适用于 Cisco Firepower 9300 的 DefensePro 用户指南

软件版本：1.01.02

最近更新日期：2016 年 4 月 4 日

重要声明

以下重要声明提供中文、法语和德语版本。

版权声明

以下版权声明提供中文、法语和德语版本。

版权声明

本产品中包括的程序受限制使用许可的约束，并且仅可与本应用结合使用。

OpenSSL 工具包适用双重许可，即 OpenSSL 许可和原有的 SSLeay 许可同时适用于该工具包。有关实际的许可文本，请参阅以下信息。事实上，两种许可均为 BSD 样式的开源许可。如有任何与 OpenSSL 相关的许可问题，请联系 openssl-core@openssl.org。

OpenSSL 许可

版权所有 (c) 1998-2011 OpenSSL Project。保留所有权利。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的重新分发必须保留上述版权声明、本条件列表及以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。
3. 所有提及该软件功能或使用的广告资料都必须显示以下内容：

   该产品包括由 OpenSSL Project 开发的软件，以便用于 OpenSSL Toolkit。(http://www.openssl.org/)
4. 不经事先书面许可，不得将名称“OpenSSL 工具包”和“OpenSSL Project”用于促销和宣传本软件的衍生产品。有关书面许可的信息，请联系 openssl-core@openssl.org。
5. 未经 OpenSSL Project 事先书面许可，从本软件的衍生产品不得称为“OpenSSL”，也不得在其名称中显示“OpenSSL”。
6. 无论何种形式的再分发都必须保留以下内容：

   “该产品包括由 OpenSSL Project 开发的软件，以便用于 OpenSSL 工具包 (http://www.openssl.org/)”

该软件由 OpenSSL PROJECT 按“原样”提供，但对于所有明示或暗示的担保（包括但不限于特定目的的适销性和适用性的暗示担保），均不承担任何责任。在任何情况下，OpenSSL PROJECT 或其参与者对于以任何方式使用该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损害（包括但不限于替代货物或服务的采购；用途丧失、数据丢失或利润损失；或业务中断），均不承担任何责任，无论导致前述损害的原因与责任推断如何，也无论是否因合同、严格责任或侵权（包括疏忽或其他原因）造成该等损害，即使已被告知发生此类损害的可能性。

此产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

原始 SSLeay 许可

版权所有 (C) 1995-1998 Eric Young (eay@cryptsoft.com) 保留所有权利。

该数据包是由 Eric Young (eay@cryptsoft.com) 编写的 SSL 实施。* 该应用与 Netscapes SSL 兼容。

只要符合以下条件，则本加密库可免费用于商业和非商业用途。以下条件适用于在该分发中出现的所有代码，可以是 RC4、RSA、lhash、DES 等代码，而不仅是 SSL 代码。包括在该分发中的 SSL 文档受相同版权条款限制，但其版权持有人是 Tim Hudson (tjh@cryptsoft.com)。

版权仍为 Eric Young 所有，因此不会删除代码中的任何版权声明。

如果在产品中使用该数据包，则应在所用库的部分的作者中署名 Eric Young。

此内容可以在程序启动时以文本消息的形式，也可以包括在随数据包提供的文档（在线或文本）中。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的再次分发必须保留版权声明、该条件列表和以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。
3. 所有提及该软件功能或使用的广告资料都必须显示以下内容：

   “本产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件”，如果加密库中使用的例行程序不涉及加密，可省去“加密”一词 :-)。
4. 如果您加入来自应用目录（应用代码）的任何 Windows 特定代码（或其衍生代码），则必须包括以下确认内容：

   “此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件”

该软件由 ERIC YOUNG 按“原样”提供，不承担任何明示或暗示的担保，包括但不限于用于特定用途的适销性和适用性的暗示担保。在任何情况下，作者或参与者对于以任何方式使用该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损害（包括但不限于替代货物或服务的采购；用途丧失、数据丢失或利润损失；或业务中断），均不承担任何责任，无论导致前述损害的原因与责任推断如何，也无论是否因合同、严格责任或侵权（包括疏忽或其他原因）造成该等损害，即使已被告知发生此类损害的可能性。

不得更改此代码的任何公开提供的版本或衍生代码的许可证和分发条款，即不可简单复制此代码或将其置于其他分发许可证之下 [包括 GNU 公共许可证]。

本产品包含 Rijndael 密码

Vincent Rijmen、Antoon Bosselaers 和 Paulo Barreto 设计的 Rijndael 算法在公共域中实施，并使用以下许可证进行分发：

@version 3.0（2000 年 12 月）

Rijndael 密码的优化 ANSI C 代码（现为 AES）

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

OnDemand Switch 可能会使用依据包括 LinuxBios 和 Filo 开源项目的 GNU 通用公共许可协议版本 2 (GPL v.2) 获得许可的软件组件。向 Radware 申请即可获得 LinuxBios 和 Filo 的源代码。可通过以下地址查看许可证副本：http://www.gnu.org/licenses/old-licenses/gpl-2.0.html。

特此将本代码置于公共域中。

本产品包含由 OpenBSD Project 开发的代码。

版权所有 © 1983、1990、1992、1993、1995，加州大学董事会。保留所有权利。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的重新分发必须保留上述版权声明、本条件列表及以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。
3. 未经事先明确书面许可，不得使用该大学校名及其参与者姓名宣传或推广本软件的衍生产品。

本产品包括由 Markus Friedl 开发的软件。本产品包括由 Theo de Raadt 开发的软件。本产品包括由 Niels Provos 开发的软件。本产品包括由 Dug Song 开发的软件。本产品包括由 Aaron Campbell 开发的软件。本产品包括由 Damien Miller 开发的软件。本产品包括由 Kevin Steves 开发的软件。本产品包括由 Daniel Kouril 开发的软件。本产品包括由 Wesley Griffin 开发的软件。本产品包括由 Per Allansson 开发的软件。本产品包括由 Nils Nordman 开发的软件。

本产品包括由 Simon Wilkinson 开发的软件。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的重新分发必须保留上述版权声明、本条件列表及以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。

本产品包含从 RSA Data Security, Inc. MD5 消息摘要算法衍生的工作成果。对于用于任何特定目的的 MD5 消息摘要算法的适销性或适用性，RSA Data Security, Inc. 不做任何陈述。这些成果按“原样”提供，不提供任何形式的明示或暗示担保。

Notice traitant du copyright

Les programmes intégrés dans ce produit sont soumis à une licence d’utilisation limitée et ne peuvent être utilisés qu’en lien avec cette application.

L’implémentation de Rijindael par Vincent Rijmen, Antoon Bosselaers et Paulo Barreto est du domaine public et distribuée sous les termes de la licence suivante:

@version 3.0 (Décembre 2000)

Code ANSI C code pour Rijndael (actuellement AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>.

Le commutateur OnDemand peut utiliser les composants logiciels sous licence, en vertu des termes de la licence GNU General Public License Agreement Version 2 (GPL v.2), y compris les projets à source ouverte LinuxBios et Filo. Le code source de LinuxBios et Filo est disponible sur demande auprès de Radware. Une copie de la licence est répertoriée sur: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

Ce code est également placé dans le domaine public.

Ce produit renferme des codes développés dans le cadre du projet OpenSSL. Copyright ©1983, 1990, 1992, 1993, 1995

Les membres du conseil de l'Université de Californie. Tous droits réservés.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou dans tout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
3. Le nom de l'université, ainsi que le nom des contributeurs ne seront en aucun cas utilisés pour approuver ou promouvoir un produit dérivé de ce programme sans l'obtention préalable d'une autorisation écrite.

Ce produit inclut un logiciel développé par Markus Friedl. Ce produit inclut un logiciel développé par Theo de Raadt. Ce produit inclut un logiciel développé par Niels Provos.

Ce produit inclut un logiciel développé par Dug Song.

Ce produit inclut un logiciel développé par Aaron Campbell. Ce produit inclut un logiciel développé par Damien Miller.

Ce produit inclut un logiciel développé par Kevin Steves. Ce produit inclut un logiciel développé par Daniel Kouril.

Ce produit inclut un logiciel développé par Wesley Griffin. Ce produit inclut un logiciel développé par Per Allansson.

Ce produit inclut un logiciel développé par Nils Nordman. Ce produit inclut un logiciel développé par Simon Wilkinson.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou dans tout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.

LE LOGICIEL MENTIONNÉ CI-DESSUS EST FOURNI TEL QUEL PAR LE DÉVELOPPEUR ET TOUTE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE.

EN AUCUN CAS L'AUTEUR NE POURRA ÊTRE TENU RESPONSABLE DES DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS S'Y LIMITER, L'ACQUISITION DE BIENS OU DE SERVICES DE REMPLACEMENT, LA PERTE D'USAGE, DE DONNÉES OU DE PROFITS OU L'INTERRUPTION DES AFFAIRES), QUELLE QU'EN SOIT LA CAUSE ET LA THÉORIE DE RESPONSABILITÉ, QU'IL S'AGISSE D'UN CONTRAT, DE RESPONSABILITÉ STRICTE OU D'UN ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE), DÉCOULANT DE QUELLE QUE FAÇON QUE CE SOIT DE L'USAGE DE CE LOGICIEL, MÊME S'IL A ÉTÉ AVERTI DE LA POSSIBILITÉ D'UN TEL DOMMAGE.

Copyrightvermerke

Die in diesem Produkt enthalten Programme unterliegen einer eingeschränkten Nutzungslizenz und können nur in Verbindung mit dieser Anwendung benutzt werden.

Die Rijndael-Implementierung von Vincent Rijndael, Anton Bosselaers und Paulo Barreto ist öffentlich zugänglich und wird unter folgender Lizenz vertrieben:

@version 3.0 (December 2000)

Optimierter ANSI C Code für den Rijndael cipher (jetzt AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

Der OnDemand Switch verwendet möglicherweise Software, die im Rahmen der DNU Allgemeine Öffentliche Lizenzvereinbarung Version 2 (GPL v.2) lizensiert sind, einschließlich LinuxBios und Filo Open Source-Projekte. Der Quellcode von LinuxBios und Filo ist bei Radware auf Anfrage erhältlich. Eine Kopie dieser Lizenz kann eingesehen werden unter http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

Dieser Code wird hiermit allgemein zugänglich gemacht.

Dieses Produkt enthält einen vom OpenBSD-Projekt entwickelten Code Copyright ©1983, 1990, 1992, 1993, 1995

The Regents of the University of California. Alle Rechte vorbehalten.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.
3. Weder der Name der Universität noch die Namen der Beitragenden dürfen ohne ausdrückliche vorherige schriftliche Genehmigung verwendet werden, um von dieser Software abgeleitete Produkte zu empfehlen oder zu bewerben.

Dieses Produkt enthält von Markus Friedl entwickelte Software. Dieses Produkt enthält von Theo de Raadt entwickelte Software. Dieses Produkt enthält von Niels Provos entwickelte Software.

Dieses Produkt enthält von Dug Song entwickelte Software. Dieses Produkt enthält von Aaron Campbell entwickelte Software. Dieses Produkt enthält von Damien Miller entwickelte Software. Dieses Produkt enthält von Kevin Steves entwickelte Software.

Dieses Produkt enthält von Daniel Kouril entwickelte Software. Dieses Produkt enthält von Wesley Griffin entwickelte Software. Dieses Produkt enthält von Per Allansson entwickelte Software. Dieses Produkt enthält von Nils Nordman entwickelte Software. Dieses Produkt enthält von Simon Wilkinson entwickelte Software.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.

SÄMTLICHE VORGENANNTE SOFTWARE WIRD VOM AUTOR IM IST-ZUSTAND (“AS IS”) BEREITGESTELLT. JEGLICHE AUSDRÜCKLICHEN ODER IMPLIZITEN GARANTIEN, EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF DIE IMPLIZIERTEN GARANTIEN DER MARKTGÄNGIGKEIT UND DER ANWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK, SIND AUSGESCHLOSSEN.

UNTER KEINEN UMSTÄNDEN HAFTET DER AUTOR FÜR DIREKTE ODER INDIREKTE SCHÄDEN, FÜR BEI VERTRAGSERFÜLLUNG ENTSTANDENE SCHÄDEN, FÜR BESONDERE SCHÄDEN, FÜR SCHADENSERSATZ MIT STRAFCHARAKTER, ODER FÜR FOLGESCHÄDEN EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF, ERWERB VON ERSATZGÜTERN ODER ERSATZLEISTUNGEN; VERLUST AN NUTZUNG, DATEN ODER GEWINN; ODER GESCHÄFTSUNTERBRECHUNGEN) GLEICH, WIE SIE ENTSTANDEN SIND, UND FÜR JEGLICHE ART VON HAFTUNG, SEI ES VERTRÄGE, GEFÄHRDUNGSHAFTUNG, ODER DELIKTISCHE HAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER ANDERE), DIE IN JEGLICHER FORM FOLGE DER BENUTZUNG DIESER SOFTWARE IST, SELBST WENN AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WURDE.

标准保修

以下标准保修提供中文、法语和德语版本。

标准保修

Radware 对其所有产品（下称“产品”）提供有限保修。自发货日期起一年内，Radware 对其硬件产品的材料和工艺瑕疵提供保修。自采购日期起最多 90 日内，Radware 对其软件提供漏洞修复的标准保修。如果产品装置在前述期间内的任何时间发生故障，Radware 将自行决定维修或更换产品。

对于硬件保修服务或维修，产品必须退回至由 Radware 指定的服务设备。将产品退回至 Radware 的运费应由客户支付，而将产品返回至客户的运费应由 Radware 支付。请参阅客户采购订单“标准保修”部分概述的具体细节。

如果产品和/或瑕疵组件发生使用不当、疏忽、意外或安装不当，或者由非 Radware 授权服务人员进行维修或修改，除非其他人员进行的此类维修经过 Radware 的书面同意，否则 Radware 将免于承担其标准保修下的所有义务。

除上述内容外，所有 RADWARE 产品（硬件和软件）均按“原样”提供，不承担任何明示或暗示的担保，包括但不限于用于特定用途的适销性和适用性的暗示担保。

Garantie standard

Radware octroie une garantie limitée pour l’ensemble de ses produits (“Produits”). Le matériel informatique (hardware) Radware est garanti contre tout défaut matériel et de fabrication pendant une durée d’un an à compter de la date d’expédition. Les logiciels (software) Radware sont fournis avec une garantie standard consistant en la fourniture de correctifs des dysfonctionnements du logiciels (bugs) pendant une durée maximum de 90 jours à compter de la date d’achat. Dans l’hypothèse où un Produit présenterait un défaut pendant ladite (lesdites) période(s), Radware procédera, à sa discrétion, à la réparation ou à l’échange du Produit.

S’agissant de la garantie d’échange ou de réparation du matériel informatique, le Produit doit être retourné chez un réparateur désigné par Radware. Le Client aura à sa charge les frais d’envoi du Produit à Radware et Radware supportera les frais de retour du Produit au client. Veuillez consulter les conditions spécifiques décrites dans la partie “Garantie Standard” du bon de commande client.

Radware est libérée de toutes obligations liées à la Garantie Standard dans l’hypothèse où le Produit et/ou le composant défectueux a fait l’objet d’un mauvais usage, d’une négligence, d’un accident ou d’une installation non conforme, ou si les réparations ou les modifications qu’il a subi ont été effectuées par d’autres personnes que le personnel de maintenance autorisé par Radware, sauf si Radware a donné son consentement écrit à ce que de telles réparations soient effectuées par ces personnes.

SAUF DANS LES CAS PREVUS CI-DESSUS, L’ENSEMBLE DES PRODUITS RADWARE (MATERIELS ET LOGICIELS) SONT FOURNIS “TELS QUELS” ET TOUTES GARANTIES EXPRESSES OU IMPLICITES SONT EXCLUES, EN CE COMPRIS, MAIS SANS S’Y RESTREINDRE, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE ET D’ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

保修和责任限制

以下保修和责任限制提供中文、法语和德语版本。

保修和责任限制

在任何情况下，对于因使用本用户指南所述的产品（包括硬件和软件），或因本用户指南本身的任何缺陷或差错而造成的任何损害，RADWARE LTD. 或其任何附属公司不承担任何责任。这包括但不限于任何直接、间接、意外、特殊、惩罚性或后果性损害（包括但不限于替代货物或服务的采购；用途丧失、数据丢失或利润损失；或业务中断）。即使 RADWARE 已被告知发生此类损害的可能性，上述限制仍然适用。由于某些司法管辖区不允许排除或限制偶然或后果性损害的暗示担保或责任，因此，上述限制或排除可能对您不适用。

Limitations de la Garantie et Responsabilité

RADWARE LTD. OU SES ENTITIES AFFILIES NE POURRONT EN AUCUN CAS ETRE TENUES RESPONSABLES DES DOMMAGES SUBIS DU FAIT DE L'UTILISATION DES PRODUITS (EN CE COMPRIS LES MATERIELS ET LES LOGICIELS) DECRITS DANS CE MANUEL D'UTILISATION, OU DU FAIT DE DEFAUT OU D'IMPRECISIONS DANS CE MANUEL D'UTILISATION, EN CE COMPRIS, SANS TOUTEFOIS QUE CETTE ENUMERATION SOIT CONSIDEREE COMME LIMITATIVE, TOUS DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPECIAUX, EXEMPLAIRES, OU ACCESSOIRES (INCLUANT, MAIS SANS S'Y RESTREINDRE, LA FOURNITURE DE PRODUITS OU DE SERVICES DE REMPLACEMENT; LA PERTE D'UTILISATION, DE DONNEES OU DE PROFITS; OU L'INTERRUPTION DES AFFAIRES). LES LIMITATIONS CI-DESSUS S'APPLIQUERONT QUAND BIEN MEME RADWARE A ETE INFORMEE DE LA POSSIBLE EXISTENCE DE CES DOMMAGES. CERTAINES JURIDICTIONS N'ADMETTANT PAS LES EXCLUSIONS OU LIMITATIONS DE GARANTIES IMPLICITES OU DE RESPONSABILITE EN CAS DE DOMMAGES ACCESSOIRES OU INDIRECTS, LESDITES LIMITATIONS OU EXCLUSIONS POURRAIENT NE PAS ETRE APPLICABLE DANS VOTRE CAS.

Haftungs- und Gewährleistungsausschluss

IN KEINEM FALL IST RADWARE LTD. ODER EIN IHR VERBUNDENES UNTERNEHMEN HAFTBAR FÜR SCHÄDEN, WELCHE BEIM GEBRAUCH DES PRODUKTES (HARDWARE UND SOFTWARE) WIE IM BENUTZERHANDBUCH BESCHRIEBEN, ODER AUFGRUND EINES FEHLERS ODER EINER UNGENAUIGKEIT IN DIESEM BENUTZERHANDBUCH SELBST ENTSTANDEN SIND. DAZU GEHÖREN UNTER ANDEREM (OHNE DARAUF BEGRENZT ZU SEIN) JEGLICHE DIREKTEN; IDIREKTEN; NEBEN; SPEZIELLEN, BELEGTEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH ABER NICHT BEGRENZT AUF BESCHAFFUNG ODER ERSATZ VON WAREN ODER DIENSTEN, NUTZUNGSAUSFALL, DATEN- ODER GEWINNVERLUST ODER BETRIEBSUNTERBRECHUNGEN). DIE OBEN GENANNTEN BEGRENZUNGEN GREIFEN AUCH, SOFERN RADWARE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SEIN SOLLTE. EINIGE RECHTSORDNUNGEN LASSEN EINEN AUSSCHLUSS ODER EINE BEGRENZUNG STILLSCHWEIGENDER GARANTIEN ODER HAFTUNGEN BEZÜGLICH NEBEN- ODER FOLGESCHÄDEN NICHT ZU, SO DASS DIE OBEN DARGESTELLTE BEGRENZUNG ODER DER AUSSCHLUSS SIE UNTER UMSTÄNDEN NICHT BETREFFEN WIRD.

安全说明

以下安全说明提供中文、法语和德语版本。

安全说明

小心

容易触碰的断开设备应通过建筑物的基础设施布线方式接入。

由于存在触电风险以及能源、机械和火灾隐患，任何涉及开启面板或更换组件的操作程序必须只能由具备资质的维修人员执行。

为了减少火灾和触电风险，在拆卸盖板或面板前请先断开设备的电源线路。

下图显示贴在双电源 Radware 平台上的警告标签。

图 1：触电危险标签

小心	ATTENTION
本装置拥有多个电源。在维修之前，请断开所有电源避免触电。	Cette unité a plus d'une source d'alimentation électrique. Débranchez toutes les sources d'alimentations électriques avant toute maintenance pour éviter les chocs électriques.

中文版双电源系统安全警告

下图为双电源 Radware 平台的警告。

图 2：中文版双电源系统安全警告

本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

中文版双电源系统安全警告翻译：

本装置拥有多个电源。在维修之前，请断开所有电源避免触电。

维修

除非您具备相关资格，否则请勿执行操作说明中未包含的任何维修操作。装置内部无可维修部件。

高电压

必须尽可能避免在电压不足的情况下对打开的仪器进行任何调整、维护和维修作业，当作业不可避免时，必须由了解相关危害的熟练人员执行相关作业。

即使仪器已断开电源，仪器内部的电容器仍可能处于充电状态。

接地

将本设备连接至电源线路之前，必须将本设备的保护接地固定螺钉连接至建筑物的基础设施的保护接地。

激光

本设备为符合 IEC60825 - 1:1993 + A1:1997 + A2:2001 标准的 1 类激光产品。

熔断器

确保更换时仅使用符合额定电流要求的指定类型的熔断器。必须避免使用修理过的熔断器和发生短路的熔断器盒。当熔断器所提供的保护可能遭受破坏时，必须停止运行仪器并确保防止任何误操作。

线路电压

将本仪器连接至电源线路之前，确保电源电压符合本仪器的要求。有关设备正确额定功率的信息，请参阅规格说明。

48V 直流供电平台的输入电压容差为直流 36-72V。

规格变更

规格如有变更，恕不另行通知。

注意：本设备已经过测试并符合依照 FCC 规则 15B 部分和 EN55022 A 类、EN 55024；EN 61000-3-2；EN 61000-3-3；IEC 61000 4-2 到 4-6、IEC 61000 4-8 以及 IEC 61000-4-11For CE MARK Compliance 对 A 类数字设备的限制。
这些限制旨在提供合理保护，使设备在商业环境下运行时免于有害干扰。本设备产生、使用且可能发射无线电射频能量，如果不遵照说明手册进行安装和使用，则可能会对无线电通信造成有害干扰。如果在住宅区运行该设备，则有可能导致有害干扰，在这种情况下，用户必须校正此类干扰，费用自行承担。

致北美用户的特别通知

对于北美地区的电源连接，请选择一根满足以下要求的电源线： UL 认证列名和 CSA 认证 3 芯芯线，[18 AWG]，末端采用额定功率为 125 V、[10 A] 的模塑插头，最小长度 1.5 米 [六英尺]，但不超过 4.5 米。对于欧洲地区的电源连接，请选择一根满足以下要求的电源线：符合国际协调标准并标有“<HAR>”，3 芯芯线，电线最小截面积为 0.75 平方毫米，额定功率 300 V，具有 PVC 绝缘护套。电源线必须具有额定电压和电流为 250 V、3 A 的模塑插头。

限制进出的场所

在限制进出的场所内应仅安装直流供电设备。

安装规范

本设备必须遵照国家/地区电气规范进行安装。对于北美地区，必须遵照美国国家电气规范的条款 110-16、110-17 和 110-18 以及加拿大电气规范第 12 节的规定安装设备。

装置互联

连接装置 RS232 和以太网接口的线缆必须为 UL 认证 DP-1 型或 DP-2 型。（注意 - 处于非 LPS 电路中时)

过电流保护

对于各电源输入，若易于接触的分支电路通过额定 15 A 过电流保护设备传输，必须通过建筑布线接入。

可更换电池

如果设备具有可更换电池，并更换了错误类型的电池，则可能发生爆炸。某些锂电池会出现这种情况，以下情况适用：

- 如果电池置于**操作人员触及区**中，那么电池附近会有标记，并且在操作和维修说明中存在表述。
- 如果电池置于设备中的他处，电池附近会有标记，或在维修说明中存在表述。

此记号或说明包括以下文本警告：小心

如果更换类型错误的电池，则存在爆炸风险。请根据说明处理用过的电池。

小心 - 为降低触电和火灾风险

1. 本设备旨在允许直流供电电路的接地导体与接地导体设备进行连接。请参阅安装说明。
2. 所有维修必须由具备资格的维修人员进行。装置内部无用户可维修的部件。
3. 请勿插入、打开或尝试操作明显损坏的装置。
4. 请确保装置中机箱的通风口未堵塞。
5. 仅使用其类型和额定功率与标记于安全标签（临近容纳保险丝的电源接入装置）上的类型和功率相同的保险丝进行更换。
6. 请勿在最高环境温度高于 40°C/104°F 的地点操作设备。
7. 在尝试拆除和/或检查总电源保险丝之前，请确保从墙壁插座中拔出电源线。

   1 类激光产品及对最新激光标准 IEC 60 825-1:1993 + A1:1997 + A2:2001 和 EN 60825-1:1994+A1:1996+ A2:2001 的参考

丹麦、芬兰、挪威、瑞典的交流装置（标于产品上）：

- 丹麦 - “Unit is class I - unit to be used with an AC cord set suitable with Denmark deviations.The cord includes an earthing conductor.The Unit is to be plugged into a wall socket outlet which is connected to a protective earth.Socket outlets which are not connected to earth are not to be used!”
- 芬兰 -（标记标签和手册中）- “Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan”
- 挪威（标记标签和手册中）- “Apparatet må tilkoples jordet stikkontakt”
- 装置旨在连接挪威的 IT 电力系统。
- 瑞典（标记标签和手册中）- “Apparaten skall anslutas till jordat uttag.”

要连接电源连接，请执行以下操作：

1. 将电源线连接到位于设备后面板上的主插座。
2. 将电源线连接到接地交流电源插座。

小心

触电和能量隐患风险。断开一个电源仅会断开一个电源模块。要完全隔离装置，请断开所有电源。

Instructions de sécurité

AVERTISSEMENT

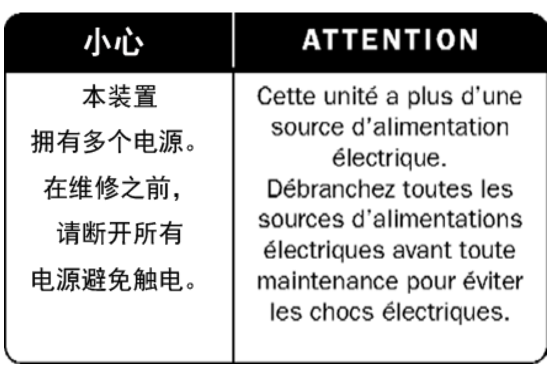
Un dispositif de déconnexion facilement accessible sera incorporé au câblage du bâtiment.

En raison des risques de chocs électriques et des dangers énergétiques, mécaniques et d’incendie, chaque procédure impliquant l’ouverture des panneaux ou le remplacement de composants sera exécutée par du personnel qualifié.

Pour réduire les risques d’incendie et de chocs électriques, déconnectez le dispositif du bloc d’alimentation avant de retirer le couvercle ou les panneaux.

La figure suivante montre l’étiquette d’avertissement apposée sur les plateformes Radware dotées de plus d’une source d’alimentation électrique.

Figure 3: Étiquette d’avertissement de danger de chocs électriques



AVERTISSEMENT DE SÉCURITÉ POUR LES SYSTÈMES DOTÉS DE DEUX SOURCES D’ALIMENTATION ÉLECTRIQUE (EN CHINOIS)

La figure suivante représente l’étiquette d’avertissement pour les plateformes Radware dotées de deux sources d’alimentation électrique.

Figure 4: Avertissement de sécurité pour les systèmes dotes de deux sources d’alimentation électrique (en chinois)

本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

Traduction de la Avertissement de sécurité pour les systèmes dotes de deux sources d’alimentation électrique (en chinois):

Cette unité est dotée de plus d’une source d’alimentation électrique. Déconnectez toutes les sources d’alimentation électrique avant d’entretenir l’appareil ceci pour éviter tout choc électrique.

ENTRETIEN

N’effectuez aucun entretien autre que ceux répertoriés dans le manuel d’instructions, à moins d’être qualifié en la matière. Aucune pièce à l’intérieur de l’unité ne peut être remplacée ou réparée.

HAUTE TENSION

Tout réglage, opération d’entretien et réparation de l’instrument ouvert sous tension doit être évité. Si cela s’avère indispensable, confiez cette opération à une personne qualifiée et consciente des dangers impliqués.

Les condensateurs au sein de l’unité risquent d’être chargés même si l’unité a été déconnectée de la source d’alimentation électrique.

MISE A LA TERRE

Avant de connecter ce dispositif à la ligne électrique, les vis de protection de la borne de terre de cette unité doivent être reliées au système de mise à la terre du bâtiment.

LASER

Cet équipement est un produit laser de classe 1, conforme à la norme IEC60825 - 1: 1993 + A1: 1997 + A2: 2001.

FUSIBLES

Assurez-vous que, seuls les fusibles à courant nominal requis et de type spécifié sont utilisés en remplacement. L’usage de fusibles réparés et le court-circuitage des porte-fusibles doivent être évités. Lorsqu’il est pratiquement certain que la protection offerte par les fusibles a été détériorée, l’instrument doit être désactivé et sécurisé contre toute opération involontaire.

TENSION DE LIGNE

Avant de connecter cet instrument à la ligne électrique, vérifiez que la tension de la source d’alimentation correspond aux exigences de l’instrument. Consultez les spécifications propres à l’alimentation nominale correcte du dispositif.

Les plateformes alimentées en 48 CC ont une tolérance d’entrée comprise entre 36 et 72 V CC. MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC
61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l’équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s’il n’est pas installé et utilisé conformément au manuel d’instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l’utilisateur devra corriger le problème à ses propres frais.

NOTICE SPÉCIALE POUR LES UTILISATEURS NORD-AMÉRICAINS

Pour un raccordement électrique en Amérique du Nord, sélectionnez un cordon d'alimentation homologué UL et certifié CSA 3 - conducteur, [18 AWG], muni d'une prise moulée à son extrémité, de 125 V, [10 A], d'une longueur minimale de 1,5 m [six pieds] et maximale de 4,5m...Pour la connexion européenne, choisissez un cordon d'alimentation mondialement homologué et marqué "<HAR>", 3 - conducteur, câble de 0,75 mm2 minimum, de 300 V, avec une gaine en PVC isolée. La prise à l'extrémité du cordon, sera dotée d'un sceau moulé indiquant: 250 V, 3 A.

ZONE A ACCÈS RESTREINT

L'équipement alimenté en CC ne pourra être installé que dans une zone à accès restreint. CODES

D'INSTALLATION

Ce dispositif doit être installé en conformité avec les codes électriques nationaux. En Amérique du Nord, l'équipement sera installé en conformité avec le code électrique national américain, articles 110-16, 110 -17, et 110 -18 et le code électrique canadien, Section 12.

INTERCONNEXION DES UNÎTES

Les câbles de connexion à l'unité RS232 et aux interfaces Ethernet seront certifiés UL, type DP-1 ou DP-2. (Remarque- s'ils ne résident pas dans un circuit LPS).

PROTECTION CONTRE LES SURCHARGES

Un circuit de dérivation, facilement accessible, sur le dispositif de protection du courant de 15 A doit être intégré au câblage du bâtiment pour chaque puissance consommée.

BATTERIES REMPLAÇABLES

Si l'équipement est fourni avec une batterie, et qu'elle est remplacée par un type de batterie incorrect, elle est susceptible d'exploser. C'est le cas pour certaines batteries au lithium, les éléments suivants sont donc applicables:

- Si la batterie est placée dans une zone d'accès opérateur, une marque est indiquée sur la batterie ou une remarque est insérée, aussi bien dans les instructions d'exploitation que d'entretien.
- Si la batterie est placée ailleurs dans l'équipement, une marque est indiquée sur la batterie ou une remarque est insérée dans les instructions d'entretien.

Cette marque ou remarque inclut l'avertissement textuel suivant: AVERTISSEMENT

RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UN MODÈLE INCORRECT. METTRE AU REBUT LES BATTERIES CONFORMÉMENT AUX INSTRUCTIONS.

Attention - Pour réduire les risques de chocs électriques et d'incendie

1. Cet équipement est conçu pour permettre la connexion entre le conducteur de mise à la terre du circuit électrique CC et l'équipement de mise à la terre. Voir les instructions d'installation.
2. Tout entretien sera entrepris par du personnel qualifié. Aucune pièce à l'intérieur de l'unité ne peut être remplacée ou réparée.
3. NE branchez pas, n'allumez pas ou n'essayez pas d'utiliser une unité manifestement endommagée.
4. Vérifiez que l'orifice de ventilation du châssis dans l'unité n'est PAS OBSTRUE.
5. Remplacez le fusible endommagé par un modèle similaire de même puissance, tel qu'indiqué sur l'étiquette de sécurité adjacente à l'arrivée électrique hébergeant le fusible.
6. Ne faites pas fonctionner l'appareil dans un endroit, où la température ambiante dépasse la valeur maximale autorisée. 40°C/104°F.
7. Débranchez le cordon électrique de la prise murale AVANT d'essayer de retirer et/ou de vérifier le fusible d'alimentation principal.

PRODUIT LASER DE CLASSE 1 ET RÉFÉRENCE AUX NORMES LASER LES PLUS RÉCENTES: IEC 60 825-1:

1993 + A1: 1997 + A2: 2001 ET EN 60825-1: 1994+A1: 1996+ A2: 2001

Unités à CA pour le Danemark, la Finlande, la Norvège, la Suède (indiqué sur le produit):

- Danemark - Unité de classe 1 - qui doit être utilisée avec un cordon CA compatible avec les déviations du Danemark. Le cordon inclut un conducteur de mise à la terre. L'unité sera branchée à une prise murale, mise à la terre. Les prises non-mises à la terre ne seront pas utilisées!
- Finlande (Étiquette et inscription dans le manuel) - Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan
- Norvège (Étiquette et inscription dans le manuel) - Apparatet må tilkoples jordet stikkontakt
- L'unité peut être connectée à un système électrique IT (en Norvège uniquement).
- Suède (Étiquette et inscription dans le manuel) - Apparaten skall anslutas till jordat uttag.

Pour brancher à l'alimentation électrique:

1. Branchez le câble d'alimentation à la prise principale, située sur le panneau arrière de l'unité.
2. Connectez le câble d'alimentation à la prise CA mise à la terre. AVERTISSEMENT

Risque de choc électrique et danger énergétique. La déconnexion d'une source d'alimentation électrique ne débranche qu'un seul module électrique. Pour isoler complètement l'unité, débranchez toutes les sources d'alimentation électrique.

ATTENTION

Risque de choc et de danger électriques. Le débranchement d'une seule alimentation stabilisée ne débranche qu'un module "Alimentation Stabilisée". Pour Isoler complètement le module en cause, il faut débrancher toutes les alimentations stabilisées.

Attention: Pour Réduire Les Risques d'Électrocution et d'Incendie

1. Toutes les opérations d'entretien seront effectuées UNIQUEMENT par du personnel d'entretien qualifié. Aucun composant ne peut être entretenu ou remplacée par l'utilisateur.
2. NE PAS connecter, mettre sous tension ou essayer d'utiliser une unité visiblement défectueuse.
3. Assurez-vous que les ouvertures de ventilation du châssis NE SONT PAS OBSTRUÉES.
4. Remplacez un fusible qui a sauté SEULEMENT par un fusible du même type et de même capacité, comme indiqué sur l'étiquette de sécurité proche de l'entrée de l'alimentation qui contient le fusible.
5. NE PAS UTILISER l'équipement dans des locaux dont la température maximale dépasse 40 degrés Centigrades.
6. Assurez vous que le cordon d'alimentation a été déconnecté AVANT d'essayer de l'enlever et/ou vérifier le fusible de l'alimentation générale.

Sicherheitsanweisungen

VORSICHT

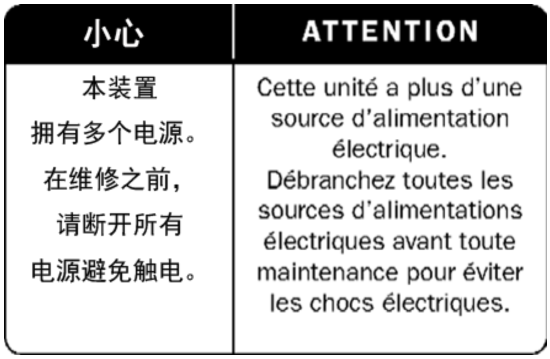
Die Elektroinstallation des Gebäudes muss ein unverzüglich zugängliches Stromunterbrechungsgerät integrieren.

Aufgrund des Stromschlagrisikos und der Energie-, mechanische und Feuergefahr dürfen Vorgänge, in deren Verlauf Abdeckungen entfernt oder Elemente ausgetauscht werden, ausschließlich von qualifiziertem Servicepersonal durchgeführt werden.

Zur Reduzierung der Feuer- und Stromschlaggefahr muss das Gerät vor der Entfernung der Abdeckung oder der Paneele von der Stromversorgung getrennt werden.

Folgende Abbildung zeigt das VORSICHT-Etikett, das auf die Radware-Plattformen mit Doppelspeisung angebracht ist.

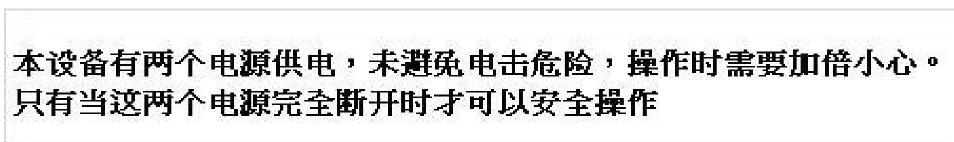
Figure 5: Warnetikett Stromschlaggefahr



SICHERHEITSHINWEIS IN CHINESISCHER SPRACHE FÜR SYSTEME MIT DOPPELSPEISUNG

Die folgende Abbildung ist die Warnung für Radware-Plattformen mit Doppelspeisung.

Figure 6: Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung


本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

Übersetzung von [Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung]:

Die Einheit verfügt über mehr als eine Stromversorgungsquelle. Ziehen Sie zur Verhinderung von Stromschlag vor Wartungsarbeiten sämtliche Stromversorgungsleitungen ab.

WARTUNG

Führen Sie keinerlei Wartungsarbeiten aus, die nicht in der Betriebsanleitung angeführt sind, es sei denn, Sie sind dafür qualifiziert. Es gibt innerhalb des Gerätes keine wartungsfähigen Teile.

HOCHSPANNUNG

Jegliche Einstellungs-, Instandhaltungs- und Reparaturarbeiten am geöffneten Gerät unter Spannung müssen so weit wie möglich vermieden werden. Sind sie nicht vermeidbar, dürfen sie ausschließlich von qualifizierten Personen ausgeführt werden, die sich der Gefahr bewusst sind.

Innerhalb des Gerätes befindliche Kondensatoren können auch dann noch Ladung enthalten, wenn das Gerät von der Stromversorgung abgeschnitten wurde.

ERDUNG

Bevor das Gerät an die Stromversorgung angeschlossen wird, müssen die Schrauben der Erdungsleitung des Gerätes an die Erdung der Gebäudeverkabelung angeschlossen werden.

LASER

Dieses Gerät ist ein Laser-Produkt der Klasse 1 in Übereinstimmung mit IEC60825 - 1: 1993 + A1:1997 + A2:2001 Standard.

SICHERUNGEN

Vergewissern Sie sich, dass nur Sicherungen mit der erforderlichen Stromstärke und der angeführten Art verwendet werden. Die Verwendung reparierter Sicherungen sowie die Kurzschließung von Sicherungsfassungen muss vermieden werden. In Fällen, in denen wahrscheinlich ist, dass der von den Sicherungen gebotene Schutz beeinträchtigt ist, muss das Gerät abgeschaltet und gegen unbeabsichtigten Betrieb gesichert werden.

LEITUNGSSPANNUNG

Vor Anschluss dieses Gerätes an die Stromversorgung ist zu gewährleisten, dass die Spannung der Stromquelle den Anforderungen des Gerätes entspricht. Beachten Sie die technischen Angaben bezüglich der korrekten elektrischen Werte des Gerätes.

Plattformen mit 48 V DC verfügen über eine Eingangstoleranz von 36-72 V DC. ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to 4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

BESONDERER HINWEIS FÜR BENUTZER IN NORDAMERIKA

Wählen Sie für den Netzstromanschluss in Nordamerika ein Stromkabel, das in der UL aufgeführt und CSA-zertifiziert ist 3 Leiter, [18 AWG], endend in einem gegossenen Stecker, für 125 V, [10 A], mit einer Mindestlänge von 1,5 m [sechs Fuß], doch nicht länger als 4,5 m. Für europäische Anschlüsse verwenden Sie ein international harmonisiertes, mit “<HAR>” markiertes Stromkabel, mit 3 Leitern von mindestens 0,75 mm2, für 300 V, mit PVC-Umkleidung. Das Kabel muss in einem gegossenen Stecker für 250 V, 3 A enden.

BEREICH MIT EINGESCHRÄNKTEM ZUGANG

Das mit Gleichstrom betriebene Gerät darf nur in einem Bereich mit eingeschränktem Zugang montiert werden.

INSTALLATIONSCODES

Dieses Gerät muss gemäß der landesspezifischen elektrischen Codes montiert werden. In Nordamerika müssen Geräte entsprechend dem US National Electrical Code, Artikel 110 - 16, 110 - 17 und 110 - 18, sowie dem Canadian Electrical Code, Abschnitt 12, montiert werden.
VERKOPPLUNG VON GERÄTEN Kabel für die Verbindung des Gerätes mit RS232- und Ethernet- müssen UL-zertifiziert und vom Typ DP-1 oder DP-2 sein. (Anmerkung: bei Aufenthalt in einem nicht-LPS-Stromkreis)

ÜBERSTROMSCHUTZ

Ein gut zugänglicher aufgeführter Überstromschutz mit Abzweigstromkreis und 15 A Stärke muss für jede Stromeingabe in der Gebäudeverkabelung integriert sein.

AUSTAUSCHBARE BATTERIEN

Wird ein Gerät mit einer austauschbaren Batterie geliefert und für diese Batterie durch einen falschen Batterietyp ersetzt, könnte dies zu einer Explosion führen. Dies trifft zu für manche Arten von Lithiumsbatterien zu, und das folgende gilt es zu beachten:

- Wird die Batterie in einem Bereich für Bediener eingesetzt, findet sich in der Nähe der Batterie eine Markierung oder Erklärung sowohl im Betriebshandbuch als auch in der Wartungsanleitung.
- Ist die Batterie an einer anderen Stelle im Gerät eingesetzt, findet sich in der Nähe der Batterie eine Markierung oder einer Erklärung in der Wartungsanleitung.

Diese Markierung oder Erklärung enthält den folgenden Warntext: VORSICHT

EXPLOSIONSGEFAHR, FALLS BATTERIE DURCH EINEN FALSCHEN BATTERIETYP ERSETZT WIRD. GEBRAUCHTE BATTERIEN DEN ANWEISUNGEN ENTSPRECHEND ENTSORGEN.

- Denmark - “Unit is class I - mit Wechselstromkabel benutzen, dass für die Abweichungen in Dänemark eingestellt ist. Das Kabel ist mit einem Erdungsdraht versehen. Das Kabel wird in eine geerdete Wandsteckdose angeschlossen. Keine Steckdosen ohne Erdungsleitung verwenden!”
- Finland - (Markierungsetikett und im Handbuch) - Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan

- Norway - (Markierungsetikett und im Handbuch) - Apparatet må tilkoples jordet stikkontakt Ausschließlich für Anschluss an IT-Netzstromsysteme in Norwegen vorgesehen
- Sweden - (Markierungsetikett und im Handbuch) - Apparaten skall anslutas till jordat uttag.

Anschluss des Stromkabels:

1. Schließen Sie das Stromkabel an den Hauptanschluss auf der Rückseite des Gerätes an.
2. Schließen Sie das Stromkabel an den geerdeten Wechselstromanschluss an. VORSICHT

Stromschlag- und Energiegefahr Die Trennung einer Stromquelle trennt nur ein Stromversorgungsmodul von der Stromversorgung. Um das Gerät komplett zu isolieren, muss es von der gesamten Stromversorgung getrennt werden.

Vorsicht - Zur Reduzierung der Stromschlag- und Feuergefahr

1. Dieses Gerät ist dazu ausgelegt, die Verbindung zwischen der geerdeten Leitung des Gleichstromkreises und dem Erdungsleiter des Gerätes zu ermöglichen. Siehe Montageanleitung.
2. Wartungsarbeiten jeglicher Art dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Es gibt innerhalb des Gerätes keine vom Benutzer zu wartenden Teile.
3. Versuchen Sie nicht, ein offensichtlich beschädigtes Gerät an den Stromkreis anzuschließen, einzuschalten oder zu betreiben.
4. Vergewissern Sie sich, dass sie Lüftungsöffnungen im Gehäuse des Gerätes NICHT BLOCKIERT SIND.
5. Ersetzen Sie eine durchgebrannte Sicherung ausschließlich mit dem selben Typ und von der selben Stärke, die auf dem Sicherheitsetikett angeführt sind, das sich neben dem Stromkabelanschluss, am Sicherungsgehäuse.
6. Betreiben Sie das Gerät nicht an einem Standort, an dem die Höchsttemperatur der Umgebung 40°C überschreitet.
7. Vergewissern Sie sich, das Stromkabel aus dem Wandstecker zu ziehen, BEVOR Sie die Hauptsicherung entfernen und/oder prüfen.

电磁干扰声明

以下声明提供中文、法语和德语版本。

电磁干扰声明

规格变更

规格如有变更，恕不另行通知。

注意：本设备已经过测试并符合依照 FCC 规则 15B 部分和 EN55022 A 类、EN 55024；EN 61000-3-2；EN 61000-3-3；IEC 61000 4-2 到 4-6、IEC 61000 4-8 以及 IEC 61000-4-11For CE MARK Compliance 对 A 类数字设备的限制。
这些限制旨在提供合理保护，使设备在商业环境下运行时免于有害干扰。本设备产生、使用且可能发射无线电射频能量，如果不遵照说明手册进行安装和使用，则可能会对无线电通信造成有害干扰。如果在住宅区运行该设备，则有可能导致有害干扰，在这种情况下，用户必须校正此类干扰，费用自行承担。

VCCI 电磁干扰声明

图 7：A 类 VCCI 认证设备声明

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

A 类 VCCI 认证设备声明翻译：

这是基于日本电磁干扰控制委员会 (VCCI) 标准的 A 类产品。如果在生活环境中使用本设备，可能会造成无线电干扰，在这种情况下，用户可能需要采取校正措施。

KCC 韩国

图 8：KCC - 韩国通信委员会广播和通信设备证书

图 9：A 类 KCC 认证设备声明韩文版

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

A 类 KCC 认证设备声明韩文版翻译：

本设备为工业型（A 类）电磁波适用性设备，销售商或用户须注意，本设备用于家庭以外的场所。

BSMI

图 10：A 类 BSMI 认证设备声明

A 类 BSMI 认证设备声明翻译：

这是 A 类产品，如用于生活环境，本产品可能会造成无线电干扰，在这种情况下，将要求用户采取适当措施。

Déclarations sur les Interférences Électromagnétiques

MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC
61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger le problème à ses propres frais.

DÉCLARATIONS SUR LES INTERFÉRENCES ÉLECTROMAGNÉTIQUES VCCI

Figure 11: Déclaration pour l'équipement de classe A certifié VCCI

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Traduction de la Déclaration pour l'équipement de classe A certifié VCCI:

Il s'agit d'un produit de classe A, basé sur la norme du Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Si cet équipement est utilisé dans un environnement domestique, des perturbations radioélectriques sont susceptibles d'apparaître. Si tel est le cas, l'utilisateur sera tenu de prendre des mesures correctives.

KCC Corée

Figure 12: KCC—Certificat de la commission des communications de Corée pour les equipements de radiodiffusion et communication.

Figure 13: Déclaration pour l'équipement de classe A certifié KCC en langue coréenne

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Translation de la Déclaration pour l'équipement de classe A certifié KCC en langue coréenne:

Cet équipement est un matériel (classe A) en adéquation aux ondes électromagnétiques et le vendeur ou l'utilisateur doit prendre cela en compte. Ce matériel est donc fait pour être utilisé ailleurs qu' á la maison.

BSMI

Figure 14: Déclaration pour l’équipement de classe A certifié BSMI

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻
干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Translation de la Déclaration pour l’équipement de classe A certifié BSMI:

Il s’agit d’un produit de Classe A; utilisé dans un environnement résidentiel il peut provoquer des interférences, l’utilisateur devra alors prendre les mesures adéquates.

Erklärungen zu Elektromagnetischer Interferenz

ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to 4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

ERKLÄRUNG DER VCCI ZU ELEKTROMAGNETISCHER INTERFERENZ

Figure 15: Erklärung zu VCCI-zertifizierten Geräten der Klasse A

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Übersetzung von Erklärung zu VCCI-zertifizierten Geräten der Klasse A:

Dies ist ein Produkt der Klasse A gemäß den Normen des Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Wird dieses Gerät in einem Wohnbereich benutzt, können elektromagnetische Störungen auftreten. In einem solchen Fall wäre der Benutzer verpflichtet, korrigierend einzugreifen.

KCC KOREA

Figure 16: KCC—Korea Communications Commission Zertifikat für Rundfunk-und Nachrichtentechnik

Figure 17: Erklärung zu KCC-zertifizierten Geräten der Klasse A

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Übersetzung von Erklärung zu KCC-zertifizierten Geräten der Klasse A:

Verkäufer oder Nutzer sollten davon Kenntnis nehmen, daß dieses Gerät der Klasse A für industriell elektromagnetische Wellen geeignete Geräten angehört und dass diese Geräte nicht für den heimischen Gebrauch bestimmt sind.

