和以太网 0/2 端口：

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport monitor ethernet 0/0
ciscoasa(config-if)# switchport monitor ethernet 0/2
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show running-config interface	显示运行配置中的接口配置。
switchport access vlan	将交换机端口分配给 VLAN。
switchport protected	防止一个交换机端口与相同 VLAN 上的其他交换机端口进行通信，以提高安全性。

switchport protected

对于带有内置交换机的型号（例如 ASA 5505 自适应安全设备），可在接口配置模式下使用 **switchport protected** 命令来防止一个交换机端口与相同 VLAN 上受保护的其他交换机端口进行通信。如果 VLAN 上的一个交换机端口的安全性受到影响，可使用此功能来提高其他交换机端口的安全性。

switchport protected

no switchport protected

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，接口不受保护。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果一个 DMZ 托管 3 台网络服务器，对每个交换机端口应用 **switchport protected** 命令可将这些网络服务器相互隔离开。内部网络和外部网络都可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间不能进行通信。

此命令不限制与不受保护的端口之间的通信。

示例

以下示例配置 7 个交换机端口。以太网 0/4、0/5 和 0/6 端口被分配给 DMZ 网络，且这些端口相互受到保护：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/5
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/6
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

...
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show running-config interface	显示运行配置中的接口配置。
switchport access vlan	将交换机端口分配给 VLAN。
switchport mode	将 VLAN 模式设置为接入模式或中继模式。
switchport trunk allowed vlan	将 VLAN 分配给中继端口。

switchport trunk

对于带有内置交换机的型号（例如 ASA 5505 自适应安全设备），可在接口配置模式下使用 **switchport trunk** 命令向中继端口分配 VLAN。使用此命令的 **no** 形式可以从中继删除 VLAN。

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

语法说明

allowed vlans *vlan_range*	标识可分配给中继端口的一个或多个 VLAN。VLAN ID 为 1 至 4090。 可通过以下方式之一标识 *vlan_range*： • 单个编号 (n) • 范围 (n-x) 用逗号将编号和范围隔开，例如： 5,7-10,13,45-100 可以用空格代替逗号，但此命令保存到配置中后，其中的空格将会变成逗号。 可以在此命令中包含本地 VLAN，但这不是必需的；本地 VLAN 始终可通过端口，无论它是否包含在此命令中。
native vlan *vlan*	将本地 VLAN 分配给中继。本地 VLAN 上通过中继发送的数据包不会被修改。 例如，如果某个端口被分配 VLAN 2、VLAN 3 和 VLAN 4，其中的 VLAN 2 是本地 VLAN，则 VLAN 2 上进入该端口且带有 802.1Q 报头的数据包不会被修改。进入该端口但没有 802.1Q 报头的帧将被发送到 VLAN 2。 每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

默认值

默认情况下，不会向中继分配 VLAN。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
7.2(2)	此命令经过修改，现在允许每个交换机端口可以有多于 3 个 VLAN。此外，此命令现在还允许配置多个中继端口，而不仅限于一个中继端口。现在，此命令使用逗号而不是空格来分隔 VLAN ID。
7.2(4)/8.0(4)	通过 **native vlan** 关键字引入了本地 VLAN 支持。

使用指南

如果想创建中继端口以允许多个 VLAN 通过交换机端口，可使用 **switchport mode trunk** 命令将模式设置为中继模式，然后使用 **switchport trunk** 命令向中继分配多个 VLAN。交换机端口至少被分配一个 VLAN 后才能传递流量。如果将模式设置为中继模式但未配置 **switchport trunk allowed vlan** 命令，交换机端口将会保持 “ 线路协议关闭 ” 状态，且不能参与流量转发。中继模式仅适用于增强型安全许可证。使用 **switchport mode trunk** 命令将模式设置为中继模式后，**switchport trunk** 命令才会生效。

注意　此命令不向后兼容版本 7.2(1)；版本 7.2(1) 不能标识用于分隔 VLAN 的逗号。如果使用较低版本，请务必用空格分隔 VLAN，且使用的 VLAN 数量不可超过 3 个。

示例

以下示例配置七个 VLAN 接口（包括故障切换接口，该接口使用 **failover lan** 命令进行配置）。VLAN 200、201 和 202 都在以太网 0/1 上中继。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 201
ciscoasa(config-if)# nameif dept1
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 202
ciscoasa(config-if)# nameif dept2
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.3.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200-202
ciscoasa(config-if)# switchport trunk native vlan 5
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show running-config interface	显示运行配置中的接口配置。
switchport access vlan	将交换机端口分配给 VLAN。
switchport mode	将 VLAN 模式设置为接入模式或中继模式。
switchport protected	防止一个交换机端口与相同 VLAN 上的其他交换机端口进行通信，以提高安全性。

synack-data

要设置要对包含数据的 TCP SYNACK 数据包执行的操作，请在 tcp-map 配置模式下使用 **synack-data** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令是使用 **set connection advanced-options** 命令启用的 TCP 规范化策略的一部分。

synack-data {**allow** | **drop**}

no synack-data

语法说明

allow	允许包含数据的 TCP SYNACK 数据包。
drop	丢弃包含数据的 TCP SYNACK 数据包。

默认值

默认操作是丢弃包含数据的 TCP SYNACK 数据包。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
TCP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。

使用指南

要启用 TCP 规范化，请使用模块化策略框架：

1. **tcp-map** - Identifies the TCP normalization actions.
   a. **synack-data** - 在 tcp-map 配置模式下，可以输入 **synack-data** 命令及许多其他命令。
2. **class-map** - Identify the traffic on which you want to perform TCP normalization.
3. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced-options** - 确定创建的 tcp 映射。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

示例

以下示例将 ASA 设置为允许包含数据的 TCP SYNACK 数据包：

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# synack-data allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
```

```
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

相关命令

命令	说明
class-map	为服务策略标识流量。
policy-map	标识要应用于服务策略中的流量的操作。
set connection advanced-options	启用 TCP 规范化。
service-policy	将服务策略应用于接口。
show running-config tcp-map	显示 TCP 映射配置。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

synchronization

要启用 BGP 与内部网关协议 (IGP) 系统之间的同步，请在地址系列配置模式下使用 **synchronization** 命令。要使思科 IOS 软件无需等待 IGP 便通告网络路由，请使用此命令的 **no** 形式。

synchronization

no synchronization

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

通常，BGP 发言方不会向外部邻居通告路由，除非路由是本地路由或存在于 IGP 中。默认情况下，BGP 与 IGP 之间的同步被禁用，以允许思科 IOS 软件无需等待来自 IGP 的验证便可通告网络路由。使用此功能，自主系统中的路由器和访问服务器可在 BGP 将某个路由分配给其他自主系统之前获得该路由。

如果自主系统中的路由器不作为 BGP 发言方，请使用 **synchronization** 命令。

示例

以下示例展示如何在地址系列配置模式下启用同步。路由器先验证其 IGP 中的网络路由，再对外通告该路由。

```
ciscoasa(config)# router bgp 65120
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# synchronization
```

syn-data

要允许或丢弃包含数据的 SYN 数据包，请在 tcp-map 配置模式下使用 **syn-data** 命令。要删除此指定，请使用此命令的 **no** 形式。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

语法说明

allow	允许包含数据的 SYN 数据包。
drop	丢弃包含数据的 SYN 数据包。

默认值

默认情况下允许包含 SYN 数据的数据包。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
TCP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

将 **tcp-map** 命令与模块化策略框架基础设施结合使用。使用 **class-map** 命令定义流量类并使用 **tcp-map** 命令定制 TCP 检查。使用 **policy-map** 命令应用新 TCP 映射。使用 **service-policy** 命令激活 TCP 检查。

使用 **tcp-map** 命令进入 TCP 映射配置模式。在 tcp-map 配置模式下使用 **syn-data** 命令可丢弃包含数据的 SYN 数据包。

根据 TCP 规范，需要实施 TCP 才能接受 SYN 数据包包含的数据。由于此实施细微且隐晦，有些实施可能无法正确处理此方面。要避免因终端系统实施不正确而造成任何漏洞继而引致嵌入式攻击，可选择丢弃包含数据的 SYN 数据包。

示例

以下示例展示如何在所有 TCP 数据流中丢弃包含数据的 SYN 数据包：

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# syn-data drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