BSMI

Figure 18: Erklärung zu BSMI-zertifizierten Geräten der Klasse A

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Übersetzung von Erklärung zu BSMI-zertifizierten Geräten der Klasse A:

Dies ist ein Class A Produkt, bei Gebrauch in einer Wohnumgebung kann es zu Funkstörungen kommen, in diesem Fall ist der Benutzer verpflichtet, angemessene Maßnahmen zu ergreifen.

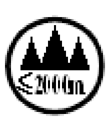
海拔和气候警告

此警告仅适用于中华人民共和国。

1. 对于在非热带气候条件下运行的设备而言，Tma：为制造商规范允许的最大环境温度，或者为 25°C，采用两者中的较大者。
2. 关于在海拔不超过 2000m 或者在非热带气候地区使用的设备，附加警告要求如下：

关于在海拔不超过 2000m 的地区使用的设备，必须在随时可见的位置处粘贴包含如下内容或者类似用语的警告标 记、或者附件 DD 中的符号。

“ 只可在海拔不超过 2000m 的位置使用。”

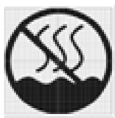


关于在非热带气候地区使用的设备，必须在随时可见的位置处粘贴包含如下内容的警告标记：

附件 DD：有关新安全警告标记的说明。DD.1 海拔警告标记

标记含义：设备的评估仅基于 2000m 以下的海拔高度，因此设备只适用于该运行条件。如果在海拔超过 2000m 的位置使用设备，可能会存在某些安全隐患。

DD.2 气候警告标记



标记含义：设备的评估仅基于温带气候条件，因此设备只适用于该运行条件。如果在热带气候地区使用设备，可能会存在某些安全隐患。

文档约定

下文介绍本指南使用的约定和符号：

项目	说明	说明	Beschreibung
示例	示例场景	Un scénario d’exemple	Ein Beispielszenarium
小心：	可能对设备、软件或数据造成损害	Endommagement possible de l’équipement, des données ou du logiciel	Mögliche Schäden an Gerät, Software oder Daten
注意：	其他信息	Informations complémentaires	Zusätzliche Informationen
目标	陈述和说明	Références et instructions	Eine Erklärung und Anweisungen
提示：	建议或解决方法	Une suggestion ou solution	Ein Vorschlag oder eine Umgehung
警告：	可能对操作人员造成人身伤害	Blessure possible de l’opérateur	Verletzungsgefahr des Bedieners

目录

第 1 章 - 简介

本指南介绍适用于 Cisco Firepower 9300 的 DefensePro 版本 1.01 及其使用方法。

除非另有特别说明，否则本指南中介绍的操作步骤均使用 APSolute Vision™ 版本 3.30 执行。

本章介绍 Radware 的 DefensePro 并提供对其主要功能和模块的一般解释。

本章包含以下各节：

DefensePro - 概述

Radware 的获奖产品 DefensePro™ 是一款实时入侵防御系统 (IPS) 和 DoS 保护设备，其通过保护应用基础设施免遭现有和新出现的基于网络的威胁来维持业务的连续性，这些威胁无法被传统 IPS 检测到，例如网络和应用资源的不当使用、恶意软件传播、身份验证失败和信息盗用。

通过主动签名更新，DefensePro 具有对基于漏洞的传统攻击的全方位保护，可防御已知的攻击，包括蠕虫、特洛伊木马、bot、基于 SSL 的攻击以及 VoIP 攻击。

与市场上依赖静态签名的其他产品不同，DefensePro 提供独特的基于行为自动生成的实时签名，预防非基于漏洞的攻击和零分钟攻击，例如：网络和应用泛洪、HTTP 页面泛洪、恶意软件传播、网络应用黑客攻击、旨在致使身份验证方案失败的暴力破解攻击等，均不会阻止合法用户的流量，并且无需人为干预。

DefensePro 系统组件

Radware DefensePro 是内联入侵防御和拒绝服务攻击防御系统，可实时检测和防御网络威胁。DefensePro 检测传入和传出流量是否存在潜在攻击行为，保障网络免受有害恶意流量的影响。

DefensePro 系统包含以下组件：

- **DefensePro 设备** - 术语*设备*指虚拟平台和 DefensePro 产品。
- **管理界面** - APSolute Vision 及其他界面。
- **Web 上的 Radware 安全更新服务。**

适用于 Cisco Firepower 9300 的 DefensePro

适用于 Cisco Firepower 9300 的 Radware *DefensePro* 是一个虚拟平台，在 Cisco Firepower 9300 平台上提供分布式拒绝服务 (DDoS) 检测和规避功能。Firepower 9300 是思科传输安全服务的新方法。Firepower 9300 可托管若干应用，例如 DDoS 保护器、IPS 和防火墙。应用或服务可链接到已启用的应用，为其他安全平台应用和最终客户提供服务。Firepower 9300 可以部署在各类部署场景中以支持不同的客户使用案例。

适用于 Cisco Firepower 9300 的 DefensePro 平台可以在最多三个计算刀片上运行。每个计算刀片托管以下组件：

- **Firepower 9300 软件基础设施实例** - 包含基于 Linux 的操作环境，具有可通过各种 API 访问的一系列通用服务，例如，日志记录、软件映像管理等。
- **基础设施顶层的一个或多个安全应用** - 这些应用可由思科或第三方提供。适用于 Cisco Firepower 9300 的 Radware 的 DefensePro 就是这种第三方应用之一。适用于 Cisco Firepower 9300 的 DefensePro 在基于 KVM 的虚拟机上运行。多个服务（例如，适用于 Cisco Firepower 9300 的 DefensePro、IPS 和防火墙）可以在一个刀片上共存。服务可链接。例如，适用于 Cisco Firepower 9300 的 DefensePro 可以首先内联并保护客户和其他应用免受拒绝服务攻击

Firepower 9300 的机箱管理由思科统一管理器执行，其中 Radware APSolute Vision 管理适用于 Cisco Firepower 9300 的 DefensePro 应用。

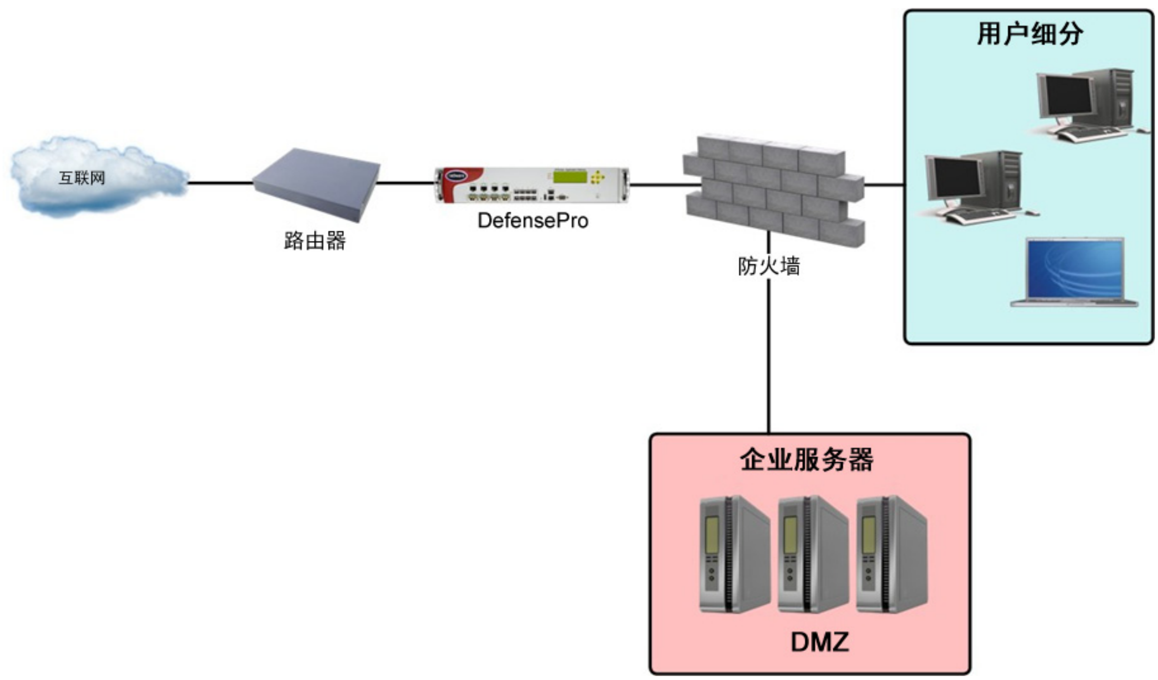
使用调配适用于 Cisco Firepower 9300 的 DefensePro 的 XML 文件执行初始启动配置。

有关适用于 Cisco Firepower 的 DefensePro 安装、维护和升级的信息，请咨询思科技术支持部门。

典型部署

下图显示企业中 DefensePro IPS 的内联安装。在此部署中，DefensePro 位于网关，保护主机、服务器和网络资源免受即将到来的网络攻击。DefensePro 还保护 DMZ 服务器免受针对 Web、邮件、VoIP 和其他服务的攻击。此 Radware 部署位于企业网关，在 DMZ 服务器之前，DefensePro 在此为企业服务器、用户、路由器和防火墙提供边界保护。

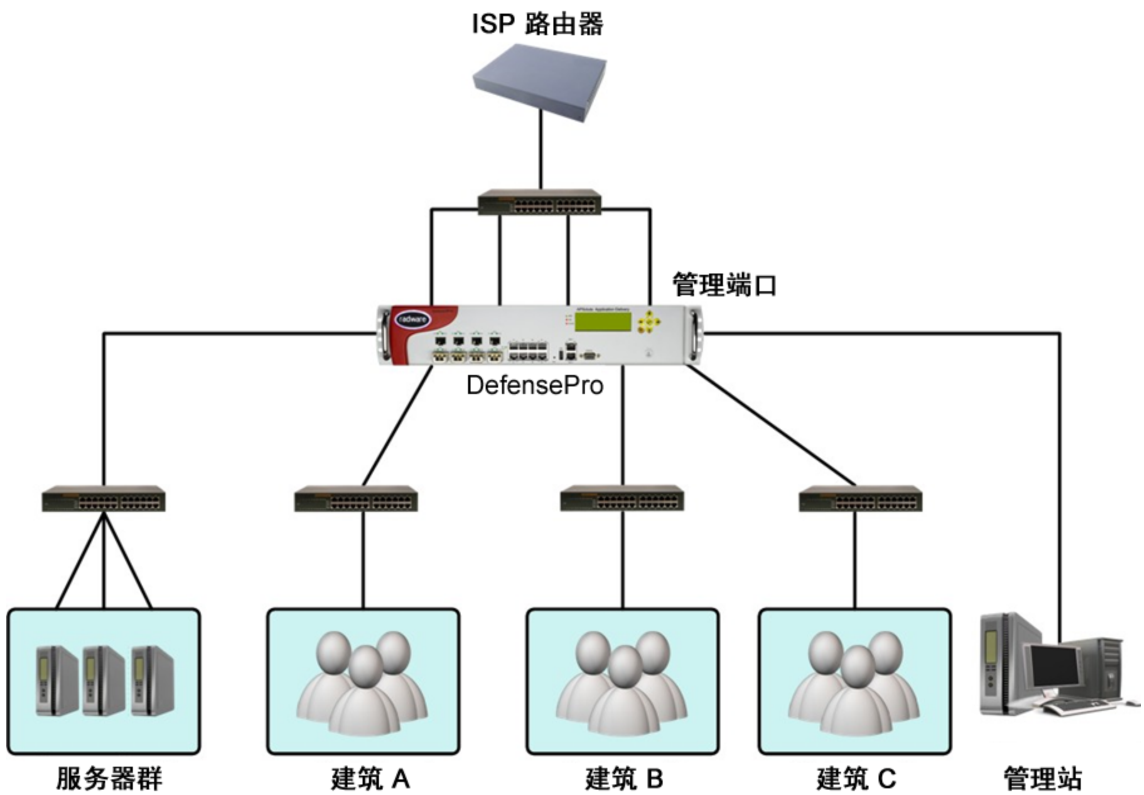
图 19：典型的 DefensePro 部署



网络连接

下图显示 DefensePro 典型的网络拓扑。

图 20：典型的网络连接



管理界面 - APSolute Vision 及其他界面

APSolute Vision 是 DefensePro 的主管理界面。

DefensePro 设备的其他管理界面包括：

- 基于 Web 的网络管理 (WBM)
- 命令行界面 (CLI)

您可以使用任意管理系统执行大部分任务。但是，大部分情况下，本指南所述的管理任务都使用 APSolute Vision。

APSolute Vision 为一款图形应用，允许您对单个或多个 DefensePro 部署进行集中配置、修改、监控和生成报告。

DefensePro 功能

本节简要介绍 DefensePro 的主要功能，并包括以下主题：

安全保护

注意： DefensePro 版本和平台可能会影响 DefensePro 设备所支持的安全策略类型。

组织中的安全策略为一套规章制度，定义安全网络的构成及其对安全违规的反应。您可以通过使用全局安全设置、网络保护策略和服务器保护策略来为贵组织实施安全策略。您可以调整安全策略以满足上至不同网段下至单个服务器的安全需求，为贵组织提供综合保护。

每条策略由多个规则构成。策略中的各规则定义网段或服务器，一个或多个要应用的保护配置文件，以及当设备检测到攻击时所要采取的操作。

各保护配置文件定义针对特定网络威胁提供防护的安全防御。例如，签名保护配置文件防御入侵企图，而行为 DoS 配置文件可防御针对创建拒绝服务的泛洪攻击。

注意

- 除非特别标注，否则本书中配置安全策略的操作步骤与使用 APSolute Vision 相关。
- 管理界面上不支持某些保护。

DefensePro 的多层安全方法组合了检测和缓解大范围网络和服务器攻击的功能。

适用于 Cisco Firepower 9300 的 DefensePro 支持*网络范围的保护*。网络范围的保护包括以下内容：

- **行为 DoS** - 防御零日泛洪攻击，包括 SYN 泛洪、TCP 泛洪、UDP 泛洪、ICMP 和 IGMP 泛洪。
- **SYN 泛洪保护** - 防御使用 SYN Cookie 的任意类型的 SYN 泛洪攻击。SYN 泛洪攻击通常针对特定服务器，目的在于消耗服务器资源。但是，您可以将 SYN 保护配置为网络保护，允许对多个网络元素提供更为简便的保护。
- **基于签名的保护** - 使用 *DoS 屏蔽*保护，可防御造成拒绝服务效果的已知泛洪攻击和泛洪攻击工具。
- **数据包异常保护。**

隧道流量检测

运营商、服务提供商和大型组织使用各类隧道协议由一个地点向另一个地点传输数据。此过程使用 IP 网络完成，以使得网络元素无法了解封装在隧道中的数据。

隧道指流量路由基于源 IP 地址和目标 IP 地址。当使用隧道时，IPS 设备和负载均衡器无法定位相关信息，因为它们的判定基于已知偏移中 IP 数据包内的信息，而原始 IP 数据包则被封装在隧道中。

您可以在不同环境中安装 DefensePro，可能包括使用不同隧道协议的封装流量。一般来说，有线运营商对其隧道部署 MPLS 和 L2TP，而移动运营商则部署 GRE 和 GTP。

1.01 版本的 DefensePro 可检测可能使用各类封装协议的流量。在某些情况下，外部报头（隧道数据）是 DefensePro 需要检测的数据。在其他情况下，DefensePro 需要检测内部数据（IP 报头甚至负载）。

1.01 版本的 DefensePro 可对 BDoS 保护和 DoS 屏蔽保护检测以下类型的隧道流量：

- VLAN (802.1Q) 和 MPLS 流量

  注意：作为保护准则一部分，检测此类 L2 隧道在如托管安全服务提供商 (MSSP) 的环境中很必要。
- 封装的 GRE 流量
- 封装的 L2TP 流量
- 封装的 GTP 流量
- 封装的 IP-in-IP 流量
- 封装的 QinQ (802.1ad) 流量

DefensePro 始终绕过（透传）IPsec 流量。

DefensePro 实时安全报告

APSolute Vision 提供 DefensePro 设备的实时攻击视图和安全服务警告。当 DefensePro 检测到攻击时，本次攻击会被报告为安全事件。

DefensePro 的安全监控允许您对实时和历史攻击进行分析。

当检测到攻击时，DefensePro 会自动生成应对措施，您可使用各类监控工具对应对措施进行观察和分析。DefensePro 为您提供显示实时网络流量和应用行为参数的监控工具。安全监控还提供由高级统计算法生成，代表正常行为基准的统计参数。

历史安全报告 - APSolute Vision 报告器

APSolute Vision 报告器是历史安全报告引擎，提供以下功能：

- 可定制的控制面板、报告和通知
- 面向安全运营中心 (SOC) 和网络运营中心 (NOC) 的高级突发事件处理
- 标准安全报告
- 彻底的调查分析能力
- 票证工作流程管理

DefensePro 平台和型号

适用于 Cisco Firepower 9300 的 DefensePro 运行于 KVM 虚拟基础设施上。有关详细信息，请咨询思科技术支持部门。

相关文档

有关 DefensePro 的信息，请参阅以下文档：

- DefensePro 版本说明
- APSolute Vision 文档
- APSolute Vision 报告器文档

DefensePro 版本说明

有关 DefensePro 的相关版本信息，请参阅 *DefensePro 版本说明*。

APSolute Vision 文档

APSolute Vision 文档包括以下内容：

- **APSolute Vision 安装和维护指南** - 请参阅此指南了解以下信息：
  - 安装 APSolute Vision。
  - 初始化 APSolute Vision。
- **APSolute Vision 用户指南** - 请参阅此指南了解以下信息：
  - APSolute Vision 功能。
  - APSolute Vision 界面导航。
  - 用户管理 - 例如，添加用户和定义用户权限。
  - 添加和删除 DefensePro 设备。
  - 配置站点 - 一组受管设备的物理或逻辑表现。
  - 受管设备上的管理和维护任务；例如，调度 APSolute Vision 和设备任务、制作备份等。
  - APSolute Vision CLI。
  - 监控 APSolute Vision - 例如，版本、服务器、数据库、设备配置文件、控制 APSolute Vision 操作、备份 APSolute Vision 数据库。
  - 管理审计和警报。
- **APSolute Vision 在线帮助** - 请参阅此帮助，了解有关监控受管设备的信息。

APSolute Vision 报告器文档

请参阅 APSolute Vision 报告器在线帮助和 *APSolute Vision 报告器用户指南*，了解有关 APSolute Vision 报告器及其使用方法的信息。

第 2 章 - 入门

本章介绍在您设置和配置 DefensePro 安全策略之前需要执行的操作。

有关适用于 Cisco Firepower 9300 的 DefensePro 安装、维护和升级的信息，请咨询思科技术支持部门。

有关 APSolute Vision 服务器物理规格和基本设置的相关信息和操作步骤，请参阅 *APSolute Vision 安装和维护指南*中的相关信息并遵循其中的说明，然后再执行本章中介绍的其他任务。

本章包含以下各节：

登录 APSolute Vision

要开始使用 APSolute Vision，您应先登录 APSolute Vision 网络应用，称为*基于 Web 的管理* (WBM)。

首次登录 APSolute Vision WBM 需要 *APSolute Vision 激活许可证*（具有 **vision-activation** 前缀）。许可证基于 APSolute Vision G1 或 G2 端口的 MAC 地址，由 CLI 命令 net ip get 显示。您可以向 Radware 技术支持部门申请该许可证。另外，您还可以使用 radware.com 上的许可证生成器获得许可证。

多达 50 名的用户可同时访问 APSolute Vision 服务器。

APSolute Vision 支持角色型访问控制 (RBAC) 以管理用户权限。您可以通过身份验证服务器或本地 APSolute Vision 用户数据库管理凭证和权限。

要以现有用户身份登录 APSolute Vision

1. 在网络浏览器中，输入 APSolute Vision 服务器的主机名或 IP 地址。
2. 在登录对话框中，指定以下内容：
   - “用户名”(User Name) - 您的用户名。
   - “密码”(Password) - 您的用户密码。根据服务器的配置，您可能需要立即更改您的密码。默认设置：radware。
   - （地球图标）- APSolute Vision 图形用户界面的语言。
3. 点击**登录 (Login)**。

更改本地用户的密码

如果通过 APSolute Vision *本地用户*表（而非通过身份验证服务器，例如 RADIUS）管理您的用户凭证，您可以在登录时或在 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*首选项 (Preferences)* 视角中更改用户密码。有关密码要求的信息，请参阅 APSolute Vision 密码要求，第 99 页。

如果密码已过期，您必须在 *APSolute Vision 登录* (*APSolute Vision Login*) 对话框中更改密码。

注意：有关管理 APSolute Vision 用户的信息，请参阅管理 APSolute Vision 用户，第 79 页。

要更改本地用户的密码

1. 在 *AAPSolute Vision 设置 (APSolute Vision Settings)* 视图*首选项 (Preferences)* 视角中，依次选择**用户首选项 (User Preferences) > 用户密码设置 (User Password Settings)**。
2. 配置参数并点击**更新密码 (Update Password)**。

表 1：用户密码设置参数

参数	说明
当前用户名 (Current Username)	（只读）当前用户名。
当前密码 (Current Password)	当前密码。
新密码 (New Password)	新密码。
确认新密码 (Confirm New Password)	新密码。

APSolute Vision 用户界面概述

本节包含以下主题：

APSolute Vision 界面遵循一贯的分层结构，按功能组织以便轻松访问选项。您可以从高功能级别开始，并逐步向下展开特定模块、功能或对象。

注意：对 APSolute Vision 界面元素的访问和其中的权限由角色型访问控制 (RBAC) 决定。有关详细信息，请参阅 *APSolute Vision 用户指南*。有关详细信息，请参阅角色型访问控制 (RBAC)，第 80 页和配置 APSolute Vision 的本地用户，第 90 页。

APSolute Vision 设置视图

点击主屏幕顶部的 （设置）按钮选择 *APSolute Vision 设置 (APSolute Vision Settings)* 视图。

APSolute Vision 设置 (APSolute Vision Settings) 视图包括以下视角：

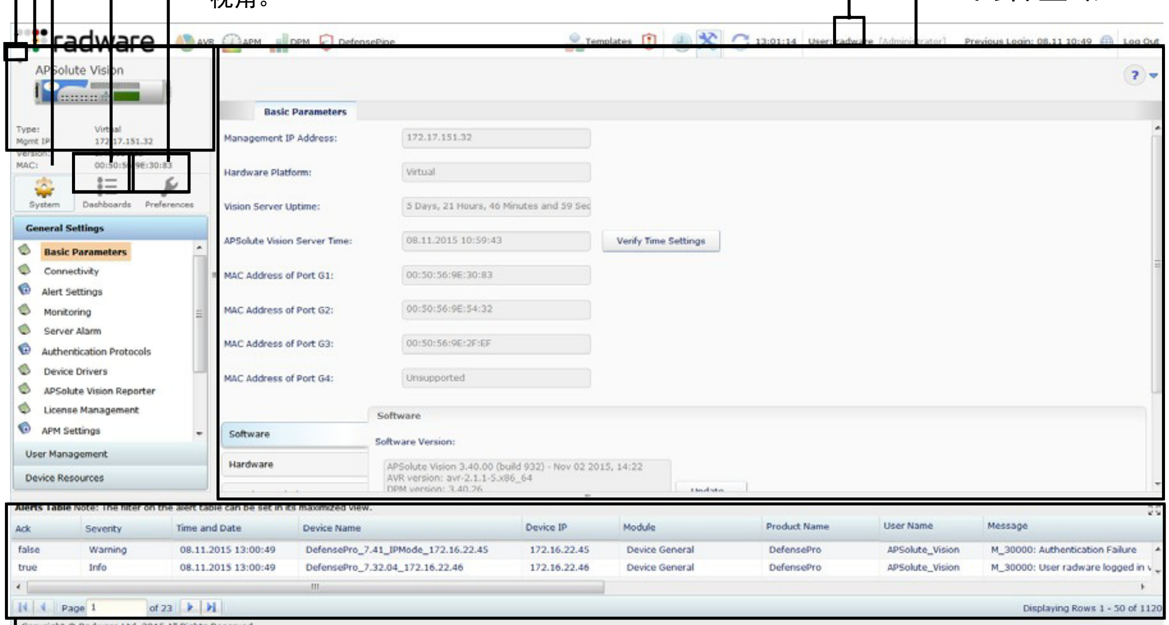
- **系统 (System)** - 有关详细信息，请参阅设置视图 - 系统视角，第 44 页。对 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角的访问仅限管理员。
- **控制面板 (Dashboards)** - 有关详细信息，请参阅设置视图 - 控制面板视角，第 43 页。
- **首选项 (Preferences)** - 有关详细信息，请参阅设置视图 - 首选项视角，第 43 页。

点击相关按钮（**系统 (System)**、**控制面板 (Dashboards)** 或**首选项 (Preferences)**）显示您所需的视角。

在 *APSolute Vision 设置 (APSolute Vision Settings)* 视图的左上角，APSolute Vision 会显示 *APSolute Vision 设备属性 (APSolute Vision device-properties) 窗格*。有关详细信息，请参阅 APSolute Vision 设备属性窗格，第 43 页。

当您将鼠标悬停在“设备”(device) 窗格中的设备节点上时，系统会显示弹出窗口。有关详细信息，请参阅设备属性悬停弹出窗口，第 43 页。

图 21：设置视图（显示系统视角）



APSolute Vision 设备属性窗格

*APSolute Vision 设备属性 (APSolute Vision device-properties) 窗格*显示当前选定设备的以下参数。

- *设备类型（Alteon、AppWall、DefensePro 或 LinkProof NG）和用户定义的设备名称。*
- *显示设备是否锁定的图标。*
- *设备前面板的图片。当设备锁定时，您可以点击 按钮重置或关闭设备。*
- **状态 (Status) -** 设备一般状态：**开启 (Up)**、**关闭 (Down)** 或**维护 (Maintenance)**。
- **锁定者 (Locked By)** - 如果设备被锁定，为锁定设备的用户。
- **类型 (Type)** - 平台和外观。
- **管理 IP (Mngt IP)** - 设备的主机或 IP 地址。
- **版本 (Version)** - 设备版本。
- **MAC** - MAC 地址。
- **许可证 (License)** - 设备的许可证。
- **设备驱动程序 (Device Driver)** - 设备驱动程序名称。

设备属性悬停弹出窗口

当您将鼠标悬停在“设备”(device) 窗格中的设备节点上时，弹出窗口会显示以下参数：

- **设备名称 (Device Name)** - 用户定义的设备名称。
- **状态 (Status) -** 设备一般状态：**开启 (Up)**、**关闭 (Down)** 或**维护 (Maintenance)**。
- **锁定者 (Locked By)** - 如果设备被锁定，为锁定设备的用户。
- **管理 IP 地址 (Management IP Address)** - 设备的主机或 IP 地址。
- **设备类型 (Device Type)** - 设备类型，即 **DefensePro**。
- **版本 (Version)** - 设备版本。
- **MAC** - MAC 地址。
- **许可证 (License)** - 设备的许可证。
- **外形 (Form Factor)** - 此字段显示外形：**虚拟 (Virtual)**。
- **平台 (Platform)** - 平台类型。
- **HA 状态 (HA Status)**。
- **设备驱动程序 (Device Driver)** - 设备驱动程序名称。

设置视图 - 首选项视角

使用*首选项 (Preferences)* 视角更改您的密码。

设置视图 - 控制面板视角

具有适当角色的用户可以使用 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*控制面板 (Dashboards)* 视角访问以下项目：

- **应用 SLA 控制面板 (Application SLA Dashboard) -** 有关详细信息，请参阅使用应用 SLA 控制面板，第 491 页。
- **安全控制中心 (Security Control Center)** - 有关详细信息，请参阅使用安全控制中心，第 495 页。

设置视图 - 系统视角

- 管理员可以使用 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角执行以下操作：
- **监控或管理 APSolute Vision 服务器的常规设置** - 监控和管理 APSolute Vision 服务器的常规设置包括以下项目：
  - APSolute Vision 服务器的常规属性、详细信息和统计信息
  - APSolute Vision 服务器的统计信息
  - 连接
  - 警报浏览器和安全警报
  - 监控参数
  - 服务器警告阈值
  - 身份验证协议
  - 设备驱动程序
  - APSolute Vision Reporter for DefensePro
  - 许可证
  - 应用性能监控 (APM)
  - DefensePipe URL
  - 高级常规参数
  - 显示格式
  - 维护文件
- **管理和监控用户** - 用户可以同时依次管理多个设备。使用 APSolute Vision RBAC，管理员可以允许用户在设备上的各类访问控制级别。RBAC 提供一组预定义角色，您可以按用户和按工作范围（设备或设备组）进行分配。RBAC 定义同时受内部 (APSolute Vision 中) 和通过远程身份验证 (借助 RADIUS 或 TACACS+）支持。
- **管理设备资源** - 例如，设备备份文件。

注意：有关 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角中展示的大部分操作的详细信息，请参阅管理和监控 APSolute Vision 系统，第 101 页。

设备窗格

具有适当角色的用户可以使用*设备 (device) 窗格*来添加或删除 APSolute Vision 服务器管理的 Radware 设备。

点击靠近左上角的小按钮显示“设备”(device) 窗格，您可以将受管设备组织为高可用性*集群*和*站点*。

站点通常是共享属性（例如位置、服务或设备类型）的一组设备。您还可以嵌套站点，即各站点可以包含子站点和设备。在角色型访问控制 (RBAC) 情景中，站点允许管理员定义每个用户的范围。

当您双击“设备”(device) 窗格中的设备时，APSolute Vision 会显示“设备属性”(device-properties) 窗格和您在设备上最后查看的视角以及对应的内容区域。

您可以对 APSolute Vision 显示的站点和设备进行过滤。过滤器适用于树中的所有站点和设备。过滤器不会更改树的内容，仅更改 APSolute Vision 向您显示树的方式。默认情况下，APSolute Vision 会显示您有权查看的所有站点和设备。根据您的 RBAC 权限，APSolute Vision 会在树中的各个节点末尾附加与该级别上过滤器相匹配的设备数量。

您可以根据以下条件过滤 APSolute Vision 显示的站点和设备：

- **状态 (Status) - 打开 (Up)、关闭 (Down)、维护 (Maintenance) 或未知 (Unknown)**。
- **类型 (Type)** - **Alteon**、**AppWall**、**DefensePro** 或 **LinkProof NG**。*物理容器 (Physical Containers)* 选项卡不会显示此字段。
- **名称 (Name)** - 设备、站点的名称或名称中包含的字符串（例如，值 **aRy** 匹配名为 **Primary1** 和 **SecondaryABC** 的元素）。
- **IP 地址 (IP Address)** - IP 地址、IP 范围或 IP 掩码。

在配置过滤器条件后，要应用过滤器，请点击 按钮应用过滤器。点击 按钮取消过滤器。

图 22：设备窗格（未扩展）

配置视角

使用*配置 (Configuration)* 视角配置 Radware 设备。在“设备”(device) 窗格中选择要配置的设备。

您可以在内容区域中查看和修改设备配置。

以下几点适用于*配置 (Configuration)* 视角中的所有配置任务：

- 要配置设备，您必须将其锁定。有关详细信息，请参阅 APSolute Vision 文档。
- 当您更改字段值（并且存在**提交 (Submit)** 操作挂起的配置）时，选项卡标题会变为带有星号 (*) 的斜体字。
- 默认情况下，表在每个表页面最多可显示 20 行。
- 您可以在表条目上执行以下一个或多个操作：
  - 将新条目添加到表，并定义其参数。
  - 编辑现有表条目的一个或多个参数。
  - 删除表条目。
  - 设备配置信息仅保存在受管设备上，而不会保存在 APSolute Vision 数据库中。

要将信息提交至设备，当在配置对话框或配置页面中修改设置时，您必须点击**提交 (Submit)**。

某些配置更改需要立即重启设备。当您提交配置更改时，设备会立即重启。

某些配置更改需要重启设备才能生效，但您可以保存更改但不立即重启。当您提交更改但不重启时，*属性 (Properties)* 窗格会在您重启设备之前显示“需要重启”(Reboot Required) 的通知。

如果需要，请点击**更新策略 (Update Policies)** 实施策略-配置更改。设备的策略-配置更改保存在 DefensePro 设备上，但在您执行设备配置更新之前，设备不会应用更改。如果新配置需要执行“更新策略”(Update Policies) 操作才能生效，则会显示带有橙色背景的按钮。

图 23：“更新策略”(Update Policies) 按钮

图 24：“需要更新策略”(Update Policies Required) 按钮

示例 *配置 (Configuration)* 视角中的设备选择

以下示例显示您要查看或更改 Radware 设备配置参数时所要做出的选择：

1. 通过逐步向下展开站点和子站点，在“设备”(device) 窗格中选择所需设备。
2. 通过点击“设备属性”(device-properties) 窗格中的 图标锁定设备。图标会变为 （锁定的挂锁图片）。
3. 点击 Configuration 打开*配置 (Configuration)* 视角。
4. 导航至“内容”(content) 窗格中的配置对象。

监控视角

在*监控 (Monitoring)* 视角中，您可以监控物理设备和接口，以及逻辑对象。

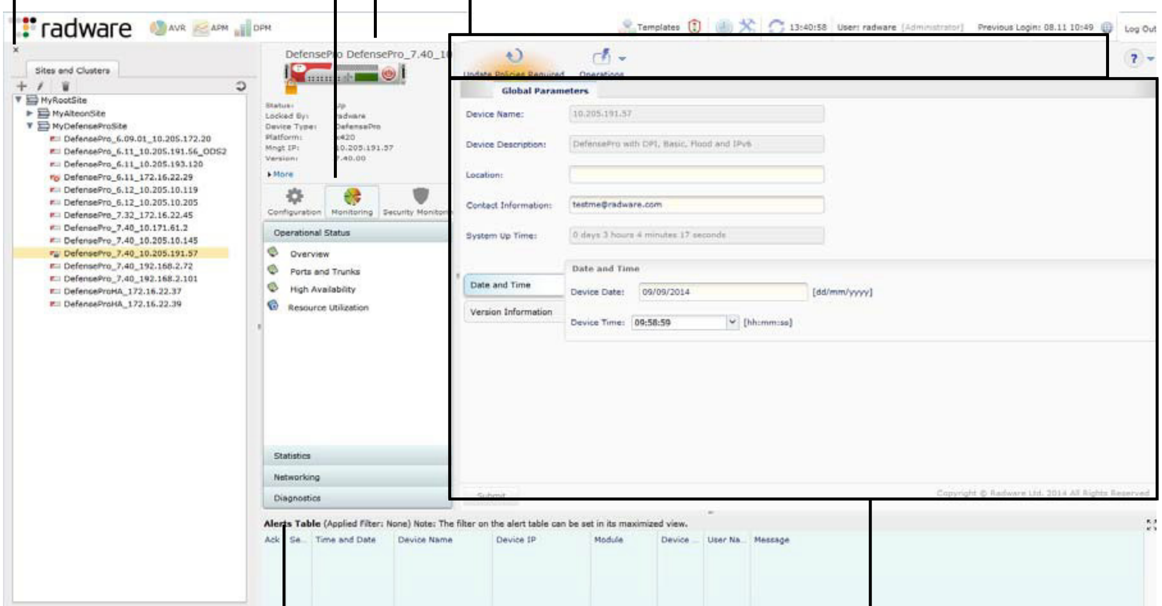
图 25：监控视角 - DefensePro

“设备”(Device) 窗格 - 包括*站点和集群 (Sites and Clusters)* 树和*物理容器 (Physical Containers)* 树。仅*站点和集群 (Sites and Clusters)* 树与 DefensePro 相关。

正在显示*监控 (Monitoring)* 视角。

“设备属性”(Device-properties) 窗格。

DefensePro 配置-管理按钮。



“内容”(Content) 窗格。

警报表 (Alerts Table) - 显示 APSolute Vision 警报、设备警报和 DefensePro 配置消息。

安全监控视角

对于 DefensePro 和 DefenseFlow，APSolute Vision 会显示*安全监控 (Security Monitoring)* 视角。

安全监控 (Security Monitoring) 视角对单个设备和多个设备均可用。多个设备的安全监控支持两个报告类别：*控制面板 (Dashboard) 视图*和*流量监控 (Traffic Monitoring)*。单个设备的安全监控支持另外两个报告类别：*保护监控 (Protection Monitoring)* 和 *HTTP 报告 (HTTP Reports)*。

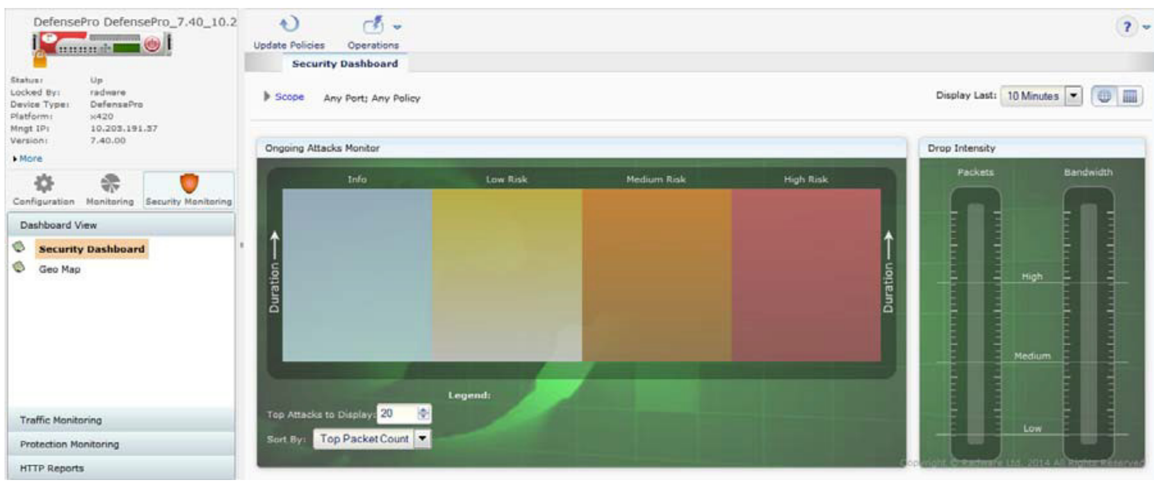
您可以对 APSolute Vision 显示的站点和设备进行过滤。过滤器不会更改树的内容，仅更改 APSolute Vision 向您显示树的方式。

在*安全监控 (Security Monitoring)* 视角中，您可以访问一系列实时安全监控工具，这些工具提供有关 DefensePro 设备已检测到的当前攻击的可视性。*属性 (Properties)* 窗格显示有关当前选定设备的信息。

安全监控 (Security Monitoring) 视图包括以下选项卡：

- **控制面板 (Dashboard) 视图** - 包括以下部分：
  - **安全控制面板 (Security Dashboard)** - 网络中的所有当前活动攻击的图形摘要视图，具有彩色标记的攻击类别标识、图形威胁级别指示和即时逐步向下展开的攻击详细信息。
  - **当前攻击 (Current Attacks)** - 以表格格式显示的当前攻击的视图，具有攻击类别的图形标记、威胁级别指示、逐步向下展开的攻击详细信息以及对保护策略的便捷访问以进行即时微调。
- **流量监控 (Traffic Monitoring)** - 显示网络信息的实时图表和表格，攻击流量和合法流量已根据指定的流量方向和协议进行过滤。
- **保护监控 (Protection Monitoring)** - 实时图表和表格，具有策略统计信息、根据指定流量方向和协议的保护，以及已获知的流量基准。
- **HTTP 报告 (HTTP Reports)** - 实时图表和表格，具有策略统计信息、根据指定流量方向和协议的保护，以及已获知的流量基准。

图 26：安全监控视角 - 显示安全控制面板



注意：有关*安全监控 (Security Monitoring)* 视角的详细信息，请参阅使用实时安全监控，第 427 页。

APSolute Vision 站点和 DefensePro 设备

APSolute Vision 中的站点是一组受管设备（例如受管 DefensePro 设备）的物理或逻辑表现。站点可以基于地理位置、管理职能和设备类型等。每个站点可以包含嵌套的站点和设备。

在您能够通过 APSolute Vision 配置 DefensePro 设备和安全策略之前，DefensePro 设备必须存在于并连接到 APSolute Vision 服务器上。*站点*和 DefensePro 设备会显示在*系统 (System)* 选项卡中。

仅具有适当权限的用户可以向 APSolute Vision 服务器添加站点和 DefensePro 设备。

有关 APSolute Vision 站点的详细信息，请参阅 *APSolute Vision 用户指南*。

向 APSolute Vision 添加和从中删除 DefensePro 设备

在您能够在 APSolute Vision 中管理 Radware 设备之前，您需要在“设备”(device) 窗格中将设备添加到适当的站点树。

当添加设备时，您可以为其定义名称。您还可以提供设备连接信息，包括设备与 APSolute Vision 服务器之间通信的身份验证参数（凭证）。

在提交设备连接信息后，APSolute Vision 服务器会验证其是否可以连接设备。然后，APSolute Vision 会检索并存储设备信息和许可信息。

在连接建立后，您可以修改某些连接信息并对设备进行配置。

当添加设备或修改设备属性时，您可以指定 APSolute Vision 服务器是否将自身配置为设备事件的目标，并指定 APSolute Vision 服务器是否从设备删除自身地址以外的设备事件的所有收件人。

在添加设备后，您可以（根据*设备类型*）创建主设备和备用设备的集群，或主设备和辅助设备的集群。

- 设备不可具有与站点相同的名称。
- 不同站点中的设备不可具有相同的名称。
- 要更改设备名称，您必须首先将设备从站点树中删除，然后将其添加到所需的目标站点。
- 要在站点间移动设备，您必须首先将设备从站点树中删除，然后将其添加到所需的目标站点。
- 如果要将设备更换为您希望对其分配相同管理 IP 地址的新设备，您就必须从站点删除该设备，然后重新创建设备进行更换。
- 删除设备后，您不再能够查看该设备的历史报告。
- 删除设备时，也会同时删除设备警告和安全监控信息。
- HTTP 和 HTTPS 用于从受管设备下载/向受管设备上传各类文件，包括：配置文件、证书和密钥文件（仅限 HTTP）、攻击签名文件、设备软件文件等。

要添加新的 DefensePro 设备

1. 在“设备”(device) 窗格*站点和集群 (Sites and Clusters)* 树中，导航至并选择您希望为其添加设备的站点名称。
2. 点击选项卡工具栏中的 （添加）按钮。
3. 从**类型 (Type)** 下拉列表中，根据需要选择 **DefensePro**。
4. 配置参数，并点击**提交 (Submit)**。

   在 APSolute Vision 连接到设备后，基本设备信息会显示在“内容”(content) 窗格中，而设备属性信息会显示在“设备属性”(device-properties) 窗格中。

表 2：设备属性：常规参数

参数	说明
类型 (Type)	设备或站点的类型。在这种情况下，选择 DefensePro。
名称 (Name)	设备的名称。您可以更改默认值。 **注意：**一旦将设备添加到 APSolute Vision 配置中，您就无法更改设备名称。

表 3：设备属性：SNMP 参数

参数	说明
管理 IP (Management IP)	如在受管设备上定义的管理 IP 地址。 **注意：**一旦将设备添加到 APSolute Vision 配置，您就无法更改设备 IP 地址。
SNMP 版本 (SNMP Version)	用于连接的 SNMP 版本。
SNMP 读取社区 (SNMP Read Community) （仅当 **SNMP 版本 (SNMP Version)** 为 **SNMPv1** 或 **SNMPv2** 时显示此参数。）	SNMP 读取社区名称。
SNMP 写入社区 (SNMP Write Community) （仅当 **SNMP 版本 (SNMP Version)** 为 **SNMPv1** 或 **SNMPv2** 时显示此参数。）	SNMP 写入社区名称。
用户名 (User Name) （仅当 **SNMP 版本 (SNMP Version)** 为 **SNMPv1** 或 **SNMPv3** 时显示此参数。）	SNMP 连接的用户名。 最大字符数：18
使用身份验证 (Use Authentication) （仅当 **SNMP 版本 (SNMP Version)** 为 **SNMPv1** 或 **SNMPv3** 时显示此参数。）	指定设备是否验证用户成功连接。 默认值：“已禁用”(Disabled)
身份验证协议 (Authentication Protocol) （仅当选中**使用身份验证 (Use Authentication)** 复选框时才显示此参数。）	用于身份验证的协议。 值：MD5、SHA 默认值：MD5
身份验证密码 (Authentication Password) （仅当选中**使用身份验证 (Use Authentication)** 复选框时才显示此参数。）	用于身份验证的密码。

表 3：设备属性：SNMP 参数（续）

参数	说明
使用隐私 (Use Privacy) （仅当选中**使用身份验证 (Use Authentication)** 复选框时才显示此参数。）	指定设备是否加密 SNMPv3 流量以实现额外的安全性。 默认值：“已禁用” (Disabled)
隐私密码 (Privacy Password) （仅当选中**使用隐私 (Use Privacy)** 复选框时显示此参数。）	用于隐私设备的密码。

表 4：设备属性：HTTP/S 访问参数

参数	说明
验证 HTTP 访问 (Verify HTTP Access)	指定 APSolute Vision 是否验证对受管设备的 HTTP 访问。 默认值：“已启用” (Enabled) **注意：**此选项不用于 Alteon。
验证 HTTPS 访问 (Verify HTTPS Access)	指定 APSolute Vision 是否验证对受管设备的 HTTPS 访问。 默认值：“已启用” (Enabled)
用户名 (User Name)	HTTP 和 HTTPS 通信的用户名。 默认值：“管理员” (admin) 最大字符数：18
密码 (Password)	HTTP 和 HTTPS 通信所用的密码。 默认值：“管理员” (admin)
HTTP 端口 (HTTP Port)	HTTP 与设备通信的端口。默认值：80
HTTPS 端口 (HTTPS Port)	HTTPS 与设备通信的端口。默认值：443

表 5：设备属性：事件通知参数

参数	说明
为设备事件注册此 APSolute Vision 服务器 (Register This APSolute Vision Server for Device Events)	指定 APSolute Vision 服务器是否将自身配置为设备事件的目标。 值： ● “已启用”(Enabled) - APSolute Vision 服务器将自身配置为设备事件（例如，陷阱、警报、IRP 消息和数据包-报告数据）的目标。 ● “已禁用”(Disabled) - *对于新设备*，APSolute Vision 服务器添加设备时不将自身注册为事件目标。 *对于现有设备*，APSolute Vision 服务器将自身作为设备事件的目标删除。 默认值：“已启用”(Enabled) **注意：**每当您点击对话框中的**提交 (Submit)** 时，APSolute Vision 就会运行此操作。
注册 APSolute Vision 服务器 IP (Register APSolute Vision Server IP)（仅当选中**为设备事件注册此 APSolute Vision 服务器 (Register This APSolute Vision Server for Device Events)** 复选框时，此参数才可用。）	受管设备向其发送事件的 APSolute Vision 服务器端口和 IP 地址。
删除设备事件的所有其他目标 (Remove All Other Targets of Device Events)（仅当选中**为设备事件注册此 APSolute Vision 服务器 (Register This APSolute Vision Server for Device Events)** 复选框时，此参数才可用。）	指定 APSolute Vision 服务器是否从设备删除自身地址以外的所有设备事件（例如，陷阱和 IRP 消息）的收件人。 默认值：“已禁用”(Disabled) **注意：**每当您点击对话框中的**提交 (Submit)** 时，APSolute Vision 就会运行此操作。例如，如果您选中该复选框并点击**提交 (Submit)** - 稍后，陷阱目标会添加到陷阱目标-地址表 - 当您下次在对话框中点击**提交 (Submit)** 时，APSolute Vision 会删除其他地址。有关详细信息，请参阅为设备事件注册的 APSolute Vision 服务器 - DefensePro，第 53 页

要编辑设备连接信息

1. 在“设备”(device) 窗格*站点和集群 (Sites and Clusters)* 树中，选择设备名称。
2. 点击 （编辑）按钮。
3. 修改操作步骤要添加新 DefensePro 设备，第 49 页中所述的参数，并点击**提交 (Submit)**。

要删除设备

1. 在“设备”(device) 窗格*站点和集群 (Sites and Clusters)* 树中，选择设备名称，并点击 （删除）按钮。
2. 点击确认对话框中的**是 (Yes)**。设备会从受管设备列表中删除。

为设备事件注册 APSolute Vision 服务器 - DefensePro

在“设备属性”(Device Properties) 对话框的*事件通知 (Event Notification)* 选项卡中（请参阅表 5 - 设备属性：事件通知参数，第 52 页），您可以指定 APSolute Vision 服务器是否将自身配置为设备事件的目标（**为设备事件注册此 APSolute Vision 服务器 (Register This APSolute Vision Server for Device Events)** 复选框），以及指定 APSolute Vision 服务器是否从设备删除自身地址以外的所有设备事件的收件人（**删除设备事件的所有其他目标 (Remove All Other Targets of Device Events)** 复选框）。每当您点击对话框中的**提交 (Submit)** 时，APSolute Vision 就会运行这些操作。

从技术上说，多个 APSolute Vision 服务器可以管理同一个 DefensePro 设备。

当同一个 DefensePro 设备由多个 APSolute Vision 服务器管理时，设备会发送以下内容：

- 管理该 DefensePro 设备的所有 APSolute Vision 服务器的陷阱。包含所有 APSolute Vision 服务器条目的“目标地址”(Target Address) 表和“目标参数”(Target Parameters) 表。
- *仅面向最后在设备上注册的 APSolute Vision 服务器*的数据包 - 报告数据。

小心：如果清除**为设备事件注册此 APSolute Vision 服务器 (Register This APSolute Vision Server for Device Events)** 复选框，警报浏览器、安全报告和 APSolute Vision 报告器则可能无法收集和显示有关设备的信息。

在 APSolute Vision 中锁定和解锁 DefensePro 设备

当有权在特定设备上执行设备配置时，您必须在配置该设备之前将其锁定。锁定该设备可确保其他用户无法同时进行配置更改。在您解锁设备、断开连接后，在*设备锁超时时间*已过或*管理员*将其解锁后，设备仍旧保持锁定状态。

使用基于 Web 的管理或使用 CLI 锁定某个设备，不适用于在其他 APSolute Vision 服务器上配置的相同设备。

注意：仅一个 APSolute Vision 服务器应管理任意一个 Radware 服务器。当设备处于锁定状态时：

- “设备”(device) 窗格中的设备图标会包括一个适用于 DefensePro 的小锁标志 - 。
- “配置”(Configuration) 窗格会以只读模式显示给对该设备具有配置权限的其他用户。
- 如果适用，则**提交 (Submit)** 按钮可用。
- 如果适用，则会显示 （添加）按钮。

要锁定单个设备

1. 在“设备”(device) 窗格中，选择设备。
2. 在“设备属性”(Device-properties) 窗格中，点击 （设备图样左下角已解锁的挂锁图样）。图样会变为 （已锁定的挂锁图片）。

要解锁单个设备

1. 在“设备”(device) 窗格中，选择设备。
2. 在“设备属性”(Device-properties) 窗格中，点击 （设备图样左下角的已锁定挂锁图样）。图样会变为 （解锁的挂锁图片）。

要锁定多个设备

1. 在“设备”(device) 窗格中，选择要锁定的设备。
2. 点击 （查看）按钮。
3. 在“设备属性”(Device-properties) 窗格中，点击 （已解锁的挂锁图样）。

要解锁多个设备

1. 在“设备”(device) 窗格中，选择要解锁的设备。
2. 点击 （查看）按钮。
3. 在“设备属性”(Device-properties) 窗格中，点击 （已解锁的挂锁图样）。

使用 APSolute Vision 中的通用 GUI 元素

本节包含以下内容：

用于管理表条目的图标和命令

下表列出当您使用 APSolute Vision 基于 Web 的管理对表条目（行）进行管理时可用的图标/按钮和对应的命令。可用的命令取决于功能。图标始终位于左侧的表上方。当鼠标光标（指针）悬停在图标上时，图标显示的色彩会从单色（灰色）变成彩色。

注意

- 仅当设备锁定时，您可以配置和控制受管设备（请参阅锁定和解锁设备，第 162 页）。
- APSolute Vision 文档会显示彩色状态下的图标和按钮。

表 6：用于管理表条目的图标和命令

图标/按钮	命令	说明
	添加 (Add)	打开 “添加新的...” (Add New...) 选项卡配置新条目。
	编辑 (Edit)	打开 “编辑...” (Edit...) 选项卡修改选定的现有条目。
	复制 (Duplicate)	打开 “添加新的...” (Add New...) 选项卡，其中含有选定条目的值（索引除外）。
	删除 (Delete)	删除选择。
	导出 (Export)	导出选定条目。
	查看 (View)	打开 “查看...” (View...) 选项卡查看选定条目的值。

过滤表行

对于 APSolute Vision 和受管设备中的多个表，您可以根据表列中的值过滤表行。

过滤器将布尔 AND 运算符用于您指定的过滤条件。即，过滤后的表会显示匹配*所有*搜索参数而不是*任何*搜索参数的行。例如，如果表包括列*策略*和*端口*，而您过滤的策略值为 **ser**，端口值为 **80**，则过滤后的表会显示策略参数值包括 **ser** 以及策略参数值包括 **80** 的行。

要过滤表行

1. 执行以下操作：

   — 如果表列显示下拉列表（带箭头，像这样的 Search ），请点击该箭头并选择要过滤的值。

   — 如果表列显示白色文本框（像这样的 Search ），请键入要按其过滤的值。

   注意

   — 对于文本框，过滤器会使用*包含 (contains)* 算法。即，如果您输入的字符串仅仅*包含*在值中，则过滤器会将其视为匹配。例如，如果您在文本框中输入 **ser**，则过滤器返回具有值 **er**、**service1** 和 **service2** 的行。

   — 如果列顶部的框为灰色（像这样的 ），您就无法根据该参数进行过滤。

2. 点击 （过滤器）按钮或按 **Enter** 键。

第 3 章 - 管理设备运行和维护

本章介绍以下操作和维护任务：

注意

- 您无法使用 APSolute Vision 升级适用于 Cisco Firepower 9300 的 DefensePro。有关适用于 Cisco Firepower 9300 的 DefensePro 的设备升级信息，请参阅相关版本说明。
- 适用于 Cisco Firepower 9300 的 DefensePro 不支持 APSolute Vision *模板*功能。
- 使用 APSolute Vision 更新签名文件与适用于 Cisco Firepower 9300 的 DefensePro 不相关。

更新 DefensePro 设备上的策略配置

您可以在单个操作过程中将以下配置更改应用到 DefensePro 设备：

- 网络保护策略
- 类

要更新 DefensePro 设备上的策略配置

> 在“设备”(device) 窗格中，选择设备，然后点击 Update Policies 按钮。

重启或关闭 DefensePro 设备

您可以从 APSolute Vision 激活设备重启（重置）或设备关闭。

设备上的某些配置更改需要重启设备才能使配置生效。您可以从 APSolute Vision 激活设备重启。

要重启设备

1. 锁定设备。
2. 在*属性 (Properties)* 窗格中，点击作为设备图片一部分的（开-关）按钮。
3. 选择**重置 (Reset)**。

要关闭设备

1. 锁定设备。
2. 在*属性 (Properties)* 窗格中，点击作为设备图片一部分的（开-关）按钮。
3. 选择**关闭 (Shut Down)**。

将设备的日志文件下载到 APSolute Vision 客户端

您可以将 DefensePro 日志文件下载到 APSolute Vision 客户端系统。日志文件由设备自动生成，并且包含配置错误报告。日志文件可用于调试。

要下载设备日志文件

1. 在“设备”(device) 窗格中，选择设备。
2. 点击 Operations（操作）图标的箭头。
3. 点击**导出日志文件 (Export Log File)**。
4. 配置下载参数，并点击**提交 (Submit)**。

表 7：设备日志文件下载参数

参数	说明
下载方式 (Download Via)	（只读）用于下载日志文件的协议。 值：HTTPS
另存为 (Save As)	将下载的日志文件另存为客户端系统上的文本文件。输入或浏览保存的日志文件的位置，并选择或输入文件名。

下载技术支持和配置文件

出于调试目的，DefensePro 设备可以生成 TAR 文件，其中包含 Radware 技术支持部门所需的技术信息。该文件包括各类 CLI 命令的输出，例如，客户端表的打印输出。

您可以下载 DefensePro 技术支持文件，并将其发送给 Radware 技术支持部门。

管理 DefensePro 设备配置

本节介绍如何管理在 APSolute Vision 上配置的 DefensePro 设备的配置。

DefensePro 配置文件内容

配置文件内容分为两部分：

- **需要重启设备的命令** - 这些命令包括应用安全状态、设备运行模式、微调参数等。仅在设备重启后从此部分复制和粘贴的命令才生效。此部分标题为：以下命令将仅在设备重启后生效！
- **无需重启设备的命令** - 从本部分复制和粘贴的命令会在粘贴后立即生效。此部分中的命令不限于 SNMP。此部分标题为：以下命令在执行时立即生效！

命令按实施顺序显示在各部分中。

在文件末尾，设备会打印配置文件的签名。此签名用于验证文件的可靠性，并验证其未损坏。每当配置文件上传到设备时，都会对该签名进行验证。如果有效性检查失败，设备会接受配置，但会向用户发送配置文件已被篡改且无法保证其可以使用的通知。签名文件如文件签名：063390ed2ce0e9dfc98c78266a90a7e4。

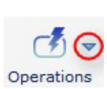
下载设备配置文件

您可以从受管设备将配置文件下载到 APSolute Vision 进行备份。如果您选择下载到 APSolute Vision 服务器，那么在 APSolute Vision 数据库中始终会保存一份副本。

默认情况下，在 APSolute Vision 服务器上每个设备最多可以保存五 (5) 份配置文件。您可以在“APSolute Vision 设置”(APSolute Vision Setup) 页面中更改此参数，最大值为 10。当达到限制时，系统会提示您删除最旧的文件。

注意：您可以在 APSolute Vision 调度程序中调度配置文件备份。有关详细信息，请参阅在调度程序中配置任务，第 64 页。

要下载设备配置文件

1. 在“设备”(device) 窗格中，选择设备。
2. 点击 

（操作）图标的箭头。
3. 选择**导出配置文件 (Export Configuration File)**。
4. 配置下载参数，然后点击**保存 (Save)**。

表 8：设备配置文件下载参数

参数	说明
下载到 (Download to)	备份设备配置文件的位置。 值：“客户端”(Client)、“服务器”(Server)
下载方式 (Download Via)	（只读）用于下载配置文件的协议。值：HTTPS
另存为 (Save As)	将下载的配置文件另存为客户端系统上的文本文件。 在服务器上，默认名称为设备名称和备份日期和时间的组合。您可以更改默认名称。
包括私钥 (Include Private Keys)	当启用时，证书私钥信息会包括在下载的文件中。您必须包括私钥信息以恢复私钥，否则设备会恢复为默认密钥。

恢复设备配置

您可以将 DefensePro 或 DefenseFlow 配置从 APSolute Vision 服务器或客户端系统上的备份配置文件恢复到 DefensePro 或 DefenseFlow 设备。当您将配置文件上传到设备时，上传的配置文件会覆盖现有的设备配置。

在恢复操作完成后，您必须重启设备。

小心：不支持导入已编辑的配置文件。

小心：不支持导入不同版本的配置文件。

要恢复设备的配置

1. 在“设备”(device) 窗格中，选择设备。
2. 点击 Operations（操作）图标的箭头。
3. 点击**导入配置文件 (Import Configuration File)**。
4. 配置上传参数，并点击**提交 (Submit)**。
5. 上传完成后，重启设备。

表 9：设备配置文件上传参数

参数	说明
上传自 (Upload from)	要发送的备份设备配置文件的位置。 值：“客户端”(Client)、“服务器”(Server)
上传方式 (Upload Via)	（只读）用于上传配置文件的协议。值：HTTPS
文件名 (File Name)	当从客户端系统上传时，输入或浏览要上传的配置文件名称。 当从服务器上传时，选择要上传的配置。
口令 (Passphrase) （此参数仅对 Alteon 设备可用。）	HTTPS 的口令。

重置 DefensePro 基准

重置基准 - 已获知的统计信息会清除基准流量统计信息并重置默认的正常基准。仅当受保护网络的特征已完全更改，并且需要更改带宽配额以适应网络更改时，才重置基准统计信息。

您可以重置包含 BDoS 或 DNS 保护配置文件的所有网络保护策略的基准，或重置包含 BDoS 或 DNS 保护配置文件的网络保护配置文件的选定网络保护策略的基准。

要重置 BDoS 基准统计信息

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > BDoS 保护 (BDoS Protection) > 重置 BDoS 基准 (Reset BDoS Baseline)**。
2. 选择是重置包含 BDoS 配置文件的所有网络保护策略的基准，还是重置包含 BDoS 配置文件的特定网络保护策略的基准。
3. 点击**提交 (Submit)**。

要重置 DNS 基准统计信息

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > BDoS 保护 (BDoS Protection) > 重置 DNS 基准 (Reset DNS Baseline)**。
2. 选择是重置包含 DNS 配置文件的所有网络保护策略的基准，还是重置包含 DNS 配置文件的特定网络保护策略的基准。
3. 点击**提交 (Submit)**。

调度 APSolute Vision 和设备任务

以下主题介绍如何在 APSolute Vision 调度程序中调度操作：

- 调度概述，第 63 页
- 在调度程序中配置任务，第 64 页
- 任务参数，第 65 页

注意：有关如何调度 APSolute Vision 服务器操作的信息，请参阅 *APSolute Vision 用户指南*或 APSolute Vision 在线帮助。

调度概述

您可以对 APSolute Vision 服务器和受管设备调度各类操作。已调度操作称为*任务*。

APSolute Vision 调度程序跟踪任务上次执行时间及这些任务下次执行的时间。当您为多个设备配置任务时，任务会按顺序在每个设备上运行。当任务在一个设备上完成后，就会在下一个设备上开始运行。如果任务在设备上未能完成，调度程序将在下一个列出的设备上激活任务。

当您创建任务并指定其运行时间时，该时间将依照您本地操作系统的时间。然后，APSolute Vision 会存储该时间，将其转换为 APSolute Vision 服务器的时区，然后相应地进行运行。即，一旦您配置了任务，该任务会根据 APSolute Vision 的时间设置运行，而不考虑对本地操作系统时间设所做的任何更改。

小心：如果 APSolute Vision 客户端时区与 APSolute Vision 服务器或受管设备的时区不同，请考虑时间偏差。

当定义任务时，您可以选择是启用还是禁用该任务。所有已配置的任务都存储在 APSolute Vision 数据库中。

您可以定义以下类型的 DefensePro 相关的已调度任务：

- 备份设备配置
- 备份 APSolute Vision 报告器数据
- 重启设备

注意

- APSolute Vision 展示的某些任务对某些 DefensePro 版本而言是不可操作/不相关的。
- 您可以从*监控 (Monitoring)* 视角手动执行其中某些操作。有关详细信息，请参阅：

- 重启或关闭 DefensePro 设备，第 60 页
- 下载设备配置文件，第 61 页

在调度程序中配置任务

任务 (Tasks) 表是查看和配置任务（已调度操作）的起点。

任务 (Tasks) 表显示各已配置任务的以下信息。

表 10：任务表参数

参数	说明
任务类型 (Task Type)	要执行的任务类型。
名称 (Name)	已配置任务的名称。
已启用 (Enabled)	任务在被选定时会根据已定义的计划运行。禁用的任务不会被激活，但任务会保存在数据库中。
说明 (Description)	用户定义的任务说明。
当前的状态 (Current Status)	任务的当前状态。值：“等待中”(Waiting)、“进行中”(In progress)
上次执行状态 (Last Execution Status)	上次任务是否成功运行。当任务被禁用或尚未开始时，状态为**从未执行 (Never Executed)**。
上次执行时间 (Last Execution Time)	上次任务运行的日期和时间。当任务被禁用或尚未开始时，此字段为空。
下次执行时间 (Next Execution Time)	下次任务运行的日期和时间。当任务被禁用时，此字段为空。
运行 (Run)	任务运行的频率，例如，每日或每周。如果已定义计划开始时间，则会显示计划开始日期。

要配置已调度任务

1. 在主工具栏中，点击已调度任务的信息。（调度程序）图标。*任务 (Tasks)* 表显示各已调度任务的信息。
2. 执行以下操作之一：
   — 要向表添加条目，请点击（添加）按钮。然后，选择任务类型，并点击提交 (Submit)。系统会显示选定任务类型的对话框。
   — 要编辑表中的条目，请选择此条目并点击（编辑）按钮。
3. 配置任务参数，并点击**提交 (Submit)**。所有任务配置都包括基本参数和调度参数。其他参数则取决于您选择的任务类型。

要运行现有任务

1. 在主工具栏中，点击（调度程序）图标。*任务 (Tasks)* 表显示各已调度任务的信息。
2. 选择所需任务，并点击（运行任务）按钮。

任务参数

以下各节介绍 DefensePro 相关的调度程序任务：

- APSolute Vision 报告器备份 - 参数，第 65 页
- 设备配置备份 - 参数，第 67 页
- 设备重启任务，第 69 页

APSolute Vision 报告器备份 - 参数

*APSolute Vision 报告器备份*任务会创建 APSolute Vision 报告器数据并将其导出至指定目标。备份包括所有 APSolute Vision 报告器数据。

注意

- APSolute Vision 在*存储位置*中存储 APSolute Vision 报告器数据的最多三次迭代。在第三次报告器备份后，系统会删除最早的备份。
- 默认情况下，*存储位置*为 APSolute Vision 服务器中硬编码的位置。
- *存储位置*中的备份文件名为指定文件名的前五个字符加上 10 个字符的时间戳。当任务导出备份文件时，文件名为任务配置中指定的文件名。
- 存储位置中的备份文件包括调度程序生成的硬编码说明。

表 11：APSolute Vision 报告器备份：常规参数

参数	说明
名称 (Name)	任务的名称。 默认值：选定的任务类型名称。如果存在使用此名称的现有任务，**n** 会附加到名称的末尾，其中 **n** 为下一个可用的序列号。
说明 (Description)	用户定义的任务说明。
已启用 (Enabled)	任务在被选定时会根据已定义的计划运行。禁用的任务不会被激活，但任务配置会保存在数据库中。

表 12：APSolute Vision 报告器备份：计划参数

<table>
<tr><th>参数</th><th>说明</th></tr>
<tr><td>运行 (Run)</td><td>任务运行的频率。
选择频率，然后配置相关时间和日/日期参数。
值：
● “一次”(Once) - 任务仅在指定的日期和时间运行一次。
● “分钟”(Minutes) - 按照任务起点之间指定的分钟数间隔运行任务。待定：最低
● “每日”(Daily) - 任务每日在指定时间运行。
● “每周”(Weekly) - 任务每周在指定日的指定时间运行。
注意：任务根据 APSolute Vision 客户端上配置的时间运行。</td></tr>
<tr><td>时间 (Time)[1]</td><td>任务运行的时间。</td></tr>
<tr><td>日期 (Date)[2]</td><td>任务运行的日期。</td></tr>
<tr><td>分钟 (Minutes)[3]</td><td>任务运行的间隔（以分钟为单位）。</td></tr>
<tr><td>总是运行 (Run Always)[4]</td><td>指定任务是否总是运行，或仅在定义的期间内运行。
值：
● “已启用”(Enabled) - 任务立即激活，并无限期运行下去，无开始或结束时间。任务会在通过计划 (Schedule) 选项卡中“频率”(Frequency) 配置的首个“时间”(Time) 运行。
● “已禁用”(Disabled) - 任务（在计划 (Schedule) 选项卡中指定的“时间”(Time) 和“频率”(Frequency)）从指定的“开始日期”(Start Date) 的“开始时间”(Start Time) 到“结束日期”(End Date) 的“结束时间”(End Time) 内运行。
默认值：“已启用”(Enabled)</td></tr>
<tr><td>开始日期 (Start Date)[5]</td><td rowspan="2">任务激活的开始日期和时间。</td></tr>
<tr><td>开始时间 (Start Time)</td></tr>
<tr><td>结束日期 (End Date)</td><td rowspan="2">任务不再运行的日期和时间。</td></tr>
<tr><td>结束时间 (End Time)</td></tr>
</table>

1 – 仅当指定的**运行 (Run)** 值为**一次 (Once)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
2 – 仅当指定的**运行 (Run)** 值为**一次 (Once)** 时，此参数才可用。
3 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)** 时，此参数才可用。
4 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
5 – 仅当取消选中**总是运行 (Run Always)** 复选框时，此参数才可用。

表 13：APSolute Vision 报告器备份：目标参数

参数	说明
协议 (Protocol)	APSolute Vision 用于此任务的协议。 值： ● FTP ● SCP ● SFTP ● SSH 默认值：FTP
IP 地址 (IP Address)	服务器的 IP 地址。
目录 (Directory)	无空格的导出目录路径。仅允许使用字母数字字符和下划线 (_)。
备份文件名称 (Backup File Name)	无空格的备份名称，最多 15 个字符。仅允许使用字母数字字符和下划线 (_)。
用户 (User)	用户名。
密码 (Password)	用户密码。
确认密码 (Confirm Password)	用户密码。

设备配置备份 - 参数

*设备配置备份*任务会保存指定设备的配置备份。

注意：默认情况下，在 APSolute Vision 服务器上，您可以为每个设备最多保存五 (5) 个配置文件。您可以在 APSolute Vision *设置 (Setup)* 选项卡中更改此参数。

表 14：设备配置备份：常规参数

参数	说明
名称 (Name)	任务的名称。 默认值：选定的任务类型名称。如果存在使用此名称的现有任务，**n** 会附加到名称的末尾，其中 **n** 为下一个可用的序列号。
说明 (Description)	用户定义的任务说明。
已启用 (Enabled)	任务在被选定时会根据已定义的计划运行。禁用的任务不会被激活，但任务配置会保存在数据库中。

表 15：设备配置备份：调度参数

参数	说明
运行 (Run)	任务运行的频率。 选择频率，然后配置相关时间和日/日期参数。 值： ● “一次”(Once) - 任务仅在指定的日期和时间运行一次。 ● “分钟”(Minutes) - 按照任务起点之间指定的分钟数间隔运行任务。 ● “每日”(Daily) - 任务每日在指定时间运行。 ● “每周”(Weekly) - 任务每周在指定日的指定时间运行。 **注意：**任务根据 APSolute Vision 客户端上配置的时间运行。
时间 (Time)[1]	任务运行的时间。
日期 (Date)[2]	任务运行的日期。
分钟 (Minutes)[3]	任务运行的间隔（以分钟为单位）。
总是运行 (Run Always)[4]	指定任务是否总是运行，或仅在定义的期间内运行。 值： ● “已启用”(Enabled) - 任务立即激活，并无限期运行下去，无开始或结束时间。任务会在通过*计划 (Schedule)* 选项卡中“频率”(Frequency) 配置的首个“时间”(Time) 运行。 ● “已禁用”(Disabled) - 任务（在*计划 (Schedule)* 选项卡中指定的“时间”(Time) 和“频率”(Frequency)）从指定的“开始日期”(Start Date) 的“开始时间”(Start Time) 到“结束日期”(End Date) 的“结束时间”(End Time) 内运行。 默认值：“已启用”(Enabled)
开始日期 (Start Date)[5]	任务激活的开始日期和时间。
开始时间 (Start Time)	
结束日期 (End Date)	任务不再运行的日期和时间。
结束时间 (End Time)	

1 – 仅当指定的**运行 (Run)** 值为**一次 (Once)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
2 – 仅当指定的**运行 (Run)** 值为**一次 (Once)** 时，此参数才可用。
3 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)** 时，此参数才可用。
4 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
5 – 仅当取消选中**总是运行 (Run Always)** 复选框时，此参数才可用。

表 16：设备配置备份：参数的参数

参数	说明
包括私钥 (Include Private Keys)	指定是否在支持私钥的设备中的配置文件中包括证书私钥信息。 默认值：“已禁用”(Disabled)

表 17：设备配置备份：设备列表参数

参数	说明
可用 (Available) 列表和*选定 (Selected)* 列表。*可用 (Available)* 列表显示可用的设备。*选定 (Selected)* 列表显示此任务备份其配置的设备。	

设备重启任务

设备重启(Device Reboot) 任务会重启指定的设备。

表 18：设备重启：常规参数

参数	说明
名称 (Name)	任务的名称。 默认值：选定的任务类型名称。如果存在使用此名称的现有任务，**n** 会附加到名称的末尾，其中 **n** 为下一个可用的序列号。
说明 (Description)	用户定义的任务说明。
已启用 (Enabled)	任务在被选定时会根据已定义的计划运行。禁用的任务不会被激活，但任务配置会保存在数据库中。

表 19：设备重启：调度参数

参数	说明
运行 (Run)	任务运行的频率。 选择频率，然后配置相关时间和日/日期参数。 值： ● “一次”(Once) - 任务仅在指定的日期和时间运行一次。 ● “分钟”(Minutes) - 按照任务起点之间指定的分钟数间隔运行任务。 ● “每日”(Daily) - 任务每日在指定时间运行。 ● “每周”(Weekly) - 任务每周在指定日的指定时间运行。 **注意**：任务根据 APSolute Vision 客户端上配置的时间运行。
时间 (Time)[1]	任务运行的时间。
日期 (Date)[2]	任务运行的日期。
分钟 (Minutes)[3]	任务运行的间隔（以分钟为单位）。
总是运行 (Run Always)[4]	指定任务是否总是运行，或仅在定义的期间内运行。 值： ● “已启用”(Enabled) - 任务立即激活，并无限期运行下去，无开始或结束时间。任务会在通过*计划 (Schedule)* 选项卡中“频率”(Frequency) 配置的首个“时间”(Time) 运行。 ● “已禁用”(Disabled) - 任务（在*计划 (Schedule)* 选项卡中指定的“时间”(Time) 和“频率”(Frequency)）从指定的“开始日期”(Start Date) 的“开始时间”(Start Time) 到“结束日期”(End Date) 的“结束时间”(End Time) 内运行。 默认值：“已启用”(Enabled)
开始日期 (Start Date)[5]	任务激活的开始日期和时间。
开始时间 (Start Time)	
结束日期 (End Date)	任务不再运行的日期和时间。
结束时间 (End Time)	

1 – 仅当指定的**运行 (Run)** 值为**一次 (Once)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
2 – 仅当指定的**运行 (Run)** 值为**一次 (Once)** 时，此参数才可用。
3 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)** 时，此参数才可用。
4 – 仅当指定的**运行 (Run)** 值为**分钟 (Minutes)**、**每日 (Daily)** 或**每周 (Weekly)** 时，此参数才可用。
5 – 仅当取消选中**总是运行 (Run Always)** 复选框时，此参数才可用。

表 20：设备重启：设备列表参数

参数	说明
可用 (Available) 列表和*选定 (Selected)* 列表。*可用 (Available)* 列表显示可用的设备。“选定”(Selected) 列表会显示此任务重启的设备。	

更新攻击说明文件

您可以在 APSolute Vision 服务器上查看攻击描述文件的最新更新的时间，并且您可以更新该文件。

攻击描述文件包含 DefensePro 可以处理的所有不同攻击的描述。您可以通过输入攻击名称来查看特定描述。当首次配置 APSolute Vision 时，您应将最新的攻击描述文件下载到 APSolute Vision 服务器。该文件用于实时和历史报告，显示来自 DefensePro 设备的攻击的攻击描述。

APSolute Vision 和 DefensePro 设备上的文件版本应相同。Radware 建议在 APSolute Vision 和单个设备上按常规间隔同步该文件的常规更新。

注意：Radware 还建议，每当您在 DefensePro 设备上更新签名文件时，也更新攻击描述文件。

当更新攻击描述文件时，APSolute Vision 会直接从 Radware.com 或启用的代理文件服务器下载该文件。

要查看攻击描述文件最近更新的日期和时间

1. 在 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角中，依次选择**常规设置 (General Settings) > 基本参数 (Basic Parameters)**。
2. 选择*攻击描述文件 (Attack Descriptions File)* 选项卡。

表 21：攻击描述文件参数

参数	说明
攻击描述最后更新 (Attack Descriptions Last Update)	APSolute Vision 服务器上攻击描述文件最新更新的时间。

要更新攻击描述文件

1. 在 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角中，依次选择**常规设置 (General Settings) > 基本参数 (Basic Parameters)**。
2. 执行以下操作之一：
   - 要从 Radware 更新攻击描述文件，请选择 **Radware.com** 单选按钮。
   - 要从 APSolute Vision 客户端主机更新该文件，请执行以下操作：
     a. 选择**客户端 (Client)** 单选按钮。
     b. 在**文件名 (File Name)** 文本框中，输入攻击描述文件的文件路径或点击**浏览 (Browse)** 导航至并选择该文件。
3. 点击**更新 (Update)**。*警报 (Alerts)* 窗格会显示成功或失败通知，以及是否使用代理服务器执行的操作。

第 4 章 - 管理 DefensePro 设置

您可以对选定 DefensePro 设备配置以下设置参数：

配置 DefensePro 全局参数

本节包含以下主题：

查看和配置基本全局参数

您可以查看和配置以下项目：

- 基本设备设置参数
- 设备上的时间和日期设置
- 设备硬件和软件版本

要查看和配置基本全局参数

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup)** > **全局参数 (Global Parameters)**。
2. 如果需要，请配置参数，然后点击**提交 (Submit)**。

表 22：全局参数：常规参数

参数	说明
设备名称 (Device Name)	（只读）设备上配置的设备名称。
设备描述 (Device Description)	（只读）设备上配置的设备说明。
基本 MAC 地址 (Base MAC Address)	（只读）设备上第一个端口的 MAC 地址。
位置 (Location)	如果需要，则为设备位置。
联系信息 (Contact Information)	如果需要，则为联系人信息。
系统启动时间 (System Up Time)	（只读）自上次设备重启以来，设备启动的时长。

表 23：全局参数：日期和时间参数

参数	说明
设备日期 (Device Date)	设备上的日期设置。点击该字段修改日期。
设备时间 (Device Time)	设备上的时间设置。点击该字段修改时间。

表 24：全局参数：版本信息参数

参数	说明
软件版本 (Software Version)	（只读）设备上产品软件的版本。
硬件版本 (Hardware Version)	（只读）设备硬件的版本。

管理证书

本节介绍 DefensePro 的证书，以及如何使用 APSolute Vision 管理证书。

本节包含以下主题：

证书

证书是识别服务器或用户的数字签名指标，通常以电子密钥或值的形式提供。数字证书代表单个业务或组织公钥的认证，但同时也可用于显示已获证明持有者的权限和角色。它还可以包括来自验证身份的第三方的信息。需要进行身份验证，确保通信或事务中的用户是其所声称的身份。

基本的证书包括以下内容：

- 证书持有者身份
- 证书序列号
- 证书到期日期
- 证书持有者公钥的副本
- 认定数字证书由有效机构颁发的证书颁发机构 (CA) 的身份及其数字签名

密钥

密钥是发件人用来加密要通过互联网发送的数据的数字变量集。通常使用一对公钥和私钥。私钥保密，仅供其所有者加密和解密数据之用。公钥分发范围较广，而且不保密。公钥用于加密数据和验证签名。发件人使用一个密钥加密或解释数据。收件人还使用该密钥对来自发件人的数据进行身份验证。

使用密钥可确保未经授权的个人无法破译数据。只有具有合适密钥，才能轻易地破译或理解信息。无合适密钥进行破译和防止伪造时，将无法解读被盗或复制的数据。DefensePro 支持以下密钥大小长度：512、1024 或 2048 字节。

自签证书

自签证书不包括第三方验证。当您使用安全的 WBM（即 HTTP 会话）时，DefensePro 设备会使用证书进行识别。默认情况下，设备具有自签 Radware SSL 证书。您还可以指定自己的自签 SSL 证书。

修改选定设备的证书信息

您可以查看和修改选定设备的证书信息。

要查看和修改选定设备的证书信息

> *在配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates)**。

  证书 (Certificates) 表显示存储在设备上的各个证书的信息。您可以在此添加、编辑和删除证书。您也可以导入和导出证书，并显示证书文本。

配置证书

您可以创建或修改自签证书以保证对基于 Web 的管理 (WBM) 进行安全访问。

您还可以为新证书创建证书签名请求和密钥。

要创建或修改证书或密钥

1. *在配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates)**。
2. 执行以下操作之一：
   — 要添加证书，请点击（添加）。
   — 要编辑证书，请双击证书名称。
3. 配置证书参数并点击**提交 (Submit)**。

表 25：证书参数

参数	说明
名称 (Name)	密钥或证书的名称。 **小心：**请勿定义长度超过 49 个字符的证书名称。这可能会损坏“证书” (Certificates) 表。
类型 (Type)	认证的类型。 值： ● 证书 (Certificate) ● 客户端 CA 证书 (Certificate of Client CA)[1] ● 证书签名请求 (Certificate Signing Request) ● “密钥”(Key) - 当您选择*密钥 (Key)* 时，仅“密钥大小”(Key Size) 和“口令”(Passphrase) 字段可用。 默认值：“密钥”(Key)
密钥大小 (Key Size)	密钥大小（以字节为单位）。 较大的密钥大小提供更高级别的安全性。Radware 建议证书具有的大小为 1024 及以上字节的密钥。使用此大小的证书会使得伪造数字签名或解码加密消息变得极为困难。 值：“512 字节”(512 Bytes)、“1024 字节”(1024 Bytes)、“2048 字节”(2048 Bytes) 默认值：“1024 字节”(1024 Bytes)
通用名称 (Common Name)	组织的域名（例如，www.radware.com）或 IP 地址。
组织 (Organization)	组织的名称。
邮件地址 (Email Address)	您希望包括在证书内的任何邮件地址。
密钥口令 (Key Passphrase)	密钥口令加密存储中的密钥，导出密钥时需要使用。由于私钥是 PKI 数据最敏感的部分，因此必须使用口令进行保护。口令应至少具有四个字符，Radware 建议使用基于字母、数字和符号的强度较高的口令。
验证密钥口令 (Verify Key Passphrase)	在您定义密钥口令后，请重新输入以供验证。
区域 (Locality)	城市名称。
州/省 (State/Province)	省、自治区或直辖市。
组织单位 (Organization Unit)	组织内部的部门或单位。
国家/地区名称 (Country Name)	组织所在国家/地区。
证书到期 (Certificate Expiration)	证书有效的持续时间（日）。值：1-4,294,967,295 (4 GB) 默认值：365

1 – 如果您选择的选项未被允许使用（根据您正在使用的证书类型），设备会向您发出警报，告知错误消息。

配置默认证书属性

使用证书默认值定义贵组织在创建签名请求或自签证书时使用的默认参数。

要配置默认属性，APSolute Vision 服务器与相关设备之间的连接必须使用 SNMPv3。

要配置默认证书属性

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates) > 默认属性 (Default Attributes)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 26：默认证书参数

参数	说明
通用名称 (Common Name)	组织的域名。例如，www.radware.com。
区域 (Locality)	城市名称。
州/省 (State/Province)	省、自治区或直辖市。
组织 (Organization)	组织的名称。
组织单位 (Organization Unit)	组织内部的部门或单位。
国家/地区名称 (Country Name)	组织所在国家/地区。
邮件地址 (Email Address)	要包括在证书中的任何邮件地址。

导入证书

您可以从其他计算机导出密钥和证书，并将证书导出到现有的签名请求以完成其过程。

密钥和证书以 PEM 格式进行导入。如果拥有密钥和证书的单独 PEM 文件，您就必须使用相同的条目名称连续导入证书。

要导入证书或密钥

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates)**。
2. 点击表下方的**导入 (Import)** 按钮。
3. 配置参数，然后点击**提交 (Submit)**。

表 27：导入证书参数

参数	**说明**
条目名称 (Entry Name)	通过导入创建的新条目名称，或覆盖或完成密钥或 CSR 的现有条目名称。
条目类型 (Entry Type)	值： ● “密钥”(Key) - 从备份导入密钥或从其他系统导出密钥。要完成配置，您将需要将证书导入此密钥。 ● “证书”(Certificate) - 从备份导入证书或从其他计算机导出证书。必须将证书导入到匹配的密钥或签名请求中。 ● “客户端 CA 证书”(Certificate of Client CA) - 导入客户端 CA 证书。 默认值：“密钥”(Key) **注意：**在基于 Web 的管理中，DefensePro 支持以下三种其他选项：“中间 CA 证书”(Intermediate CA Certificate)、“证书和密钥”(Certificate and Key)、“SSH 公钥”(SSH Public Key)。
口令 (Passphrase) （仅当**条目类型 (Entry Type)** 为**密钥 (Key)** 时此参数可用。）	由于私钥是 PKI 数据最敏感的部分，因此必须使用口令进行保护。口令应至少具有四个字符，Radware 建议使用基于字母、数字和符号的强度较高的密码。
验证口令 (Verify Passphrase) （仅当**条目类型 (Entry Type)** 为**密钥 (Key)** 时此参数可用。）	由于私钥是 PKI 数据最敏感的部分，因此必须使用口令进行保护。口令应至少具有四个字符，Radware 建议使用基于字母、数字和符号的强度较高的密码。
文件名 (File Name)	要导入的证书文件。

导出证书

密钥、证书和签名请求导出用于备份用途、将现有配置移到其他系统或用于完成签名请求过程。您可以通过复制和粘贴密钥或下载文件，从设备导出证书。密钥和证书导出到 PEM 格式的文件中。

注意：在系统启动时无需 Radware 密码即可创建 Radware 密钥，因此无需 Radware 密码即可导出 Radware 密钥。

要导出证书或密钥

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates)**。
2. 点击表下方的**导出 (Export)** 按钮。
3. 配置参数，然后点击**提交 (Submit)**。

表 28：导出证书参数

参数	**说明**
条目名称 (Entry Name)	选择要导出的条目名称。默认情况下，系统会显示“证书”(Certificates) 表中选定证书的名称。
条目类型 (Entry Type)	根据选定的条目名称，您可以导出证书、证书链、客户端 CA 证书、密钥或证书签名请求。
口令 (Passphrase)	导出密钥时需要口令。使用创建或导出密钥时输入的口令。您必须输入密钥口令才能验证您是否有权导出密钥。

显示证书内容

您可以显示*证书 (Certificates)* 表中列出的密钥、证书或签名请求的内容。内容会以加密文本格式显示出来，供复制-粘贴用途，例如，将签名请求发送到证书签名授权机构。

要显示证书内容

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 证书 (Certificates)**。
2. 点击表下方的**显示 (Show)**。
3. 选择要显示的条目名称。默认情况下，系统会显示“证书”(Certificates) 表中选定证书的名称。
4. 如果需要，请选择密钥的条目类型和密码。
5. 点击**显示 (Show)** 显示*证书 (Certificate)* 字段中的内容。

升级 DefensePro 设备的许可证

您可以使用许可操作步骤升级设备的功能。

适用于 Cisco Firepower 9300 的 DefensePro 对 DefensePro 应用无需许可证，但需要*吞吐量许可证*以支持有用的吞吐量。

当订购吞吐量许可证时，必须包括以下内容：

- 设备*或*设备上配置的任何管理 IP 地址的 MAC 地址（*配置 (Configuration)* 视角，依次选择**设置 (Setup) > 网络 (Networking) > IP 管理 (IP Management)**）。
- 吞吐量许可证 ID，每当使用新许可证时会更改。

您将通过邮件收到新的吞吐量许可密钥。当您在*许可证升级 (License Upgrade)* 窗格中输入新的吞吐量许可证后，旧许可证即无法重复使用。

要在收到新的吞吐量许可密钥后升级吞吐量许可证

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 许可证升级 (License Upgrade)**。
2. 输入新许可证密钥的配置许可证升级参数，然后点击提交 (Submit)。

表 29：DefensePro 许可证升级参数

参数	说明
吞吐量许可密钥 (Throughput License Key)	设备吞吐量许可证的密钥。
吞吐量许可证方法 (Throughput License Method)	（只读）用于生成许可证的方法。 值： ● IP - 许可证生成器使用设备的 IP 地址生成许可证。 ● MAC - 许可证生成器使用设备的 MAC 地址生成许可证。
IP 地址 (IP Address) （仅当**吞吐量许可证方法 (Throughput License Method)** 为 **IP** 时显示此参数。）	（只读）设备的 IP 地址。
MAC （仅当**吞吐量许可证方法 (Throughput License Method)** 为 **MAC** 时显示此参数。）	（只读）设备的 MAC 地址。
吞吐量许可证 ID (Throughput License ID)	（只读）用于生成吞吐量许可证的 ID。

配置 DefensePro 中的日期和时间设置

本节介绍配置基本的 DefensePro 日期和时间设置，以及配置 DefensePro 夏令时，第 79 页。

适用于 Cisco Firepower 9300 的 DefensePro 不支持网络时间协议 (NTP) 同步。

适用于 Cisco Firepower 9300 的 DefensePro 与主机的时间和日期同步。

您无法更改适用于 Cisco Firepower 9300 的 DefensePro 上的时间和日期。但是您*可以*设置夏令时参数。另外，您可以在 CLI 中设置使用命令 services ntp time-zone 设置时区。

配置 DefensePro 夏令时

DefensePro 支持夏令时。您可以配置夏令时的开始和结束日期和时间。在夏令时期间，设备会自动向系统时钟增加一个小时。设备还会指示自身使用的是标准时间还是夏令时。

注意：当手动配置系统时钟时，仅当夏令时开始或结束时系统时间才会更改。在夏令时期间启用夏令时时，设备则不会更改系统时间。

要配置 DefensePro 夏令时

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 全局参数 (Global Parameters) > 时间设置 (Time Settings) > 夏令时 (Daylight Saving)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 30：夏令时参数

参数	说明
已启用 (Enabled)	启用或禁用夏令时。默认值：“已禁用”(Disabled)
开始时间 (Begins at)	夏令时的开始日期和时间。
结束时间 (Ends at)	夏令时的结束日期和时间。
当前模式 (Current Mode)	指定设备使用标准时还是夏令时。

配置 DefensePro 网络设置

本节包含以下主题：

配置 DefensePro 网络设置的基本参数

使用*基本 (Basic)* 窗格配置“IP 分段”(IP Fragmentation) 参数。

IPv4 和 IPv6 支持

DefensePro 支持 IPv6 和 IPv4 协议并为 IPv6/IPv4 数据包提供功能完善的 IPS 和 DoS 防御解决方案。管理仅在 IPv4 中可用。

DefensePro 支持 IPv6 数据包和 ICMPv6 数据包的处理，包括以下功能：

- 使用 IPv6 地址设置网络
- 应用安全策略
- 阻止攻击
- 安全报告

IP 分片

当 IP 数据包长度过长无法传输时，数据包发起器或传输数据包的其中一个路由器必须将数据包分段为多个较短的数据包。

使用 IP 分段，DefensePro 可以分类 IP 分段的第 4 层信息。设备会识别属于相同数据报的所有分段，然后相应地对这些分段进行分类和转发。设备不会重组原始 IP 数据包，但即使数据报到达故障设备，也会将分段的数据报转发至其目标。

流量排除

当 DefensePro 通过与设备上配置的任何网络策略均不匹配的所有流量时发生*流量排除*。

在适用于 Cisco Firepower 9300 的 DefensePro 中，流量排除行为始终处于启用状态。即，设备总是通过与设备上配置的任何网络策略均不匹配的所有流量。

配置基本网络参数

本节介绍如何配置基本网络参数。

要配置基本网络参数

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 网络 (Networking) > 基本 (Basic)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 31：基本：IP 分段参数

参数	说明
启用 IP 分段 (Enable IP Fragmentation)	指定是否启用 IP 分段。
排队限制 (Queuing Limit)	设备为乱序分段 IP 数据报分配的 IP 数据包百分比。 值：0-100 默认值：25
老化时间 (Aging Time)	设备在队列中保留分段数据报的时间（以秒为单位）。 值：1-255 默认值：1

配置网络设置中的 IP 接口管理

DefensePro 在其第二层接口（端口、中继和 VLAN）上定义的所有 IP 接口之间执行路由。DefensePro 还会根据其他网络层（例如第 4 层和第 7 层）执行路由。

要配置 IP 接口

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 网络 (Networking) > IP 管理 (IP Management)**。
2. 执行以下操作之一：
   - 要添加 IP 接口，请点击 ➕（添加）按钮。
   - 要编辑 IP 接口，请双击该行。
3. 配置参数，然后点击**提交 (Submit)**。

表 32：IP 接口参数

参数	说明
IP 地址 (IP Address)	接口的 IP 地址。
掩码 (Mask)	关联的子网掩码。
端口 (Port)	接口标识符，例如 G-1。
广播地址 (Broadcast Address)	指定是否将一或零填充到广播地址的主机 ID 中。 值： ● “填充 1”(Fill 1) - 将一填充到广播地址的主机 ID 中。 ● “填充 0”(Fill 0) - 将零填充到广播地址的主机 ID 中 默认值：“填充 1”(Fill 1)
VLAN 标记 (VLAN Tag)	与此 IP 接口关联的 VLAN 标记。当多个 VLAN 与相同的交换机端口关联时，交换机必须确定将来自该特定端口的传入流量定向至哪个 VLAN。VLAN 标记在第 2 层报头中提供指示，使得交换机可以做出正确决策。

配置 DefensePro 中的 IP 路由

本节介绍 DefensePro 中的 IP 路由。

DefensePro 设备使用 IP 路由表将管理 IP 数据包转发至其目标。此表存储了目标信息以及到达目标的方法。默认情况下，直接连接到设备的所有网络都会在 IP 路由表中进行注册。其他条目则可以通过路由协议进行静态配置或动态创建。

要配置要在 DefensePro 中管理的 IP 路由

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 网络 (Networking) > IP 管理 (IP Management) > IP 路由 (IP Routing)**。
2. 执行以下操作之一：
   - 要添加静态路由，请点击（添加）按钮。
   - 要编辑静态路由，请双击该行。
3. 配置静态路由参数，然后点击**提交 (Submit)**。
4. 配置全局高级参数。
5. 点击**提交 (Submit)**。

注意

- 当编辑静态路由时，您仅可以修改**指标 (Metric)** 字段。
- **类型 (Type)** 字段仅显示在*静态路由 (Static Routes)* 表中。无法对其进行配置。

表 33：IP 路由：基本（静态路由）参数

参数	说明
目标网络 (Destination Network)	向其定义路由的目标网络。
网络掩码 (Netmask)	目标子网的网络掩码。
下一跳 (Next Hop)	朝向目标子网下一跳的 IP 地址。（下一跳总是处于设备本地的子网上。）
通过接口 (Via Interface)	（只读）值 **3**（只读），管理界面的值。
类型 (Type)	（只读）此字段显示在“静态路由”(Static Routes) 表中。 值： ● “本地”(Local) - 可以从设备直接到达子网。 ● “远程”(Remote) - 无法从设备直接到达子网。
指标 (Metric)	为此路由定义或计算的指标值。

表 34：IP 路由高级参数

参数	说明
启用代理 ARP (Enable Proxy ARP)	启用时，网络主机应答未在接收接口上配置的网络地址的 ARP 请求。代表其他主机的代理 ARP 请求可将发送至该主机的所有 LAN 流量有效地定向至代理主机。然后，捕获的流量会通过其他接口路由到目标主机。 默认值：“已启用”(Enabled)
存在 ICMP 错误时启用发送陷阱	互联网控制消息协议 (ICMP) 是互联网协议簇的核心协议之一，网络计算机操作系统用其发送错误消息 - 例如，指示请求的服务不可用，或无法到达主机或路由器。 默认值：“已启用”(Enabled) **注意：**当此选项启用时，当存在 ICMP 错误消息时会发送陷阱。

配置 ARP 表

当代理 ARP 启用时，网络主机应答未在接收接口上配置的网络地址的 ARP 请求。代表其他主机的代理 ARP 请求可将发送至该主机的所有 LAN 流量有效地定向至代理主机。然后，捕获的流量会通过其他接口路由到目标主机。

您可以在本地路由器上配置和管理静态 ARP 条目。

要配置 ARP 表

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 网络 (Networking) > IP 管理 (IP Management) > ARP 表 (ARP Table)**。
2. 执行以下操作之一：
   - 要添加新条目，请点击（添加）按钮。
   - 要编辑条目，请双击该行。
3. 配置 ARP 参数并点击**提交 (Submit)**。
4. 如果需要，请修改高级参数；然后点击**提交 (Submit)**。

表 35：ARP：条目参数

参数	说明
端口 (Port)	站所在的接口号。
IP 地址 (IP Address)	站的 IP 地址。
MAC 地址 (MAC Address)	站的 MAC 地址。
类型 (Type)	条目类型。 值： ● “其他”(Other) - 不是动态或静态。 ● “无效”(Invalid) - 使 ARP 条目无效并有效地删除该条目。 ● “动态”(Dynamic) - 从 ARP 协议获知条目。如果条目在预先确定的时间内不活动，则将节点从表中删除。 ● “静态”(Static) - 条目由网络管理站配置且保持不变。

表 36：ARP：高级参数

参数	说明
非活动 ARP 超时 (Inactive ARP Timeout)	非活动 ARP 缓存条目在设备将其删除之前保留在 ARP 表中的时间（以秒为单位）。如果 ARP 缓存条目在指定期间内未刷新，则认为该地址存在问题。 值：10-86,400

为 DefensePro 网络设置配置 DNS

您可以配置 DefensePro 作为域名服务 (DNS) 客户端运行。当 DNS 客户端被禁用时，则无法解析 IP 地址。当 DNS 客户端被启用时，您必须配置服务器，DefensePro 将为该服务器发出查询以进行主机名解析。

您可以设置 DNS 参数并定义动态 DNS 的主 DNS 服务器和备用 DNS 服务器。此外，您可以设置静态 DNS 参数。

要配置 DNS 设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 网络 (Networking) > DNS**。
2. 配置基本 DNS 客户端参数，并点击**提交 (Submit)**。
3. 要添加或修改静态 DNS 条目，请执行以下操作之一：
   - 要添加条目，请点击（添加）按钮。
   - 要修改条目，请双击表中的条目。
4. 配置参数，并点击**提交 (Submit)**。

表 37：DNS 客户端参数

参数	说明
DNS 客户端 (DNS Client)	指定 DefensePro 设备是否作为 DNS 客户端运行以解析 IP 地址。 值：“启用”(Enable)、“禁用”(Disable) 默认值：“禁用”(Disable)
主 DNS 服务器 (Primary DNS Server)	DefensePro 向其发送查询的主 DNS 服务器的 IP 地址。
备用 DNS 服务器 (Alternative DNS Server)	DefensePro 向其发送查询的备用 DNS 服务器的 IP 地址。
静态 DNS 表 静态 DNS 主机。 点击（添加）按钮添加新的静态 DNS。各静态 DNS 的配置包括以下参数： ● “主机名”(Host Name) - 指定 IP 地址的域名 ● “IP 地址”(IP Address) - 指定域名的 IP 地址	

配置 DefensePro 设备安全设置

本节包含以下主题：

为 DefensePro 设备安全设置配置访问协议

除了使用 APSolute Vision 管理 DefensePro 设备以外，您还可以使用基于 Web 的管理 (WBM) 和命令行界面 (CLI)。

您可以将 DefensePro 设备连接到以下项目：

- 设备上通过 HTTP 和 HTTPS 的 WBM
- 通过 Telnet 和 SSH 的 CLI
- Web 服务

要为 WBM 和 CLI 配置访问协议

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 访问协议 (Access Protocols)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 38：访问协议 Web 访问参数