相关命令

命令	说明
class	指定要用于流量分类的类映射。
policy-map	配置策略，即流量类与一个或多个操作的关联。
set connection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

sysopt connection permit-vpn

对于通过 VPN 隧道进入 ASA 然后被解密的流量，可在全局配置模式下使用 **sysopt connection permit-vpn** 命令来允许这些流量绕过接口访问列表。组策略和每个用户的授权访问列表仍适用于此类流量。要禁用此功能，请使用此命令的 **no** 形式。

sysopt connection permit-vpn

no sysopt connection permit-vpn

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	现在，此命令在默认情况下已启用。此外，此命令现在仅允许绕过接口访问列表；组策略或每个用户的访问列表仍保持有效。
7.1(1)	此命令从 **sysopt connection permit-ipsec** 更改为现在的形式。
9.0(1)	增加了多情景模式支持。

使用指南

默认情况下，ASA 允许 VPN 流量在 ASA 接口上中断；您无需在接口访问列表中允许 IKE 或 ESP（或者其他 VPN 数据包类型）。默认情况下，您也不需要对解密 VPN 数据包的本地 IP 地址使用接口访问列表。由于通过 VPN 安全机制成功中断了 VPN 隧道，因此，此功能可简化配置和最大程度地提高 ASA 性能，而且不会带来任何安全风险。（组策略和每个用户的授权访问列表仍适用于此类流量。）

通过输入 **no sysopt connection permit-vpn** 命令，可以要求将接口访问列表应用于本地 IP 地址。要创建访问列表并将其应用于接口，请参阅 **access-list** 和 **access-group** 命令。访问列表适用于本地 IP 地址，但不适用于在 VPN 数据包解密之前使用的原始客户端 IP 地址。

示例

以下示例要求解密 VPN 流量符合接口访问列表：

```
ciscoasa(config)# no sysopt connection permit-vpn
```

相关命令

命令	说明
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。
sysopt connection tcpmss	覆盖 TCP 最大分段大小或确保最大分段大小不小于指定大小。
sysopt connection timewait	强制每个 TCP 连接在最后常规 TCP 关闭序列后短暂停留在 TIME_WAIT 状态。

sysopt connection preserve-vpn-flows

要在隧道中断并恢复后的超时期间保留并恢复通过隧道传输的有状态 (TCP) IPsec 局域网到局域网流量，请使用 **sysopt connection preserve-vpn-flows** 命令。要禁用此功能，请使用此命令的 **no** 形式。

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

语法说明

此命令没有任何参数或关键字。

默认值

默认禁用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

如果启用了永久性的 IPsec 隧道数据流传输功能，则只要在超时期间重新创建了隧道，数据就可以继续成功传输，因为安全设备仍可以访问原始数据流中的状态信息。

此命令仅支持 IPsec 局域网到局域网隧道（包括网络扩展模式）， 不支持 AnyConnect/SSL VPN 和 IPsec 远程访问隧道。

示例

以下示例指定保留隧道的状态信息，且在隧道中断并在超时期间重新建立后恢复通过隧道传输的 IPsec 局域网到局域网 VPN 流量：

```
ciscoasa(config)# no sysopt connection preserve-vpn-flows
```

要查看此功能是否已启用，请为 sysopt 输入 show run all 命令：

```
ciscoasa(config)# show run all sysopt
```

随后将显示结果示例。为了便于说明，在以下示例以及之后的所有示例中，preserve-vpn-flows 条目以粗体显示：

```
no sysopt connection timewait
sysopt connection tcpmss 1380
```

```
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

要对现有的 VPN 数据流重新分类，请在全局配置模式下使用 **sysopt connection reclassify-vpn** 命令。要禁用此功能，请使用此命令的 **no** 形式。

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令
9.0(1)	增加了多情景模式支持。

使用指南

当有 VPN 隧道投入使用时，此命令会对现有的 VPN 数据流重新分类，以确保会中断并重新创建需要加密的数据流。

此命令仅适用于局域网到局域网 VPN 和动态 VPN。此命令对 EZVPN 和 VPN 客户端连接无效。

示例

以下示例启用 VPN 重新分类：