参数	说明
启用 Web 访问 (Enable Web Access)	指定是否启用对 Web 服务器的访问。 默认值：“已禁用”(Disabled)
L4 端口 (L4 Port)	向其分配 WBM 的端口。 默认值：80
Web 帮助 URL (Web Help URL)	Web 帮助文件的位置（路径）。

表 39：访问协议安全 Web 访问参数

参数	说明
启用安全 Web 访问 (Enable Secured Web Access)	指定是否启用对 Web 服务器的安全访问。 默认值：“已禁用”(Disabled)
L4 端口 (L4 Port)	HTTPS 通过其获得请求的端口。 默认值：443
证书 (Certificate)	安全 Web 服务器用于加密的证书文件。

表 40：访问协议 Telnet 参数

参数	说明
启用 Telnet (Enable Telnet)	指定是否启用对设备的 Telnet 访问。 默认值：“已禁用”(Disabled)
L4 端口 (L4 Port)	Telnet 所用的 TCP 端口。 默认值：23
会话超时时间 (Session Timeout)	设备在非活动期间保持连接的时段（以分钟为单位）。如果当预定义的期间结束时会话仍处于非活动状态，则会话会终止。 值：1-120 默认值：5 **注意：**为了避免影响设备性能，系统每隔 10 秒钟检查超时时间。因此，实际的超时时间可能比配置的时间最多长 10 秒钟。
身份验证超时时间 (Authentication Timeout)	完成身份验证过程所需的超时时间（以秒为单位）。 值：10-60 默认值：30

表 41：访问协议 SSH 参数

参数	说明
启用 SSH (Enable SSH)	指定是否启用对设备的 SSH 访问。 默认值：“已禁用”(Disabled)
L4 端口 (L4 Port)	SSH 服务器连接的源端口。 默认值：22
会话超时时间 (Session Timeout)	设备在非活动期间保持连接的时段（以分钟为单位）。如果当预定义的期间结束时会话仍处于非活动状态，则会话会终止。 值：1-120 默认值：5 **注意：**为了避免影响设备性能，系统每隔 10 秒钟检查超时时间。因此，实际的超时时间可能比配置的时间最多长 10 秒钟。
身份验证超时时间 (Authentication Timeout)	完成身份验证过程所需的超时时间（以秒为单位）。 值：10-60 默认值：10

表 42：访问协议 Web 服务参数

参数	说明
启用 Web 服务 (Enable Web Services)	指定是否启用对 Web 服务的访问。 默认值：“已启用”(Enabled)

在 DefensePro 设备安全设置中配置 SNMP

简单网络管理协议 (SNMP) 是一个应用层协议，可促进 APSolute Vision 和网络设备之间管理信息的交换。

Radware 设备可以使用 SNMP 的所有版本：SNMPv1、SNMPv2c 和 SNMPv3。

默认 Radware 用户在 SNMPv1 中进行配置。

小心：APSolute Vision 不支持 SNMPv2c 陷阱。到达 APSolute Vision 的 SNMPv2c 陷阱会被丢弃。

注意：当您使用 SNMPv3 将 Radware 设备添加到 APSolute Vision 时，用户名和身份验证详细信息必须与在此设备上配置的某个用户匹配。

以下主题介绍在选定设备上配置 SNMP 的操作步骤：

- 配置 DefensePro SNMP 用户，第 88 页
- 配置 SNMP 社区设置，第 89 页
- 配置 SNMP 组表，第 90 页
- 配置 SNMP 访问设置，第 90 页
- 配置 SNMP 通知设置，第 91 页
- 配置 SNMP 视图设置，第 92 页
- 配置 SNMP 目标参数表，第 92 页
- 配置 SNMP 目标地址，第 93 页
- 配置 SNMP 支持的版本，第 94 页

配置 DefensePro SNMP 用户

通过 SNMPv3 基于用户的管理，每个用户可以根据用户名和身份验证方法拥有不同的权限。您可以定义能连接到设备的用户，并存储每个 SNMP 用户的访问参数。

注意：在 SNMP 配置中，用户名也称为安全名。

要为使用 SNMPv3 连接的设备配置具有身份验证和隐私的 SNMP 用户

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > SNMP 用户表 (SNMP User Table)**。
2. 执行以下操作之一：
   - 要添加用户，请点击 ＋（添加）。
   - 要编辑条目，请双击该行。
3. 配置 SNMP 用户参数并点击**提交 (Submit)**。

表 43：SNMP 用户参数

参数	说明
用户名 (User Name)	用户名，也称为安全名。该名称最多可包含 18 个字符。
身份验证协议 (Authentication Protocol)	身份验证过程中使用的协议。 值： ● 无 (None) ● MD5 ● SHA 默认值：“无”(None)
身份验证密码 (Authentication Password)	如果指定了身份验证协议，请输入身份验证密码。
隐私协议 (Privacy Protocol)	用于加密的算法。 值： ● “无”(None) - 数据未加密。 ● DES - 设备使用数据加密标准。 默认值：“无”(None)
隐私密码 (Privacy Password)	如果指定了隐私协议，请输入用户隐私密码。

配置 SNMP 社区设置

“SNMP 社区表”(SNMP Community Table) 仅用于 SNMP 版本 1 和 2，以便将社区字符串关联到用户。当用户通过 SNMPv1 或 SNMPv2 连接设备时，设备会检查 SNMP 数据包中发送的社区字符串。根据特定的社区字符串，设备会将社区字符串映射到预定义用户（属于拥有某些访问权限的组）。
因此，当使用 SNMPv1 或 SNMPv2 时，必须定义用户、组和访问权限。

使用*社区表 (Community Table)* 将社区字符串与用户名关联，反之亦然，并可以限制地址范围，从该地址可以接受 SNMP 请求并向其发送陷阱。

注意：您无法更改与您当前正在使用的用户名相关联的社区字符串。

要配置 SNMP 社区设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 社区 (Community)**。
2. 执行以下操作之一：
   - 要添加 SNMP 社区条目，请点击 +（添加）。
   - 要编辑条目，请双击该行。
3. 配置 SNMP 社区参数并点击**提交 (Submit)**。

表 44：SNMP 社区参数

参数	说明
索引 (Index)	此条目的描述性名称。此名称在创建后无法修改。 默认值：“公共”(public)
社区名称 (Community Name)	社区字符串。 默认值：“公共”(public)
安全名称 (Security Name)	当通知生成时，安全名会识别所使用的 SNMP 社区。 默认值：“公共”(public)
传输标记 (Transport Tag)	指定一组目标地址，SNMP 可从这些地址接受 SNMP 请求，并可向这些地址发送陷阱。在“SNMP 目标地址”(SNMP Target Addresses) 表中定义按此标记识别的目标地址。“SNMP 目标地址”(SNMP Target Addresses) 表中必须至少有一个条目包含指定的传输标记。 如果未指定标记，当接收 SNMP 请求或发送陷阱时，不会检查地址。

配置 SNMP 组表

为用户组定义 SNMPv3 权限。根据连接方法，如果需要向同一用户授予不同的权限，您可以将用户关联到多个组。您可以为不同的用户和安全模型创建具有相同组名的多个条目。

在 *SNMP 访问 (SNMP Access)* 表中为用户组定义访问权限。

要配置 SNMP 组设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 组表 (Group Table)**。
2. 执行以下操作之一：
   - 要添加组条目，请点击 +（添加）。
   - 要编辑条目，请双击该行。
3. 配置参数，然后点击**提交 (Submit)**。

表 45：SNMP 组参数

参数	说明
组名 (Group Name)	SNMP 组的名称。
安全模型 (Security Model)	代表所需**安全模型 (Security Model)** 的 SNMP 版本。安全模型是可供组使用的预定义的权限集。根据 SNMP 版本定义这些权限集。通过选择此参数的 SNMP 版本，您可以确定要使用的权限集。 值： • SNMPv1 • SNMPv2c • 基于用户 (SNMPv3)(User Based [SNMPv3]) 默认值：SNMPv1
安全名称 (Security Name)	如果使用基于用户的安全模型，安全名会识别通知生成时所使用的用户。对于其他安全模型，安全名会识别通知生成时所使用的 SNMP 社区。

配置 SNMP 访问设置

SNMP 访问 (SNMP Access) 表将组和安全模型与定义 MIB 对象子集的 SNMP 视图绑定起来。您可以为各个组和安全模型定义可访问的 MIB 对象。可以根据**读取视图名称 (Read View Name)**、**写入视图名称 (Write View Name)** 和**通知视图名称 (Notify View Name)** 参数访问 MIB 对象，以便执行读取、写入或通知操作。

要配置 SNMP 访问设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 访问 (Access)**。
2. 执行以下操作之一：
   - 要添加访问条目，请点击 +（添加）。
   - 要编辑条目，请双击该行。
3. 配置 SNMP 访问参数并点击**提交 (Submit)**。

表 46：SNMP 访问参数

参数	说明
组名 (Group Name)	组的名称。
安全模型 (Security Model)	安全模型是可供组使用的预定义的权限集。根据 SNMP 版本定义这些权限集。 选择代表所需“安全模型”(Security Model) 的 SNMP 版本以确定要使用的权限。 值： ● SNMPv1 ● SNMPv2c ● “基于用户”(User Based) - 即 SNMPv3 默认值：SNMPv1
安全级别 (Security Level)	访问所需的安全级别。 值： ● “无身份验证”(No Authentication) - 不需要身份验证或隐私。 ● “身份验证和无隐私”(Authentication & No Privacy) - 需要身份验证，但不需要隐私。 ● “身份验证和隐私”(Authentication & Privacy) - 同时需要身份验证和隐私。 默认值：“无身份验证”(No Authentication)
读取视图名称 (Read View Name)	指定 MIB 树中哪些对象可由此组读取的视图名称。
写入视图名称 (Write View Name)	指定 MIB 树中哪些对象可由此组写入的视图名称。
通知视图名称 (Notify View Name)	指定 MIB 树中哪些对象可由此组在通知（陷阱）中进行访问的视图名称。

配置 SNMP 通知设置

您可以选择接收通知的管理目标，以及发送到各个选定管理目标的通知类型。“标记”(Tag) 参数识别一组目标地址。*目标地址 (Target Address)* 表（包含“通知”(Notify) 表中指定标记）中的条目会接收通知。

要配置 SNMP 通知设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 通知 (Notify)**。
2. 执行以下操作之一：
   - 要添加 SNMP 通知条目，请点击 （添加）。
   - 要编辑条目，请双击该行。
3. 配置 SNMP 通知参数并点击**提交 (Submit)**。

表 47：SNMP 通知参数

参数	说明
名称 (Name)	此条目的描述性名称，例如，通知类型。
标记 (Tag)	定义向其发送此通知的目标地址的字符串。在其标记列表中具有此标记的所有目标地址都会向其发送此通知。

配置 SNMP 视图设置

您可以定义 MIB 树的子集，以便在“访问表”(Access Table) 中使用。不同条目可以具有相同的名称。具有相同名称的所有条目的合集定义 MIB 树的子集，并且可以通过其名称在“访问表”(Access Table) 中被引用。

要配置 SNMP 视图设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 视图 (View)**。
2. 执行以下操作之一：
   - 要添加 SNMP 视图条目，请点击 （添加）。
   - 要编辑条目，请双击该行。
3. 配置 SNMP 视图参数并点击**提交 (Submit)**。

表 48：SNMP 视图参数

参数	说明
视图名称 (View Name)	此条目的名称。
子树 (Sub-Tree)	MIB 子树的对象 ID。
类型 (Type)	指定条目中定义的对象包括在 MIB 视图中还是从 MIB 视图中排除。 值：“已包括”(Included)、“已排除”(Excluded) 默认值：“已包括”(Included)

配置 SNMP 目标参数表

“目标参数”(Target Parameters) 表定义用于向特定管理目标发送通知的消息处理和安全参数。“目标参数”(Target Parameters) 表中的条目在“目标地址”(Target Addresses) 表中被引用。

要配置 SNMP 目标参数

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 目标参数表 (Target Parameters Table)**。
2. 执行以下操作之一：
   - 要添加目标参数条目，请点击 （添加）。
   - 要编辑条目，请双击该行。
3. 配置目标参数设置并点击**提交 (Submit)**。

表 49：SNMP 目标参数

参数	说明
名称 (Name)	目标参数条目的名称。 最大字符数：32
消息处理模型 (Message Processing Model)	当生成 SNMP 通知时要使用的 SNMP 版本。值：SNMPv1、SNMPv2c、SNMPv3 默认值：SNMPv1 **小心：**APSolute Vision 不支持 SNMPv2c 陷阱。到达 APSolute Vision 的 SNMPv2c 陷阱会被丢弃。
安全模型 (Security Model)	代表所需“安全模型”(Security Model) 的 SNMP 版本。 安全模型是可供组使用的预定义的权限集。根据 SNMP 版本定义这些权限集。通过选择此参数的 SNMP 版本，您可以确定要使用的权限集。 值： ● SNMPv1 ● SNMPv2c ● “基于用户”(User Based) - 即 SNMPv3 默认值：SNMPv1 **小心：**APSolute Vision 不支持 SNMPv2c 陷阱。到达 APSolute Vision 的 SNMPv2c 陷阱会被丢弃。
安全名称 (Security Name)	如果使用基于用户的安全模型，安全名会识别通知生成时所使用的用户。对于其他安全模型，安全名会识别通知生成时所使用的 SNMP 社区。
安全级别 (Security Level)	指定发送陷阱之前是否对其进行身份验证和加密。 值： ● “无身份验证”(No Authentication) - 不需要身份验证或隐私。 ● “身份验证和无隐私”(Authentication and No Privacy) - 需要身份验证，但不需要隐私。 ● “身份验证和隐私”(Authentication and Privacy) - 同时需要身份验证和隐私。 默认值：“无身份验证”(No Authentication)

配置 SNMP 目标地址

在 SNMPv3 中，“目标地址”(Target Addresses) 表包含用于生成陷阱的传输地址。如果条目的标记列表包含来自“SNMP 通知表”(SNMP Notify Table) 中的标记，则选中此目标用于接收通知。对于 SNMP 版本 1 和 2，此表用于限制从其接受 SNMP 请求和可能向其发送 SNMP 陷阱的地址范围。如果社区表中条目的“传输标记”(Transport Tag) 不为空，传输标记就必须包括在“目标地址表”(Target Addresses Table) 中的一个或多个条目中。

要配置 SNMP 目标地址

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > 目标地址 (Target Address)**。
2. 执行以下操作之一：
   - 要添加目标地址，请点击 （添加）。
   - 要编辑条目，请双击该行。
3. 配置目标地址参数并点击**提交 (Submit)**。

表 50：SNMP 目标地址参数

参数	说明
名称 (Name)	目标地址条目的名称。
IP 地址和 L4 端口 [IP 端口号] (IP Address and L4 Port [IP-port number])	用作 SNMP 陷阱目标的管理站（APSolute Vision 服务器）的 IP 地址和 TCP 端口。该值的格式为 <IP 地址 >-<TCP 端口>，其中 <TCP 端口> 必须为 162。例如，如果 **IP 地址和 L4 端口 (IP Address and L4 Port)** 的值为 1.2.3.4-162，则 1.2.3.4 为 APSolute Vision 服务器的 IP 地址，而 162 为 SNMP 陷阱的端口号。 **注意：**APSolute Vision 仅监听端口 162 上的陷阱。
掩码 (Mask)	管理站的子网掩码。
标记列表 (Tag List)	指定多组目标地址。标记以空格分隔。列表中包含的标记可能是来自“通知”(Notify) 表的标记或来自“社区”(Community) 表的“传输”(Transport) 标记。每个标记可以显示在多个标记列表中。当网络设备上发生重要事件时，标记列表会识别向其发送通知的目标。 默认值：v3Traps
目标参数名称 (Target Parameters Name)	当发送 SNMP 陷阱时使用的目标参数集。在“目标参数”(Target Parameters) 表中定义“目标”(Target) 参数。

配置 SNMP 支持的版本

要配置 SNMP 支持的版本

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > SNMP > SNMP 版本 (SNMP Versions)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 51：SNMP 支持的版本参数

参数	说明
支持的 SNMP 版本 (Supported SNMP Versions)	当前支持的 SNMP 版本。
重置后支持的 SNMP 版本	重置设备后 SNMP 代理所支持的 SNMP 版本。选择要支持的 SNMP 版本。清除不支持的版本。

在 DefensePro 设备安全设置中配置设备用户

对各个设备，您可以配置经过授权可通过任何已启用的访问方法（Web、Telnet、SSH、SWBM）访问该设备的一组用户。当启用配置跟踪时，用户可以接收有关对设备所做更改的邮件通知。

要为选定设备配置设备用户

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 用户表 (Users Table)**。
2. 执行以下操作之一：
   - 要添加用户，请点击（添加）按钮。
   - 要编辑条目，请双击该行。
3. 配置参数，然后点击**提交 (Submit)**。

表 52：设备用户参数

参数	说明
用户名 (User Name)	用户的名称。
密码 (Password)	用户的密码。然后，重复密码进行验证。
邮件地址 (Email Address)	将向其发送通知的用户邮件地址。
发送陷阱的最低严重性级别 (Minimal Severity for Sending Traps)	发送给此用户的陷阱的最低严重性级别。 值： ● “无”(None) - 用户不会收到任何陷阱。 ● “信息”(Info) - 用户收到严重性级别为信息或更高的陷阱。 ● “警告”(Warning) - 用户收到严重性级别为“警告”(Warning)、“错误”(Error) 和“致命”(Fatal) 的陷阱。 ● “错误”(Error) - 用户收到严重性级别为“错误”(Error) 和“致命”(Fatal) 的陷阱。 ● “致命”(Fatal) - 用户仅收到严重性级别为“致命”(Fatal) 的陷阱。 默认值：“无”(None)
启用配置跟踪 (Enable Configuration Tracing)	选定时，指定用户会收到设备中所作配置更改的通知。 每当可配置的变量值发生更改，同一 MIB 条目中所有变量的信息都会报告给指定用户。当缓冲区已满或当 60 秒超时时间已过时，设备会收集报告并在单条通知消息中发送这些报告。 通知消息包含以下详细信息： ● 已更改的 MIB 变量名称。 ● 变量的新值。 ● 配置更改的时间。 ● 使用的配置工具（APSolute Vision、Telnet、SSH、WBM）。 ● 用户名（当适用时）。
访问级别 (Access Level)	用户访问 WBM 和 CLI 的级别。 默认值：“读取-写入”(Read-Write)

要配置设备用户的高级参数

1. *在配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 用户表 (Users Table)**。
2. *在高级参数 (Advanced Parameters)* 选项卡中配置参数，然后点击**提交 (Submit)**。

表 53：设备用户的高级参数

参数	说明
身份验证模式 (Authentication Mode)	用户访问设备的身份验证方法。 值： ● “本地用户表”(Local User Table) - 设备使用“用户表”(User Table) 对访问进行身份验证。 ● “RADIUS 和本地用户表”(RADIUS and Local User Table) - 设备使用 RADIUS 服务器对访问进行身份验证。如果对 RADIUS 服务器的请求超时，设备会使用“用户表”(User Table) 对访问进行身份验证。 默认值：“本地用户表”(Local User Table)

在 DefensePro 设备安全设置中配置高级参数

对设备的访问可以限制于指定的物理接口。连接至不安全网段的接口可以配置为丢弃指向设备本身的某些或全部管理流量。管理员可以允许针对设备的特定类型的管理流量（例如 SSH），同时拒绝其他类型的管理流量（例如 SNMP）。如果入侵者企图通过已禁用的端口访问设备，设备会拒绝访问，并生成系统日志和 CLI 陷阱作为通知。

要为选定设备配置访问权限

1. *在配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 高级 (Advanced)**。
2. 要编辑端口的权限，请双击相关行。
3. 选中或清除复选框以允许或拒绝访问，然后点击**提交 (Submit)**。

表 54：端口权限参数

参数	说明
端口 (Port)	（只读）物理端口的名称。
SNMP 访问 (SNMP Access)	选定时，允许使用 SNMP 对端口进行访问。
Telnet 访问 (Telnet Access)	选定时，允许使用 Telnet 对端口进行访问。
SSH 访问 (SSH Access)	选定时，允许使用 SSH 对端口进行访问。
Web 访问 (Web Access)	选定时，允许使用 WBM 对端口进行访问。
SSL 访问 (SSL Access)	选定时，允许使用 SSL 对端口进行访问。

配置端口 Ping

您可以定义哪些物理接口可以执行 ping。当向不允许 ping 的接口发送 ping 时，数据包会被丢弃。默认情况下，设备的所有接口允许 ping。

要定义要 ping 的端口

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 高级 (Advanced) > Ping 端口 (Ping Ports)**。
2. 要编辑端口 ping 设置，请双击相关行。
3. 选中或清除复选框以允许或不允许 ping，然后点击**提交 (Submit)**。

配置设备管理的身份验证协议

本节包括以下内容：

-

配置设备管理的 RADIUS 身份验证

DefensePro 通过对访问设备的用户（以管理为目的）进行身份验证，提供更高的安全性。凭借 RADIUS 身份验证，您可以使用 RADIUS 服务器确定是否允许用户使用 CLI、Telnet、SSH 或基于 Web 的管理来访问设备管理。您还可以选择当 RADIUS 服务器不可用时，是否使用设备“本地用户表”(Local User Table)。

凭借设备管理的 RADIUS 身份验证，DefensePro 在访问接受响应中搜索服务类型属性 (AVP 6)（内置于所有 RADIUS 服务器）。读写（管理员）用户权限内置于所有 RADIUS 服务器中（服务类型值 6）。只读用户权限赋予服务类型 7 并且必须在 RADIUS 字典中定义。

注意

- 默认的**身份验证模式 (Authentication Mode)** 为**本地用户表 (Local User Table)** - *无* RADIUS。要修改配置，请在*配置 (Configuration)* 视角*设备安全 (Device Security)* 选项卡导航窗格中选择**用户表 (Users Table)**。然后，在*高级参数 (Advanced Parameters)* 选项卡中，从*身份验证模式 (Authentication Mode)* 下拉列表中选择您需要的选项，并点击**提交 (Submit)**。
- DefensePro 设备必须能够访问 RADIUS 服务器并且允许设备访问。

要配置设备管理的 RADIUS 身份验证

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 设备安全 (Device Security) > 身份验证协议 (Authentication Protocols) > RADIUS 身份验证 (RADIUS Authentication)**。
2. 配置受管 Radware 设备的 RADIUS 身份验证参数，然后点击提交 (Submit)。

表 55：RADIUS 身份验证：常规参数

参数	说明
超时 (Timeout)	设备重试之前或者如果超出重试值，在设备确认服务器已离线之前，设备等待 RADIUS 服务器应答的时间长度。 默认值：1
重试 (Retries)	RADIUS 服务器对首次连接尝试无响应后，连接 RADIUS 服务器的重试次数。在指定的重试次数后，如果所有连接尝试均失败（超时），则会使用备用 RADIUS 服务器。 默认值：2
客户端有效期 (Client Lifetime)	客户端身份验证的持续时间（以秒为单位）。如果客户端在有效期内再次登录，DefensePro 将不会使用 RADIUS 服务器对客户重新进行身份验证。如果客户端在有效期到期后再次登录，DefensePro 将会对客户端重新进行身份验证。 默认值：30

表 56：RADIUS 身份验证：主要参数

参数	说明
L4 端口 (L4 Port)	主 Radius 服务器的访问端口号。 值：1645、1812 默认值：1645
密钥 (Secret)	主 Radius 服务器的身份验证密码。 最大字符数：64 **注意：**当 DefensePro 存储密钥时，DefensePro 会被加密。因此，配置文件中的密钥长度大于您配置的字符数。
验证密钥 (Verify Secret)	当定义密码时，重新输入进行验证。
服务器 IP 地址类型 (Server IP Address Type)	值：IPv4、IPv6
服务器 IP 地址 (Server IP Address)	主 Radius 服务器的 IP 地址。

表 57：RADIUS 身份验证：备用参数

参数	说明
L4 端口 (L4 Port)	备用 Radius 服务器的访问端口号。 值：1645、1812 默认值：1645
密钥 (Secret)	备用 Radius 服务器的身份验证密码。 最大字符数：64 **注意：**当 DefensePro 存储密钥时，DefensePro 会被加密。因此，配置文件中的密钥长度大于您配置的字符数。
验证密钥 (Verify Secret)	当定义密码时，重新输入进行验证。
服务器 IP 地址类型 (Server IP Address Type)	值：IPv4、IPv6
服务器 IP 地址 (Server IP Address)	备用 Radius 服务器的 IP 地址。

配置 DefensePro 安全设置的设置

在配置服务器保护策略或网络保护策略及其保护配置文件之前，您必须启用想要使用的保护功能，并配置保护功能的全局参数。

注意：在设备上启用保护功能后，设备需要重启。但是，仅当在相同导航分支内启用功能后您才需要重启。

本节包含以下主题：

配置 DoS 屏蔽保护

DoS 屏蔽机制可防御已知的泛洪攻击和泛洪攻击工具，这些攻击和工具会导致拒绝服务效果，造成计算机资源对预期用户不可用。

注意

- 默认情况下，DoS 屏蔽保护已启用。
- 管理界面上也支持此功能。

DoS 屏蔽配置文件可防御以下攻击：

- 已知的 TCP、UDP 和 ICMP 泛洪。
- 互联网中可用的已知的攻击工具。
- 由 bot 创建的已知泛洪，为自动化攻击。

DoS 屏蔽保护使用来自*Radware 签名 (Radware Signatures)* 数据库的签名。此数据库持续更新并防御所有已知威胁。

Radware 签名配置文件包括所有 DoS 屏蔽签名，作为签名数据库和已包括 DoS 屏蔽保护的 Radware 预定义配置文件的一部分。要创建包括 DoS 屏蔽保护的配置文件，您可以配置*威胁类型 (Threat Type)* 属性设置为**泛洪 (Floods)** 的配置文件。

Radware 还提供预定义的配置文件 *All-DoS-Shield*，该配置文件提供对所有已知 DoS 攻击的保护。当需要仅限 DoS 的解决方案时应用 *All-DoS-Shield* 配置文件。请注意，如果应用了 DoS 屏蔽 Radware 定义的配置文件，您就无法在相同的安全策略中应用其他签名配置文件。

要防范拒绝服务，DoS 屏蔽对流经设备的流量进行采样，并使用预定义的操作对识别为 DoS 攻击的流量的带宽进行限制。

大多数网络可以承受带宽消耗可忽略的间歇性攻击。对此类攻击无需执行任何对抗性操作。当攻击开始消耗大量网络带宽时则会成为网络威胁。DoS 屏蔽使用高级采样算法检测此类事件以优化性能，自动发生作用以解决问题。

DoS 屏蔽考虑两种保护状态：

- **休止状态 (Dormant state)** - 表明采样机制在活动的干预前用于识别。仅当进入网络的数据包数量超过预定义的限制时，休止状态的保护才变为活动状态。
- **活动状态 (Active state)** - 表明在匹配攻击签名的各个数据包上实施操作，不进行采样。

DoS 屏蔽会对匹配休止和活动状态的数据包进行计数。流量样本会与休止状态中的保护列表进行比较。当达到指定数量的数据包时，保护状态会更改为活动。

DoS 屏蔽模块使用并行工作的两个过程。一个过程以统计方式监控流量，检查是否任何休止状态的保护已变为活动状态。然后，当 DoS 屏蔽检测到保护处于活动状态时，模块就会将通过设备的各个数据包与*当前活动的保护 (Currently Active Protections)* 列表进行比较。模块将不匹配活动签名的某些数据包与休止保护列表进行比较。模块会不作检测而将剩余的数据包转发到网络。

要配置 DoS 屏蔽保护

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > DoS 屏蔽 (DoS Shield)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 58：DoS 屏蔽参数

参数	说明
启用 DoS 屏蔽 (Enable DoS Shield)	指定是否启用 DoS 屏蔽功能。 **注意：**如果禁用了保护，请在配置保护配置文件之前启用它。
采样时间 (Sampling Time)	DoS 屏蔽将各休止攻击的预定义阈值与匹配攻击的数据包计数器当前值进行比较的频繁程度（以秒为单位）。 默认值：5 **注意：**如果采样时间过短，即计数器和阈值之间存在频繁的比较，因此常规流量突发可能会被认为是攻击。如果采样时间过长，DoS 屏蔽机制就无法足够快速地检测真正的攻击。
数据包采样率 (Packet Sampling Ratio)	数据包采样率。例如，如果指定值为 5001，则 DoS 屏蔽机制检查每 5001 个数据包中的 1 个。 默认值：5001

要在网络保护策略中包括 DoS 屏蔽保护

> 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 网络保护策略 (Network Protection Policies) >** （添加）**> 操作 (Action) > 签名保护配置文件 (Signature Protection Profile) > All-DoS-Shield**。有关详细信息，请参阅管理 DefensePro 网络保护策略，第 125 页。

配置全局行为 DoS 保护

行为 DoS（行为拒绝服务）保护，您可以将其用于网络保护策略中，为网络防御零日网络泛洪攻击。这些攻击使可用的网络带宽充满无关流量，拒绝合法用户使用网络资源。攻击源自公共网络并威胁与互联网连接的组织。

行为 DoS 配置文件检测流量异常，并可通过识别异常流量的足迹来防范零日、未知、泛洪攻击。

网络泛洪保护类型包括：

- TCP 泛洪 - 包括 SYN 泛洪、TCP Fin + ACK 泛洪、TCP Reset 泛洪、TCP SYN + ACK 泛洪和 TCP 分段泛洪
- ICMP 泛洪
- IGMP 泛洪

BDoS 保护的主要优势在于能够检测统计流量异常，并根据启发式协议信息分析生成准确的 DoS 攻击足迹。这可以确保准确的攻击过滤，并将误报的风险降到最低。创建新签名的默认平均时间介于 10 和 18 秒之间。因为泛洪攻击可持续数分钟，有时甚至数小时，所以这个时间相对较短。

启用 BDoS 保护

在您配置 BDoS 保护配置文件之前，请启用 BDoS 保护。您也可以更改 BDoS 保护的默认全局设备设置。BDoS 保护全局设置适用于在设备上具有 BDoS 配置文件的所有网络保护策略。

要启用 BDoS 保护并配置全局设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > BDoS 保护 (BDoS Protection)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 59：BDoS 保护（全局）：基本参数

参数	说明
启用 BDoS 保护 (Enable BDoS Protection)	指定是否启用 BDoS 保护。 **注意：**更改此参数的设置需要重启才能生效。
获知响应期 (Learning Response Period)	基准首先加权的初始期。 默认获知响应期和建议的获知响应期都是一周。 如果流量速率合理地波动（例如，TCP 或 UDP 流量基准每日更改超过 50%），请将获知响应设置为一个月。仅对测试用途使用一日的响应期。 值：“日”(Day)、“周”(Week)、“月”(Month) 默认值：“周”(Week)
启用流量统计信息采样 (Enable Traffic Statistics Sampling)	指定 BDoS 模块是否在 BDoS 足迹的创建阶段使用流量统计信息采样。当 BDoS 模块尝试生成实时签名，并且流量速率较高时，则设备仅评估部分流量。根据流量速率，BDoS 模块会自动微调采样因素。BDoS 模块会筛选低流量速率（低于 100K PPS）的所有流量以及高流量速率（高于 100K PPS）的部分流量。 默认值：“已启用”(Enabled) **注意：**为获得最佳性能，Radware 建议该参数为*已启用 (Enabled)*。

表 59：BDoS 保护（全局）：基本参数（续）

参数	说明
足迹严格性 (Footprint Strictness)	当行为 DoS 模块检测到新的攻击时，模块会生成攻击足迹以阻止攻击流量。如果行为 DoS 模块无法生成满足足迹严格性条件的足迹，则模块会发布攻击通知，但不会阻止攻击。严格性越高，足迹越准确。但是，严格性越高越会增加设备无法生成足迹的可能性。 值： ● “高”(High) - 足迹中至少需要两个布尔 AND 运算符，且无其他布尔 OR 值。此级别会降低误报率，但会增加漏报率。 ● “中”(Medium) - 足迹中至少需要一个布尔 ADN 运算符，且最多需要另外两个布尔 OR 值。 ● “低”(Low) - 允许行为 DoS 模块建议的任何足迹。此级别能够最好地阻止攻击，但会增加误报率。 默认值：“低”(Low) **注意：** ● DefensePro 始终将校验和字段和序列号字段视为*高*足迹严格性字段。因此，仅具有校验和或序列号的足迹总是被视为是*高*足迹严格性。 ● 表 61 - 足迹严格性示例，第 103 页显示足迹严格性要求的示例。

表 60：BDoS 保护（全局）：高级参数

参数	说明
这些设置影响定期攻击行为。这些设置用于有效地检测和阻止这些攻击类型。	
阻止状态下非攻击流量的持续时间 (Duration of Non-attack Traffic in Blocking State)	阻止状态下*攻击程度*降至并保持在硬编码阈值的时间（以秒为单位）。当时间结束时，DefensePro 会声明攻击已被终止。 值：45-300 默认值：45
异常或非严格性状态下非攻击流量的持续时间 (Duration of Non-attack Traffic in Anomaly or Non-Strictness State)	异常或非严格性状态下*攻击程度*降至并保持在硬编码阈值的时间（以秒为单位）。当时间结束时，DefensePro 会声明攻击已被终止。 值：45-300 默认值：45
重置 BDoS 基准 (Reset BDoS Baseline)	点击以重置 BDoS 基准。然后，选择是重置包含 BDoS 配置文件的所有网络保护策略的基准，还是重置包含 BDoS 配置文件的特定网络保护策略的基准；然后点击**提交 (Submit)**。 重置基准 - 已获知的统计信息会清除基准流量统计信息并重置默认的正常基准。仅当受保护网络的特征已完全更改，并且需要更改带宽配额以适应网络更改时，才重置基准统计信息。

表 60：BDoS 保护（全局）：高级参数（续）

参数	说明
获知抑制阈值 (Learning Suppression Threshold)	*指定带宽*的百分比，在此之下时，DefensePro 会抑制 BDoS 基准获知。 在 DefensePro 偶尔处理极少流量的场景中，获知抑制阈值功能有助于保留良好的 BDoS 基准值。 存在两种 DefensePro 偶尔处理极少流量的典型场景： ● 路径外部署 - 在路径外部署中，在检测到攻击时触发 DefensePro - 此时流量会通过 DefensePro 转移进行迁移。在攻击期间，流量会通过 DefensePro 转移和路由。平时，无流量通过 DefensePro（维护消息除外）。当没有流量转移至 DefensePro 时，必须抑制 BDoS 获知以防止极低值影响基准，最终提高对误报的易感性。 ● 一天当中流量速率剧烈变化的环境。 *指定带宽*指*网络保护 (Network Protection)* 选项卡（**BDoS 配置文件 (BDoS Profiles) > 出站流量 (Outbound Traffic)|入站流量 (Inbound Traffic)**）下的*出站流量 (Outbound Traffic)* 和*入站流量 (Inbound Traffic)* 参数。 获知抑制阈值适用于所有 BDoS 配置文件和控制器，但 DefensePro 会为每个网络保护策略和指定的*方向 (Direction)*（*网络保护 (Network Protection)* 选项卡，**网络保护策略 (Network Protection Policy) > 方向 (Direction)**）计算阈值。对*单向 (One Way)* 策略，获知抑制阈值考虑入站带宽。DefensePro 将*双向 (Two Way)* 策略视为两个策略，因此获知抑制阈值会计算每个策略的带宽（入站/出站）。 值： ● 0 - 指定 BDoS 配置文件*不*使用获知抑制阈值。 ● 1-50 默认值：0

表 61：足迹严格性示例

足迹示例	低严格性	中严格性	高严格性
TTL	是	否	否
TTL AND 数据包大小	是	是	否
TTL AND 数据包大小 AND 目标端口	是	是	是

配置 BDoS 足迹绕行

您可以定义不会用作实时签名一部分的足迹绕行类型和值。即使当保护引擎表明该流量为实时签名候选项，您所定义的类型和值也不会用于阻止规则（实时签名）内的 OR 或 AND 运算符中。

要配置足迹绕行

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > BDoS 保护 (BDoS Protection) > BDoS 足迹绕行 (BDoS Footprint Bypass)**。
2. 从**足迹绕行控制器 (Footprint Bypass Controller)** 下拉列表中，选择您想要为其配置足迹绕行的攻击保护，并点击 （搜索）按钮。该表会显示选定攻击保护的绕行类型和值。
3. 要编辑绕行类型设置，请双击对应的行。
4. 配置选定绕行类型的足迹绕行参数，然后点击**提交 (Submit)**。

表 62：BDoS 足迹绕行参数

参数	说明
足迹绕行控制器 (Footprint Bypass Controller)	（只读）您为其配置足迹绕行的选定攻击保护。
绕行字段 (Bypass Field)	（只读）要配置的选定绕行类型。
绕行状态 (Bypass Status)	绕行选项。 值： ● “绕行”(Bypass) - 当生成足迹时，行为 DoS 模块绕过选定“绕行字段”(Bypass Field) 的所有可能值。 ● “接受”(Accept) - 当生成足迹时，行为 DoS 模块仅绕过选定**绕行字段 (Bypass Field)** 的指定值（如果存在这种值）。
绕行值 (Bypass Values)	如果*绕行状态 (Bypass Status)* 参数值为**接受 (Accept)**，当生成足迹时，行为 DoS 机制不会使用对应的选定*绕行字段 (Bypass Field)* 的指定*绕行值 (Bypass Values)*。有效的*绕行值 (Bypass Values)* 根据选定的*绕行字段 (Bypass Field)* 而变化。*绕行值 (Bypass Values)* 字段中的多个值必须用逗号分隔。

配置 DoS 流量早期阻止

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不可操作。

选择 DoS 流量早期阻止的数据包报头字段

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不可操作。

配置全局 SYN 泛洪保护

SYN 泛洪攻击通常针对特定服务器，目的在于消耗服务器资源。但是，您可以将 SYN 保护配置为网络保护，允许对多个网络元素提供更为简便的保护。

在您为网络保护策略配置 SYM 配置文件之前，确保已启用 SYN 保护，并且已配置 SYN 泛洪保护全局参数。

要配置全局 SYN 泛洪保护

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > SYN 泛洪保护设置 (SYN Flood Protection Settings)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 63：DNS 泛洪保护：常规参数

参数	说明
启用 SYN 泛洪保护 (Enable SYN Flood Protection)	指定是否在设备上启用 SYN 泛洪保护。 默认值：“已启用”(Enabled) **注意：**更改此参数的设置需要重启才能生效。

表 64：SYN 保护参数：高级参数

参数	说明
跟踪时间 (Tracking Time)	定向至单个受保护目标的 SYN 数据包数量必须少于终止阈值，使针对该目标的攻击状态终止的持续时间（以秒为单位）。 值：1-10 默认值：5

配置全局数据包异常保护

管理界面上*不*支持此功能。

数据包异常保护针对数据包异常进行检测并提供保护。

配置数据包异常保护

使用以下步骤合理地配置数据包异常保护。

要配置数据包异常保护

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > 数据包异常 (Packet Anomaly)**。
2. 双击相关行。
3. 配置参数，然后点击**提交 (Submit)**。

   有关这些参数及其默认配置的详细信息，请参阅表 65 - 数据包异常保护参数，第 106 页。

表 65：数据包异常保护参数

<table>
<tr><th>参数</th><th>说明</th></tr>
<tr><td>ID</td><td>（只读）数据包异常保护的 ID 编号。该 ID 是在发送给 APSolute Vision 安全日志的陷阱中所显示的 Radware ID。</td></tr>
<tr><td>保护名称 (Protection Name)</td><td>（只读）数据包异常保护的名称。</td></tr>
<tr><td>操作 (Action)</td><td>当检测到数据包异常时设备所采取的操作。该操作仅针对指定的数据包异常保护。
值：
● “丢弃”(Drop) - 设备丢弃异常数据包并发布陷阱。
● “报告”(Report) - 设备对异常数据包发布陷阱。如果报告操作 (Report Action) 为处理 (Process)，则数据包会前往剩下的设备模块。如果报告操作 (Report Action) 为绕行 (Bypass)，则数据包会绕过剩下的设备模块。
● “不报告”(No Report) - 设备对异常数据包不发布任何陷阱。如果报告操作 (Report Action) 为处理 (Process)，则数据包会前往剩下的设备模块。如果报告操作 (Report Action) 为绕行 (Bypass)，则数据包会绕过剩下的设备模块。
注意：点击丢弃全部 (Drop All) 可将所有数据包异常保护的操作设置为丢弃 (Drop)。点击报告全部 (Report All) 可将所有数据包异常保护的操作设置为报告 (Report)。点击全部不报告 (No Report All) 可将所有数据包异常保护的操作设置为不报告 (No Report)。</td></tr>
<tr><td>风险 (Risk)</td><td>与指定异常的陷阱相关联的风险。
值：“信息”(Info)、“低”(Low)、“中”(Medium)、“高”(High)
默认值：“信息”(Info)</td></tr>
<tr><td>报告操作 (Report Action)</td><td>当指定操作 (Action) 为报告 (Report) 或不报告 (No Report) 时，DefensePro 设备在异常数据包上采取的操作。报告操作仅针对指定的数据包异常保护。
值：
● “绕行”(Bypass) - 异常数据包绕过设备。
● “处理”(Process) - DefensePro 模块处理异常数据包。如果异常数据包为攻击的一部分，则 DefensePro 可以规避此次攻击。
注意：您无法为以下数据包异常保护选择处理 (Process)：
● 104 - “IP 报头或总长度无效”(Invalid IP Header or Total Length)
● 107 - “IPv6 报头不一致”(Inconsistent IPv6 Headers)
● 131 - “L4 报头长度无效”(Invalid L4 Header Length)</td></tr>
</table>

表 66：数据包异常保护的默认配置

异常	说明
IPv4 报头或总长度无效 (Invalid IPv4 Header or Total Length)	IP 数据包报头长度与实际报头长度不匹配，或者 IP 数据包总长度与实际的数据包长度不匹配。 ID：104 默认操作：“丢弃”(Drop) 默认风险：“低”(Low) 报告操作：“绕行”(Bypass)[1]
TTL 少于或等于 1 (TTL Less Than or Equal to 1)	TTL 字段值小于或等于 1。 ID：105 默认操作：“报告”(Report) 默认风险：“低”(Low) 默认报告操作：“处理”(Process)
IPv6 报头不一致 (Inconsistent IPv6 Headers)	不一致的 IPv6 报头。 ID：107 默认操作：“丢弃”(Drop) 默认风险：“低”(Low) 报告操作：“绕行”(Bypass)
已达到 IPv6 跳数限制 (IPv6 Hop Limit Reached)	IPv6 跳数限制不得大于 1。 ID：108 默认操作：“报告”(Report) 默认风险：“低”(Low) 默认报告操作：“处理”(Process)
不支持的 L4 协议 (Unsupported L4 Protocol)	UDP、TCP、ICMP 或 IGMP 以外的流量。 ID：110 默认操作：“不报告”(No Report) 默认风险：“低”（Low） 默认报告操作：“处理”(Process)
TCP 标志无效 (Invalid TCP Flags)	TCP 标志组合不符合标准。 ID：113 默认操作：“丢弃”(Drop) 默认风险：“低”(Low) 默认报告操作：“绕行”(Bypass)
L4 报头长度无效 (Invalid L4 Header Length)	第 4 层的长度，TCP/UDP/SCTP 报头无效。 ID：131 默认操作：“丢弃”(Drop) 默认风险：“低”(Low) 报告操作：“绕行”(Bypass)

1 - 您无法为此数据包异常保护选择*处理 (Process)*。

配置全局 DNS 泛洪保护

您可将 DNS 泛洪保护用于网络保护策略中，为网络防御零日 DNS 泛洪攻击。这些攻击令可用的 DNS 带宽充满无关流量，拒绝合法用户的 DNS 查找。攻击源自公共网络并威胁与互联网连接的组织。

DNS 泛洪配置文件检测流量异常，并可通过识别异常流量的足迹来防范零日、未知、DNS 泛洪攻击。

DNS 泛洪保护类型可包括以下 DNS 查询类型：

- A
- MX
- PTR
- AAAA
- 文本
- SOA
- NAPTR
- SRV
- 其他

DNS 泛洪保护可以检测 DNS 流量中的统计异常，并根据启发式协议信息分析生成准确的攻击足迹。这可以确保准确的攻击过滤，并将误报的风险降到最低。创建新签名的默认平均时间介于 10 和 18 秒之间。因为泛洪攻击可持续数分钟，有时甚至数小时，所以这个时间相对较短。

在您配置 DNS 泛洪保护配置文件之前，请确保已启用 DNS 泛洪保护。您也可以更改 DNS 泛洪保护的默认全局设备设置。DNS 泛洪保护全局设置适用于在设备上具有 DNS 泛洪配置文件的所有网络保护策略。

要启用 DNS 泛洪保护并配置全局设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > DNS 泛洪保护 (DNS Flood Protection)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 67：DNS 泛洪保护：常规参数

参数	说明
启用 DNS 泛洪保护 (Enable DNS Flood Protection)	指定是否启用 DNS 泛洪保护。 **注意：**更改此参数的设置需要重启才能生效。
获知响应期 (Learning Response Period)	基准首先加权的初始期。 默认获知响应期和建议的获知响应期都是一周。 如果流量速率合理地波动（例如，TCP 或 UDP 流量基准每日更改超过 50%），请将获知响应设置为一个月。仅对测试用途使用一日的响应期。 值：“日”(Day)、“周”(Week)、“月”(Month) 默认值：“周”(Week)

表 67：DNS 泛洪保护：常规参数（续）

参数	说明
足迹严格性 (Footprint Strictness)	当 DNS 泛洪保护模块检测到新的攻击时，模块会生成攻击足迹以阻止攻击流量。如果模块无法生成满足足迹严格性条件的足迹，则模块会发布攻击通知，但不会阻止攻击。严格性越高，足迹越准确。但是，严格性越高越会增加模块无法生成足迹的可能性。 值： ● “高”(High) - 足迹中至少需要两个布尔 AND 运算符，且无其他布尔 OR 值。此级别会降低误报率，但会增加漏报率。 ● “中”(Medium) - 足迹中至少需要一个布尔 ADN 运算符，且最多需要另外两个布尔 OR 值。 ● “低”(Low) - 允许 DNS 泛洪保护模块建议的任何足迹。此级别能够最好地阻止攻击，但会增加误报率。 默认值：“低”(Low) **注意：**DNS 泛洪保护模块始终将校验和字段和序列号字段视为*高*足迹严格性字段。因此，仅具有校验和或序列号的足迹总是被视为是*高*足迹严格性。表 70 - DNS 足迹严格性示例，第 110 页显示足迹严格性要求的示例。

表 68：DNS 泛洪保护：缓解操作参数

参数	说明
当启用保护并且设备检测到 DNS 泛洪攻击已开始时，设备会以逐步升级的顺序（选项卡上显示的顺序）实施缓解操作。如果首个启用的缓解操作未能（在特定的*升级期 (Escalation Period)* 后）令人满意地规避攻击，设备就会实施下一个更严厉的已启用的缓解操作，以此类推。系统总是实施*综合速率限制 (Collective Rate Limit)* 作为最严厉的缓解操作，限制对受保护服务器的所有 DNS 查询的速率。	
启用签名速率限制 (Enable Signature Rate Limit)	指定设备是否限制与实时签名匹配的 DNS 查询的速率。 默认值：“已启用”(Enabled)
启用综合速率限制 (Enable Collective Rate Limit)	（只读）设备限制对受保护服务器的所有 DNS 查询的速率。 值：“已启用”(Enabled)
重置 DNS 基准 (Reset DNS Baseline)	点击以重置 DNS 基准。然后，选择是重置包含 DNS 配置文件的所有网络策略规则的基准，还是重置包含 DNS 配置文件的特定网络保护策略的基准；然后点击**提交 (Submit)**。 重置基准 - 已获知的统计信息会清除基准流量统计信息并重置默认的正常基准。仅当受保护网络的特征已完全更改，并且需要更改带宽配额以适应网络更改时，才重置基准统计信息。

表 69：DNS 泛洪保护：高级参数

参数	说明
这些设置影响定期攻击行为。这些设置用于有效地检测和阻止这些攻击类型。	
阻止状态下非攻击流量的持续时间 (Duration of Non-attack Traffic in Blocking State)	阻止状态下*攻击程度*降至并保持在硬编码阈值的时间（以秒为单位）。当时间结束时，DefensePro 会声明攻击已被终止。 值：45-300 默认值：45
异常或非严格性状态下非攻击流量的持续时间 (Duration of Non-attack Traffic in Anomaly or Non- Strictness State)	异常或非严格性状态下*攻击程度*降至并保持在硬编码阈值的时间（以秒为单位）。当时间结束时，DefensePro 会声明攻击已被终止。 值：45-300 默认值：45
重置 DNS 基准 (Reset DNS Baseline)	点击以重置 DNS 基准。然后，选择是重置包含 DNS 配置文件的所有网络保护策略的基准，还是重置包含 DNS 配置文件的特定网络保护策略的基准；然后点击**提交 (Submit)**。 重置基准 - 已获知的统计信息会清除基准流量统计信息并重置默认的正常基准。仅当受保护网络的特征已完全更改，并且需要更改带宽配额以适应网络更改时，才重置基准统计信息。

表 70：DNS 足迹严格性示例

足迹示例	低严格性	中严格性	高严格性
DNS 查询	是	否	否
DNS 查询 AND DNS ID	是	是	否
DNS 查询 AND DNS ID AND 数据包大小	是	是	是

配置 DNS 足迹绕行

您可以定义不会用作实时签名一部分的足迹绕行类型和值。即使当保护引擎表明该流量为实时签名候选项，您所定义的类型和值也不会用于阻止规则（实时签名）内的 OR 或 AND 运算符中。

要配置 DNS 足迹绕行

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 安全设置 (Security Settings) > DNS 泛洪保护 (DNS Flood Protection) > DNS 足迹绕行 (DNS Footprint Bypass)**。
2. 从*足迹绕行控制器 (Footprint Bypass Controller)* 列表中，选择您想要为其配置足迹绕行的 DNS 查询类型，并点击（搜索）按钮。该表显示选定 DNS 查询类型的绕行字段。
3. 要编辑绕行类型设置，请双击对应的行。
4. 配置选定绕行字段的足迹绕行参数，然后点击**提交 (Submit)**。

表 71：DNS 足迹绕行参数

参数	说明
足迹绕行控制器 (Footprint Bypass Controller)	（只读）您为其配置足迹绕行的选定 DNS 查询类型。
绕行字段 (Bypass Field)	（只读）要配置的选定“绕行字段”(Bypass Field)。
绕行状态 (Bypass Status)	绕行选项。 值： ● “绕行”(Bypass) - 当生成足迹时，DNS 泛洪保护模块绕过选定绕行字段的所有可能值。 ● “接受”(Accept) - 当生成足迹时，DNS 泛洪保护模块仅绕过选定绕行字段的指定值（如果存在这种值）。
绕行值 (Bypass Values)	当“绕行状态”(Bypass Status) 参数值为**接受 (Accept)** 时使用。DNS 泛洪保护仅绕过选定绕行类型的值，同时可以使用所有其他值。这些值根据所选“绕行字段”(Bypass Field) 而变化。字段中的值必须用逗号分隔。

配置 DNS 流量早期阻止

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不可操作。

选择 DNS 流量早期阻止的数据包报头字段

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不可操作。

配置 DefensePro 报告设置的设置

本节包含以下主题：

配置 DefensePro 系统日志设置

DefensePro 可以向最多五个系统日志服务器发送事件陷阱。您可以向每个 DefensePro 设备配置合适的信息。

注意：与配置每个单独的设备相反，Radware 建议配置 APSolute Vision 服务器以传达来自所有设备的系统日志消息。

要配置系统日志设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 报告设置 (Reporting Settings) > 系统日志 (Syslog)**。
2. 执行以下操作之一：
   - 要启用系统日志功能，请选中**启用系统日志 (Enable Syslog)** 复选框。
   - 要禁用系统日志功能，请清除**启用系统日志 (Enable Syslog)** 复选框。默认值：“已启用”(Enabled)
3. 执行以下操作之一：
   - 要添加条目，请点击（添加）按钮。
   - 要修改条目，请双击表中的条目。
4. 配置参数，然后点击**提交 (Submit)**。

表 72：适用于 Cisco Firepower 9300 的 DefensePro 中的系统日志参数

参数	说明
启用系统日志服务器 (Enable Syslog Server)	指定是否启用系统日志服务器。 默认值：“已启用”(Enabled) **注意：**设备使用 UDP 发送系统日志消息。即，设备发送系统日志消息，但是不对消息传输进行验证。该*状态 (Status)* 在 DefensePro 系统日志监控 (DefensePro Syslog Monitor)（*监控 (Monitoring)* 视角 > *资源利用率 (Resource Utilization)* 选项卡 > **系统日志监控 (Syslog Monitor)**）中为 **N/R**。
系统日志服务器 (Syslog Server)	运行系统日志服务 (syslogd) 的设备的 IP 地址或主机名。
源端口 (Source Port)	系统日志源端口。 默认值：514 **注意：**端口 0 指定随机端口。
目标端口 (Destination Port)	系统日志目标端口。 默认值：514

表 72：适用于 Cisco Firepower 9300 的 DefensePro 中的系统日志参数（续）

参数	说明
设备 (Facility)	发件人的设备类型。这会随系统日志消息发送。您可以使用此参数辨别不同的设备，并定义拆分消息的规则。 值： ● “授权消息”(Authorization Messages) ● “时钟后台守护程序”(Clock Daemon) ● “时钟后台守护程序 2”(Clock Daemon2) ● “FTP 后台守护程序”(FTP Daemon) ● “内核消息”(Kernel Messages) ● “行式打印机子系统”(Line Printer Subsystem) ● “本地 0”(Local 0) ● “本地 1”(Local 1) ● “本地 2”(Local 2) ● “本地 3”(Local 3) ● “本地 4”(Local 4) ● “本地 5”(Local 5) • “本地 6”(Local 6) • “本地 7”(Local 7) • “日志警报”(Log Alert) • “日志审计”(Log Audit) • “邮件系统”(Mail System) • “网络新闻子系统”(Network News Subsystem) • “NTP 后台守护程序”(NTP Daemon) • “Syslogd 消息”(Syslogd Messages) • “系统后台守护程序”(System Daemons) • “用户级别消息”(User Level Messages) • UUCP 默认值：“本地使用 6”(Local Use 6)

在 DefensePro 设备上启用配置审计

当设备的配置审计在 APSolute Vision 服务器和设备上启用时，使用 APSolute Vision 在设备上进行的任何配置更改都会在审计数据库中创建两条记录，一条来自 APSolute Vision 服务器，一条来自设备审计消息。

注意： 为了防止受管设备超载和性能下降，默认情况下，该功能被禁用。

要启用受管设备的配置审计

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 高级参数 (Advanced Parameters) > 配置审计 (Configuration Audit)**。
2. 选中**启用配置审计 (Enable Configuration Auditing)** 复选框并点击**提交 (Submit)**。

配置安全报告设置

为了支持历史和实时安全监控功能，并对每个攻击事件提供深入的攻击信息，DefensePro 会在设备和 APSolute Vision 之间建立数据报告协议。此协议称为统计实时协议 (SRP)，使用 UDP 数据包发送攻击信息。

您可以启用由 DefensePro 使用的报告信道以接收有关攻击的信息，并根据这些攻击的各种风险等级来报告检测到的攻击。

此外，DefensePro 可以为 APSolute 服务器提供采样捕获的数据包，这些数据包被 DefensePro 设备识别为特定攻击的一部分。DefensePro 将封装于 UDP 数据包中的这些数据包发送到指定的 IP 地址。

注意

- DefensePro 不提供来自 DefensePro 质疑为可疑来源的采样捕获的数据包。（DefensePro 支持选项以质疑 HTTP 泛洪保护、SYN 泛洪保护、DNS 泛洪保护和 SSL 保护中的来源。）
- DefensePro 不提供采样 GRE 封装的捕获的数据包。

您还可以将 DefensePro 设备配置为发送捕获的攻击数据包以及攻击事件以供进一步的离线分析。数据包报告和 SRP 使用相同的默认端口 2088。

要配置适用于 Cisco Firepower 9300 的 DefensePro 中的安全报告设置

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 报告设置 (Reporting Settings) > 高级报告设置 (Advanced Reporting Settings)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 73：高级报告设置：安全报告参数

参数	说明
“报告间隔”(Report Interval)	报告通过报告信道发送的频率（以秒为单位）。 值：1-65,535 默认值：5
每个报告的最大警报数量 (Maximal Number of Alerts per Report)	（报告间隔内发送的）每个报告中可以显示的攻击事件的最大数量。 值：1-2000 默认值：1000
根据攻击汇聚阈值的报告 (Report per Attack Aggregation Threshold)	在事件汇聚为报告之前，报告间隔期间特定攻击的事件数量。当生成的事件数量超过汇聚阈值的值时，事件的 IP 地址值会显示为指定*任意 IP 地址*的 0.0.0.0。 值：1-50 默认值：5
用于报告的 L4 端口 (L4 Port for Reporting)	用于数据包报告和 SRP 的端口。值：1-65,535 默认值：2088
启用发送陷阱 (Enable Sending Traps)	选定时，设备使用陷阱报告通道。 默认值：“已启用”(Enabled)
发送陷阱的最小风险级别 (Minimal Risk Level for Sending Traps)	报告通道的最小风险级别。系统会报告具有指定或更高风险值的攻击。 默认值：“低”(Low)
启用发送系统日志 (Enable Sending Syslog)	选定时，设备使用系统日志报告通道。 默认值：“已启用”(Enabled)
发送系统日志的最小风险级别 (Minimal Risk Level for Sending Syslog)	报告通道的最小风险级别。系统会报告具有指定或更高风险值的攻击。 默认值：“低”(Low)
启用发送终端回应 (Enable Sending Terminal Echo)	选定时，设备使用终端回应报告通道。 默认值：“已禁用”(Disabled)
发送终端回应的最小风险级别 (Minimal Risk Level for Sending Terminal Echo)	报告通道的最小风险级别。系统会报告具有指定或更高风险值的攻击。 默认值：“低”(Low)
启用安全日志记录 (Enable Security Logging)	选定时，设备使用安全日志记录报告通道。

表 74：高级报告：数据包报告和数据包跟踪参数

参数	说明
注意：此选项卡中的参数仅应用于数据包报告。本版本不支持数据包跟踪功能。	
启用数据包报告 (Enable Packet Reporting)	指定 DefensePro 设备是否发送采样攻击数据包以及攻击事件。 默认值：“已启用”(Enabled)
每个报告的最大数据包 (Maximum Packets per Report)	设备可以在报告间隔内发送的数据包的最大数量。 值：1-65,535 默认值：100
目标 IP 地址 (Destination IP Address)	数据包报告的目标 IP 地址。默认值：0.0.0.0 **注意：**即使多个 APSolute Vision 服务器在管理设备，对数据包报告也仅可配置一个目标 IP 地址。

表 75：高级报告设置：netForensics 参数

参数	说明
启用 netForensics 报告 (Enable netForensics Reporting)	选定时，使用 netForensics 报告代理启用报告。 默认值：“已禁用”(Disabled)
代理 IP 地址 (Agent IP Address)	netForensics 代理的 IP 地址。
L4 端口 (L4 Port)	用于 netForensics 报告的端口。 值：1-65,535 默认值：555

表 76：高级报告设置：数据报告目标参数

参数	说明
目标 IP 地址 (Destination IP Address)	数据报告的目标地址。 该表最多可以包含 10 个地址。默认情况下，当您向设备窗格中的树添加 DefensePro 设备时，如果该表中有空间，就会自动添加地址。 要添加地址，请点击 （添加）按钮。输入目标 IP 地址，并点击**提交 (Submit)**。

配置 DefensePro 集群设置

使用*集群 (Clustering)* 选项卡配置适用于 Cisco Firepower 9300 的 DefensePro 的多个实例的集群。

集群允许多个 DefensePro 实例支持集群成员间的 SYN 泛洪保护。

在同一 Firepower 9300 平台上运行 DefensePro 的若干单独的实例，每个实例配置了相同的保护和网络，这能够提高受保护网络的保护容量。Firepower 9300 的内部交换机可以共享 DefensePro 实例间的流量负载。每个 DefensePro 实例经单独配置并可作为独立实例运行。因此，对在相同受保护网络上定义的部分或全部实例上的保护进行激活，则（基于 Firepower 9300 交换机的负载共享机制）能够对实例间的流量启用负载共享，从而实现更高的设备容量。

Web cookie 身份验证涉及质询响应过程，其中每个实例都要求 HTTP 会话具有持续性。由于 Firepower 9300 负载共享交换机会根据 L4 参数分发流量，可能会发生 HTTP 会话的持续性问题。多实例集群允许验证在同一 Firepower 9300 上的 DefensePro 实例之间保持 Web cookie 的持续性。这可以通过一个内部机制实现：该机制使用一个定义为*集群主节点*的集群实例定期同步实例间的 cookie。

注意：有关安装适用于 Cisco Firepower 9300 的 DefensePro 的信息，请参阅相关思科文档。

要配置集群

1. 在*配置 (Configuration)* 视角中，依次选择**设置 (Setup) > 高级参数 (Advanced Parameters) > 集群 (Clustering)**。
2. 配置参数，然后点击**提交 (Submit)**。

表 77：集群参数

参数	说明
设备管理信道 IP 地址 (Device-Management-Channel IP Address)	（只读）DefensePro 设备管理信道的 IP 地址。[1]
设备管理信道默认网关 (Device-Management-Channel Default Gateway)	（只读）设备管理信道的默认网关。[1]
设备管理信道网络掩码 (Device-Management-Channel Netmask)	（只读）设备管理信道的网络掩码。[1]
集群主节点 IP 地址 (Cluster-Master IP Address)	集群主节点的 IP 地址。即集群成员向其连接的 IP 地址。 要使此 DefensePro 实例成为集群*主节点*，请在**设备管理信道 IP 地址 (Device-Management-Channel IP Address)** 字段中指定值。 要使此 DefensePro 实例成为集群*成员*，请指定主节点 DefensePro 实例的**设备管理信道 IP 地址 (Device-Management-Channel IP Address)**。 **小心：**仅当**集群状态 (Cluster State)** 为**已禁用 (Disabled)** 时，您才能在点击**提交 (Submit)** 后更改该值。

表 77：集群参数（续）

参数	说明
集群状态 (Cluster State)	集群或集群成员的状态。 值： ● “已启用”(Enabled) - 以下项之一： — 当此 DefensePro 实例为主节点时 - 启用集群。 — 当此 DefensePro 实例为集群成员时 - 加入集群。 ● “已禁用”(Disabled) - 以下项之一： — 当此 DefensePro 实例为主节点时 - 禁用集群并解除与集群的关系。 — 当此 DefensePro 实例为集群成员时 - 离开集群。 默认值：“已禁用”(Disabled)

1 - Firepower 引导程序 XML 文件定义该值。每当适用于 Cisco Firepower 的 DefensePro 实例初始化时，则读取引导程序 XML 文件。

第 5 章 - 管理类

*类*定义 DefensePro 中相同类型的实体的元素组。本章包含以下各节：

您可以基于以下选项配置类：

- **网络 (Networks)** - 要分类网络保护策略中的流量。
- **情景组 (Context Groups)** - 要分类网络保护策略中的流量。
- **应用端口 (Application ports)** - 要根据第 4 层目标端口定义或修改应用。
- **MAC 地址 (MAC addresses)** - 要分类其源或目标为透明网络设备的流量。
- **SGT** - 要配置适用于 Cisco Firepower 9300 的 DefensePro 的“安全组标记”(Security Group Tags) (SGT)。

在您创建或修改类后，配置会保存在 APSolute Vision 数据库中。您必须激活配置才能将配置下载到设备。您还可以查看设备上的当前类配置。在创建类后，您无法修改类的名称或应用类的配置。

配置网络类

在适用于 Cisco Firepower 9300 的 DefensePro 中，您可以在网络保护策略中使用网络类匹配源或目标流量。网络类通过名称进行标识，由网络地址和 IPv4 掩码或 IPv6 前缀定义。

要配置网络类

1. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > 网络 (Networks)**。
2. 要添加或修改网络类，请执行以下操作之一：
   - 要添加类，请点击 （添加）按钮。
   - 要编辑类，请双击表中的条目。
3. 配置网络类参数，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ()。

表 78：网络类参数

参数	说明
网络名称 (Network Name)	网络类的名称。 网络名称区分大小写。 网络名称不能是 IP 地址。 最大字符数：64
条目类型 (Entry Type)	指定网络是否由子网和掩码或 IP 范围定义。 值：“IP 掩码”(IP Mask)、“IP 范围”(IP Range) 值：“IP 掩码”(IP Mask)、“IP 范围”(IP Range)
网络类型 (Network Type)	值：IPv4、IPv6
网络地址 (Network Address)	网络地址。
前缀 (Prefix)	您可以按以下方式之一输入子网掩码： ● 点分十进制表示法的子网掩码 - 例如，255.0.0.0 或 255.255.0.0。 ● IP 前缀，即掩码位数 - 例如，8 或16。

配置情景组类

您可以使用情景组类定义网段。使用这些类来分类安全策略中的流量。

每个 DefensePro 设备均支持最大 64 个情景组类。每个情景组类均包含最大 32 个离散标记和 32 个范围。即，每个 DefensePro 设备实际上最多支持 64^2 个定义。

要配置情景组类

1. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > 情景组 (Context Groups)**。
2. 执行以下操作之一：
   – 要添加条目，请点击 +（添加）按钮。
   – 要编辑条目，请双击表中的条目。
3. 配置参数，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ( )。

表 79：情景组类参数

参数	说明
情景组名称 (Context Group Name)	组的名称。 最大字符数：19
组模式 (Group Mode)	值： ● “离散”(Discrete) - 设备接口参数中定义的单个情景组。 ● “范围”(Range) - 设备接口参数中定义的一组按次序排列的情景组号。 默认值：“离散”(Discrete)
标记 (Tag) （此参数仅对**离散 (Discrete)** 模式可用。）	情景组号。 值：0-4095
范围起始值 (Range From) （此参数仅对**范围 (Range)** 模式可用。）	范围中的第一个情景组。 值：0-4095 **注意：**创建情景组后，您无法修改该值。
范围结束值 (Range To) （此参数仅对**范围 (Range)** 模式可用。）	范围中的最后一个情景组。 值：0-4095

配置应用类

应用类为 UDP 和 TCP 流量的第 4 层端口组。每个类通过其唯一名称进行标识，并且您可以在一个类中定义多个第 4 层端口。您无法修改标准应用的预定义应用类；但您可以添加该类的条目。您可以将用户定义的类添加到*应用端口组 (Application Port Group)* 表，并修改这些类。

要配置应用类

1. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > 应用 (Applications)**。
2. 要添加或修改应用类，请执行以下操作之一：
   - 要添加类，请点击 （添加）按钮。
   - 要编辑类，请双击表中的条目。
3. 配置应用类参数，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ()。

表 80：应用类参数

参数	说明
端口组名称 (Ports Group Name)	应用端口组的名称。 要将大量范围与同一端口组关联，请对您想要包括在组中的所有范围使用相同的名称。每个范围在“应用端口组”(Application Port Group) 表中显示为具有相同名称的单独行。
条目类型 (Type of Entry)	（只读） 值：“系统定义”(System Defined)、“用户定义”(User Defined)
起始 L4 端口 (From L4 Port)	范围中的第一个端口。
结束 L4 端口 (To L4 Port)	范围中的最后一个端口。 要定义具有单个端口的组，请为**起始 L4 端口 (From L4 Port)** 和**结束 L4 端口 (To L4 Port)** 参数设置相同的值。

配置 MAC 地址类

MAC 组识别其源或目标为透明网络设备的流量。

要配置 MAC 地址类

1. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > 地址 (Addresses)**。
2. 要添加或修改 MAC 地址类，请执行以下操作之一：
   - 要添加类，请点击 + （添加）按钮。
   - 要编辑类，请双击表中的条目。
3. 输入 MAC 组的名称以及与该组关联的 MAC 地址，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ( )。

配置 SGT 类

每个 DefensePro 可以具有零个或一个已启用的“安全组标记”(Security Group Tag) (SGT)。

当 SYN 泛洪保护模块收到要质询的数据包，并且该数据包包括 SGT 时，DefensePro 会将数据包中的 SGT 替换为 DefensePro 配置中启用的 SGT。当 DefensePro *无*启用的 SGT 或要质询数据包*不*包括 SGT，则 DefensePro 按原样质询数据包。

注意

- 每个 DefensePro 最多支持 16 个 SGT。
- 给定时间仅可以启用一个 SGT 值。
- 更改 SGT 状态（已启用/已禁用）需要更新策略操作生效。

要配置 SGT

1. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > SGT**。
2. 执行以下操作之一：
   - 要添加条目，请点击（添加）按钮。
   - 要编辑条目，请双击表中的条目。
3. 配置参数，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ()。

表 81：SGT 类参数

参数	说明
名称 (Name)	SGT 的名称。 最大字符数：20
值 (Value)	SGT 数字值。 值：0-65535 默认值：0
状态 (Status)	值：“已启用”(Enabled)、“已禁用”(Disabled) 默认值：“已禁用”(Disabled) **注意：**如果 DefensePro 配置中存在启用的 SGT 值，如果您启用另一个值，则 DefensePro 会自动禁用上一个启用的值，并发布相应消息。

第 6 章 - 管理 DefensePro 网络保护策略

网络保护策略使用*保护配置文件 (protection profiles)* 保护您所配置的网络。每个网络保护策略使用一个或多个应用于预定义网段上的保护*配置文件*。此外，每个策略包括当检测到攻击时所要采取的操作。

在您配置“网络保护”(Network Protection) 策略和配置文件之前，请确保您已启用所有所需保护，并在**设置 (Setup) > 安全设置 (Security Settings)** 下已配置对应的全局保护参数。

注意：术语*网络保护策略 (Network Protection Policy)* 和*网络策略 (network policy)* 在 APSolute Vision 和文档中可互换使用。

表 82 - DefensePro 保护，第 125 页介绍适用于 Cisco Firepower 9300 的 DefensePro 版本 1.01 所支持的保护。

表 82：DefensePro 保护

保护	说明
DoS 屏蔽 (DoS Shield)	防御可造成拒绝服务效果的已知泛洪攻击和泛洪攻击工具。
行为 DoS (Behavioral DoS)	防御零日 DoS/DDoS 泛洪攻击。
SYN 保护 (SYN Protection)	防御使用 SYN cookie 的 SYN 泛洪攻击。
DNS 保护 (DNS Protection)	防御零日 DNS 泛洪攻击。

配置网络保护策略

每个网络保护策略由两部分组成：

- 定义受保护网段的分类。
- 当匹配的网段上检测到攻击时应用的操作。该操作定义应用到网段的保护配置文件，以及是否阻止恶意流量。系统总是会报告恶意流量。

注意：术语*网络保护策略*和*网络策略*在 APSolute Vision 和文档中可互换使用。

您可以配置的网络保护策略的最大数量取决于 DefensePro 的版本。在适用于 Cisco Firepower 9300 的 DefensePro 中，您最多可以配置 50 个策略。

在您配置策略前，请确保您已配置以下项目：

- 将被需要用于定义受保护网段的类。
- 网络保护配置文件。有关详细信息，请参阅：
  - 为网络保护配置签名保护，第 129 页
  - 为网络保护配置 BDoS 配置文件，第 140 页
  - 为网络保护配置 SYN 配置文件，第 143 页
  - 为网络保护配置 DNS 泛洪保护配置文件，第 148 页

小心：当您配置策略时，APSolute Vision 会存储配置更改，但不会将配置更改下载到设备。要将更改应用到设备上，您必须激活配置更改。*激活最新更改*也被称为*更新策略*。

要配置网络保护策略

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 网络保护策略 (Network Protection Policies)**。
2. 执行以下操作之一：
   - 要添加条目，请点击 ＋（添加）按钮。
   - 要编辑表中的条目，请双击该条目。
3. 配置网络保护策略参数，然后点击**提交 (Submit)**。
4. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ( )。

表 83：网络保护策略：常规参数

参数	说明
已启用 (Enabled)	指定是否启用策略。
策略名称 (Policy Name)	网络保护策略的名称。 最大字符数：19 **小心：**名称不得包括逗号 (,)。

表 84：网络保护策略：分类参数

参数	说明
SRC 网络输入 (SRC Network Input)	**SRC 网络 (SRC Network)** 参数的输入方法。 值： ● “从列表”(From List) - **SRC 网络 (SRC Network)** 参数为下拉列表，其中包含所有配置的网络类（*配置 (Configuration)* 视角，**类 (Classes) > 网络 (Networks)**）。 ● “用户定义值”(User-Defined Value) - **SRC 网络 (SRC Network)** 参数是一个文本字段，可以包含用户定义的 IP 地址。 默认值：“从列表”(From List)
SRC 网络 (SRC Network)	策略使用的数据包源。如果 **SRC 网络输入 (SRC Network Input)** 为**从列表 (From List)**，则从列表中选择所需值。如果 **SRC 网络输入 (SRC Network Input)** 为**用户定义值 (User-Defined Value)**，则请键入 IP 地址。要指定*任意*网络，该字段可能包含值**任意 (any)** 或为空。

表 84：网络保护策略：分类参数（续）

参数	说明
DST 网络输入 (DST Network Input)	**DST 网络 (DST Network)** 参数的输入方法。 值： ● “从列表”(From List) - **DST 网络 (DST Network)** 参数为下拉列表，其中包含所有配置的网络类（*配置 (Configuration)* 视角，**类 (Classes) > 网络 (Networks)**）。 ● “用户定义值”(User-Defined Value) - **DST 网络 (DST Network)** 参数是一个文本字段，可以包含用户定义的 IP 地址。 默认值：“从列表”(From List)
DST 网络 (DST Network)	策略使用的数据包目标。如果 **DST 网络输入 (DST Network Input)** 为**从列表 (From List)**，则从列表中选择所需值。如果 **DST 网络输入 (DST Network Input)** 为**用户定义值 (User-Defined Value)**，则请键入 IP 地址。要指定*任意*网络，该字段可能包含值**任意 (any)** 或为空。
方向 (Direction)	策略与其相关的流量方向。 值： ● “单向”(One Way) - 保护应用到由源到目标（匹配策略的网络定义）的会话。 ● “双向”(Two Way) - 保护应用到匹配策略的网络定义的会话，而无论其方向如何。 默认值：“单向”(One Way)
情景 (Context)	策略使用的情景组类。 值： ● *“类”(Classes) 选项卡中显示的情景组类。* ● *无 (None)。*

表 85：网络保护策略：操作参数

参数	说明
保护配置文件 (Protection Profiles)	（显示在表中，而不是配置中）应用到此策略中定义的网段的配置文件。
BDoS 配置文件 (BDoS Profile)	应用到此策略中定义的网段的 BDoS 配置文件。 **注意：**您可以点击旁边的按钮打开对话框，您可以在对话框中添加和修改配置文件。
DNS 配置文件 (DNS Profile)	应用到此策略中定义的网段的 DNS 保护配置文件。 **注意：**您可以点击旁边的按钮打开对话框，您可以在对话框中添加和修改配置文件。
签名保护配置文件 (Signature Protection Profile)	应用到此策略中定义的网段的签名保护配置文件。 **注意：**您可以点击旁边的按钮打开对话框，您可以在对话框中添加和修改配置文件。
SYN 泛洪配置文件 (SYN Flood Profile)	应用到此策略中定义的网段的 SYN 泛洪配置文件。 **注意：**您可以点击旁边的按钮打开对话框，您可以在对话框中添加和修改配置文件。

表 85：网络保护策略：操作参数（续）

参数	说明
操作 (Action)	此策略下所有攻击的默认操作。 值： ● “阻止并报告”(Block and Report) - 终止恶意流量，并且生成和记录安全事件。 ● “仅报告”(Report Only) - 将恶意流量转发至其目标，并且生成和记录安全事件。 默认值：“阻止并报告”(Block and Report) **注意：**签名特定的操作会覆盖策略的默认操作。

表 86：网络保护策略数据包报告设置参数

参数	说明
数据包报告 (Packet Reporting)	指定设备是否将采样攻击数据包发送到 APSolute Vision 供离线分析。 默认值：“已禁用”(Disabled) **小心：**当在此处启用此功能时，为了使该功能生效，必须启用全局设置（*配置 (Configuration)* 视角，**设置 (Setup) > 报告设置 (Reporting Settings) > 高级报告设置 (Advanced Reporting Settings) > 数据包报告和数据包跟踪 (Packet Reporting and Packet Trace) > 启用数据包报告 (Enable Packet Reporting)**）。
策略上的数据包报告配置优先 (Packet Reporting Configuration on Policy Takes Precedence)	指定此策略上的数据包报告功能配置是否优先于相关联的配置文件中数据包报告功能的配置。

要删除一个或多个网络保护策略

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 网络保护策略 (Network Protection Policies)**。
2. 选择一行或多行。
3. 点击（删除网络保护策略）按钮。

为网络保护配置签名保护

通过将每个数据包与签名数据库中存储的一组签名进行比较，签名保护可以检测并防范面向网络的攻击、面向操作系统 (OS) 的攻击和面向应用的攻击。

本节包含以下主题：

适用于 Cisco Firepower 的 DefensePro 中的签名保护

在适用于 Cisco Firepower 的 DefensePro 中，您可以使用 All-DoS-Shield 配置文件和/或添加用户定义的签名来配置签名保护。

All-DoS-Shield 配置文件中的签名限于“偏移掩码模式条件”(Offset Mask Pattern Condition) (OMPC) 参数。OMPC 参数是定义模式查询规则的一组攻击参数。有关详细信息，请参阅表 95 - 签名的过滤参数：OMPC 参数：第 136 页。

Radware 为 All-DoS-Shield 配置文件提供一组预定义的签名配置文件供现场安装。

当 Radware 创建相关的新 OMPC 签名时，All-DoS-Shield 配置文件就会更新。

您无法编辑 All-DoS-Shield 配置文件，但您可以根据环境的需求创建新的配置文件。例如，如果仅需要使用一小组自定义签名，就可以创建这些签名的新配置文件以及新的威胁类型属性（请参阅表 96 - 属性类型，第 138 页）。

注意

- Radware 漏洞研究团队 (VRT) 负责研究、处理和缓解漏洞、DDoS 工具以及 DDoS 恶意软件。
- 如果需要协助创建新的签名，您可以根据服务协议联系相关的 Radware 部门。

签名保护的配置注意事项

您可以配置策略以使用情景组、应用端口和物理端口。

有关策略和保护方向设置的含义，请参阅表 87 - 策略方向的含义，第 129 页。

配置包含签名保护配置文件的策略时，您可以将“方向”(Direction) 设置为*单向 (One Way)* 或*双向 (Two Way)*。

配置保护时，您可以将“方向”(Direction) 值设置为*入站 (Inbound)*、*出站 (Outbound)* 或*入-出站 (In-Outbound)*。

当大多数攻击（例如蠕虫感染）通过其入站模式被检测出来时，某些攻击则需要检测受感染主机所发起的出站模式。例如，特洛伊木马需要检测受感染主机所发起的出站模式。

配置“源”(Source) = *任意 (Any)* 且“目标”(Destination) = *任意 (Any)* 的策略仅检测*入-出站 (In-Outbound)* 攻击。

表 87：策略方向的含义

策略方向	策略操作	数据包方向	签名方向		
			入站	出站	入站或出站
起止	单向	外至内	检测	忽略	检测
		内至外	忽略	检测	忽略
起止	双向	外至内	检测	忽略	检测
		内至外	忽略	检测	检测
任意到任意	无	无	忽略	忽略	检测

配置签名保护配置文件

签名保护配置文件包含要保护的网段的一个或多个*规则 (rules)*。每个规则定义签名数据库上的查询。DefensePro 从匹配该组规则的签名数据库中激活保护。每当您下载已更新的签名数据库时，用户定义的配置文件就会更新。

要配置签名保护配置文件，必须配置全局“DoS 屏蔽”(DoS Shield) 参数。有关详细信息，请参阅配置 DoS 屏蔽保护，第 99 页。

您可以在 DefensePro 设备上最多配置 300 个签名保护配置文件。配置文件中的每个规则可以包括一个或多个来自各个*属性类型*的条目。规则根据以下逻辑在签名数据库上定义查询：

- 相同*类型*的值使用逻辑 OR 组合。
- 不同*类型*的值使用逻辑 AND 组合。

规则在配置文件中使用逻辑 OR 组合。

签名内所有过滤器间的关系为逻辑 AND。

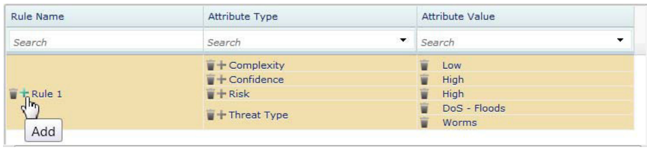
注意：配置文件中的规则为*隐式*。即，当您定义值时，匹配特定选定属性的所有签名*加上不*具有该类型属性的所有签名。此逻辑确保包括*可能*与受保护网络相关的签名 - 即使这些签名与网络中的应用非明显关联。

要配置签名保护配置文件

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 配置文件 (Profiles)**。
2. 执行以下操作之一：
   - 要添加配置文件，请点击 ＋（添加）按钮，并输入配置文件名。
   - 要编辑配置文件，请双击表中的条目。
   - 要显示与配置文件的已配置保护关联的签名列表，请双击表中的条目，然后点击**显示匹配的签名 (Show Matching Signatures)**。
3. 按以下方式对配置文件的规则进行配置：
   - 要配置新规则：
     a. 点击规则表上方的 ＋（添加）按钮。
     b. 在**规则名称 (Rule Name)** 文本字段中，键入新规则的名称。
     c. 从**属性类型 (Attribute Type)** 下拉列表中，选择所需值。
     d. 在**属性值 (Attribute Value)** 下拉列表中，键入所需值。
     e. 点击**提交 (Submit)**。

— 要编辑规则的属性类型和/或属性值：

a. 在表的*规则名称 (Rule Name)* 列中，移动鼠标至相关规则的名称并点击小添加按钮。*添加签名配置文件规则 (Add Signature Profile Rule)* 选项卡会打开，其中含有选定规则的名称。



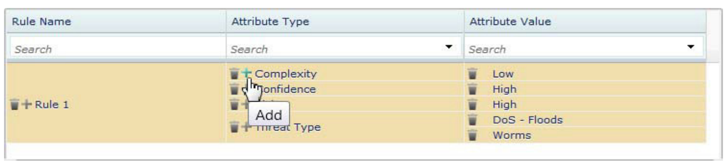
b. 从**属性类型 (Attribute Type)** 下拉列表中，选择所需值。

c. 在**属性值 (Attribute Value)** 下拉列表中，选择或键入所需值。

d. 点击**提交 (Submit)**。

— 要编辑规则的属性值：

a. 在表的*属性类型 (Attribute Type)* 列中，移动鼠标至相关规则的相关属性类型，并点击小添加按钮。*添加签名配置文件规则 (Add Signature Profile Rule)* 选项卡会打开，其中含有规则的名称和选定属性类型的名称。



b. 在**属性值 (Attribute Value)** 下拉列表中，选择或键入所需值。

c. 点击**提交 (Submit)**。

注意：或者，要编辑现有配置文件的属性类型和/或属性，您可以执行以下操作（如 APSolute Vision 版本 3.20 及更早版本所支持）：

a. 点击规则表上方的 （添加）按钮。

b. 在**规则名称 (Rule Name)** 文本字段中，键入您要修改的规则名称。

c. 从**属性类型 (Attribute Type)** 下拉列表中，选择所需值。

d. 在**属性值 (Attribute Value)** 下拉列表中，键入所需值。

e. 点击**提交 (Submit)**。

4. 根据您的需要重复步骤 3 - 为配置文件配置更多规则，为规则配置更多属性或为现有属性配置更多值。

5. 要保存签名配置文件配置，请点击**提交 (Submit)**。

表 88：签名配置文件参数

参数	说明
配置文件名称 (Profile Name)	签名配置文件的名称。对于新配置文件，请输入配置文件的名称。
匹配的签名数量 (Number of Matching Signatures)	（只读）匹配配置文件的签名数量。 匹配的签名数量取决于属性类型的匹配方法（请参阅查看和修改属性类型属性，第 139 页）。“匹配方法”(Match Method)“最低”(Minimum) 仅与属性类型“复杂性”(Complexity)、“信任”(Confidence) 和“风险”(Risk) 相关，其具有升序-降序级别的属性值。 “最低”指定*属性值 (Attribute Value)* 包括较低级别“属性值”(Attribute Values) 的结果。例如，对于属性类型*风险 (Risk)*，当*匹配方法 (Match Method)* 为*最低 (Minimum)* 时，*属性值高 (Attribute Value High)* 仅匹配*高 (High)*，而不匹配*信息 (Info)*、*低 (Low)* 或*中 (Medium)*。*最低 (Minimum)* 为*复杂性 (Complexity)*、*信任 (Confidence)* 和*风险 (Risk)* 的默认值。
显示匹配的签名 (Show Matching Signatures)	仅当编辑配置文件时，系统才会显示此按钮。点击以显示与配置文件已配置的保护关联的签名列表。

表 89：签名配置文件规则表参数

参数	说明
该表显示选定配置文件已配置规则的详细信息。每个规则可以包含多个属性类型，每个属性类型可以包含一个或多个属性值。	
规则名称 (Rule Name)	签名配置文件规则的名称。
属性类型 (Attribute Type)	预定义属性类型的列表，基于定义新攻击时考虑到的各方面因素。
属性值 (Attribute Value)	已定义属性类型的值。

配置签名保护签名

签名是保护配置文件的构成单位。每个签名包含一个或多个保护*过滤器*和*属性*，确定哪些为恶意数据包，以及对这类数据包的处理方法。

签名设置参数定义一旦在流量中识别到恶意数据包的签名时，对这类数据包的跟踪方法以及处理方法。每个攻击均受*跟踪*功能的约束，该功能定义当数据包与签名匹配时如何处理该数据包。这些功能的主要目的在于确定数据包是否有害，以及是否要应用适当的操作。

签名表为您提供过滤器，允许您查看 Radware 和用户定义的签名。您可以定义过滤条件，从而使匹配该条件的所有签名都显示在签名表中。您还可用添加用户定义的签名。

存在两种签名类型：用户定义的签名和 Radware 定义的签名。Radware 定义的签名称为静态签名。您仅能编辑和删除用户定义的签名。对于 Radware 定义的签名，您仅能编辑常规参数。

注意：您仅能编辑和删除用户定义的签名。对于 Radware 定义的签名，您仅能编辑常规参数。

小心：即使属性不完全匹配，DefensePro 也可能会自动将用户定义的签名添加到现有的配置文件。如果要配置任何用户定义的签名，您就必须在*默认*属性之外再指定属性 - 越多越好。用户定义的签名的默认属性仅包括“风险”(Risk) 和“信任”(Confidence)。除非您指定其他属性，否则用户定义的签名中所有其他属性均为空。如果用户定义的签名中所有其他属性均为空，则 DefensePro 会将签名与现有的*静态*配置文件（例如 DoS-ALL、DoS-SSL、Fraud 和 All-DoS-Shield）进行匹配，并将其中缺少的属性（为空）视为现有属性（具有默认值）。这会导致 DefensePro 将用户定义的签名添加到静态配置文件，这种处理是错误的。因此，Radware 建议您尽可能多地指定其他属性，并防止 DefensePro 错误地使用用户定义的签名。

要查看签名保护签名

> 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 签名 (Signatures)**。

注意：要查看所有签名，请清除表列顶部的文本框，然后点击 （过滤）按钮。

要查看签名保护签名并按签名参数过滤表

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 签名 (Signatures)**。
2. 选择**按 ID 过滤 (Filter by ID)** 选项按钮。
3. 在列标题下的框中输入搜索条件。
4. 点击 （过滤）按钮。

要查看签名保护签名并按属性参数过滤表

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 签名 (Signatures)**。
2. 选择**按属性过滤 (Filter by Attribute)** 选项按钮。
3. 在列标题下的框中输入搜索条件。

   注意：例如，对于**属性类型 (Attribute Type)**，从预定义的属性类型列表中选择，这些预定义的属性类型基于定义新攻击时考虑到的各方面因素。

4. 点击 （过滤）按钮。

要配置签名保护签名

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 签名 (Signatures)**。
2. 要添加或编辑签名，请执行以下操作之一：
   - 要添加签名，请点击 + （添加）按钮。
   - 要编辑签名，请显示所需签名，然后双击该签名。
3. 配置参数，然后点击**提交 (Submit)**。

表 90：签名参数

参数	说明
签名名称 (Signature Name)	签名的名称。 最大字符数：29
签名 ID (Signature ID)	（只读）由系统分配到签名的 ID。
已启用 (Enabled)	指定签名是否可以用于保护配置文件。
跟踪时间 (Tracking Time)	测量活动阈值的时间（毫秒）。当超过阈值的大量数据包在配置的跟踪时间段内通过设备时，设备会将其识别为攻击。 默认值：1000
跟踪类型 (Tracking Type)	（只读）指定当受到攻击时，DefensePro 如何确定要阻止或丢弃的流量。 值：“采样”(Sampling) - 此选项可配合 DoS 屏蔽机制。
操作模式 (Action Mode)	当检测到攻击时 DefensePro 所采取的操作。 值： ● “丢弃”(Drop) - DefensePro 丢弃数据包。 ● “仅报告”(Report Only) - DefensePro 将数据包转发至定义的目标。 ● “重置源”(Reset Source) - DefensePro 向数据包源 IP 地址发送 TCP-Reset 数据包。 ● “重置目标”(Reset Destination) - DefensePro 向数据包目标地址发送 TCP-Reset 数据包。 ● “双向重置”(Reset Bidirectional) - DefensePro 同时向数据包源 IP 地址和数据包目标 IP 地址发送 TCP-Reset 数据包。 默认值：“丢弃”(Drop) **注意：**
方向 (Direction)	保护检测路径。保护可以检测仅传入流量，仅传出流量，或同时检测二者。 值：“入站”(Inbound)、“出站”(Outbound)、“入站和出站”(Inbound & Outbound) 默认值：“入站和出站”(Inbound & Outbound)

表 90：签名参数（续）

参数	说明
激活阈值 (Activation Threshold)	各跟踪时间段内允许的攻击数据包的最大数量。当攻击数据包在跟踪时间段内传输时会被识别为合法流量。 当**跟踪类型 (Tracking Type)** 的值为**全部丢弃 (Drop All)** 时，DefensePro 会忽略此参数。 默认值：50
丢弃阈值 (Drop Threshold)	在已检测到攻击后，DefensePro 在其之上时开始丢弃过量流量的 PPS。 当**跟踪类型 (Tracking Type)** 的值为**全部丢弃 (Drop All)** 时，配置文件会忽略此参数。 默认值：50
终止阈值 (Termination Threshold)	当攻击 PPS 速率降至此阈值之下时，配置文件将攻击由主用模式更改为非主用模式。 当**跟踪类型 (Tracking Type)** 的值为**全部丢弃 (Drop All)** 时，DefensePro 会忽略此参数。 默认值：50
数据包报告 (Packet Reporting)	允许将采样攻击数据包发送到 APSolute Vision 供离线分析。 默认值：“已禁用”(Disabled)

表 91：签名：攻击描述

<table>
<tr><th>参数</th><th>说明</th></tr>
<tr><td colspan="2">（只读）静态签名的描述。
您无法为用户定义的签名配置描述。</td></tr>
</table>

表 92：签名：过滤器表

<table>
<tr><th>参数</th><th>说明</th></tr>
<tr><td colspan="2">过滤器是保护的组件，每个过滤器包含一个特定的攻击签名，扫描并分类预定义的流量。过滤器将已扫描的数据包与签名数据库中的攻击签名进行匹配。
对于每个自定义的保护，您可以定义自定义的过滤器。当自定义保护定义时，您无法使用来自其他保护的过滤器。
要添加过滤器，请选择添加新的过滤器 (Add New Filter)。
要编辑过滤器，请选择过滤器并选择编辑过滤器 (Edit Filter)。</td></tr>
</table>

表 93：签名：属性表

<table>
<tr><th>参数</th><th>说明</th></tr>
<tr><td colspan="2">您为签名选择的属性确定规则创建过程中使用的攻击特征。
要添加属性值，请在表中点击 +（添加）按钮。</td></tr>
</table>

表 94：签名的过滤器参数：常规参数

参数	说明
每个过滤器均具有指定名称以及指定的协议属性参数。	
过滤器名称 (Filter Name)	签名过滤器的名称。
协议 (Protocol)	使用的协议。 值： ● ICMP ● ICMPv6 ● IP ● 非 IP (Non IP) ● TCP ● UDP 默认值：IP **小心：**请勿选择**非 IP (Non IP)** 选项。因为该选项会产生意外结果。
源应用端口 (Source Application Port)	仅用于 UDP 和 TCP 流量。 从预定义“应用端口组”(Application Port Groups) 列表中选择。
目标应用端口 (Destination Application Port)	仅用于 UDP 和 TCP 流量。 从预定义“应用端口组”(Application Port Groups) 列表中选择。

表 95：签名的过滤器参数：OMPC 参数

参数	说明
“偏移掩码模式条件”(Offset Mask Pattern Condition) (OMPC) 参数是定义模式查询规则的一组攻击参数。OMPC 规则会查找最多四个字节的固定大小的模式（使用固定偏移掩码）。当攻击签名为 TCP/IP 报头字段或固定偏移的数据/负载中的模式时，这对攻击识别就很有用。	
OMPC 条件 (OMPC Condition)	OMPC 条件。 值： ● 等于 (Equal) ● 大于 (Greater Than) ● 不适用 (Not Applicable) ● 小于 (Less Than) ● 不等于 (Not Equal) 默认值：“不适用”(Not Applicable)
OMPC 长度 (OMPC Length)	OMPC（偏移掩码模式条件）数据的长度。 值： ● 不适用 (Not Applicable) ● 1 字节 (1 Byte) ● 2 字节 (2 Bytes) ● 3 字节 (2 Bytes) ● 4 字节 (4 Bytes) 默认值：“1 字节”(1 Byte)

表 95：签名的过滤器参数：OMPC 参数（续）

参数	说明
OMPC 偏移量 (OMPC Offset)	数据包中的位置，数据检查从该位置开始在 IP/TCP 报头中查找特定位数。 值：0-1513 默认值：0
OMPC 相对偏移量 (OMPC Offset Relative to)	指定选定偏移量相对的 OMPC 偏移量。 值： ● 无 (None) ● IP 报头 (IP Header) ● IP 数据 (IP Data) ● L4 数据 (L4 Data) ● L4 报头 (L4 Header) ● 以太网 默认值：“无”(None)
OMPC 模式 (OMPC Pattern)	OMPC 规则尝试查找的数据包内固定大小的模式。 值：十六进制数的组合（0-9，a-f）。该值由 **OMPC 长度 (OMPC Length)** 参数定义。 **OMPC 模式 (OMPC Pattern)** 定义包含八个符号。当 **OMPC 长度 (OMPC Length)** 小于四个字节时，请在其后补上零。 例如，当 **OMPC 长度 (OMPC Length)** 为两个字节时，**OMPC 模式 (OMPC Pattern)** 可以是 abcd0000。 默认值：00000000
OMPC 掩码 (OMPC Mask)	OMPC 数据的掩码。 值：十六进制数的组合（0-9，a-f）。该值由“OMPC 长度”(OMPC Length) 参数定义。 **OMPC 掩码 (OMPC Mask)** 定义包含八个符号。当 **OMPC 长度 (OMPC Length)** 值小于四个字节时，请在其后补上零。 例如，当 **OMPC 长度 (OMPC Length)** 为两个字节时，“OMPC 掩码”(OMPC Mask) 可以是 abcd0000。 默认值：00000000

配置签名保护属性

属性是*基于规则的*配置文件配置过程中设置的保护策略的组件。属性根据类型组织，基于定义新攻击时考虑到的各方面因素（例如环境、应用、威胁级别、风险级别等）而组织。

每个签名都分配有不同类型的属性。当创建签名时，Radware 漏洞研究团队 (VRT) 会分配这些属性作为描述签名的手段。

您可以使用现有的属性、添加新属性或从列表中删除属性。

注意：您可以查看属性类型的属性，而对于属性类型“复杂性”(Complexity)、“信任”(Confidence) 和“风险”(Risk)，您还可以指定*匹配方法 (Match Method)*（*最低 (Minimum)* 或*精确 (Exact)*）。有关详细信息，请参阅查看和修改属性类型属性，第 139 页。

属性派生自“签名”(Signatures) 数据库，并在有任何更新时动态添加。

要配置签名保护属性

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 属性 (Attributes)**。
2. 要查看属性：
   — 要查看所有属性，请选择“全部”(All) 并点击 （搜索）按钮。
   — 要查看单个属性类型的属性，请选择该属性类型并点击 （搜索）按钮。
3. 要添加新属性：
   a. 请点击 （添加）按钮。
   b. 选择属性类型，并输入属性名称。
   c. 点击**提交 (Submit)**。

表 96：属性类型

属性类型	说明
应用 (Applications)	易受此漏洞威胁的应用。 例如：Web 服务器、邮件服务器、浏览器参数可选，即属性可能包含也可能不包含值。 可以存在多个值。
复杂性 (Complexity)	作为攻击查询机制的一部分所执行的分析级别。该参数可以仅存在单个值。 值： ● “低”(Low) - 此签名对设备性能的影响可忽略。 ● “高”(High) - 此签名对设备性能的影响较大。
信任 (Confidence)	对某次攻击可信任的确定程度。信任级别和攻击所关联的误报级别相反。例如，如果攻击信任级别设置为高，其误报级别则为低。 该参数必填。 该参数可以仅存在单个值。 值：“低”(Low)、“高”(High)、“中”(Medium)
组 (Groups)	允许您创建自定义的攻击组。
平台 (Platforms)	易受此漏洞影响的操作系统。 例如：Windows、Linux、Unix 参数可选，即属性可能包含也可能不包含值。 可以存在多个值。
风险 (Risk)	与攻击相关的风险。例如，攻击对网络产生严重影响而被定义为高风险攻击。 该参数必填。 该参数可以仅存在单个值。 值：“信息”(Info)、“低”(Low)、“中”(Medium)、“高”(High)
服务 (Services)	易受此漏洞威胁的协议。 例如：FTP、HTTP、DNS 该参数可选；即参数可能包含也不可能包含值。 该参数可以仅存在单个值。
目标 (Target)	威胁的目标 - 客户端或服务器端。
威胁类型 (Threat Type)	能最佳描述签名的威胁。 例如：泛洪、蠕虫 可以存在多个值。

查看和修改属性类型属性

您可以查看设备支持的属性类型的以下属性：

- **攻击中多个值 (Multiple Values in Attack)** - 指定属性类型是否可以在任意一个签名中包含多个值。
- **规则中多个值 (Multiple Values in Rule)** - 指定属性类型是否可以在任意一个签名配置文件规则中包含多个值。
- **静态签名中多个值 (Multiple Values in Static)** - 指定属性类型是否可以在来自签名文件的签名中包含多个值。
- **匹配方法 (Match Method)** - 仅与属性类型**复杂性 (Complexity)**、**信任 (Confidence)** 和**风险 (Risk)** 相关，其具有升序-降序级别的*属性值 (Attribute Values)*。

  值：

  – “最低”(Minimum) - 指定*属性值 (Attribute Values)* 包括最低级别属性值的结果。例如，对于属性类型*风险 (Risk)*，当*匹配方法 (Match Method)* 为**最低 (Minimum)** 时，*属性值高 (Attribute Value High)* 仅匹配**高 (High)**，而不匹配**信息 (Info)**、**低 (Low)** 或**中 (Medium)**。**最低 (Minimum)** 为**复杂性 (Complexity)**、**信任 (Confidence)** 和**风险 (Risk)** 的默认值。