```
ciscoasa(config)# sysopt connection reclassify-vpn
```

相关命令

命令	说明
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。
sysopt connection permit-vpn	允许来自 IPsec 隧道的任何数据包而不检查任何接口访问列表。

命令	说明
sysopt connection tcpmss	覆盖 TCP 最大分段大小或确保最大分段大小不小于指定大小。
sysopt connection timewait	强制每个 TCP 连接在最后常规 TCP 关闭序列后短暂停留在 TIME_WAIT 状态。

sysopt connection tcpmss

要确保 TCP 最大分段大小不超过您设置的值且不小于指定大小，请在全局配置模式下使用 **sysopt connection tcpmss** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

语法说明

bytes	以字节为单位设置 TCP 最大分段大小，范围在 48 和任何最大值之间。默认值为 1380 字节。将 *bytes* 设置为 0 可禁用此功能。 对于 **minimum** 关键字，*bytes* 代表允许的最大值下限。
minimum	覆盖不小于 *bytes* 值（48 到 65535 字节）的最大分段大小。默认情况下，此功能已禁用（设置为 0）。

默认值

默认最大值为 1380 字节。默认情况下，minimum 功能已禁用（设置为 0）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

主机和服务器在首次建立连接时都可以设置最大分段大小。如果主机或服务器设置的最大分段大小超过您使用 **sysopt connection tcpmss** 命令设置的值，ASA 将会覆盖最大分段大小并插入您设置的值。如果主机或服务器设置的最大分段大小小于您使用 **sysopt connection tcpmss minimum** 命令设置的值，ASA 将会覆盖最大分段大小并插入您设置的 “ 最小 ” 值（最小值实际上是允许的最大值下限）。例如，如果您将最大分段大小和最小分段大小分别设置为 1200 字节和 400 字节，当主机请求的最大分段大小是 1300 字节时，ASA 会更改数据包以请求 1200 字节（最大值）。如果另一台主机请求的最大分段大小是 300 字节，ASA 会更改数据包以请求 400 字节（最小值）。

默认值（1380 字节）为报头信息预留了空间，即使加上报头信息，总数据包大小也不会超过 1500 字节（这是以太网的默认 MTU）。请参阅以下计算公式：

1380 字节数据 + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 字节

如果主机或服务器没有请求最大分段大小，ASA 会假设使用的是 RFC 793 规定的默认值（536 字节）。

如果您将最大分段大小设置为大于 1380，数据包可能会进行分段，具体取决于 MTU 大小（默认值为 1500）。如果有很多分段，当 ASA 使用碎片防护功能时，其性能可能会受到影响。设置最小大小可防止 TCP 服务器向客户端发送大量小型 TCP 数据包，继而影响服务器和网络的性能。

注意　如果出现 IPFRAG 系统日志消息 209001 和 209002，可以增加 *bytes* 值，但一般情况下不建议这样做。

示例

以下示例将最大分段大小和最小分段大小分别设置为 1200 和 400：

```
ciscoasa(config)# sysopt connection tcpmss 1200
ciscoasa(config)# sysopt connection tcpmss minimum 400
```

相关命令

命令	说明
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。
sysopt connection permit-ipsec	允许来自 IPsec 隧道的任何数据包而不检查任何接口 ACL。
sysopt connection timewait	强制每个 TCP 连接在最后常规 TCP 关闭序列后短暂停留在 TIME_WAIT 状态。

sysopt connection timewait

要强制每个 TCP 连接在最后正常 TCP 关闭序列后短暂停留在 TIME_WAIT 状态至少 15 秒，请在全局配置模式下使用 **sysopt connection timewait** 命令。要禁用此功能，请使用此命令的 **no** 形式。如果终端主机应用的默认 TCP 中断序列是同时关闭序列，您可能想要使用此功能。

sysopt connection timewait

no sysopt connection timewait

注意　RST 数据包（不是常规 TCP 关闭序列）也会触发 15 秒延迟。ASA 在接收到连接的最后一个数据包（FIN/ACK 或 RST）后，会保留连接 15 秒。

语法说明

此命令没有任何参数或关键字。

默认值

默认禁用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 的默认行为是跟踪关闭序列，并在两个 FIN 以及最后一个 FIN 分段得到确认后释放连接。这种快速启发式释放使 ASA 可以根据最常见的关闭序列（又称为常规关闭序列）保持较高的连接速率。但在同时关闭序列中，事务的两个终端都会发起关闭序列；与之相反，在常规关闭序列中，如果一个终端关闭，另一个终端会先进行确认再发起自身的关闭序列（请参阅 RFC 793）。因此，在同时关闭序列中，快速释放会强制连接的一端停留在 CLOSING 状态。当处于 CLOSING 状态时，使用很多套接字可能会降低终端主机的性能。例如，某些 WinSock 大型机客户端会表现出这种行为，因此会降低大型机服务器的性能。使用 **sysopt connection timewait** 命令可以预留同时关闭序列完成所需的时间。

示例

以下示例启用等待功能：