  – “精确”(Exact) - 指定**属性值 (Attribute Values)** 仅使用其自身的结果。例如，当**属性类型 (Attribute Type)** 为**风险 (Risk)**，**匹配方法为精确 (Match Method Exact)** 时，则**属性值高 (Attribute Value High)** 仅用于高风险结果。

您可以为属性类型**复杂性 (Complexity)**、**信任 (Confidence)** 和**风险 (Risk)** 更改**匹配方法 (Match Method)**。

要查看设备支持的属性类型

> 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 属性 (Attributes) > 属性类型属性 (Attribute Type Properties)**。

要更改复杂性、信任和风险属性类型的匹配方法

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > 签名保护 (Signature Protection) > 属性 (Attributes) > 属性类型属性 (Attribute Type Properties)**。
2. 双击属性类型。
3. 从**匹配方法 (Match Method)** 下拉列表中，选择**最低 (Minimum)** 或**精确 (Exact)**。
4. 点击**提交 (Submit)**。

为网络保护配置 BDoS 配置文件

当您配置行为 DoS 配置文件时，需要配置带宽和配额设置。合理且准确地设置带宽和配额值很重要，因为初始基准和攻击检测灵敏度是基于这些值的。

要配置 BDoS 配置文件，必须启用 BDoS 保护（*配置 (Configuration)* 视角，**设置 (Setup) > 安全设置 (Security Settings) > BDoS 保护 (BDoS Protection)**）。

适用于 Cisco Firepower 9300 的 DefensePro 最多支持 50 个配置文件。包括行为 DoS 配置文件的策略的建议设置如下：

- 配置包含行为 DoS 配置文件的规则，这些规则使用源 = 任意的网络、公共网络和目标 = 受保护网络的网络。建议创建多个行为 DoS 规则，每个规则保护特定服务器分段（例如，DNS 服务器分段、Web 服务器分段、邮件服务器分段等）。这可以确保对普通流量基准的获知得到优化。
- 不推荐定义源和目标设置为 *“任意” (Any)* 的网络，因为设备全局收集统计信息，与入站和出站方向无关。这可能导致检测攻击的灵敏度下降。
- 当规则的方向设置为 *“单向” (One Way)* 时，规则仅防范传入攻击。当规则的方向设置为 *“双向” (Two Way)* 时，规则同时防范传入和传出攻击。在这两种情况下，会为传入和传出模式收集流量统计信息以实现最优检测。

您可以配置足迹绕行以绕过指定的足迹类型或值。有关详细信息，请参阅配置 BDoS 足迹绕行，第 104 页。

要配置 BDoS 配置文件

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > BDoS 配置文件 (BDoS Profiles)**。
2. 执行以下操作之一：
   - 要添加配置文件，请点击 （添加）按钮。
   - 要编辑配置文件，请双击表中的条目。
3. 配置参数，然后点击**提交 (Submit)**。

表 97：BDoS 配置文件参数

参数	说明
配置文件名称 (Profile Name)	BDoS 配置文件的名称。
启用透明优化 (Enable Transparent Optimization)	指定是否启用透明优化。 某些网络环境对数据包丢弃更为敏感（例如 VoIP），因此需要将 IPS 设备丢弃合法流量的可能性降至最低。此透明优化可发生在 BDoS 关闭反馈迭代期间，直至生成最终足迹。 **注意：**当启用透明优化时，配置文件在最终足迹生成（需要数秒）之前不会缓解攻击。

表 98：BDoS 配置文件泛洪保护设置参数

参数	说明
SYN 泛洪 (SYN Flood)	选择要应用的网络泛洪保护类型。
TCP ACK + FIN 泛洪 (TCP ACK + FIN Flood)	
TCP RST 泛洪 (TCP RST Flood)	
TCP SYN + ACK 泛洪 (TCP SYN + ACK Flood)	
TCP 分段泛洪 (TCP Fragmentation Flood)	
UDP 泛洪 (UDP Flood)	
ICMP 泛洪 (ICMP Flood)	
IGMP 泛洪 (IGMP Flood)	

表 99：BDoS 配置文件带宽参数

参数	说明
入站流量 (Inbound Traffic)	链路上预期最大入站流量带宽（以千比特/秒为单位）。DefensePro 从带宽和配额设置派生初始基准。 值：1-2、147、483、647 **小心：**您必须配置此设置以启动行为 DoS 保护。
出站流量 (Outbound Traffic)	链路上预期最大出站流量带宽（以千比特/秒为单位）。DefensePro 从带宽和配额设置派生初始基准。 值：1-2、147、483、647 **小心：**您必须配置此设置以启动行为 DoS 保护。

表 100：BDoS 配置文件配额设置参数

参数	说明
Radware 建议您最初将这些字段留空，以便自动使用默认值。要在创建配置文件后查看默认值，请双击表中的条目。然后，您即可根据自己的网络性能调整配额值。 **小心：**当您更改带宽设置时（*入站流量*或*出站流量*），配额设置会自动更改为适合带宽的默认值。 **注意：**总配额值可能会超过 100%，这是因为每个值代表每个协议的最大容量。	
TCP	总流量中 TCP 流量的最大预期百分比。
UDP	总流量中 UDP 流量的最大预期百分比。
ICMP	总流量中 ICMP 流量的最大预期百分比。
IGMP	总流量中 IGMP 流量的最大预期百分比。

表 101：BDoS 配置文件高级参数

参数	说明
UDP 数据包速率灵敏度 (UDP Packet Rate Sensitivity)	“数据包速率检测灵敏度”(UDP Packet Rate Sensitivity) - 即 BDoS 引擎认为 UDP PPS 速率值（基准和当前）所达到的程度。 此参数仅与 BDoS UDP 保护相关。 值： ● 禁用 (Disable) ● 低 (Low) ● 中 (Medium) ● 高 (High) 默认值：“低”(Low) **注意**：在某些传统版本中，此参数标记为**正则化级别 (Level Of Regularization)**。

表 102：BDoS 配置文件数据包报告和跟踪设置参数

参数	说明
数据包报告 (Packet Report)	指定配置文件是否将采样攻击数据包发送到 APSolute Vision 以供离线分析。 **注意**：当启用此功能时，为了使该功能生效，则必须启用全局设置（*配置 (Configuration)* 视角，**设置 (Setup) > 报告设置 (Reporting Settings) > 高级报告设置 (Advanced Reporting Settings) > 数据包报告和数据包跟踪 (Packet Reporting and Packet Trace) > 启用数据包报告 (Enable Packet Reporting)**）。
数据包跟踪 (Packet Trace)	*本版本不支持数据包跟踪功能。*

为网络保护配置 SYN 配置文件

SYN 配置文件可防御 SYN 泛洪攻击。

在 SYN 泛洪攻击期间，攻击者会发送大量 TCP SYN 数据包，请求新的 TCP 连接而不完成 TCP 握手，或完成 TCP 握手但不请求数据。这会令服务器充满连接队列，从而拒绝向合法 TCP 用户提供服务。

在您配置 SYN 配置文件之前，请先确保执行了以下操作：

- 已启用 SYN 泛洪保护，并且已配置全局参数（*配置 (Configuration)* 视角，**设置 (Setup) > 安全设置 (Security Settings) > SYN 泛洪保护 (SYN Flood Protection)**）。
- 您可以更改全局设置。SYN 泛洪全局设置适用于设备上的所有配置文件。有关详细信息，请参阅配置全局 SYN 泛洪保护，第 107 页。

要配置 SYN 保护配置文件

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > SYN 保护配置文件 (SYN Protection Profiles)**。
2. 要添加或修改配置文件，请执行以下操作之一：
   - 要添加配置文件，请点击 +（添加）按钮。输入配置文件名称，并点击**提交 (Submit)**。
   - 要编辑配置文件，请双击表中的条目。
3. 要向配置文件添加 SYN 泛洪保护，请执行以下操作：
   a. 请点击 +（添加）按钮。
   b. 从*配置文件名称 (Profile Name)* 下拉列表中，选择保护。
   c. 点击**提交 (Submit)**。
4. 要为配置文件定义其他 SYN 泛洪保护，请点击**转至保护表 (Go To Protection Table)**。

注意：SYN 配置文件应包含您想要应用于网络保护策略中的所有 SYN 泛洪保护。

表 103：SYN 保护配置文件参数

参数	说明
配置文件名称 (Profile Name)	（只读）配置文件的名称。
SYN 保护表 (SYN Protection Table)	包含对选定配置文件应用的保护。 要添加保护，请在表中点击 +（添加）按钮，选择保护名称，并点击**提交 (Submit)**。 **注意**：在每个网络保护策略中，您仅可以使用一个 SYN 配置文件。因此，请确保您想要应用到规则的所有保护均包含在对该策略指定的配置文件中。
转至保护表 (Go To Protection Table)	打开*SYN 保护 (Syn Protections)* 对话框，您在其中可以添加和修改 SYN 保护。

定义 SYN 泛洪保护

在定义 SYN 泛洪保护后，您可以将其添加到 SYN 配置文件。

要配置 SYN 保护

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > SYN 保护配置文件 (SYN Protection Profiles) > SYN 保护 (SYN Protections)**。
2. 要添加或修改保护，请执行以下操作之一：
   - 要添加保护，请点击 +（添加）按钮。
   - 要编辑保护，请双击表中的条目。
3. 配置参数，然后点击**提交 (Submit)**。

表 104：SYN 泛洪保护参数

参数	说明
保护名称 (Protection Name)	供轻易识别攻击以供配置和报告的名称。 **注意**：预定义的 SYN 保护对大多数常见应用可用：FTP、HTTP、HTTPS、IMAP、POP3、RPS、RTSP、SMTP 和 Telnet。阈值由 Radware 预定义。您可以更改这些攻击的阈值。
保护 ID (Protection ID)	（只读）分配给保护的 ID 编号。
应用端口组 (Application Port Group)	代表您想要保护的应用的 TCP 端口组。从列表选择预定义端口组，或对该字段留空以选择任意端口。
激活阈值 (Activation Threshold)	特定目标每秒接收的 SYN 数据包数量，在此数量之上时 DefensePro 开始执行缓解操作。 值：1-150,000 默认值：2500
终止阈值 (Termination Threshold)	指定*跟踪时间*[1] 内特定目标每秒接收的 SYN 数据包数量，在此数量之下时 DefensePro 停止进行缓解操作。 值：0-150,000 默认值：1500
风险 (Risk)	向此攻击分配的风险级别以供报告用途。 值：“信息”(Info)、“低”(Low)、“中”(Medium)、“高”(High) 默认值：“低”(Low)
源类型 (Source Type)	（只读）指定 SYN 保护是预定义的（静态）保护还是用户定义的（用户）保护。

1 - 您可以在**设置 (Setup) > 安全设置 (Security Settings) > SYN 泛洪保护 (SYN Flood Protection) > 跟踪时间 (Tracking Time)** 中配置该值。

Radware 推荐的验证类型值

表 105：验证类型值参数

协议	目标端口	验证类型
FTP_CNTL	21	确认
HTTP	80	请求
HTTPS	443	请求
IMAP	143	确认
POP3	110	确认
RPC	135	确认
RTSP	554	请求
SMTP	25	确认
TELNET	23	确认

管理 SYN 保护配置文件参数

在定义了 SYN 保护配置文件之后，您可以为该配置文件配置身份验证参数。

默认情况下，适用于 Cisco Firepower 9300 的 DefensePro 版本 1.01 使用 Safe-Reset 身份验证方法。即，当 DefensePro 收到 SYN 数据包时，DefensePro 会以具有无效“序列号”(Sequence Number) 字段作为 cookie 的 ACK 数据包进行响应。如果客户端以 RST 和 cookie 进行响应，DefensePro 就会丢弃 RST 数据包，并将源 IP 地址添加到 TCP 身份验证表。来自相同源的下一个 SYN 数据包（通常是重新传输上一个 SYN 数据包）会通过 DefensePro，然后对服务器批准该会话。DefensePro 会在指定的一段时间内保存源 IP 地址。

借助适用于 Cisco Firepower 9300 的 DefensePro 版本 1.01，您还可以修改 SYN 保护配置文件参数，这些参数将在以下操作步骤中进行说明。

要配置 SYN 保护配置文件参数

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > SYN 保护配置文件 (SYN Protection Profiles) > 配置文件参数 (Profiles Parameters)**。
2. 双击相关配置文件。
3. 配置参数，然后点击**提交 (Submit)**。

表 106：SYN 泛洪保护配置文件参数

参数	说明
配置文件名称 (Profile Name)	（只读）配置文件的名称。
将 TCP 重置用于支持的协议 (Use TCP Reset for Supported Protocols)	指定 DefensePro 是对 HTTP、HTTPS、SMTP 和*自定义协议*流量使用 TCP-Reset 方法，而不使用 Safe-Reset 方法。 Radware 建议在包括 HTTP、HTTPS 和 SMTP 流量的对称和仅限入口的环境中启用此选项。 默认值：“已禁用”(Disabled)

表 106：SYN 泛洪保护配置文件参数（续）

参数	说明
HTTP 身份验证	
使用 HTTP 身份验证 (Use HTTP Authentication)	指定 DefensePro 是否使用 SYN cookie 对 HTTP 流量的传输层进行身份验证，然后使用指定的 *HTTP 身份验证方法 (HTTP Authentication Method)* 对 HTTP 应用层进行身份验证。 值： ● “已启用”(Enabled) - DefensePro 使用 SYN cookie 对 HTTP 流量的传输层进行身份验证，然后使用指定的 *HTTP 身份验证方法*对 HTTP 应用层进行身份验证。 ● “已禁用”(Disabled) - DefensePro 使用指定的 TCP *身份验证方法*处理 HTTP 流量。 默认值：“已禁用”(Disabled)

HTTP 身份验证方法 (HTTP Authentication Method)	配置文件用于对应用层的 HTTP 流量进行身份验证的方法。
	值：
	● “302 重定向”(302-Redirect) - DefensePro 使用“302 重定向”(302-Redirect) 响应代码对 HTTP 流量进行身份验证。
	● JavaScript - DefensePro 使用其生成的 JavaScript 对象对 HTTP 流量进行身份验证。
	默认值：“302 重定向”(302-Redirect)
	注意：
	● 某些攻击工具能够处理 302 重定向响应。*302 重定向* HTTP 身份验证方法针对使用这些工具的攻击没有效果。*JavaScript* HTTP 身份验证方法需要在支持 JavaScript 的客户端侧使用引擎，因此可认为 JavaScript 选项更为强大。但是，*JavaScript* 选项也有某些限制，在某些场景中存在这些限制。
	● 使用 *JavaScript* HTTP 身份验证方法时所存在的限制：
	— 如果浏览器不支持 JavaScript 调用，则浏览器不会应答质询。
	— 当*仅*使用 JavaScript 通过其他（主）页面访问作为子页面的受保护服务器时，用户会话将会失败（即浏览器不会应答该质询。）例如，如果受保护服务器提供使用 JavaScript 标记请求的内容，DefensePro JavaScript 会被封闭在原始的 JavaScript 块内。这会违反 JavaScript 规则，从而导致质询失败。在以下示例中，该请求访问安全的服务器。返回的质询页面再次包含非法的 <script> 标记，因此，浏览器不进行重定向而将该页面丢弃。
	<script> setTimeout(function(){
	var js=document.createElement(“script”);
	js.src=”http://mysite.site.com.domain/service/
	appMy.jsp?dlid=12345”;
	document.getElementsByTagName(“head”)[0].appe n
	dChild(js);
	},1000);
	</script>

TCP 重置

Radware 建议在包括 HTTP、HTTPS 和 SMTP 流量的对称和仅限入口的环境中启用 TCP-Reset 选项。

小心：当 DefensePro 实施 TCP-Reset 机制时，根据相关的 RFC（对于 HTTP、HTTPS 和 SMTP），当原始连接重置时（在这种情况下，由 TCP-Reset 机制重置），必须自动发起新的连接。对于完全遵循 RFC 此方面标准规范的浏览器，连接将自动重新发起，而在*身份验证期间*，用户将经历大约三秒左右的延迟而无额外延迟。（身份验证期由 **TCP 身份验证表老化 (Authentication Table Aging)** 参数确定，默认情况下，该参数值为 20 分钟。）对于未完全遵循 RFC 此方面标准规范的浏览器，合法用户将收到连接重置的通知，并将需要手动重试连接。重试连接后，在身份验证期间，用户将能够浏览而无额外延迟。

当选中**对支持的协议使用 TCP 重置 (Use TCP Reset for Supported Protocols)** 复选框时，DefensePro 会对 HTTP、HTTPS、SMTP 和*自定义协议*的流量使用 TCP-Reset 身份验证方法，而不使用身份验证方法，对于适用于 Cisco Firepower 9300 的 DefensePro 版本 1.01，该方法为 Safe-Reset）。

*自定义协议*指您为要处理的 TCP-Reset 方法定义的流量。为了让您能够执行此操作，DefensePro 展示了两个系统定义的应用端口组：**TCPReset-ACK** 和 **TCPReset-Data**。这些应用端口组为虚拟组，其被定义为具有第 4 层端口 0（零）。（有关定义自定义协议流量的操作步骤，请参阅操作步骤 为 TCP-Reset 方法定义自定义协议流量，第 148 页。）

当 DefensePro 实施 TCP-Reset 方法时，DefensePro 会尝试按照以下顺序将数据包与相关应用端口组进行匹配：

1. HTTP
2. HTTPS
3. SMTP
4. TCPReset-Data
5. TCPReset-ACK

DefensePro 会根据与相关应用端口组之一相匹配的首个数据包处理会话中的数据包。

当启用 TCP-Reset 选项时，DefensePro 会执行以下操作：

1. 当其收到 SYN 数据包时，DefensePro 会使用原始目标 IP 地址和 MAC 在“序列号”(Sequence Number) 字段中以带有 cookie 的 SYN-ACK 数据包进行应答，而无任何其他身份验证参数 (cookie)。
2. 如果响应为带有 cookie 的 ACK：
   - 在具有 **TCPReset-Data** 应用端口组的 HTTP 或 HTTPS 流量或*自定义协议*流量中，DefensePro 会等待来自客户端的首个数据包。（如果 DefensePro 在首个数据包之前收到无数据的 ACK，则 DefensePro 会丢弃该数据包。）当 DefensePro 设备收到数据时，会以 RST 数据包进行应答，并将源 IP 地址保存在 TCP 身份验证表中。
   - 对于具有 **TCPReset-ACK** 应用端口组的 SMTP 或*自定义协议*流量，DefensePro 会以 RST 数据包进行应答，并将源 IP 地址保存在 TCP 身份验证表中。

   注意：HTTP、HTTPS 和 SMTP 源通过重发 SYN 来自动响应 RST 数据包 - 即，源自动重试打开与受保护服务器的连接。合法客户端预期可重试并打开针对受保护服务器的新连接。

3. DefensePro 会对照 TCP 身份验证表中的条目对每个 SYN 数据包进行检查。如果存在匹配，DefensePro 会将数据包转发至其他 DefensePro 检测模块，稍后将 SYN 数据包按原样转发至目标，因而受保护服务器将打开与源的连接。
4. 一旦 DefensePro 对源进行了身份验证，DefensePro 就不会在*身份验证期间*对源再次进行质询。（身份验证期由 **TCP 身份验证表老化 (Authentication Table Aging)** 参数确定，默认情况下，该参数值为 20 分钟）。

注意

- 如果 DefensePro 从同一个源收到多个 SYN，DefensePro 则会对每个 SYN 数据包实施 TCP 重置身份验证过程，直至其中一个连接通过身份验证。
- DefensePro 始终将 TCPReset-Data 行为（上述第 2 步）用于通过端口（包含在 **HTTP** 应用端口组和 **HTTPS** 应用端口组中）的流量。
- DefensePro 始终将 TCPReset-ACK 行为（上述第 2 步）用于通过端口（包含在 **SMTP** 应用端口组中）的流量。
- 当您同时选中**使用 HTTP 身份验证 (Use HTTP Authentication)** 和**将 TCP 重置用于支持的协议 (Use TCP Reset For Supported Protocols)** 复选框时，DefensePro 会使用 HTTP 身份验证方法，而不使用 TCP-Reset 方法。

要为 TCP-Reset 方法定义自定义协议流量

1. 按以下步骤创建新的应用端口组：
   a. 在*配置 (Configuration)* 视角中，依次选择**类 (Classes) > 应用 (Applications)**。
   b. 请点击 （添加）按钮。
   c. 在*端口组名称 (Ports Group Name)* 文本框中，键入 **TCPReset-ACK** 或 **TCPReset-Data** - 根据您所需的 TCP-Reset 行为（请参阅上述第 2 步）。
   d. 在**起始 L4 端口 (From L4 Port)** 文本框中，键入范围中的第一个端口。
   e. 在**结束 L4 端口 (To L4 Port)** 文本框中，键入范围中的最后一个端口。要定义具有单个端口的组，请在**起始 L4 端口 (From L4 Port)** 和**结束 L4 端口 (To L4 Port)** 文本框中键入相同的值。
   f. 要在设备上激活配置更改，请点击**更新策略 (Update Policies)** ( )。
2. 配置 SYN 保护配置文件（请参阅配置 SYN 保护配置文件，第 143 页）。
3. 为上一步中的 SYN 保护配置文件配置 SYN 保护（请参阅配置 SYN 保护，第 144 页），并根据您的需要从*应用端口组 (Application Port Group)* 下拉列表中选择 **TCPReset-ACK** 或 **TCPReset-Data**。

为网络保护配置 DNS 泛洪保护配置文件

要配置 DNS 泛洪保护配置文件，必须启用 DNS 泛洪保护（*配置 (Configuration)* 视角，**设置 (Setup) > 安全设置 (Security Settings) > DNS 泛洪保护 (DNS Flood Protection)**）。

当配置 DNS 泛洪保护配置文件时，您需要配置查询和配额设置。合理且准确地设置查询和配额值很重要，因为初始基准和攻击检测灵敏度是基于这些值的。

您可以微调 DNS 保护配置文件的最大数量（*配置 (Configuration)* 视角，**设置 (Setup) > 高级参数 (Advanced Parameters) > 微调参数 (Tuning Parameters) > 安全 (Security) > DNS 策略最大数量 (Max. Number of DNS Policies)**）。默认值和绝对最大值取决于 DefensePro 的版本。

DNS 保护配置文件仅能用于单向策略。

建议配置的策略包括 DNS 保护配置文件，这些规则使用源 = 任意的网络、公共网络和目标 = 受保护网络的网络。

您可以配置足迹绕行以绕过指定的足迹类型或值。

要配置 DNS 保护配置文件

1. 在*配置 (Configuration)* 视角中，依次选择**网络保护 (Network Protection) > DNS 保护配置文件 (DNS Protection Profiles)**。
2. 执行以下操作之一：
   - 要添加配置文件，请点击（添加）按钮。
   - 要编辑配置文件，请双击表中的条目。
3. 配置参数，然后点击**提交 (Submit)**。

表 107：DNS 保护配置文件：常规参数

参数	说明
名称 (Name)	配置文件的名称。

表 108：DNS 保护配置文件：查询保护和配额参数

参数	说明
Radware 建议您最初将这些字段留空，以便自动使用默认值。要在创建配置文件后查看默认值，请双击表中的条目。然后，您即可根据自己的网络性能调整配额值。 **注意：**总配额值可能会超过 100%，这是因为每个值代表每个协议的最大容量。	
A 查询 (A Query)	对于要保护的各个 DNS 查询类型，请指定配额 - 总 DNS 流量中 DNS 流量的最大预期百分比 - 并选中该行中的复选框。
MX 查询 (MX Query)	
PTR 查询 (PTR Query)	
AAAA 查询 (AAAA Query)	
Text 查询 (Text Query)	
SOA 查询 (SOA Query)	
NAPTR 查询 (NAPTR Query)	
SRV 查询 (SRV Query)	
其他查询 (Other Queries)	
获取默认配额 (Get Default Quotas)	在您指定**预期 DNS 查询速率 (Expected DNS Query Rate)** 后，使用硬编码的默认值配置所有配额。
预期 DNS 查询速率 (Expected DNS Query Rate)	DNS 查询的预期速率，单位为每秒查询数。

表 109：DNS 保护配置文件：手动触发器参数

参数	说明
使用手动触发器 (Use Manual Triggers)	指定配置文件是否使用用户定义的 DNS QPS 阈值，而不使用已获知的基准。 默认值：“已禁用”(Disabled)
激活阈值 (Activation Threshold)	指定的*激活期*后，每个受保护目标网络的每秒查询总数 - 在此数值之上时，DefensePro 认为就会发生攻击。 当检测到攻击时，DefensePro 会开始质询所有源。 在指定的*最大 QPS (Max QPS)*（见下文）之上时，DefensePro 会限制针对受保护网络的总 QPS 速率。 值：0-4,000,000 默认值：0
激活期 (Activation Period)	单个连接上的 DNS 流量超出**激活阈值 (Activation Threshold)** 的连续秒数（致使 DefensePro 认为存在攻击）。 值：1-30 默认值：3
终止阈值 (Termination Threshold)	在指定的**终止期 (Termination Period)** 后单个连接上每秒查询的最大数量（致使 DefensePro 认为攻击已结束）。 值：0-4,000,000 默认值：0 **注意：终止阈值 (Termination Threshold)** 必须小于或等于**激活阈值 (Activation Threshold)**。
终止期 (Termination Period)	单个连接上 DNS 流量持续低于**终止阈值 (Termination Threshold)** 的时间（秒）（致使 DefensePro 认为攻击已结束）。 值：1-30 默认值：3
最大 QPS (Max QPS)	允许的 DNS 查询的每秒最大速率。 值：0-4,000,000 默认值：0
升级期 (Escalation Period)	DefensePro 在升级到下一个指定的缓解操作之前所等待的时间（秒）。 值：0-30 默认值：3

表 110：DNS 保护配置文件：高级报告设置参数

参数	说明
数据包报告 (Packet Report)	指定 DefensePro 是否将采样攻击数据包发送到 APSolute Vision 供离线分析。 默认值：“已禁用”(Disabled) **注意：**当启用此功能时，为了使该功能生效，必须启用全局设置（*配置 (Configuration)* 视角，**设置 (Setup) > 报告设置 (Reporting Settings) > 高级报告设置 (Advanced Reporting Settings) > 数据包报告和数据包跟踪 (Packet Reporting and Packet Trace) > 启用数据包报告 (Enable Packet Reporting)**）。
数据包跟踪 (Packet Trace)	*本版本不支持数据包跟踪功能。*

表 111：DNS 保护配置文件：操作和升级参数

参数	说明
注意：仅当*手动触发器 (Manual Triggers)* 选项 *未*启用时，设备才会在此选项卡中实施这些参数。	
配置文件操作 (Profile Action)	攻击期间配置文件在 DNS 流量上采取的操作。 值：“阻止并报告”(Block & Report)、“仅报告”(Report Only) 默认值：“阻止并报告”(Block & Report)
允许的最大 QPS (Max allowed QPS)	仅当*未*启用*手动触发器 (Manual Triggers)* 选项时允许的每秒 DNS 查询的最大速率。 值：0-4,000,000 默认值：0 **注意：**当启用*手动触发器 (Manual Triggers)* 选项时， 在*手动触发器 (Manual Triggers)* 选项卡中指定的**最大 QPS (Max QPS)** 值才会优先。
签名速率限制目标 (Signature Rate-limit Target)	配置文件将不会在基准之上时进行缓解的匹配实时签名的 DNS 流量百分比。 值：0-100 默认值：0

第 7 章 - 监控和控制 DefensePro 运行状态

APSolute Vision 对 DefensePro 的在线监控可以作为网络运营中心 (NOC) 的一部分，对一些条件下可能会影响网络性能的网络和已连接设备的更改进行监控和分析。

本节包含以下主题：

监控常规 DefensePro 设备信息

概述 (Overview) 选项卡显示常规设备信息，包括设备上的软件版本和设备的硬件版本信息。

要显示选定设备的常规设备信息

\> 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > 概述 (Overview)**。

表 112：概述：基本参数

参数	说明
硬件平台 (Hardware Platform)	此设备硬件平台的类型。
正常运行时间 (Uptime)	系统正常运行的时间（天数、小时数、分钟数和秒数）。
基本 MAC 地址 (Base MAC Address)	设备上第一个端口的 MAC 地址。

表 113：概述：签名更新参数

参数	说明
Radware 签名文件版本 (Radware Signature File Version)	安装在设备上的 Radware 签名文件的版本。

表 114：概述：软件参数

参数	说明
软件版本 (Software Version)	安装在设备上的产品软件的版本。
APSolute 操作系统版本	安装在设备上的 APSolute 操作系统的版本，例如，10.31-03.01:2.06.08。
版本号 (Build)	当前软件版本的版本号。
版本状态 (Version Status)	此软件版本的状态。 值： ● “公开版”(Open) - 尚未发布 ● “最终版”(Final) - 发布的版本

表 115：概述：硬件参数

参数	说明
RAM 大小 (RAM Size)	RAM 容量（以兆字节为单位）。
闪存大小 (Flash Size)	闪存（永久）大小（以兆字节为单位）。

监控 DefensePro 资源利用率

本节包含以下主题：

监控 DefensePro CPU 使用率

您可以查看设备平均资源利用率和各加速器利用率的统计信息。

要监控选定 DefensePro 设备的设备利用率

> 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > 资源利用率 (Resource Utilization) > CPU 使用率 (CPU Utilization)**。

表 116：CPU 使用率：常规参数

参数	说明
资源利用率 (Resource Utilization)	设备 CPU 当前已使用的百分比。
RS 资源利用率 (RS Resource Utilization)	设备路由服务 (RS) 资源当前已使用的百分比。
RE 资源利用率 (RE Resource Utilization)	设备路由引擎 (RE) 资源当前已使用的百分比。
过去 5 秒钟平均利用率 (Last 5 sec. Average Utilization)	过去 5 秒钟内的资源平均利用率。
过去 60 秒钟平均利用率 (Last 60 sec. Average Utilization)	过去 60 秒钟内的资源平均利用率。

表 117：CPU 使用率：引擎利用率参数

参数	说明
引擎 ID (Engine ID)	流量引擎名称。
转发任务 (Forwarding Task)	用于流量处理的 CPU 周期百分比。
其他任务 (Other Tasks)	用于其他任务（例如老化等）的 CPU 资源百分比。
空闲任务 (Idle Task)	空闲的 CPU 资源百分比。

监控和清除 DefensePro 身份验证表

您可以查看设备身份验证表的统计信息。您还可以清除每个表的内容。

“HTTP 身份验证表”(HTTP Authentication Table) 选项卡的内容与适用于 Cisco Firepower 9300 的 DefensePro 无关。

要监控选定 DefensePro 设备的身份验证表

> 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > 资源利用率 (Resource Utilization) > 身份验证表 (Authentication Tables)**。

表 118：TCP 身份验证表监控参数

参数	说明
表大小 (Table Size)	表可容纳的源地址数量。
表利用率 (Table Utilization)	表当前已使用的百分比。
老化时间 (Aging Time)	表的老化时间（秒）。

表 119：DefensePro HTTP 身份验证表监控参数

参数	说明
表大小 (Table Size)	受保护 HTTP 服务器的源-目标对的数量。例如，如果针对两台 HTTP 服务器存在两个攻击，并且源地址相同，那么对于这两个服务器，源在表中将存在两个条目。
表利用率 (Table Utilization)	表当前已使用的百分比。
老化时间 (Aging Time)	表的老化时间（秒）。 值：60-3600 默认值：1200

表 120：DNS 身份验证表监控参数

参数	说明
表大小 (Table Size)	表可容纳的源地址数量。
表利用率 (Table Utilization)	表当前已使用的百分比。
老化时间 (Aging Time)	表的老化时间（分钟）。

要清除选定 DefensePro 设备的身份验证表

1. 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > 资源利用率 (Resource Utilization) > 身份验证表 (Authentication Tables)**。
2. 在相关选项卡中（即，**TCP 身份验证表 (TCP Authentication Table)**、**HTTP 身份验证表 (HTTP Authentication Table)** 或 **DNS 身份验证表 (DNS Authentication Table)**），点击**清除表 (Clean Table)**。

   注意：对于“TCP 身份验证表”(TCP Authentication Table) 和“HTTP 身份验证表”(HTTP Authentication Table)，**清除表 (Clean Table)** 操作可能最多需要 10 秒钟才能完成。

根据配置的策略监控 DME 利用率

此选项卡的内容与适用于 Cisco Firepower 9300 的 DefensePro 无关。

注意：如果设备未配备 DME，则会显示 0（零）值。

监控 DefensePro 系统日志信息

您可以查看有关系统日志机制的信息。

要监控 DefensePro 系统日志信息

> 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > 资源利用率 (Resource Utilization) > 系统日志监控 (Syslog Monitor)**。

表 121：DefensePro 系统日志监控参数

参数	说明
系统日志服务器 (Syslog Server)	系统日志服务器的名称。
状态 (Status)	系统日志服务器的状态。 值： ● “可达”(Reachable) - 服务器可达。 ● “不可达”(Unreachable) - 服务器不可达。 ● N/R - 指定*不相关 (not relevant)*，因为如所指定的协议，流向系统日志服务器的流量通过 UDP -（*配置 (Configuration)* 视角，**设置 (Setup) > 系统日志服务器 (Syslog Server) > 协议 (Protocol) > UDP**）。
积压工作中的消息 (Messages in Backlog)	系统日志服务器积压工作中的消息数量。

监控思科安全组标记 (SGT)

如果存在 SGT，则您可以监控启用的 SGT 的名称和值。

注意：有关适用于 Cisco Firepower 9300 的 DefensePro 中 SGT 的详细信息，请参阅配置 SGT 类，第 122 页。

要监控 SGT

> 在*监控 (Monitoring)* 视角中，依次选择**运行状态 (Operational Status) > SGT**。

表 122：SGT 监控参数

参数	说明
名称 (Name)	SGT 的名称。
值 (Value)	SGT 的值。

第 8 章 - 监控 DefensePro 集群

使用*集群状态 (Clustering Status)* 选项卡来监控适用于 Cisco Firepower 9300 的 DefensePro 中的集群节点。

要监控集群

> 在*监控 (Monitoring)* 视角中，依次选择**集群 (Clustering) > 集群状态 (Cluster Status)**。

表 123：集群监控参数

参数	说明
IP 地址 (IP Address)	集群节点的 IP 地址。
状态 (Status)	集群节点的状态。

第 9 章 - 监控 DefensePro 统计信息

监控 DefensePro 统计信息包括以下主题：

监控 DefensePro SNMP 统计信息

您可以查看设备 SNMP 层的统计信息。

要监控 DefensePro SNMP 统计信息

> 在*监控 (Monitoring)* 视角中，依次选择**统计信息 (Statistics) > SNMP 统计信息 (SNMP Statistics)**。

表 124：DefensePro SNMP 统计信息

参数	说明
SNMP 收到的数据包数量 (Number of SNMP Received Packets)	从传输服务传输至 SNMP 实体的消息总数。
SNMP 发送的数据包数量 (Number of SNMP Sent Packets)	从 SNMP 协议实体发送到传输服务的 SNMP 消息总数。
SNMP 成功的“GET”请求数量 (Number of SNMP Successful 'GET' Requests)	由 SNMP 协议实体成功检索的 MIB 对象总数，作为收到有效 SNMP GET 请求和 GET-Next PDU 的结果。
SNMP 成功的“SET”请求数量 (Number of SNMP Successful 'SET' Requests)	由 SNMP 协议实体成功修改的 MIB 对象总数，作为收到有效 SNMP SET 请求 PDU 的结果。
SNMP“GET”请求数量 (Number of SNMP 'GET' Requests)	由 SNMP 协议实体接受和处理的 SNMP GET 请求 PDU 总数。
SNMP“GET-Next”请求数量 (Number of SNMP 'GET-Next' Requests)	由 SNMP 协议实体接受和处理的 SNMP-Next 请求 PDU 总数。
SNMP“SET”请求数量 (Number of SNMP 'SET' Requests)	由 SNMP 协议实体接受和处理的 SNMP SET 请求 PDU 总数。
收到的 SNMP 错误“过大”的数量 (Number of SNMP Error “Too Big” Received)	由 SNMP 协议实体生成的 SNMP PDU 总数，其错误状态字段的值为“tooBig”。
收到的 SNMP 错误“无此名称”的数量 (Number of SNMP Error “No Such Name” Received)	由 SNMP 协议实体生成的 SNMP PDU 总数，其错误状态的值为“noSuchName”。
收到的 SNMP 错误“错误的值”的数量 (Number of SNMP Error “Bad Value” Received)	由 SNMP 协议实体生成的 SNMP PDU 总数，其错误状态字段的值为“badValue”。
收到的 SNMP 错误“一般错误”的数量 (Number of SNMP Error “Generic Error” Received)	由 SNMP 协议实体生成的 SNMP PDU 总数，其错误状态字段的值为“genErr”。
发送的 SNMP“GET”响应数量 (Number of SNMP 'GET' Responses Sent)	由 SNMP 协议实体生成的 SNMP Get 响应 PDU 总数。
发送的 SNMP 陷阱数量 (Number of SNMP Traps Sent)	由 SNMP 协议实体生成的 SNMP 陷阱 PDU 总数。

监控 DefensePro IP 统计信息

您可以监控设备 IP 层的统计信息，包括丢弃和忽略的数据包数量。这允许您快速地概述给定接口的网络拥塞状态。

要显示选定 DefensePro 设备的 IP 统计信息

> 在*监控 (Monitoring)* 视角中，依次选择**统计信息 (Statistics) > IP 统计信息 (IP Statistics)**。

表 125：DefensePro IP 统计信息参数

参数	说明
收到的 IP 数据包数量 (Number of IP Packets Received)	从接口收到的输入数据报总数，包括错误接收的数据报。
IP 报头错误数量 (Number of IP Header Errors)	由于其 IP 报头错误而被丢弃的输入数据报数量，包括错误校验和、版本号不符、其他格式错误、超过生存时间、处理这些数据报 IP 选项时发现错误等。
丢弃的 IP 数据包数量 (Number of Discarded IP Packets)	被丢弃的用于管理的输入数据报总数。 此计数器不包括任何等待重组时丢弃的数据报。
收到的有效 IP 数据包数量 (Number of Valid IP Packets Received)	成功传输至 IP 用户协议（包括 ICMP）的输入数据报总数。
已传输的数据包总数（包括丢弃的数据包） (Number of Transmitted Packets (Inc. Discards))	本地 IP 用户协议（包括 ICMP）提供给请求传输的 IP 的 IP 数据报总数。 此计数器不包括被计入已转发 IP 数据包数量的任何数据报。
TX 上丢弃的数据包数量 (Number of Discarded Packets on TX)	未遭遇任何阻止其传输至其目标的问题却被丢弃（例如缺少缓冲空间）的输出 IP 数据报数量。 如果已转发 IP 数据包满足此（任意的）丢弃标准，则此计数器会包括被计入已转发 IP 数据包数量的任何数据报。

表 126：DefensePro 路由器统计信息参数

参数	说明
转发的 IP 数据包数量 (Number of IP Packets Forwarded)	此实体不是其最终 IP 目标的输入数据报数量，作为尝试查找路由以将这些数据报转发至该最终目标所导致的结果。在不作为 IP 网关的实体中，此计数器仅包括通过此实体的源路由的此类数据包，以及“源路由”(Source - Route) 选项处理已成功的此类数据包。
由于“未知协议”而被丢弃的 IP 数据包数量 (Number of IP Packets Discarded Due to 'Unknown Protocol')	成功接收，但由于未知或不支持的协议而被丢弃的经本地处理的数据报数量。
由于“无路由”而被丢弃的 IP 数据包数量 (Number of IP Packets Discarded Due to 'No Route')	由于未发现任何路由而将 IP 数据报传输至其目标导致被丢弃的 IP 数据报数量。 **注意：**此计数器包括满足无路由标准而被计入已转发 IP 数据包数量的任何数据包。这包括由于其所有默认网关关闭而致使主机无法将其路由的任何数据报。
收到的 IP 分段数量 (Number of IP Fragments Received)	在此实体需要重组的已接收的 IP 分段数量。
重组成功的 IP 分段数量 (Number of IP Fragments Successfully Reassembled)	重组成功的 IP 数据报数量。
重组失败的 IP 分段数量 (Number of IP Fragments Failed Reassembly)	由 IP 重组算法检测到的失败数量，例如超时、错误等。注意：由于某些算法（尤其是 RFC 815 中的算法）按分段收到时的状态对其进行组合，因而可能失去对分段数量的跟踪，导致这不一定是被丢弃的 IP 分段的计数。
重组成功的 IP 数据报数量 (Number of IP Datagrams Successfully Reassembled)	在此实体已重组成功的 IP 数据报数量。
由于分段失败而被丢弃的 IP 数据报数量 (Number of IP Datagrams Discarded Due to Fragmentation Failure)	由于需要在此实体对 IP 数据报进行分段但却无法对其进行分段而被丢弃的 IP 数据报数量，原因诸如设置了 IP 数据报的“不分段”(Don't Fragment) 标志。
生成的 IP 数据报分段数量 (Number of IP Datagrams Fragments Generated)	由于在此实体进行的分段而生成 IP 数据报分段数量。
丢弃的有效路由条目 (Valid Routing Entries Discarded)	丢弃的有效路由条目数量。

第 10 章 - 监控和控制 DefensePro 网络

监控和控制 DefensePro 网络包括以下主题：

注意： *挂起表 (Suspend Table)* 节点的内容在适用于 Cisco Firepower 9300 的 DefensePro 中不起作用。

监控路由表信息

路由表存储了目标及如何到达这些目标的信息。

默认情况下，直接连接 DefensePro 设备的所有网络都会注册在此表中。其他条目则可以通过路由协议静态配置或动态创建。

注意： 路由表不会定期自动刷新。当您选择显示“路由表”(Routing Table) 窗格，以及当您手动刷新显示时会加载信息。

要显示选定设备的路由表信息

> 在*监控 (Monitoring)* 视角中，依次选择**网络 (Networking) > 路由 (Routing)**。

表 127：路由表监控参数

参数	说明
目标网络 (Destination Network)	向其定义路由的目标网络。
网络掩码 (Netmask)	目标子网的网络掩码。
下一跳 (Next Hop)	朝向目标子网下一跳的 IP 地址。（下一跳总是处于设备本地的子网上。）
通过接口 (Via Interface)	在适用于 Cisco Firepower 9300 的 DefensePro 中，该值为 **3**（只读），其为管理接口的值。
类型 (Type)	此字段仅显示在静态路由表中。路由的类型。 值： ● “本地”(Local) - 可以从设备直接到达子网。 ● “远程”(Remote) - 无法从设备直接到达子网。
指标 (Metric)	为此路由定义或计算的指标值。

监控 DefensePro ARP 表信息

您可以查看设备的 ARP 表，其中同时包含静态和动态条目。您可以将条目的类型由动态更改为静态。

注意：ARP 表不会定期自动刷新。当您选择显示“ARP 表”(ARP Table) 窗格时，以及当您手动刷新显示时会加载信息。

要显示选定 DefensePro 设备的 ARP 表信息

> 在*监控 (Monitoring)* 视角中，依次选择**网络 (Networking) > ARP**。

表 128：DefensePro ARP 表监控参数

参数	标题
端口 (Port)	站所在的接口号。
IP 地址 (IP Address)	站的 IP 地址。
MAC 地址 (MAC Address)	站的 MAC 地址。
类型 (Type)	条目类型。 值： ● “其他”(Other) - 不是动态或静态。 ● “动态”(Dynamic) - 条目从 ARP 协议获知。如果条目在预先确定的时间内不活动，则将节点从表中删除。 ● “静态”(Static) - 条目已由网络管理站配置且保持不变。

要将条目类型由动态更改为静态

1. 在*监控 (Monitoring)* 视角中，依次选择**网络 (Networking) > ARP**。
2. 选择条目，并选择**更改条目为静态 (Change Entry to Static)**。

仅在 DefensePro 6.x 版和 7.40 版之前的 7.x 版中支持此功能。

您可以监控 MPLS RD 信息并配置 MPLS RD。对在其之上安装设备的链路，每个 MPLS RD 均分配有两个标签，上游标签和下游标签。在不同的链路上，相同的 MPLS RD 可以分配有不同的标签。

要显示选定 DefensePro 设备的 MPLS RD 信息

1. 在*监控 (Monitoring)* 视角中，依次选择**网络 (Networking) > MPLS RD**。*MPLS RD* 表会显示当前的 MPLS RD 信息。
2. 要添加 MPLS RD，请点击 （添加）按钮。
3. 配置参数，然后点击**提交 (Submit)**。

表 129：MPLS RD 参数

参数	说明
MPLS RD	MPLS RD 名称。
类型 (Type)	描述 MPLS RD 格式。 值： ● “2 字节 : 4 字节”(2 Bytes : 4 Bytes) - AS（16 位）：数字（32 位） ● “4 字节 : 2 字节”(4 Bytes : 2 Bytes) - AS（32 位）：数字（16 位） ● “IP 地址 : 2 字节”(IP Address : 2 Bytes) - IP：数字（16 位）
上游标签 (Upper Tag)	在其上安装设备的链路的上游标签。
下游标签 (Lower Tag)	在其上安装设备的链路的下游标签。

第 11 章 - 使用实时安全监控

当检测到攻击时，DefensePro 设备会创建并报告*安全事件*，其中包括与特定攻击相关的信息。*安全监控 (Security Monitoring)* 视角显示与特定攻击相关的信息，以及实时网络流量和统计参数。使用*安全监控 (Security Monitoring)* 视角可以观察和分析设备检测到的攻击和设备实施的对策。

注意

- 您的用户权限（您的 *RBAC 用户定义*）确定*安全监控 (Security Monitoring)* 视角显示给您的 DefensePro 设备和策略。您可以仅查看和监控对您可用的 DefensePro 设备和策略所阻止的攻击。
- APSolute Vision 还可以对新的安全攻击进行管理并发布警报。
- DefensePro 会计算流量基准，并使用该基准识别流量级别中的异常情况。
- 当计算实时网络流量和统计参数时，DefensePro 不会包括超过吞吐量许可的流量。

以下主题介绍 APSolute Vision 中的安全监控：

风险级别

下表介绍 DefensePro 支持的风险级别，以对安全事件进行分级。

注意：对于某些保护，用户可以指定某个事件的风险级别。对于这些保护，下表中的说明仅是建议，而设置风险级别则由用户负责。

表 130：风险级别

风险级别	说明
信息 (Info)	该风险对正常服务运营不构成威胁。
低 (Low)	该风险对正常服务运营不构成威胁，但可能是恶意行为预备操作的一部分。
中 (Medium)	该风险对正常服务运营可能构成威胁，但不太可能造成完全的服务中断、远程代码执行或未经授权的访问。
高 (High)	该风险对正常服务可用性很有可能构成威胁，并且可能会造成完全的服务中断、远程代码执行或未经授权的访问。

使用控制面板

本节包括以下主题：

使用安全控制面板分析网络中的活动和安全事件，识别安全趋势，并分析风险。

您可以查看站点中单个设备、所有设备或网络中所有设备的安全控制面板信息。控制面板监控显示会自动刷新，提供对系统不间断的实时分析。

*安全控制面板*包括*图表视图*和*表视图*（请参阅图 27 - 安全控制面板（图表视图），第 173 页和图 28 - 安全控制面板（表视图 - 当前攻击表），第 174 页）。默认情况下，每 15 秒钟刷新一次显示。管理员可以配置刷新率（*APSolute Vision 设置 (APSolute Vision Settings)* 视图，*系统 (System)* 视角，**常规设置 (General Settings) > 监控 (Monitoring) > 报告轮询间隔 (Polling Interval for Reports)**）。

显示在安全监控图表视图中的摘要信息也可以呈现在安全监控表视图中（*当前攻击 (Current Attacks)* 表）。

要显示安全控制面板

> 在*安全监控 (Security Monitoring)* 视角中，依次选择**控制面板视图 (Dashboard View) > 安全控制面板 (Security Dashboard)**。

要在安全控制面板的图表视图和表视图之间切换

> 请点击相关按钮 （显示图表）或 （显示表），然后配置显示参数。

表 131：安全控制面板显示参数

参数	说明
范围 (Scope)	控制面板显示的物理端口和网络保护策略。 默认情况下，“范围”(Scope) 为**任何端口；任何策略 (Any Port; Any Policy)**。即，默认情况下，控制面板显示所有信息。 要控制安全控制面板在 DefensePro 中显示的信息的范围，请参阅操作步骤控制安全控制面板显示的信息的范围，第 173 页。

表 131：安全控制面板显示参数（续）

参数	说明
显示持续时间 (Display Last)	攻击终止后监视器显示攻击的持续时间。即，监视器显示当前正在发生的所有攻击或在选定时段内终止的所有攻击。 值： ● 10 分钟 (10 Minutes) ● 20 分钟 (10 Minutes) ● 30 分钟 (10 Minutes) ● 1 小时 (1 Hour) ● 2 小时 (2 Hours) ● 6 小时 (2 Hours) ● 12 小时 (2 Hours) ● 24 小时 (24 Hours) 默认值：“10 分钟”(10 Minutes)
要显示的最多攻击数 （此参数仅在图表视图中可用。）	“正在发生的攻击监视器”(Ongoing Attacks Monitor) 显示的攻击数量。 值：1-50 默认值：20 **注意：**此参数仅与“正在发生的攻击监视器”(Ongoing Attacks Monitor) 相关。
排序依据 (Sort By) （此参数仅在图表视图中可用。）	值： ●“最多数据包计数”(Top Packet Count) -“正在发生的攻击监视器”(Ongoing Attacks Monitor) 显示数据包数量最多的攻击。 ●“最多数据包计数”(Top Packet Count) -“正在发生的攻击监视器”(Ongoing Attacks Monitor) 显示具有最大带宽的攻击。 ●“最近”(Most Recent) -“正在发生的攻击监视器”(Ongoing Attacks Monitor) 显示最近的攻击。 ●“攻击状态”(Attack Status) -“正在发生的攻击监视器”(Ongoing Attacks Monitor) 根据攻击状态显示攻击。 ●“攻击风险”(Attack Risk) -“正在发生的攻击监视器”(Ongoing Attacks Monitor) 根据攻击风险显示攻击。 默认值：“最多数据包计数”(Top Packet Count) **注意：**此参数仅与“正在发生的攻击监视器”(Ongoing Attacks Monitor) 相关。

要控制安全控制面板显示的信息范围

1. 请点击 ▶ Scope。随后，两张表会打开。一张表具有*设备名称 (Device Name)* 和*端口 (Port)* 列，而另一张表具有*设备名称 (Device Name)* 和*策略 (Policy)* 列。

   注意：适用于 Cisco Firepower 9300 的 DefensePro 不支持限制“范围”(Scope) 的物理端口。

2. 执行以下操作之一：
   - 要限制安全控制面板显示的网络保护策略，请选中对应的复选框。
   - 要显示所有当前相关的网络保护策略的信息，请点击左上部的表单元格，然后选择**全选 (Select All)**。
   - 要显示数据库中的所有信息，甚至显示与特定端口或特定网络保护策略无关的信息，请点击左上部的表单元格，然后选择**全部不选 (Select None)**。

使用安全控制面板图表视图

安全控制面板图表视图包括*正在发生的攻击监视器 (Ongoing Attacks Monitor)* 和*丢弃强度 (Drop Intensity)* 计量表。

正在发生的攻击监视器 (Ongoing Attacks Monitor) 用图形方式表示当前和最近的攻击。监视器中的每个图标代表一个单独的攻击。图标类型（见图例）代表攻击所触犯的保护类型。闪烁的图标代表正在发生的攻击。图表中每个图标的水平位置表示攻击风险（请参见风险级别，第 171 页）。图表中图标的垂直位置表示攻击持续时间，在图表中位置越高，攻击存在的时间越长。最近才开始的攻击在监视器中较低位置。图标大小表示相对于相同类型的其他攻击，该攻击类型的数据丢弃量。将鼠标悬停在图标上可显示攻击的摘要信息。双击图标可显示攻击详细信息。有关详细信息，请参阅攻击详细信息，第 179 页。

丢弃强度 (Drop Intensity) 计量表提供两种计量表：“数据包”(Packets) 和“带宽”(Bandwidth)。“数据包”(Packets) 计量表表示相对于数据包总数而丢弃的数据包比率。“带宽”(Bandwidth) 计量表表示相对于（根据许可）带宽总量而丢弃的带宽比率。计量表显示经计算的范围：低（最多 30% 被丢失）、中（最多 70% 被丢失）和高（70% 以上被丢失）。

图 27：安全控制面板（图表视图）

使用安全控制面板表视图 - 当前攻击表

表视图*当前攻击 (Current Attacks)* 表显示当前和最近攻击的信息。您还可以执行以下操作：

- **使用搜索或过滤功能** - 如果列支持搜索功能，您就可以将行的顺序从升序更改为降序，反之亦然。要执行此操作，请将鼠标悬停在列上，可显示箭头并更改顺序。
- **查看特定攻击的其他信息** - 要执行此操作，请选择相关行，并点击 （查看攻击详细信息）。有关详细信息，请参阅攻击详细信息，第 179 页。
- **转至处理攻击的策略** - 要执行此操作，请点击 （转至策略）。
- **导出表中的信息至 CSV 文件** - 要执行此操作，请点击 (CSV)。然后，您可以查看文件或指定位置和文件名。

  注意：不支持导出数据包异常。
- **暂停刷新表显示** - 要执行此操作，请点击 （暂停）。当表显示*未*暂停时，会大约每 15 秒钟左右刷新一次。

图 28：安全控制面板（表视图 - 当前攻击表）

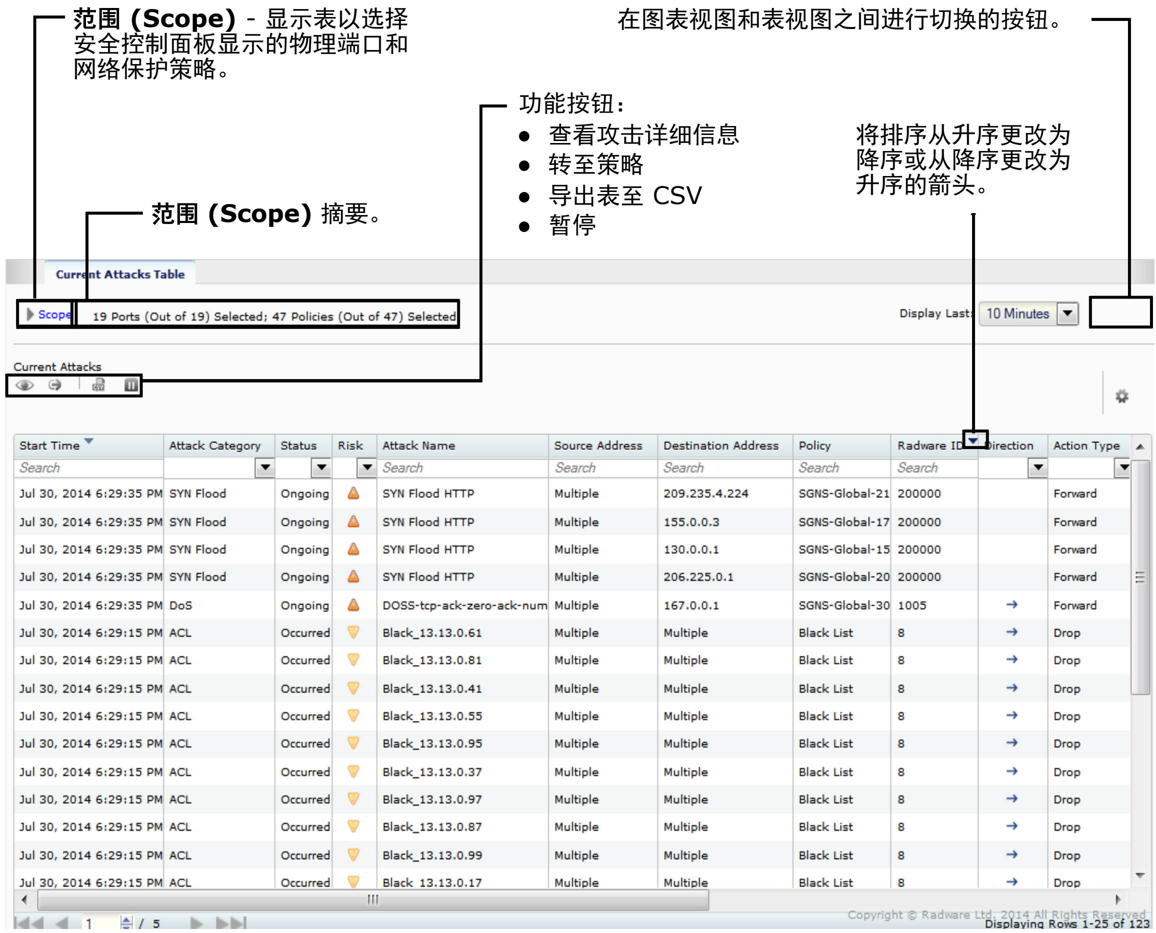


表 132：当前攻击表参数

参数	说明
开始时间 (Start Time)	攻击开始的日期和时间。
攻击类别 (Attack Category)	此攻击所属的威胁类型。 值： ● ACL ● 异常 (Anomalies) ● 反扫描 (Anti-Scanning) ● 带宽管理 (Bandwidth Management) ● 行为 DoS (Behavioral DoS) ● DNS 泛洪 (DNS Flood) ● DoS ● HTTP 泛洪 (HTTP Flood) ● 入侵 (Intrusions) ● 服务器破解 (Server Cracking) ● 状态 ACL (Stateful ACL) ● SYN 泛洪 (SYN Flood)

表 132：当前攻击表参数（续）

参数	说明
状态 (Status)	最后一次报告的攻击状态。 值： • “已开始”(Started) - 已检测到包含多个安全事件的攻击（某些攻击包含多个安全事件，例如 DoS、Scans 等）。 • “已发生”(Occurred)（基于签名的攻击）- 与签名匹配的每个数据包被报告为攻击并被丢弃。 • “正在发生”(Ongoing) - 攻击当前正在发生，开始和终止之间的时长（对于包含多个安全事件的攻击，例如 DoS、“扫描”(Scans) 等）。 • “已终止”(Terminated) - 无更多数据包与攻击的特征相匹配，设备报告攻击已结束。
风险 (Risk)	预定义的攻击严重性级别（请参阅风险级别，第 169 页）。 值： • - 高 (High) • - 中 (Medium) • - 低 (Low) • - 信息 (Info)
攻击名称 (Attack Name)	检测到的攻击的名称。
源地址 (Source Address)	攻击的源 IP 地址。如果攻击存在多个 IP 源，则此字段会显示**多个 (Multiple)**。多个 IP 地址会显示在*攻击详细信息 (Attack Details)* 窗口中。**多个 (Multiple)** 也可能指 DefensePro 无法报告特定值的情况。 **搜索 (Search)** 字符串可以是任何合法的 IPv4 或 IPv6 地址，并可以包括通配符 (*)。
目标地址 (Destination Address)	攻击的目标 IP 地址。如果攻击存在多个 IP 源，则此字段会显示**多个 (Multiple)**。多个 IP 地址会显示在*攻击详细信息 (Attack Details)* 窗口中。**多个 (Multiple)** 也可能指 DefensePro 无法报告特定值的情况。
策略 (Policy)	由此攻击触犯的已配置的网络保护策略或服务器保护策略的名称。 要查看或编辑特定攻击的策略，请选择攻击条目并点击 （转至策略）按钮。
Radware ID	由设备发布的唯一攻击标识符。
方向 (Direction)	攻击的方向，入站或出站。 值：“入”(in)、“出”(out)

表 132：当前攻击表参数（续）

参数	说明
操作类型 (Action Type)	报告的针对攻击的操作。操作在保护配置文件中指定，保护配置文件可能对系统可用/不可用，也可能与系统相关/不相关。 值： ● 绕行 (Bypass) ● 质询 (Challenge) ● “目标重置”(Destination Reset) - DefensePro 向目标地址发送 TCP-Reset 数据包。 ● “丢弃”(Drop) - DefensePro 丢弃数据包。 ● 丢弃并隔离 (Drop & Quarantine) ● “转发”(Forward) - DefensePro 将数据包转发至其目标。 ● 代理 (Proxy) ● 隔离 (Quarantine) ● “源目标重置”(Source Destination Reset) - DefensePro 同时向数据包源 IP 地址和数据包目标 IP 地址发送 TCP-Reset 数据包。 ● “源重置”(Source Reset) - DefensePro 向数据包源 IP 地址发送 TCP-Reset 数据包。 ● Http 200 Ok - DefensePro 使用预定义页面发送 200 OK 响应，并使服务器端连接保持打开状态。 ● “Http 200 Ok 重置目标”(Http 200 Ok Reset Dest) - DefensePro 使用预定义页面发送 200 OK 响应，并向服务器端发送 TCP-Reset 数据包以关闭连接。 ● “Http 403 已禁止”(Http 403 Forbidden) - DefensePro 使用预定义页面发送“403 已禁止”(403 Forbidden) 响应，并使服务器端连接保持打开状态。 ● “Http 403 已禁止重置目标”(Http 403 Forbidden Reset Dest) - DefensePro 使用预定义页面发送“403 已禁止”(403 Forbidden) 响应，并向服务器端发送 TCP-Reset 数据包以关闭连接。
总数据包计数 (Total Packet Count)	从攻击开始时已识别的攻击数据包数量。
容量 (Volume)	对于大部分保护，该值为从攻击开始时的攻击容量（以千比特为单位）。 对于 SYN 保护 (SYN cookie)，该值为丢弃的 SYN 数据包数量乘以 60 字节（SYN 数据包大小）。
设备 IP (Device IP)	受攻击的设备的 IP 地址。
应用协议 (Application Protocol)	用于发送攻击的传输协议：值： ● TCP ● UDP ● ICMP ● IP
MPLS RD	策略中处理攻击的多协议标签交换路由标识。此字段中的**无 (N/A)** 或 **0**（零）表示 MPLS RD 不可用。
VLAN 标记/情景 (VLAN Tag/Context)	策略中处理攻击的 VLAN 标记值或情景组。此字段中的**无 (N/A)** 或 **0**（零）表示 VLAN 标记或情景组不可用。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
源端口 (Source Port)[1]	攻击的第 4 层源端口。

表 132：当前攻击表参数（续）

参数	说明
目标端口 (Destination Port)	攻击的第 4 层目标端口。如果存在多个目标 L4 端口，则此字段会显示**多个 (Multiple)**。在 DefensePro 无法报告特定值的情况下，该字段会显示 **0**（零）。
物理端口 (Physical Port)	攻击数据包所到达的设备上的端口。在 DefensePro 无法报告特定值的情况下，该字段会显示 **0**（零）。
源 MSISDN (Source MSISDN)	*APSolute Vision 版本 3.0 及更高版本中* *不支持 MSISDN 解析功能。*
目标 MSISDN (Destination MSISDN)	*APSolute Vision 版本 3.0 及更高版本中* *不支持 MSISDN 解析功能。*

1 - 默认情况下，*当前攻击 (Current Attacks)* 选项卡中不显示此列。要显示该列，请点击 （表设置）按钮，然后选中相关复选框。再次点击该按钮关闭*表设置 (Table Settings)* 列表。

攻击详细信息

当您双击安全控制面板图表视图或表视图中的攻击时会显示*攻击详细信息 (Attack Details)* 选项卡。

APSolute Vision 会显示以下攻击的攻击详细信息：

- BDoS 攻击详细信息，第 178 页
- DNS 泛洪攻击详细信息，第 180 页
- DoS 攻击详细信息，第 182 页
- 数据包异常攻击详细信息，第 183 页
- SYN 泛洪攻击详细信息，第 183 页

注意：显示在这些窗口中的*攻击特征 (Attack Characteristics)* 信息在*当前攻击摘要 (Current Attack Summary)* 表的隐藏列中同样可用。

攻击描述显示来自攻击描述文件的信息。仅当已将攻击描述文件上传到 APSolute Vision 服务器时才会显示攻击描述。

除了攻击详细信息，在每个*攻击详细信息 (Attack Details)* 选项卡中，您可以执行以下操作：

- **查看来自攻击的采样数据** - 要执行此操作，请点击 （查看采样数据）。有关详细信息，请参阅采样数据选项卡，第 185 页。
- **转至处理攻击的策略** - 要执行此操作，请点击 （转至策略）。
- **将攻击详细信息选项卡中的信息导出至 CSV 文件** - 要执行此操作，请点击 (CSV)。然后，您可以查看文件或指定位置和文件名。
- **将攻击详细信息选项卡中的信息导出至 CAP 文件** - 要执行此操作，请点击 （导出攻击捕获文件），并在文件选择对话框中输入文件名。

注意

- 您可以将 CAP 文件发送到数据包分析器。
- CAP 文件中最多保存 255 字节的数据包信息。即，DefensePro 会导出全部数据包，但 APSolute Vision 会将这些数据包裁剪为 255 字节。
- 只要*当前攻击 (Current Attacks)* 表中显示该文件，那么该文件就可用。
- 仅当被违反的配置文件的保护配置中启用了数据包报告时，才会创建该文件。
- DefensePro 仅按匹配过滤器的序列导出最后一个数据包。此外，如果流量与包括多个数据包的签名相匹配，则报告的数据包将不会在过滤器中包括完整表达式。

BDoS 攻击详细信息

表 133：BDoS 攻击详细信息：特征参数

参数	说明
注意：某些字段在相关和可用时可以显示多个值。显示的值取决于攻击的当前阶段。如果字段为动态签名的一部分（即所有攻击流量中会显示特定值），则**特征 (Characteristics)** 字段会显示一个或多个相关值。	
协议 (Protocol)	攻击使用或已使用的协议。
源 L4 端口 (Source L4 Port)	攻击使用或已使用的源 L4 端口。
物理端口 (Physical Port)	攻击使用或已使用的物理端口。
数据包计数 (Packet Count)	攻击的数据包计数。
容量（千比特）(Volume (Kbits))	攻击使用或已使用的容量（以千比特为单位）。
VLAN/情景 (VLAN/Context)	策略中处理攻击的 VLAN 标记值或情景组。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。 适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
MPLS RD	攻击使用或已使用的 MPLS RD。
设备 IP (Device IP)	攻击使用或已使用的设备 IP 地址。
TTL	攻击使用或已使用的 TTL。
L4 校验和 (L4 Checksum)	攻击使用或已使用的 L4 校验和。
TCP 序列号 (TCP Sequence Number)	攻击使用或已使用的 TCP 序列号。
IP ID 编号 (IP ID Number)	攻击使用或已使用的 IP ID 编号。
分段偏移量 (Fragmentation Offset)	攻击使用或已使用的分段偏移量。
分段标志 (Fragmentation Flag)	攻击使用或已使用的分段标志。**0** 表示允许该分段。**1** 表示不允许该分段。
流标签 (Flow Label)	（仅限 IPv6）攻击使用或已使用的流量标签。
TOS	攻击使用或已使用的 ToS。
数据包大小 (Packet Size)	攻击使用或已使用的数据包大小。
ICMP 消息类型 (ICMP Message Type) （仅当协议为 ICMP 时显示。）	攻击使用或已使用的 ICMP 消息类型。
源 IP (Source IP)	攻击使用或已使用的源 IP 地址。
目标 IP (Destination IP)	攻击使用或已使用的目标 IP 地址。
源端口 (Source Ports)	攻击使用或已使用的源端口。

表 133：BDoS 攻击详细信息：特征参数（续）

参数	说明
源端口 (Source Ports)	攻击使用或已使用的源端口。
目标端口 (Destination Ports)	攻击使用或已使用的目标端口。
DNS ID	攻击使用或已使用的 DNS ID。
DNS 查询 (DNS Query)	攻击使用或已使用的 DNS 查询。
DNS 查询计数 (DNS Query Count)	攻击使用或已使用的 DNS 查询计数。

表 134：BDoS 攻击详细信息：信息参数

参数	说明
数据包大小异常区域 (Packet Size Anomaly Region)	攻击数据报的统计区域。 策略的数据包大小基准公式如下： {(AnomalyBandwidth/AnomalyPPS)/(NormalBandwidth/ NormalPPS)} 值： ● “大数据包”(Large Packets) - 攻击数据包比策略的正常数据包大小基准大约大 15%。 ● “普通数据包”(Normal Packets) - 攻击数据包在策略的正常数据包基准每一侧中大约占 15% 以内。 ● “小数据包”(Small Packets) - 攻击数据包比策略的正常数据包大小基准大约小 15%。
状态 (State)	保护过程的状态。 值： ● “足迹分析”(Footprints Analysis) - 行为 DoS 保护已检测到攻击，且当前正在确定攻击足迹。 ● “阻止”(Blocking) - 行为 DoS 保护根据创建的攻击足迹正在阻止攻击。通过封闭式反馈循环操作，行为 DoS 保护对足迹规则进行优化，实现有效范围最小的缓解规则。 ● “非攻击”(Non-attack) - 由于流量不是攻击而不作阻止任何内容 - 未检测到足迹或未达到阻止严格性级别。

表 135：BDoS 攻击详细信息：足迹参数

参数	说明
行为 DoS 保护生成的足迹阻止规则针对泛洪攻击提供有效范围最小的阻止规则。	

表 136：BDoS 攻击详细信息：攻击统计信息表

参数	说明
此表显示攻击流量（异常）和正常流量信息。红色表示攻击触发前 15 秒钟内识别为可疑的实时值。黑色表示获知的正常流量基准。表列的显示基于协议：TCP（包括所有标志）、UDP 或 ICMP。	

表 137：BDoS 攻击详细信息：攻击统计信息图表

参数	说明
该图表显示触发攻击的 15 秒钟内的相关流量类型的快照。例如，UDP 泛洪期间仅显示 UDP 流量。蓝线表示正常的适应流量基准。	

表 138：BDoS 攻击详细信息：攻击描述

参数	说明
如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

DNS 泛洪攻击详细信息

表 139：DNS 泛洪攻击详细信息：特征参数

参数	说明
注意：某些字段在相关和可用时可以显示多个值。显示的值取决于攻击的当前阶段。如果字段为动态签名的一部分（即所有攻击流量中会显示特定值），则**特征 (Characteristics)** 字段会显示一个或多个相关值。	
协议 (Protocol)	攻击使用或已使用的协议。
源 L4 端口 (Source L4 Port)	攻击使用或已使用的源 L4 端口。
物理端口 (Physical Port)	攻击使用或已使用的物理端口。
数据包计数 (Packet Count)	攻击的数据包计数。
容量（千比特）(Volume (Kbits))	攻击使用或已使用的容量（以千比特为单位）。
VLAN/情景 (VLAN/Context)	策略中处理攻击的 VLAN 标记值或情景组。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。 适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
MPLS RD	攻击使用或已使用的 MPLS RD。
设备 IP (Device IP)	攻击使用或已使用的设备 IP 地址。
TTL	攻击使用或已使用的 TTL。
L4 校验和 (L4 Checksum)	攻击使用或已使用的 L4 校验和。
IP ID 编号 (IP ID Number)	攻击使用或已使用的 IP ID 编号。
数据包大小 (Packet Size)	攻击使用或已使用的数据包大小。
目标 IP (Destination IP)	攻击使用或已使用的目标 IP 地址。
目标端口 (Destination Ports)	攻击使用或已使用的目标端口。
DNS ID	攻击使用或已使用的 DNS ID。
DNS 查询 (DNS Query)	攻击使用或已使用的 DNS 查询。
DNS 查询计数 (DNS Query Count)	攻击使用或已使用的 DNS 查询计数。
DNS An 查询计数 (DNS An Query Count)	攻击使用或已使用的 DNS An 查询计数。

表 140：DNS 泛洪攻击详细信息：信息参数

参数	说明
状态 (State)	保护过程的状态。
缓解操作 (Mitigation Action)	缓解操作。 值： ● 签名质询 (Signature Challenge) ● 签名速率限制 (Signature Rate Limit) ● 综合质询 (Collective Challenge) ● 综合速率限制 (Collective Rate Limit)

表 141：DNS 泛洪攻击：足迹

参数	说明
行为 DoS 保护生成的足迹阻止规则。足迹阻止规则针对泛洪攻击提供有效范围最小的阻止规则。	

表 142：DNS 泛洪攻击详细信息：攻击统计信息表

参数	说明
此表显示攻击流量（异常）和正常流量信息。红色表示攻击触发前 15 秒钟内识别为可疑的实时值。黑色表示获知的正常流量基准。表列的显示基于 DNS 查询类型：A、MX、PTR、AAAA、Text、SOA、NAPTR、SRV、其他。	

表 143：DNS 泛洪攻击详细信息：攻击统计信息图表

参数	说明
该图表显示触发攻击的 15 秒钟内的相关流量类型的快照。例如，UDP 泛洪期间仅显示 UDP 流量。蓝线表示正常的适应流量基准。	

表 144：DNS 泛洪攻击详细信息：攻击描述

参数	说明
如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

DoS 攻击详细信息

表 145：DoS 攻击详细信息：特征参数

参数	说明
协议 (Protocol)	攻击使用或已使用的协议。
物理端口 (Physical Port)	攻击使用或已使用的物理端口。
数据包计数 (Packet Count)	攻击的数据包计数。
源 MSISDN (Source MSISDN)	*APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
目标 MSISDN (Destination MSISDN)	*APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
VLAN/情景 (VLAN/Context)	策略中处理攻击的 VLAN 标记值或情景组。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。 适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
MPLS RD	攻击使用或已使用的 MPLS RD。
设备 IP (Device IP)	攻击使用或已使用的设备 IP 地址。

表 146：DoS 攻击详细信息：信息参数

参数	说明
操作 (Action)	采取的保护操作。
攻击者 IP (Attacker IP)	攻击者的 IP 地址。
受保护主机 (Protected Host)	受保护的主机。
受保护端口 (Protected Port)	受保护的端口。
攻击持续时间 (Attack Duration)	攻击的持续时间。
当前数据包速率 (Current Packet Rate)	当前数据包速率。
平均数据包速率 (Average Packet Rate)	平均数据包速率。

表 147：DoS 攻击详细信息：攻击描述

参数	说明
如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

数据包异常攻击详细信息

表 148：数据包异常攻击详细信息：特征参数

参数	说明
协议 (Protocol)	攻击使用或已使用的协议。
物理端口 (Physical Port)[1]	攻击使用或已使用的物理端口。
数据包计数 (Packet Count)	攻击的数据包计数。
VLAN/情景 (VLAN/Context)	策略中处理攻击的 VLAN 标记值或情景组。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
MPLS RD	攻击使用或已使用的 MPLS RD。
设备 IP (Device IP)	攻击使用或已使用的设备 IP 地址。
攻击描述 (Attack Description) 如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

1 - 未解析此参数，并且总是显示值**多个 (Multiple)**。

表 149：数据包异常攻击详细信息：攻击描述

参数	说明
如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

SYN 泛洪攻击详细信息

表 150：SYN 泛洪攻击详细信息：特征参数

参数	说明
协议 (Protocol)	攻击使用或已使用的协议。
物理端口 (Physical Port)	攻击使用或已使用的物理端口。
数据包计数 (Packet Count)	攻击的数据包计数。
源 MSISDN (Source MSISDN)	*APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
目标 MSISDN (Destination MSISDN)	*APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
容量（千比特）(Volume (Kbits))	攻击使用或已使用的容量（以千比特为单位）。
VLAN/情景 (VLAN/Context)	策略中处理攻击的 VLAN 标记值或情景组。 **注意：**VLAN 标记或情景组识别此字段中的相似信息。DefensePro 6.x 版和 7.x 版支持 VLAN 标记。适用于 Cisco Firepower 9300 的 DefensePro 支持情景组。
MPLS RD	攻击使用或已使用的 MPLS RD。

表 151：SYN 泛洪攻击详细信息：信息参数

参数	说明
当保护操作为阻止模式时显示该信息。 **小心：**如果 SYN 保护配置了“仅报告”(report-only) 模式，则“平均攻击速率”(Average Attack Rate)、“攻击阈值”(Attack Threshold) 和“攻击容量”(Attack Volume) 字段会显示 **0**（零）。	
平均攻击速率 (Average Attack Rate)	每秒受欺骗 SYN 和数据连接尝试的平均速率，每 10 秒计算一次。
攻击阈值 (Attack Threshold)	配置的攻击触发阈值，为每秒连接数的一半。
攻击容量 (Attack Volume)	攻击生命周期期间来自受欺骗 TCP 连接的数据包数量（汇聚）。这些数据包来自通过 SYN cookie 机制建立的会话，或者通过 SYN 保护受信任列表而进行传输。
攻击持续时间 (Attack Duration)	受保护端口上攻击的持续时间，格式为 hh:mm:ss。
TCP 质询 (TCP Challenge)	识别攻击的*身份验证方法 (Authentication Method)*。
HTTP 质询 (HTTP Challenge)	识别攻击：*302 Redirect* 或 *JavaScript* 的 *HTTP 身份验证方法 (HTTP Authentication Method)*。

表 152：SYN 泛洪攻击详细信息：身份验证列表利用率参数

参数	说明
TCP 身份验证列表 (TCP Auth. List)	TCP 身份验证表的当前利用率（百分比）。
HTTP 身份验证列表 (HTTP Auth. List)	HTTP 身份验证表的当前利用率（百分比）。

表 153：SYN 泛洪攻击详细信息：攻击描述

参数	说明
如果已将攻击描述文件上传到 APSolute Vision 服务器上，则为攻击描述文件对攻击的描述。	

采样数据选项卡

您可以为支持采样数据的所有攻击类型显示*采样数据 (Sampled Data)* 对话框。

采样数据 (Sampled Data) 选项卡包含采样攻击数据包数据的表。表中每一行显示一个采样攻击数据包的数据。标题栏包括数据的类别 - 例如，*行为 DoS (Behavioral DoS)*。

采样数据 (Sampled Data) 选项卡中的表包括以下列：

- **时间 (Time)**
- **源地址 (Source Address)**
- **源 MSISDN (Source MSISDN)** - *APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
- **源 L4 端口 (Source L4 Port)**
- **目标地址 (Destination Address)**
- **目标 MSISDN (Destination MSISDN)** - *APSolute Vision 版本 3.0 及更高版本中不支持 MSISDN 解析功能。*
- **目标 L4 端口 (Destination L4 Port)**
- **协议 (Protocol)**
- **VLAN/情景 (VLAN/Context)**
- **MPLS RD**
- **物理端口 (Physical Port)**

要显示“采样数据”(Sampled Data) 选项卡

1. 在*安全监控 (Security Monitoring)* 视角中选择为其显示数据的 DefensePro 设备或站点。
2. 依次选择**控制面板视图 (Dashboard View) > 安全控制面板 (Security Dashboard)**。
3. 执行以下操作之一以打开*攻击详细信息 (Attack Details)* 选项卡：
   — 在安全控制面板图表视图 ( ) 中，双击图标。
   — 在安全控制面板表视图 ( ) 中，双击相关行。
4. 点击 （查看采样数据）按钮。

您可以将*采样数据 (Sampled Data)* 对话框中表的某些行导出到 CSV 文件。

要将采样数据保存到 CSV 文件

1. 在*安全监控 (Security Monitoring)* 视角中选择为其显示数据的 DefensePro 设备或站点。
2. 依次选择**控制面板视图 (Dashboard View) > 安全控制面板 (Security Dashboard)**。
3. 执行以下操作之一以打开*攻击详细信息 (Attack Details)* 选项卡：
   — 在安全控制面板图表视图 ( ) 中，双击图标。
   — 在安全控制面板表视图 ( ) 中，双击相关行。
4. 点击 （查看采样数据）按钮。
5. 选择您希望文件中数据行开始的行。
6. 点击 (CSV) 按钮。
7. 查看文件或指定位置或文件名。

查看实时流量报告

默认情况下，所有流量均呈现在这些图表和表中。在每个图表中，您可以按协议或流量方向来过滤显示，但不可以过滤并发连接。

您可以在*流量监控 (Traffic Monitoring)* 选项卡中监控以下流量信息：

- 查看流量使用率统计信息，第 186 页
- 查看连接速率统计信息，第 189 页
- 查看并发连接统计信息，第 189 页

查看流量使用率统计信息

APSolute Vision 可以显示以下项目的流量使用率统计信息：

- **统计信息图表** - 以图表显示选定端口对的信息。图表包含选定协议的信息，或一段时间内所有协议的全部信息。

  以下各项目在图表中显示为一条曲线：

  — 入站 IP 流量 (Inbound IP traffic)

  — 出站 IP 流量 (Outbound IP traffic)

  — 已丢弃的入站流量 (Discarded inbound traffic)

  — 已丢弃的出站流量 (Discarded outbound traffic)

  — 已排除的入站流量 (Excluded inbound traffic)

  — 已排除的出站流量 (Excluded outbound traffic)

  要隐藏或显示特定流量类型的曲线，请点击图例中对应的色块。

- **流量身份验证统计信息（质询/响应）(Traffic Authentication Statistics (Challenge/Response))** - 当支持质询响应机制的保护模块中启用了相关选项时，则会显示质询响应机制的统计信息。
- **最后样本统计信息 (Last Sample Statistics)** - 显示各协议的最后读数，并为单个设备提供所有协议的全部统计信息。（此信息仅当查看单个设备时可用。）

  要查看或保存 CSV 文件，请点击 (CSV)。

提示：要获取以每秒钟数据包数或每秒钟字节数为单位的当前流量速率（按照 15 秒钟的平均速率来计算），您可以在 DefensePro 设备上使用以下 CLI 命令：

dp rtm-stats get [port number]

要显示流量使用率统计信息

1. 在*安全监控 (Security Monitoring)* 视角中，选择为其显示数据的 DefensePro 设备或站点。
2. 依次选择**流量监控 (Traffic Monitoring) > 流量使用率报告 (Traffic Utilization Report)**。
3. 根据需要更改图表和表的显示设置。
4. 对于*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)*，请根据需要为显示的流量数据设置过滤选项。显示的信息会自动刷新。

表 154：流量使用率报告：显示图表和表的参数

参数	说明
范围 (Scope) （这是显示表的链接。）	流量使用率报告显示的网络保护策略。 默认情况下，“范围”(Scope) 是**任何端口 (Any Port)** 或**任何策略 (Any Policy)**（取决于**范围 (Scope)** 下拉列表中指定的值）。即，默认情况下，流量使用率报告显示所有信息。 要控制流量使用率报告显示的信息的范围，请参阅操作步骤控制流量使用率报告显示的信息的范围，第 188 页。 **注意：**适用于 Cisco Firepower 9300 的 DefensePro 不支持限制“范围”(Scope) 的物理端口。
显示持续时间 (Display Last)	攻击终止后图表显示攻击的持续时间。即，图表显示当前正在发生的所有攻击或在选定时段内终止的所有攻击。 值： ● 10 分钟 (10 Minutes) ● 20 分钟 (10 Minutes) ● 30 分钟 (10 Minutes) ● 1 小时 (1 Hour) 默认值：“10 分钟”(10 Minutes)
范围 (Scope) （这是下拉列表。）	图表视图的范围。 值： ● “设备/物理端口”(Devices/Physical Ports) - 图表根据指定设备上的物理端口显示流量。 ● “设备/策略”(Devices/Policies) - 图表根据指定设备上的网络保护策略显示流量。 默认值：“设备/物理端口”(Devices/Physical Ports) **注意：**适用于 Cisco Firepower 9300 的 DefensePro 不支持限制“范围”(Scope) 的物理端口。
单位 (Units)	流量速率的单位。 值： ● Kbps - 每秒千比特 ● “数据包/秒”(Packet/Sec) - 每秒数据包数

要控制流量使用率报告显示的信息范围

1. 请点击 ▶ Scope。随后会打开表。表具有*设备名称 (Device Name)* 和*端口 (Port)* 列或*设备名称 (Device Name)* 和*策略 (Policy) 列* - 根据**范围 (Scope)** 下拉列表中指定的值：**设备/物理端口 (Devices/Physical Ports)** 或**设备/策略 (Devices/Policies)**。

   注意：适用于 Cisco Firepower 9300 的 DefensePro 不支持限制“范围”(Scope) 的物理端口。

2. 执行以下操作之一：
   - 要限制流量使用率报告显示的物理端口或网络保护策略，请选中对应的复选框。
   - 要显示所有当前相关的物理端口或网络保护策略的信息，请点击左上部的表单元格，然后选择**全选 (Select All)**。
   - 要显示数据库中的所有信息，甚至显示与特定端口或特定网络保护策略无关的信息，请点击左上部的表单元格，然后选择**全部不选 (Select None)**。

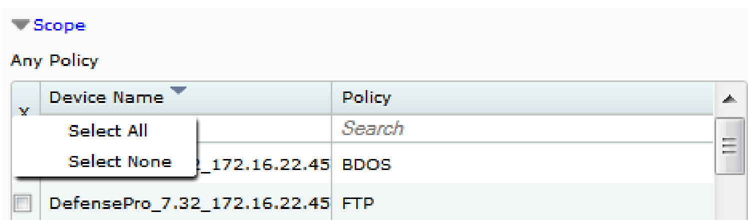


表 155：流量使用率报告：流量统计信息图表的过滤器参数

参数	说明
方向 (Direction)	图表显示的流量。 值： ● “入站”(Inbound) - 显示入站流量。 ● “出站”(Outbound) - 显示出站流量。 ● “二者”(Both) - 显示入站流量和出站流量。入站和出站的数据显示为单独的行，而非总行数。 **注意：**一对端口之间的流量方向由端口对配置中的**进入端口 (In Port)** 设置定义。
协议 (Protocol)	要显示的流量协议。 值： ● TCP - 显示 TCP 流量的统计信息。 ● UDP - 显示 UDP 流量的统计信息。 ● ICMP - 显示 ICMP 流量的统计信息。 ● IGMP - 显示 IGMP 流量的统计信息。 ● SCTP - 显示 SCTP 流量的统计信息。 ● “其他”(Other) - 显示非 TCP、UDP、ICMP、IGMP 或 SCTP 流量的统计信息。 ● “全部”(All) - 显示全部流量统计信息。

表 156：流量使用率报告：流量身份验证统计信息（质询/响应）参数

参数	说明
协议 (Protocol)	行中显示的统计信息的协议。 值：HTTP、TCP、DNS **注意：**HTTP 行与适用于 Cisco Firepower 9300 的 DefensePro 不相关。
当前攻击 (Current Attacks)	设备中当前攻击的数量。
身份验证表使用率 % (Authentication Table Utilization %)	已满的身份验证表的百分比。
质询速率 (Challenges Rate)	设备发送质询的速率 (PPS)。

表 157：流量使用率报告：最后样本统计信息参数

参数	说明
协议 (Protocol)	流量协议。 值： TCP UDP ICMP IGMP SCTP “其他”(Other) - 非 TCP、UDP、ICMP、IGMP 或 SCTP 流量的统计信息。 “全部”(All) - 全部流量统计信息。
“入站”(Inbound)	行中识别的协议的入站流量。
“出站”(Outbound)	行中识别的协议的出站流量。
“已丢弃的入站流量” (Discarded Inbound)	行中识别的协议的已丢弃入站流量。
“已丢弃的出站流量” (Discarded Outbound)	行中识别的协议的已丢弃出站流量。
“丢弃率 %”(Discard %)	行中识别的协议的已丢弃流量百分比。
“已排除的入站流量” (Excluded Inbound)	行中识别的协议的已排除入站流量。
“已排除的出站流量” (Excluded Outbound)	行中识别的协议的已排除出站流量。

查看连接速率统计信息

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不起作用。

查看并发连接统计信息

此功能在适用于 Cisco Firepower 9300 的 DefensePro 中不起作用。

保护监控

保护监控提供每个网络策略的实时流量监控，或者如果配置了 BDoS，则提供整个网络的实时流量监控，或者如果配置了 DNS，则提供 DNS 流量的实时监控。保护监控所提供的统计流量信息可以帮助您更好地了解流经受保护网络的流量，配置的保护如何工作，以及最为重要的，如何检测异常流量。

有关显示选定设备的保护信息的信息，请参阅以下页面：

- 显示攻击状态信息，第 190 页
- 监控 BDoS 流量，第 190 页
- 监控 DNS 流量，第 193 页

显示攻击状态信息

您可以显示每个已配置并已启用的保护策略的攻击摘要状态信息。当存在违背网络保护策略的攻击时，该表会为相关攻击流量在对应的行中显示表示攻击状态的图标。

要显示攻击状态信息

1. 在*安全监控 (Security Monitoring)* 视角中，选择要监控的 DefensePro 设备。
2. 依次选择**保护监控 (Protection Monitoring) > 攻击状态报告 (Attack Status Report)**。该表包括以下列：
   - 策略名称 (Policy Name)
   - IPv4-TCP
   - IPv4-UDP
   - IPv4-ICMP
   - IPv4-DNS
   - IPv6-TCP
   - IPv6-UDP
   - IPv6-ICMP
   - IPv6-DNS
3. 当表中显示攻击图标时，请点击该图标以显示对应的攻击流量信息。

监控 BDoS 流量

您可以监控包括 BDoS 保护的网络保护策略的流量。流量信息显示在*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表中。

小心：当流量匹配具有州外保护的多个网络保护策略时，APSolute Vision 显示的已丢弃流量总量代表了所有相关网络保护策略的所有已丢失流量的总和。这是因为，当流量匹配具有州外保护的多个网络保护策略时，所有这些网络保护策略计算的是相同的已丢弃流量。

要显示包括 BDoS 保护的网络策略的流量信息

1. 在*安全监控 (Security Monitoring)* 视角中，选择要监控的设备。
2. 依次选择**保护监控 (Protection Monitoring) > BDoS 流量监控报告 (BDoS Traffic Monitoring Reports)**。
3. 配置 *BDoS 流量统计信息 (BDoS Traffic Statistics)* 图表和*最后样本统计信息 (Last Sample Statistics)* 表的显示范围。

统计信息图表

该表根据指定参数显示选定网络保护策略的流量速率。

表 158：统计信息图表和最后样本统计信息表的范围参数

参数	说明
范围 (Scope)	网络保护策略。列表仅显示使用 BDoS 配置文件配置的策略。
显示持续时间 (Display Last)	攻击终止后图表显示攻击的持续时间。即，图表显示当前正在发生的所有攻击或在选定时段内终止的所有攻击。 值： ● 10 分钟 (10 Minutes) ● 20 分钟 (10 Minutes) ● 30 分钟 (10 Minutes) ● 1 小时 (1 Hour) 默认值： “10 分钟” (10 Minutes)
方向 (Direction)	*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表显示的流量方向。 值： “入站” (Inbound)、 “出站” (Inbound)
单位 (Units)	*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表根据其而显示流量的单位。 值： ● Kbps - 每秒千比特 ● “数据包/秒” (Packets/Sec) - 每秒数据包数

表 159：统计信息图表参数

参数	说明
IP 版本 (IP Version)	图表显示的流量的 IP 版本。 值：IPv4、IPv6
保护类型 (Protection Type)	要监控的保护类型。 值： ● TCP ACK FIN ● TCP FRAG ● TCP RST ● TCP SYN ● TCP SYN ACK ● UDP ● UDP FRAG ● ICMP ● IGMP
比例 (Scale)	Y 轴上信息的显示比例。 值： “线性” (Linear)、 “对数” (Logarithmic)
攻击状态 (Attack Status)	（只读）攻击的状态。

表 160：统计信息图表图例

线	说明
总流量 (Total Traffic) （ 深蓝）	设备查看到的特定保护类型和方向的总流量。
合法流量 (Legitimate Traffic) （ 浅蓝）	DefensePro 设法阻止攻击后，实际的转发流量速率。 当无攻击时， “总流量”(Total Traffic) 与 “合法流量”(Legitimate Traffic) 相等。
正常边缘 (Normal Edge) （ 绿色虚线）	统计计算的基准流量速率。
可疑边缘 (Suspected Edge) （ 橙色虚线）	表示流量变化可能为攻击的流量速率。
攻击边缘 (Attack Edge) （ 红色虚线）	表示发生攻击的流量速率。

表 161：最后样本统计信息参数

参数	说明
流量类型 (Traffic Type)	保护类型。每个特定流量类型和方向均具有设备可自动获知的基准。
基准 (Baseline)	设备预期的正常流量速率。
总流量 (Total Traffic)	设备查看到的特定流量类型和方向的总流量速率。
基准部分 % (Baseline Portion %)	速率不变基准的指示 - 即，相同方向上特定流量类型占所有其他流量的正常百分比。
RT 部分 % (RT Portion %)	相同方向上特定流量类型相对于所有其他流量的实际百分比。
合法流量 (Legitimate Traffic)	设备阻止攻击后，实际的转发流量速率。当无攻击时，RT 速率与合法速率相等。
合法部分 % (Legitimate Portion %)	设备阻止攻击后，相对于其他类型的流量，指定类型的转发流量速率的实际百分比。
攻击程度 (Degree of Attack)	评估当前攻击级别的数值。8 或更高值表示攻击。

监控 DNS 流量

您可以监控包括 DNS 泛洪保护的网络保护策略的流量。流量信息显示在*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表中。

要显示包括 DNS 保护的网络保护策略的流量信息

1. 在*安全监控 (Security Monitoring)* 视角中，选择要监控的设备。
2. 依次选择**保护监控 (Protection Monitoring) > DNS 流量监控报告 (DNS Traffic Monitoring Reports)**。
3. 配置用于显示*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表的过滤器。

统计信息图表

图表根据指定参数显示选定网络保护策略的流量速率。

表 162：统计信息图表和最后样本统计信息表的范围参数

参数	说明
范围 (Scope)	网络保护策略。列表仅显示使用 DNS 配置文件配置的规则。
方向 (Direction)	*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表显示的流量方向。 值：“入站”(Inbound)、“出站”(Inbound)
单位 (Units)	（只读）*统计信息图表 (Statistics Graph)* 和*最后样本统计信息 (Last Sample Statistics)* 表根据其而显示流量的单位。 值：QPS - 每秒查询数

表 163：统计信息图表参数

参数	说明
IP 版本 (IP Version)	图表显示的流量的 IP 版本。值：IPv4、IPv6
保护类型 (Protection Type)	要监控的 DNS 查询类型。 值： • 其他 (Other) • 文本 (Text) • A • AAAA • MX • NAPTR • PTR • SOA • SRV
比例 (Scale)	Y 轴上信息的显示比例。 值：“线性”(Linear)、“对数”(Logarithmic)
攻击状态 (Attack Status)	（只读）攻击的状态。

表 164：统计信息图表图例

线	说明
总流量 (Total Traffic)（ 深蓝）	设备查看到的特定保护类型和方向的总流量。
合法流量 (Legitimate Traffic)（ 浅蓝）	DefensePro 设法阻止攻击后，实际的转发流量速率。 当无攻击时， “总流量”(Total Traffic) 与 “合法流量”(Legitimate Traffic) 相等。
正常边缘 (Normal Edge)[1]（ 绿色虚线）	统计计算的基准流量速率。
可疑边缘 (Suspected Edge)[1]（ 橙色虚线）	表示流量变化可能为攻击的流量速率。
攻击边缘 (Attack Edge)[1]（ 红色虚线）	表示发生攻击的流量速率。

1 - 如果将保护配置为使用足迹绕行或手动触发器，则不会显示此线。

最后样本统计信息表

图表显示最后样本统计信息。

表 165：最后样本统计信息参数

参数	说明
流量类型 (Traffic Type)	保护类型。每个特定流量类型和方向均具有设备可自动获知的基准。
基准 (Baseline)	设备预期的正常流量速率。
总流量 (Total Traffic)	DefensePro 设备查看到的特定流量类型和方向的总流量速率。
基准部分 % (Baseline Portion %)	速率不变基准的指示 - 即，相同方向上特定流量类型占所有其他流量的正常百分比。
RT 部分 % (RT Portion %)	相同方向上特定流量类型相对于所有其他流量的实际百分比。
合法流量 (Legitimate Traffic)	设备阻止攻击后，实际的转发流量速率。当无攻击时，RT 速率与合法速率相等。
合法部分 % (Legitimate Portion %)	设备阻止攻击后，相对于其他类型的流量，指定类型的转发流量速率的实际百分比。
攻击程度 (Degree of Attack)	评估当前攻击级别的数值。8 或更高值表示攻击。

新安全攻击的警报

当新的攻击显示在*当前攻击 (Current Attacks)* 表（这是*安全监控 (Security Monitoring)* 视角的一部分）中时，APSolute Vision 会触发警报。

警报 (Alerts) 窗格中*模块 (Module)* 列中的值为*安全报告 (Security Reporting)*。每个 DefensePro 设备都会触发独立的安全警报。

安全警报可以是单个安全事件（即单个攻击事件），也可以由多个安全事件汇聚而成。单个攻击和多个攻击警报的格式相似。

表 166：安全警报中的信息

单个攻击安全警报中的字符串	安全警报汇聚攻击信息中的字符串
攻击类型：<攻击类别>[1]已开始。	<攻击数量> 攻击类型：<攻击类别>[1]已于 <首个攻击的开始时间> 和 <最后攻击的开始时间>[2]之间开始。
按规则检测：<网络保护策略>；	按规则检测：<网络保护策略>； [3]
攻击名称：<攻击名称>；	攻击名称：<攻击名称>； [3]
源 IP：<攻击者 IP 地址>；	源 IP：<攻击者 IP 地址>； [4]
目标 IP：<受攻击的 IP 地址>；	目标 IP：<受攻击的 IP 地址>；
目标端口：<受攻击的端口>；	目标端口：<受攻击的端口>；
操作：<操作>。	操作：<操作>。

1 - 攻击类别（对*所有*可能的 DefensePro 版本和配置）：
- ACL
- 反扫描 (Anti-Scanning)
- 行为 DoS (Behavioral DoS)
- DoS
- HTTP 泛洪 (HTTP Flood)
- 入侵 (Intrusions)
- 服务器破解 (Server Cracking)
- SYN 泛洪 (SYN Flood)
- 异常 (Anomalies)
- 状态 ACL (Stateful ACL)
- DNS
- BWM

2 - 时间格式为 dd.MM.yy hh:mm。

3 - 当攻击的字段值中存在差异时，这些值会以逗号分隔。

4 - 当攻击的字段值中存在差异时，该值为**多个 (multiple)**。值**多个 (multiple)** 也可能指 DefensePro 无法报告特定值的情况。

APSolute Vision 管理员可以限制包括在安全警报中的参数。此选项非常有用，因为用户常常在智能手机上查看经常通过电子邮件接收的安全警报。为弥补小尺寸屏幕的缺点，管理员可以选择要包括在警报中的参数。

要选择要包括在安全警报中的参数

1. 在 *APSolute Vision 设置 (APSolute Vision Settings)* 视图*系统 (System)* 视角中，依次选择**常规设置 (General Settings) > 警报浏览器 (Alert Browser) > 安全警报 (Security Alerts)**。
2. 选择警报中要包括的各参数旁边的复选框。您可以选择以下参数的任意组合：
   - 策略名称 (Policy Name)
   - 攻击名称 (Attack Name)
   - 源 IP 地址 (Source IP Address)
   - 目标 IP 地址 (Destination IP Address)
   - 目标端口 (Destination Port)
   - 操作 (Action)