```
ciscoasa(config)# sysopt connection timewait
```

相关命令

命令	说明
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。
sysopt connection permit-ipsec	允许来自 IPsec 隧道的任何数据包而不检查任何接口 ACL。
sysopt connection tcpmss	覆盖 TCP 最大分段大小或确保最大分段大小不小于指定大小。

sysopt noproxyarp

要禁用接口上 NAT 全局地址或 VPN 客户端地址的代理 ARP，请在全局配置模式下使用 **sysopt noproxyarp** 命令。要重新启用代理 ARP，请使用此命令的 **no** 形式。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

语法说明

interface_name	要禁用代理 ARP 的接口名称。

默认值

默认情况下，代理 ARP 已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(3)	此命令进行了扩展，现在，如果 VPN 客户端地址与内部网络重叠，此命令会影响 VPN 代理 ARP。

使用指南

如果 VPN 客户端地址池与现有网络重叠，默认情况下，ASA 会在所有接口上发送代理 ARP。如果有另一个接口位于同一个第 2 层域中，该接口将会看到 ARP 请求并以自身接口的 MAC 地址作出响应。其结果是，流向内部主机的 VPN 客户端返回流量会进入错误的接口并被丢弃。在这种情况下，需要对您不需要使用代理 ARP 的接口输入 **sysopt noproxyarp** 命令。

在极少数情况下，您可能要对 NAT 全局地址禁用代理 ARP。

当主机向同一以太网网络上的另一台设备发送 IP 流量时，主机需要知道该设备的 MAC 地址。ARP 是一个第 2 层协议，它将 IP 地址解析为 MAC 地址。如果主机发送 ARP 请求并询问 “Who is this IP address?”（这是谁的 IP 地址？），拥有该 IP 地址的设备会回答：“I own that IP address; here is my MAC address.”（这是我的 IP 地址；这是我的 MAC 地址。）

如果使用代理 ARP，设备会以自身的 MAC 地址对 ARP 请求作出响应，即使设备没有 IP 地址。如果您配置了 NAT 并指定一个与 ASA 接口位于同一网络上的全局地址，ASA 会使用代理 ARP。流量可到达主机的唯一方法是，ASA 使用代理 ARP 来声明 ASA MAC 地址已分配给目标全局地址。

示例

以下示例在内部接口上禁用代理 ARP：

```
ciscoasa(config)# sysopt noproxyarp inside
```

相关命令

命令	说明
alias	转换外部地址并根据转换更改 DNS 记录。
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。
sysopt nodnsalias	禁止在使用 **alias** 命令时更改 DNS A 记录地址。

sysopt radius ignore-secret

要忽略 RADIUS 记账响应中的身份验证密钥，请在全局配置模式下使用 **sysopt radius ignore-secret** 命令。要禁用此功能，请使用此命令的 **no** 形式。为了兼容某些 RADIUS 服务器，可能需要忽略密钥。

sysopt radius ignore-secret

no sysopt radius ignore-secret

语法说明

此命令没有任何参数或关键字。

默认值

默认禁用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

某些 RADIUS 服务器无法在记账确认响应的验证器哈希中包含密钥。按照此使用说明进行操作可促使 ASA 继续重传记账请求。使用 **sysopt radius ignore-secret** 命令可忽略记账确认中的密钥，从而避免重传问题。（这里标识的密钥与使用 **aaa-server host** 命令设置的密钥相同。）

示例

以下示例忽略记账响应中的身份验证密钥：

```
ciscoasa(config)# sysopt radius ignore-secret
```

相关命令

命令	说明
aaa-server host	标识 AAA 服务器。
clear configure sysopt	清除 **sysopt** 命令配置。
show running-config sysopt	显示 **sysopt** 命令配置。