   默认情况下，所有复选框均为选中状态。
3. 点击**提交 (Submit)**。

   注意：对设置所做的更改在更改和转发时生成的警报上生效。

第 12 章 - 管理 DefensePro

本章介绍管理 DefensePro 并包含以下各节：

命令行界面

访问“命令行界面”(Command Line Interface) (CLI) 需要串行电缆连接以及终端仿真应用。

DefensePro 最多支持五个同时进行的 Telnet 或 SSH 会话。

您还可以使用 CLI 进行调试。当需要调试时，DefensePro 会生成单独的以文本格式交付的文件，汇聚 Radware 技术支持部门所需的所有 CLI 命令。该文件还包括各类 CLI 命令的输出，例如*客户端 (Client)* 表、*ARP* 表等的打印输出。您可以使用 APSolute Vision 下载此文件并将其发送至 Radware 技术支持部门（请参阅下载设备配置文件，第 60 页）。

表 167：DefensePro CLI 命令和菜单

命令	说明
acl	访问控制列表。
classes	配置用于分类的流量属性。
device	设备设置。
dp	DefensePro 安全设置。
help	显示指定命令的帮助。
login	登录设备。
logout	从设备注销。
manage	设备管理配置。
net	网络配置。
ping	Ping 远程主机。
reboot	重新启动设备。
security	设备安全。
services	常规网络服务。
shutdown	关机。
ssh	通过 SSH 连接到远程主机。
statistics	设备统计信息配置。
system	设置系统参数。
telnet	通过 Telnet 连接到远程主机。
trace-route	测量到给定目标的跳数和延迟。

CLI 会话超时

当您通过 Telnet 或 SSH 登录 CLI 时，完成身份验证操作步骤会有预定义的超时时间。在与设备建立 CLI 会话后，必须在由*身份验证超时时间 (Authentication Time-out)* 参数定义的时段内插入用户名和密码。在三次错误的登录尝试后，终端会锁定 10 分钟，并且系统不再接受来自该 IP 地址的登录尝试。

对于 Telnet 或 SSH 会话，尽管会话的“会话超时”(Session Time-out) 参数为非活动状态，您仍然可以定义与设备保持连接的时间。如果当预定义时段结束时会话仍处于非活动状态，则会话会自动终止。

尽管会话的“会话超时”(Session Time-out) 参数为非活动状态，您仍然可以定义通过控制台与设备保持连接的时间段。在预定义的时间结束后，会话会自动终止。

要配置会话超时

> 对于控制台，请使用以下命令：

Manage terminal session-timeout

> 对于 SSH 会话，请使用以下命令：

Manage ssh session-timeout

> 对于 Telnet 会话，请使用以下命令：

Manage telnet session-timeout

> 对于 SSH 身份验证，请使用以下命令：

Manage ssh auth-timeout

> 对于 Telnet 身份验证，请使用以下命令：

Manage telnet auth-timeout

CLI 功能

您可以通过控制台访问、Telnet 或 SSH 使用 DefensePro CLI。CLI 可以提供以下功能：

- 一致、具有逻辑结构且直观的命令语法。
- system config 命令可以查看设备的当前配置，采用 CLI 命令行的格式。
- 使用 system config 设置命令将 system config 的输出或部分输出粘贴到其他设备的 CLI。此选项可用于轻松地复制配置。
- 帮助和命令完成键。
- 命令行编辑键。
- 命令历史记录。
- 可配置的提示。
- 可配置的 Telnet 和 SSH 横幅。
- Ping - Ping 网络上的其他主机以测试其他主机的可用性。
- 跟踪路由 - 使用以下命令：

  trace-route <目标 IP 地址>

  输出格式：

  DP#trace-route www.radware.com

trace-route to host 209.218.228.203:

1:	50ms	50ms	50ms	212.150.43.130
2:	50ms	50ms	50ms	80.74.101.129
3:	50ms	50ms	50ms	192.116.214.2
4:	*	*	*	
5:	50ms	50ms	50ms	80.74.96.40

- Telnet 客户端 - 要使用以下 CLI 命令向远程主机发起 Telnet 会话：

  telnet <IP 地址>

- SSH 客户端 - 要使用以下 CLI 命令向远程主机发起 SSH 会话：

  ssh <IP 地址>

CLI 陷阱

当通过串行电缆连接到物理 DefensePro 平台时，设备会在事件发生时生成陷阱。

要通过 CLI、Telnet 和 SSH 发送陷阱，命令为：

manage terminal traps-outputs set-on

仅限控制台：

manage terminal traps-outputs set normal

将陷阱发送给所有 CLI 用户

此选项使您可以配置是否仅向串行终端或者也向 SSH 和 Telnet 客户端发送陷阱。

Web 服务

您可以通过 SNMP、串行端口、Telnet、SSH、HTTP（通过内部 Web 应用）和 HTTPS 对 DefensePro Radware 设备进行管理。要为客户提供开发强化应用监控的功能、自定义的应用交付网络管理应用和高级自动化工具，Radware 为 DefensePro 上的 Web 服务接口提供 APSolute API 这一开放的基于标准的 SOAP (XML) API。

与 APSolute API 集成提供给客户设备性能的综合视图，包括基于外部参数的历史数据分析和趋势、性能诊断、可用性报告和维护操作自动化，并对 DefensePro 进行微调以达成最优的应用交付。

主要功能：

- 控制 Radware 产品功能和来自任何外部应用的功能。
- 启用 API 的网络设备表现为应用的软件，达到真实的软件本地集成。
- 针对多个开发平台和语言的综合 SDK。
- 广泛的样本应用代码、文档以及配置指南。
- 通过基于 Web 服务的 API 可获得 1,700 多种方法。
- 支持 SOAP/XML over HTTPS 确保灵活且安全的通信。

API 结构

APSolute API 是 SOAP/XML 接口，为利用常用开发语言（包括 Java、Visual Basic/C# 和 Perl）的第三方应用提供对 DefensePro 设备的完全访问。此接口同时允许设备配置及监控状态和性能统计信息。

APSolute API 提供两种与 DefensePro 设备交互的方法：

1. 发布 CLI 命令：

   此接口对以下项目不提供支持：

   - 非配置命令或非监控命令（例如 ping、telnet 和 trace-route）的命令。
   - 具有异步输出的命令（例如加速器相关的 CLI 命令）。
   - 对 CLI 命令的响应限于前 1000 行。
2. 通过镜像 Radware SNMP MIB 的 SOAP 命令配置和监控设备：以下命令类型可用：
   - 对于标量 MIB 参数，检索（获取）该值并更改（设置）该值。
   - 对于 MIB 表条目，创建条目、删除条目、更新条目的一个或多个参数、检索（获取）条目、检索（获取）整个表、遍历表（获取第一个条目并获取下一个）。

DefensePro Web 服务通过 HTTP 或 HTTPS 请求（例如常见的网络浏览器）运行。默认情况下，Web 服务在 DefensePro 上被禁用。

您可以使用以下方式启用 DefensePro Web 服务：

- CLI - 管理 Web 服务状态
- WBM - Web 服务窗口（服务 (Services) > Web > *Web 服务 (Web Services)* 窗口）
- APSolute Vision - *设置 (Setup)* 窗口的*访问 (Access)* 选项卡

仅当在设备上启用了 Web 或安全 Web 管理界面时您才可以启用 Web 服务。

APSolute API 软件开发套件 (SDK)

APSolute API SDK 具有全部必需的组件和文档，以允许在自定义开发的应用中快速开发控制和监控功能。它包括以下内容：

- 所有接口和模块的 Web 服务描述语言 (WSDL) 文件
- API 参考
- 产品概述
- 某些基本设备配置/监控功能的样本代码

要开始使用 APSolute API SDK，请安装 SOAP 客户端工具包（支持 SOAP 版本 1.1 及更高版本）并为工作站上的工具包安装开发环境。

附录 A - 足迹绕行字段和值

本附录介绍 BDoS 保护和 DNS 保护中的*足迹绕行 (footprint bypass)* 字段，并包含以下主要部分：

BDoS 足迹绕行字段和值

本节包含以下表：

- UDP、ICMP 和 IGMP 控制器的 BDoS 足迹绕行字段和值，第 203 页
- 所有 TCP 控制器的 BDoS 足迹绕行字段和值，第 205 页

有关详细信息，请参阅配置 BDoS 足迹绕行，第 104 页。

表 168：UDP、ICMP 和 IGMP 控制器的 BDoS 足迹绕行字段和值

控制器	字段	默认状态	默认值或“无”(N/A)[1]	注释
UDP ICMP IGMP	校验和	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	数据包 UDP 报头中的校验和值。
UDP ICMP IGMP	id-num	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	来自 IP 数据包报头的 ID 编号。
UDP ICMP IGMP	id-num-ipv6	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	来自 IPv6 数据包报头的 ID 编号。
UDP ICMP IGMP	dns-id-num	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	DNS 查询的 ID 编号。
UDP	dns-qname	接受	无	由 DNS 查询请求的域名。
UDP	dns-qcount	接受	1	单个 DNS 会话中的 DNS 查询数量。
UDP	source-port	接受	无	攻击的源端口。
UDP ICMP IGMP	frag-offset	接受	0,185	表示此分段在数据报中所属的位置。分段偏移量以 8 字节为单位计算（64 位）。
UDP ICMP	frag-offset-ipv6	接受	0，181	表示此 IPv6 分段在数据报中所属的位置。IPv6 分段偏移量以 8 字节为单位计算（64 位）。
UDP ICMP	flow-label	接受	0，181	源用以标记其请求 IPv6 路由器特殊处理的那些产品。流量通过源地址和非零流标签的组合进行唯一识别。

表 168：UDP、ICMP 和 IGMP 控制器的 BDoS 足迹绕行字段和值（续）

控制器	字段	默认状态	默认值或“无”(N/A)[1]	注释
UDP ICMP IGMP	source-ip	接受	无	攻击的源 IP 地址。
UDP ICMP	source-ip-ipv6	接受	无	攻击的源 IPv6 地址。
UDP ICMP IGMP	tos	接受	无	来自 IP 数据包报头的服务值类型。
UDP ICMP IGMP	packet-size	接受	对于 UDP 和 IGMP：无 对于 ICMP：74	数据包的大小（以字节为单位），包括数据链路报头。
UDP ICMP	packet-size-ipv6	接受	对于 UDP：无 对于 ICMP：118	IPv6 数据包的大小（以字节为单位），包括数据链路报头。
UDP	destination-port	接受	无	来自数据包报头的目标端口。
UDP ICMP IGMP	destination-ip	接受	无	目标 IP 地址。
UDP ICMP	destination-ip-ipv6	接受	无	目标 IPv6 地址。
UDP ICMP IGMP	分片	接受	无	协议分段的数据包。
UDP ICMP IGMP	ttl	接受	无	IP 数据包报头中的生存时间值。
UDP ICMP IGMP	vlan-tag	接受	无	VLAN 标记值（外部）。
ICMP IGMP	icmp-igmp-message-type	接受	无	协议消息类型值。
ICMP	icmp-message-type-ipv6	接受	无	ICMP IPv6 消息类型值。

1 - 无（即“不适用”）表示该字段无可用的特定值；仅适用常规状态**接受 (Accept)** 或**绕行 (Bypass)**。

表 169：所有 TCP 控制器的 BDoS 足迹绕行字段和值

控制器	字段	默认状态	默认值或“无”(N/A)[1]	注释
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	sequence-num	接受	无	来自相关 TCP 数据包报头的序列号值。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	id-num	接受	无	来自 IP 数据包报头的 ID 编号。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-port	接受	无	生成的攻击的源端口。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip	绕行		生成的攻击的源 IP 地址。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip-ipv6	绕行		生成的攻击的源 IPv6 地址。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	tos	接受		来自 IP 数据包报头的服务值类型。

表 169：所有 TCP 控制器的 BDoS 足迹绕行字段和值（续）

控制器	字段	默认状态	默认值或“无”(N/A)[1]	注释
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size	接受	对于 TCP-SYN、TCP-SYN-ACK：60、62、66、74 对于 TCP-RST、TCP-ACK-FIN：60 对于 TCP-Frag：无	数据包的大小（以字节为单位），包括数据链路报头。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size-ipv6	接受	对于 TCP-SYN、TCP-SYN-ACK：80、82、86、94 对于 TCP-RST、TCP-ACK-FIN：74 对于 TCP-Frag：无	IPv6 数据包的大小（以字节为单位），包括数据链路报头。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-port	接受		攻击的目标 TCP 端口。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip	接受		攻击的目标 IP 地址。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip-ipv6	接受		攻击的目标 IPv6 地址。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	ttl	接受		IP 数据包报头中的生存时间值。

表 169：所有 TCP 控制器的 BDoS 足迹绕行字段和值（续）

控制器	字段	默认状态	默认值或“无”(N/A)[1]	注释
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	vlan-tag	接受		VLAN 标记值（外部）。
TCP-FRAG	frag-offset	接受	0,185	表示此分段在数据报中所属的位置。分段偏移量以 8 字节为单位计算（64 位）。
TCP-FRAG	frag-offset-ipv6	接受	0,181	表示此 IPv6 分段在数据报中所属的位置。IPv6 分段偏移量以 8 字节为单位计算（64 位）。
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	flow-label	接受	0	源用以标记其请求 IPv6 路由器特殊处理的那些产品。流量通过源地址和非零流标签的组合进行唯一识别。

1 -“无”(N/A)（即“不适用”）表示该字段无可用的特定值；仅适用常规状态**接受 (Accept)** 或**绕行 (Bypass)**。

DNS 足迹绕行字段和值

DNS 足迹绕行类型有关以下控制器，所有这些控制器均支持相同字段、默认状态以及默认值：

- A
- AAAA
- MX
- NAPTR
- 其他 (Others)
- PTR
- SOA2
- SRV
- 文本 (Text)

表 170：DNS 足迹绕行字段和值

字段	默认状态	默认值或“无”(N/A)[1]	注释
checksum	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	数据包 UDP 报头中的校验和值。
id-num	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	来自 IP 数据包报头的 ID 编号。
id-num-ipv6	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	来自 IPv6 数据包报头的 ID 编号。
dns-id-num	接受	对于 UDP：0 对于 ICMP 和 IGMP：无	DNS 查询的 ID 编号。
dns-qname	接受	无	由 DNS 查询请求的域名。
dns-qcount	接受	1	单个 DNS 会话中的 DNS 查询数量。
source-port	接受	无	攻击的源端口。
flow-label	接受	0,181	源用以标记其请求 IPv6 路由器特殊处理的那些产品。流量通过源地址和非零流标签的组合进行唯一识别。

表 170：DNS 足迹绕行字段和值（续）

字段	默认状态	默认值或“无”(N/A)[1]	注释
source-ip	接受	无	攻击的源 IP 地址。
source-ip-ipv6	接受	无	攻击的源 IPv6 地址。
tos	接受	无	来自 IP 数据包报头的服务值类型。
packet-size	接受	对于 UDP 和 IGMP：无 对于 ICMP：74	数据包的大小（以字节为单位），包括数据链路报头。
packet-size-ipv6	接受	对于 UDP：无 对于 ICMP：118	IPv6 数据包的大小（以字节为单位），包括数据链路报头。
destination-ip	接受	无	目标 IP 地址。
destination-ip-ipv6	接受	无	目标 IPv6 地址。
fragment	接受	无	协议分段的数据包。
ttl	接受	无	IP 数据包报头中的生存时间值。
vlan-tag	接受	无	VLAN 标记值（外部）。
dns-ancount	接受	0	单次 DNS 会话中的 DNS 应答数量。
flags	接受	无	DNS 报头标志字段（AA、TC、RD 等）。

1 - 无（即“不适用”）表示该字段无可用的特定值；仅适用常规状态**接受 (Accept)** 或**绕行 (Bypass)**。

附录 B - 预定义的基本过滤器

列表可能因产品版本而有所不同。

表 171：预定义的基本过滤器

名称	说明	协议	OMPC 偏移量	OMPC 掩码
000	例行程序	IP	1	e0000000
001	优先级	IP	1	e0000000
010	即刻	IP	1	e0000000
011	闪存	IP	1	e0000000
100	ToS 闪存覆盖	IP	1	e0000000
101	CRITIC/ECP	IP	1	e0000000
110	网际网络控制	IP	1	e0000000
111	网络控制	IP	1	e0000000
aim-aol-any	AIM/AOL 即时通信工具	TCP	0	ffff0000
aol-msg	AOL 即时通信	TCP	0	0
ares_ft_udp_0	Ares_FT_udp	UDP	36	ffffffff
ares_ft_udp_1	Ares_FT_udp	UDP	40	ff000000
bearshare_download_tcp_0	BearShare_Download_tcp	TCP	0	ffffffff
bearshare_download_tcp_1	BearShare_Download_tcp	TCP	4	ffffffff
bearshare_request_file_udp_0	BearShare_Request_File_udp	UDP	0	ffffffff
bearshare_request_file_udp_1	BearShare_Request_File_udp	UDP	4	00ffffff
bittorrent_command_1_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_1_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_1_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_1_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_1_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_2_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_2_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_2_3	BitTorrent	TCP	12	ffffffff

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
bittorrent_command_2_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_5	BitTorrent	TCP	20	ffffffff
bittorrent_command_3_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_3_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_3_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_3_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_3_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_3_5	BitTorrent	TCP	20	ffff0000
bittorrent_command_4_0	BitTorrent	TCP	8	ffffff00
bittorrent_command_4_1	BitTorrent	TCP	11	ff000000
bittorrent_command_4_2	BitTorrent	TCP	11	ff000000
bittorrent_udp_1_0	BitTorrent_UDP_1	UDP	8	ffffff00
bittorrent_udp_1_1	BitTorrent_UDP_1	UDP	12	ffff0000
citrix-admin	Citrix 管理员	TCP	0	0
citrix-ica	Citrix ICA	TCP	0	0
citrix-ima	Citrix IMA	TCP	0	0
citrix-ma-client	Citrix MA 客户端	TCP	0	0
citrix-rtmp	Citrix RTMP	TCP	0	0
diameter	直径	TCP	0	0
directconnect_file_transfer_0	DirectConnect_File_transfer	TCP	0	ff000000
directconnect_file_transfer_1	DirectConnect_File_transfer	TCP	21	ffffffff
directconnect_file_transfer_2	DirectConnect_File_transfer	TCP	25	ffffffff
dns	DNS 会话	UDP	0	0
emule_tcp_file_request_0	eMule（电骡）	TCP	0	ff000000
emule_tcp_file_request_1	eMule（电骡）	TCP	4	ffff0000
emule_tcp_hello_message_0	eMule（电骡）	TCP	0	ff000000

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
emule_tcp_hello_message_1	eMule（电骡）	TCP	4	ffff0000
emule_tcp_secure_handshake_0	eMule（电骡）	TCP	0	ff000000
emule_tcp_secure_handshake_1	eMule（电骡）	TCP	4	ffff0000
ftp-session	FTP 会话	TCP	0	0
gnutella_tcp_1_0	Gnutella_TCP_1	TCP	0	ffffff00
gnutella_tcp_2_0	Gnutella_TCP_2	TCP	0	ffffffff
gnutella_tcp_2_1	Gnutella_TCP_2	TCP	4	ffffffff
gnutella_tcp_3_0	Gnutella_TCP_3	TCP	0	ffffff00
googletalk_ft_1_0	GoogleTalk_FT_1	UDP	24	ffffffff
googletalk_ft_1_1	GoogleTalk_FT_1	UDP	28	ffffffff
googletalk_ft_1_2	GoogleTalk_FT_1	UDP	32	ffffffff
googletalk_ft_1_3	GoogleTalk_FT_1	UDP	36	ffff0000
googletalk_ft_2_0	GoogleTalk_FT_2	UDP	24	ffffffff
googletalk_ft_2_1	GoogleTalk_FT_2	UDP	28	ffffffff
googletalk_ft_4_0	GoogleTalk_FT_4	UDP	67	ffffffff
googletalk_ft_4_1	GoogleTalk_FT_4	UDP	71	ffffffff
groove_command_1_0	Groove	TCP	6	ffffffff
groove_command_1_1	Groove	TCP	10	ffffffff
groove_command_1_2	Groove	TCP	14	ffffffff
groove_command_2_0	Groove	TCP	6	ffffffff
groove_command_2_1	Groove	TCP	10	ffff0000
groove_command_3_0	Groove	TCP	7	ffffffff
groove_command_3_1	Groove	TCP	11	ffffffff
groove_command_3_2	Groove	TCP	15	ffffffff
groove_command_3_3	Groove	TCP	19	ffffffff
h.225-session	H225 会话	TCP	0	0

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
hdc1	高位丢弃类 1	IP	1	fc000000
hdc2	高位丢弃类 2	IP	1	fc000000
hdc3	高位丢弃类 3	IP	1	fc000000
hdc4	高位丢弃类 4	IP	1	fc000000
http	万维网 HTTP	TCP	0	0
http-alt	HTTP 备用	TCP	0	0
https	HTTP over SSL	TCP	0	0
icecast_1	IceCast_Stream	TCP	0	ffffffff
icecast_2	IceCast_Stream	TCP	4	ffffffff
icecast_3	IceCast_Stream	TCP	8	ffff0000
icmp	ICMP	ICMP	0	0
icq	ICQ	TCP	0	0
icq_aol_ft_0	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_1	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_2	ICQ_AOL_FT	TCP	2	ffff0000
imap	互联网消息访问协议	TCP	0	0
imesh_download_tcp_0	iMesh_Download_tcp	TCP	0	ffffffff
imesh_download_tcp_1	iMesh_Download_tcp	TCP	4	ffffffff
imesh_request_file_udp_0	iMesh_Request_File_udp	UDP	0	ffffffff
imesh_request_file_udp_1	iMesh_Request_File_udp	UDP	4	00ffffff
ip	IP 流量	IP	0	0
itunesdaap_ft_0	iTunesDaap_FT	TCP	0	ffffffff
itunesdaap_ft_1	iTunesDaap_FT	TCP	4	ffffffff
itunesdaap_ft_2	iTunesDaap_FT	TCP	8	ffffff00
itunesdaap_ft_3	iTunesDaap_FT	TCP	2	ffff0000
kazaa_request_file_0	Kazaa_Request_File	TCP	0	ffffffff

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
kazaa_request_file_1	Kazaa_Request_File	TCP	4	ffffffff
kazaa_request_file_2	Kazaa_Request_File	TCP	8	ffff0000
kazaa_udp_packet_0	Kazaa_UDP_Packet	UDP	6	ffffffff
kazaa_udp_packet_1	Kazaa_UDP_Packet	UDP	4	ffff0000
ldap	LDAP	TCP	0	0
ldap	LDAP	TCP	0	0
ldc1	低位丢弃类 1	IP	1	fc000000
ldc2	低位丢弃类 2	IP	1	fc000000
ldc3	低位丢弃类 3	IP	1	fc000000
ldc4	低位丢弃类 4	IP	1	fc000000
lrp	负载报告协议	UDP	0	0
manolito_file_transfer_0_0	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_1	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_2	Manolito	TCP	0	ffffffff
manolito_file_transfer_1_0	Manolito	TCP	4	ff000000
manolito_file_transfer_1_1	Manolito	TCP	4	ff000000
manolito_file_transfer_2_0	Manolito	TCP	4	ff000000
manolito_file_transfer_2_1	Manolito	TCP	4	ff000000
mdc1	中位丢弃类 1	IP	1	fc000000
mdc2	中位丢弃类 2	IP	1	fc000000
mdc3	中位丢弃类 3	IP	1	fc000000
mdc4	中位丢弃类 4	IP	1	fc000000
meebo_get_0	MEEBO_GET	TCP	0	ffffffff
meebo_get_1	MEEBO_GET	TCP	4	ffffffff
meebo_get_2	MEEBO_GET	TCP	8	ffffffff
meebo_get_3	MEEBO_GET	TCP	12	ffffffff

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
meebo_get_4	MEEBO_GET	TCP	16	ffffffff
meebo_get_5	MEEBO_GET	TCP	20	ffffffff
meebo_get_6	MEEBO_GET	TCP	24	ffffffff
meebo_get_7	MEEBO_GET	TCP	28	ffffffff
meebo_get_8	MEEBO_GET	TCP	32	ff000000
meebo_post_0	MEEBO_POST	TCP	0	ffffffff
meebo_post_1	MEEBO_POST	TCP	4	ffffffff
meebo_post_2	MEEBO_POST	TCP	8	ffffffff
meebo_post_3	MEEBO_POST	TCP	12	ffffffff
meebo_post_4	MEEBO_POST	TCP	16	ffffffff
meebo_post_5	MEEBO_POST	TCP	20	ffffffff
meebo_post_6	MEEBO_POST	TCP	24	ffffffff
meebo_post_7	MEEBO_POST	TCP	28	ffffff00
msn-any	MSN Messenger 聊天	TCP	0	ffffffff
msn-msg	MSN Messenger 聊天	TCP	0	0
msn_msgr_ft_0	MSN_MSGR_FT	TCP	0	ffffffff
msn_msgr_ft_1	MSN_MSGR_FT	TCP	48	ffffffff
mssql-monitor	Microsoft SQL 流量监控	TCP	0	0
mssql-server	Microsoft SQL 服务器流量	TCP	0	0
nntp	网络新闻	TCP	0	0
nonip	非 IP 流量	NonIP	0	0
oracle-server1	Oracle 服务器	TCP	0	0
oracle-server2	Oracle 服务器	TCP	0	0
oracle-server3	Oracle 服务器	TCP	0	0
oracle-v1	Oracle SQL *Net 版本 1	TCP	0	0
oracle-v2	Oracle SQL *Net 版本 2	TCP	0	0

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
pop3	邮局协议第 3 版	TCP	0	0
prp	PRP	UDP	0	0
radius	RADIUS 协议	TCP	0	0
rexec	远程进程执行	TCP	0	0
rshell	远程外壳	TCP	0	0
rtp_ft_0	RTP_FT	UDP	0	ffff0000
rtp_ft_1	RTP_FT	UDP	0	ffff0000
rtp_ft_2	RTP_FT	UDP	16	ffff0000
rtsp	RTSP	TCP	0	0
sap	SAP	TCP	0	0
sctp	SCTP 流量	SCTP	0	0
skype-443-handshake	端口 443 的 Skype 签名	TCP	0	ff000000
skype-443-s-hello	端口 443 的 Skype 签名	TCP	11	ffffffff
skype-80-l-56	端口 80 的 Skype 签名	TCP	2	ffff0000
skype-80-proxy	端口 80 的 Skype 签名	TCP	0	ffffffff
skype-80-pshack	端口 80 的 Skype 签名	TCP	13	ff000000
skype-ext-l-54	Skype 签名	TCP	2	ffff0000
skype-ext-pshack	Skype 签名	TCP	13	ff000000
smtp	简单邮件传输协议	TCP	0	0
snmp	SNMP	UDP	0	0
snmp-trap	SNMP Trap	UDP	0	0
softethervpn443	SoftEther 以太网系统	TCP	0	ffffff00
softethervpn8888	SoftEther 以太网系统	TCP	0	ffffff00
soulseek_pierce_fw_0	SoulSeek_Pierce_FW	TCP	0	ffffffff
soulseek_pierce_fw_1	SoulSeek_Pierce_FW	TCP	4	ff000000
soulseek_pierce_fw_2	SoulSeek_Pierce_FW	TCP	2	ffff0000

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
ssh	安全外壳	TCP	0	0
tcp	TCP 流量	TCP	0	0
telnet	Telnet	TCP	0	0
tftp	简单文件传输协议	UDP	0	0
udp	UDP 流量	UDP	0	0
voip_sign_1	VOIP 签名	UDP	28	c03f0000
voip_sign_10	VOIP 签名	UDP	28	c03f0000
voip_sign_11	VOIP 签名	UDP	28	c03f0000
voip_sign_12	VOIP 签名	UDP	28	c03f0000
voip_sign_13	VOIP 签名	UDP	28	c03f0000
voip_sign_2	VOIP 签名	UDP	28	c03f0000
voip_sign_3	VOIP 签名	UDP	28	c03f0000
voip_sign_4	VOIP 签名	UDP	28	c03f0000
voip_sign_5	VOIP 签名	UDP	28	c03f0000
voip_sign_6	VOIP 签名	UDP	28	c03f0000
voip_sign_7	VOIP 签名	UDP	28	c03f0000
voip_sign_8	VOIP 签名	UDP	28	c03f0000
voip_sign_9	VOIP 签名	UDP	28	c03f0000
yahoo_ft_0	YAHOO_FT	TCP	0	ffffffff
yahoo_ft_1	YAHOO_FT	TCP	10	ffff0000
yahoo_get_0	YAHOO_GET	TCP	0	ffffffff
yahoo_get_1	YAHOO_GET	TCP	4	ffffffff
yahoo_get_2	YAHOO_GET	TCP	8	ffffffff
yahoo_get_3	YAHOO_GET	TCP	12	ffffffff
yahoo_get_4	YAHOO_GET	TCP	16	ff000000
yahoo_post_0	YAHOO_POST	TCP	0	ffffffff

表 171：预定义的基本过滤器（续）

名称	说明	协议	OMPC 偏移量	OMPC 掩码
yahoo_post_1	YAHOO_POST	TCP	4	ffffffff
yahoo_post_2	YAHOO_POST	TCP	8	ffffffff
yahoo_post_3	YAHOO_POST	TCP	12	ffffffff
yahoo_post_4	YAHOO_POST	TCP	16	ffff0000

附录 C - DefensePro 攻击保护 ID

此附录介绍 DefensePro 攻击保护 ID。

注意：本版本不支持下表中列出的所有保护。

表 172：DefensePro 攻击保护 ID

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
8	白名单	无				白名单遭遇不会被报告为安全事件。
9	黑名单	访问				黑名单访问违规。
70	网络泛洪 IPv4 UDP	行为 DoS				网络泛洪 IPv4 UDP。
71	网络泛洪 IPv4 ICMP	行为 DoS				网络泛洪 IPv4 ICMP。
72	网络泛洪 IPv4 IGMP	行为 DoS				网络泛洪 IPv4 IGMP。
73	网络泛洪 IPv4 TCP-SYN	行为 DoS				网络泛洪 IPv4 TCP，具有 SYN 标志。
74	网络泛洪 IPv4 TCP-RST	行为 DoS				网络泛洪 IPv4 TCP，具有 RST 标志。
75	网络泛洪 IPv4 TCP-ACK	行为 DoS				网络泛洪 IPv4 TCP，具有 ACK 标志。
76	网络泛洪 IPv4 TCP-PSH	行为 DoS				网络泛洪 IPv4 TCP，具有 PSH 标志。
77	网络泛洪 IPv4 TCP-FIN	行为 DoS				网络泛洪 IPv4 TCP，具有 FIN 标志。
78	网络泛洪 IPv4 TCP-SYN-ACK	行为 DoS				网络泛洪 IPv4 TCP，具有 SYN 和 ACK 标志。
79	网络泛洪 IPv4 TCP-FRAG	行为 DoS				网络泛洪 IPv4 TCP，具有 FRAG 标志。
80	网络泛洪 IPv6 UDP	行为 DoS				网络泛洪 IPv6 UDP。
81	网络泛洪 IPv6 ICMP	行为 DoS				网络泛洪 IPv6 ICMP。
82	网络泛洪 IPv6 IGMP	行为 DoS				网络泛洪 IPv6 IGMP。
83	网络泛洪 IPv6 TCP-SYN	行为 DoS				网络泛洪 IPv6 TCP，具有 SYN 标志。
84	网络泛洪 IPv6 TCP-RST	行为 DoS				网络泛洪 IPv6 TCP，具有 RST 标志。
85	网络泛洪 IPv6 TCP-ACK	行为 DoS				网络泛洪 IPv6 TCP，具有 ACK 标志。
86	网络泛洪 IPv6 TCP-PSH	行为 DoS				网络泛洪 IPv6 TCP，具有 PSH 标志。
87	网络泛洪 IPv6 TCP-FIN	行为 DoS				网络泛洪 IPv6 TCP，具有 FIN 标志。
88	网络泛洪 IPv6 TCP-SYN-ACK	行为 DoS				网络泛洪 IPv6 TCP，具有 SYN 和 ACK 标志。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
89	网络泛洪 IPv6 TCP-FRAG	行为 DoS				网络泛洪 IPv6 TCP，具有 FRAG 标志。
100	L2 格式无法识别	异常	低	无报告	处理	L2 格式无法识别。
103	IPv4 校验和不正确	异常	低	阻止	绕行	IPv4 校验和不正确。
104	IPv4 报头或总长度无效	异常	低	阻止	绕行	IPv4 报头或总长度无效。
105	TTL 少于或等于 1	异常	低 (Low)	报告	处理	TTL 小于或等于 1。
107	IPv6 报头不一致	异常	低	阻止	绕行	IPv6 报头不一致。
108	已达到 IPv6 跳数限制	异常	低 (Low)	报告	处理	已达到 IPv6 跳数限制。
110	L4 协议不受支持	异常	低 (Low)	无报告	处理	L4 协议不受支持。
112	TCP 报头长度无效	异常				（此异常保护仅在 DefensePro 5.11 和 5.12 中可用。） TCP 报头长度无效。
113	TCP 标记无效	异常	低	阻止	绕行	TCP 标志无效。
116	UDP 报头长度无效	异常				UDP 报头长度无效。
119	源或目标地址与本地主机相同	异常	低	阻止	绕行	源或目标 IP 地址与本地主机相同。
120	源地址与目标地址相同（LAND 攻击）	异常	低	阻止	绕行	源 IP 地址与目标 IP 地址相同（LAND 攻击）。 此签名的常见漏洞枚举器 (CVE) 为 CVE-1999-0016。
125	L4 源或目标端口为零	异常	低	阻止	绕行	第 4 层的源或目标端口为零。
131	L4 报头长度无效		低	阻止	绕行	L4 报头长度无效
150	HTTP 页面泛洪攻击	HttpFlood				HTTP 页面泛洪攻击。
240	TCP 州外	DoS				TCP 州外泛洪。
350	SCAN_TCP_SCAN	反扫描				TCP 扫描尝试。
351	SCAN_UDP_SCAN	反扫描				UDP 扫描尝试。
352	SCAN_ICMP_SCAN	反扫描				ICMP 扫描尝试。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
400	暴力 Web					暴力 Web 攻击企图突破受本地 HTTP 身份验证保护的站点内的受限区域。
401	Web 扫描					Web 漏洞扫描是一种信息收集攻击，通常先行于对已扫描的 Web 服务器的入侵攻击。攻击者试图通过发送不同类型的 HTTP 请求和分析服务器响应来收集 Web 服务器上的信息。这种情况下通常使用自动工具。
402	暴力 SMTP					暴力 SMTP 攻击企图突破受用户名和密码身份验证保护的 SMTP 邮件服务器上的受限帐户。
403	暴力 FTP					暴力 FTP 攻击企图突破受用户名和密码身份验证保护的 FTP 服务器上的受限帐户。
404	暴力 POP3					暴力 POP3 攻击企图突破受用户名和密码身份验证保护的 POP3 邮件服务器上的受限帐户。
405	暴力 SIP (UDP)					暴力 SIP (UDP) 攻击企图通过 UDP 突破 SIP 服务器（受用户名和密码身份验证保护）上的受限帐户。这种攻击也可以导致 SIP 服务器上发生注册泛洪。
406	暴力 SIP (TCP)					暴力 SIP (TCP) 攻击企图通过 TCP 突破 SIP 服务器（受用户名和密码身份验证保护）上的受限帐户。这种攻击也可以导致 SIP 服务器上发生注册泛洪。
407	暴力 MySQL					暴力 MySQL 攻击企图突破受用户名和密码身份验证保护的 MySQL 数据库服务器上受限的数据库帐户。
408	暴力 MSSQL					暴力 MSSQL 攻击企图突破受用户名和密码身份验证保护的 MSSQL 数据库服务器上受限的数据库帐户。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别（用于报告）	默认风险	默认操作	报告操作	说明
409	SIP 扫描 (UDP)					SIP 扫描攻击企图识别 SIP 服务器，以便发现漏洞或搜集服务器上现有的用户电话号码（也称为 SIP 用户或 SIP URI）。电话号码稍后可以用来发动 SPIT（SPAM over IP 电话）攻击。
410	SIP 扫描 (TCP)					SIP 扫描攻击企图识别 SIP 服务器，以便发现漏洞或搜集服务器上现有的用户电话号码（也称为 SIP 用户或 SIP URI）。电话号码稍后可以用来发动 SPIT（SPAM over IP 电话）攻击。
414	SIP 扫描 DST (TCP)					SIP 扫描攻击企图识别 SIP 服务器，以便发现漏洞或搜集服务器上现有的用户电话号码（也称为 SIP 用户或 SIP URI）。电话号码稍后可以用来发动 SPIT（SPAM over IP 电话）攻击。
416	暴力 SIP DST (TCP)					暴力 SIP DST (TCP) 攻击企图通过 TCP 突破 SIP 服务器（受用户名和密码身份验证保护）上的受限帐户。在源自服务器的会话上找到的错误响应中可检测到这种特定攻击。这种攻击也可以导致 SIP 服务器上发生注册泛洪。
417	暴力 SMB					暴力 SMB 攻击企图突破受用户名和密码身份验证保护的 SMB（文件共享）服务器上的受限帐户。
418	暴力 SIP DST (UDP)					暴力 SIP DST (UDP) 攻击企图通过 UDP 突破 SIP 服务器（受用户名和密码身份验证保护）上的受限帐户。在源自服务器的会话上找到的错误响应中可检测到这种特定攻击。这种攻击也可以导致 SIP 服务器上发生注册泛洪。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
419	SIP 扫描 DST (UDP)					SIP 扫描攻击企图识别 SIP 服务器，以便发现漏洞或搜集服务器上现有的用户电话号码（也称为 SIP 用户或 SIP URI）。电话号码稍后可以用来发动 SPIT（SPAM over IP 电话）攻击。
450	DNS 泛洪 IPv4 DNS-A	DNS 保护				DNS A 通过 IPv4 实现查询泛洪。
451	DNS 泛洪 IPv4 DNS-MX	DNS 保护				DNS MX 通过 IPv4 实现查询泛洪。
452	DNS 泛洪 IPv4 DNS-PTR	DNS 保护				DNS PTR 通过 IPv4 实现查询泛洪。
453	DNS 泛洪 IPv4 DNS-AAAA	DNS 保护				DNS AAAA 通过 IPv4 实现查询泛洪。
454	DNS 泛洪 IPv4 DNS 文本	DNS 保护				DNS 通过 IPv4 文本实现查询泛洪。
455	DNS 泛洪 IPv4 DNS-SOA	DNS 保护				DNS SOA 通过 IPv4 实现查询泛洪。
456	DNS 泛洪 IPv4 DNS-NAPTR	DNS 保护				DNS NAPTR 通过 IPv4 实现查询泛洪。
457	DNS 泛洪 IPv4 DNS-SRV	DNS 保护				DNS SRV 通过 IPv4 实现查询泛洪。
458	DNS 泛洪 IPv4 DNS 其他	DNS 保护				DNS 通过 IPv4 其他实现查询泛洪。
459	DNS 泛洪 IPv4 DNS-ALL	DNS 保护				DNS 通过 IPv4 实现查询泛洪。
460	DNS 泛洪 IPv6 DNS-A	DNS 保护				DNS A 通过 IPv6 实现查询泛洪。
461	DNS 泛洪 IPv6 DNS-MX	DNS 保护				DNS MX 通过 IPv6 实现查询泛洪。
462	DNS 泛洪 IPv6 DNS-PTR	DNS 保护				DNS PTR 通过 IPv6 实现查询泛洪。
463	DNS 泛洪 IPv6 DNS-AAAA	DNS 保护				DNS AAAA 通过 IPv6 实现查询泛洪。
464	DNS 泛洪 IPv6 DNS 文本	DNS 保护				DNS 文本通过 IPv6 实现查询泛洪。
465	DNS 泛洪 IPv6 DNS-SOA	DNS 保护				DNS SOA 通过 IPv6 实现查询泛洪。
466	DNS 泛洪 IPv6 DNS-NAPTR	DNS 保护				DNS NAPTR 通过 IPv6 实现查询泛洪。
467	DNS 泛洪 IPv6 DNS-SRV	DNS 保护				DNS SRV 通过 IPv6 实现查询泛洪。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
468	DNS 泛洪 IPv6 DNS 其他	DNS 保护				DNS 其他通过 IPv6 实现查询泛洪。
469	DNS 泛洪 IPv6 DNS-ALL	DNS 保护				DNS 通过 IPv6 实现查询泛洪。
720	SYN 泛洪保护		高	根据策略操作		根据保护策略开始、正在发生和终止攻击。
721	已启用 SYN 泛洪的保护		高 (High)	根据策略操作		当相对于首个 ACK/Data 数据包速率，SYN 速率大于每秒 1000 个数据包时正在传送的消息。
722	SYN 泛洪保护全表		中	根据策略操作		（此事件不会在5.10 及更高版本中生成。） 用于 DefensePro 的会话表保护。
723	SYN ACK 反射保护		高 (High)	根据策略操作		（此事件不会在5.10 及更高版本中生成。） 用于 SARP（SYN ACK 反射保护）。
724	SYN 保护删除分段		信息	根据策略操作		当分段的数据包在身份验证过程中到达时使用。数据包将被丢弃。
725	SYN 保护删除重置		信息	根据策略操作		当与现有会话不匹配的 RESET 数据包在身份验证过程中到达时使用。数据包将被丢弃。
726	SYN 保护脱离情景		信息 (Info)	根据策略操作		（此事件不会在5.10 及更高版本中生成。）当与现有会话不匹配的数据包在身份验证过程中到达时使用。将删除数据包，并将向源发送 RESET。
727	SYN 保护全表		中	根据策略操作		当“SYN 保护”(SYN Protection) 表已满并且模块无法处理更多并发身份验证过程时使用。只要该表已满，就会丢弃新验证的 ACK（或数据）数据包。
729	SYN 保护脱离情景		信息 (Info)	根据策略操作		当与现有会话不匹配的数据包在身份验证过程中到达时使用。将删除数据包，并将向源发送 RESET。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别（用于报告）	默认风险	默认操作	报告操作	说明
730	SYN 保护未验证 cookie		信息 (Info)	丢弃		当带有 SYN cookie（与 DefensePro 设备发送的 cookie 不匹配）的 ACK 数据包到达时使用。 仅当策略配置有“阻止并报告”(Block and Report) 时才生成此错误。
731	SYN 保护不完全		信息 (Info)	丢弃		（在 5.1x 之前的版本中此事件不相关）。当新会话在首个数据包到达之前的身份验证过程中老化时使用。
732	SYN 保护删除错误的 TCP		信息 (Info)	丢弃		当意外数据包或带有非法 TCP 标志的数据包在身份验证过程中到达时使用。数据包将被丢弃。
740	TCP 会话被丢弃	状态 ACL	高 (High)	丢弃		匹配 ACL 策略的流量报告。
741	TCP 会话得到允许	状态 ACL	信息 (Info)	转发		匹配 ACL 策略的流量报告。
742	UDP 会话被丢弃	状态 ACL	高 (High)	丢弃		匹配 ACL 策略的流量报告。
743	UDP 会话得到允许	状态 ACL	信息 (Info)	转发		匹配 ACL 规则的流量策略
744	ICMP 会话被丢弃	状态 ACL	高 (High)	丢弃		匹配 ACL 策略的流量报告。
745	ICMP 会话得到允许	状态 ACL	信息 (Info)	转发		匹配 ACL 策略的流量报告。
746	IP 会话被丢弃	状态 ACL	高	丢弃		与 ACL 中未明确支持的 ACL 策略相匹配的 IP 流量报告（即*非*诸如 TCP、UDP、ICMP、IGMP、SCTP 或支持的隧道协议的流量）。
747	IP 会话得到允许	状态 ACL	信息 (Info)	转发		与 ACL 中未明确支持的 ACL 策略相匹配的 IP 流量报告（即*非*诸如 TCP、UDP、ICMP、IGMP、SCTP 或支持的隧道协议的流量）。
748	TCP 中速流数据包	状态 ACL	中	丢弃		匹配 ACL 策略的流量报告。
749	TCP 无效重置	状态 ACL	中 (Medium)	丢弃		匹配 ACL 策略的流量报告。
750	TCP 握手违规	状态 ACL	中 (Medium)	丢弃		匹配 ACL 策略的流量报告。
751	ICMP Smurf 数据包	状态 ACL	中 (Medium)	丢弃		匹配 ACL 策略的流量报告。

表 172：DefensePro 攻击保护 ID（续）

ID 编号或范围	攻击保护名称	类别 （用于报告）	默认风险	默认操作	报告操作	说明
752	ICMP 数据包异常	状态 ACL	中	丢弃		匹配 ACL 策略的流量报告。
753	GRE 会话被丢弃	状态 ACL	高 (High)	丢弃		匹配 ACL 策略的流量报告。
754	GRE 会话得到允许	状态 ACL	信息 (Info)	转发		匹配 ACL 策略的流量报告。
755	SCTP 会话被丢弃	状态 ACL	高 (High)	丢弃		匹配 ACL 策略的流量报告。
756	SCTP 会话得到允许	状态 ACL	信息 (Info)	转发		匹配 ACL 策略的流量报告。
1,000 - 100,000	DoS 屏蔽签名或入侵保护签名	DoS				签名的范围，来自安全操作中心 (SOC) 签名文件。奇数 ID 号码为 DoS 屏蔽签名。偶数 ID 编号为入侵签名。
200000	HTTP	SynFlood	中	根据策略操作		预定义的 HTTP SYN 泛洪攻击保护。
200,001	HTTPS	SynFlood	中 (Medium)	根据策略操作		预定义的 HTTPS SYN 泛洪攻击保护。
200,002	RTSP	SynFlood	中 (Medium)	根据策略操作		预定义的 RTSP SYN 泛洪攻击保护。
200,003	FTP_CTRL	SynFlood	中 (Medium)	根据策略操作		预定义的 FTP_CTRL SYN 泛洪攻击保护。
200,004	POP3	SynFlood	中 (Medium)	根据策略操作		预定义的 POP3 SYN 泛洪攻击保护。
200,005	IMAP	SynFlood	中 (Medium)	根据策略操作		预定义的 IMAP SYN 泛洪攻击保护。
200,006	SMTP	SynFlood	中 (Medium)	根据策略操作		预定义的 SMTP SYN 泛洪攻击保护。
200,007	TELNET	SynFlood	中 (Medium)	根据策略操作		预定义的 TELNET SYN 泛洪攻击保护。
200,008	RPC	SynFlood	中 (Medium)	根据策略操作		预定义的 RPC SYN 泛洪攻击保护。
300,000 - 449,999	用户定义的自定义签名	DoS				用户定义的保护的范围。当用户创建签名时，设备按次序生成 ID 编号。
450,000 - 475,000	用户定义的连接限制保护	DoS				用户定义的连接限制保护的范围。当用户创建保护时，设备按次序生成 ID 编号。
500,000 - 599,999	用户定义的 SYN 泛洪保护	SYNFlood	低 (Low)	根据策略操作		用户定义的 SYN 泛洪保护的服务。当用户创建保护时，设备按次序生成 ID 编号。
600,000 - 675,000	用户定义的连接 PPS 限制保护	DoS				用户定义的连接 PPS 限制保护的范围。当用户创建保护时，设备按次序生成 ID 编号。

附录 D - DefensePro 支持的协议

本附录列出 DefensePro 签名可以保护的协议和操作系统。DefensePro 签名可以保护以下协议：

- BGP
- BOOTP
- Borland Interbase 协议
- CA 许可证客户端协议
- CVS
- DCERPC
- DHCP
- DNP3 (SCADA)
- DNS
- EIGRP
- Finger
- FTP
- HTTP
- HTTPS
- ICCP (SCADA)
- ICMP
- Ident
- IGAP
- IGMP
- IP
- IPP
- IRC
- ISAKMP
- LDAP
- LPR
- MaxDB
- MODBUS (SCADA)
- Motorola Timbuktu
- NBT
- NDAP
- NDMP
- NetBIOS
- NetFlow
- NFS
- NHRP
- NMAP
- NNTP
- Ntalk
- NTP
- ORACLE
- Overnet
- PCAnywhere
- POP2
- POP3
- PP
- RADIUS
- RDP
- Retrospect
- RFB (VNC)
- RIP
- Rlogin
- RTSP
- SCCP (SKINNY)
- SCTP
- 安全 IMAP
- 安全 SMTP
- SIP
- SMB
- SMS 远程控制
- SMTP
- SNMP
- SOAP
- SOCKS4
- SOCKS5
- SQL
- SSH
- SSL
- SUN-RPC
- TACACS
- TCP
- TELNET
- TFTP
- UDP
- UPNP
- WebDAV
- WHOIS
- Winny
- WINS
- XDMCP

DefensePro 签名可以保护以下操作系统：

- 3COM
- Cisco
- Juniper
- Linux
- MAC OS
- MS Windows

DefensePro 支持的协议

- MS Windows 服务器
- Unix

附录 E - 故障排除

如果设备无法预期运行，您可以对系统进行诊断或向 Radware 技术支持部门提供相关信息。

关于硬件相关问题的故障排除，请咨询思科技术支持部门。本附录包含以下小节：技术支持文件，第 231 页。

技术支持文件

DefensePro 设备可以生成技术支持文件，您可以将其保存到指定位置，并将其发送给 Radware 技术支持部门协助诊断问题。

使用 CLI，可以看到技术支持文件包括以下内容：

- **Radware 技术支持部门通常需要用来诊断 DefensePro 设备问题的数据** - 数据包括收集到的来自各类 CLI 命令的输出。
- **（通过任何管理界面）对设备所做的每项配置更改的记录** - 当设备收到其第一个命令时，即开始存储这些记录。记录按日期以升序排序。如果数据大小超过允许的最大值 (2 MB)，则最早的记录会被覆盖。除非您擦除设备配置，否则整个数据始终不会被清除。
- **dp_support.txt** - 包含 Radware 技术支持部门通常需要用来诊断 DefensePro 设备问题的数据。数据包括收集到的来自各类 CLI 命令的输出。
- **auditLog.log** - 包含（通过任何管理界面）对设备所做的每项配置更改的记录。当设备收到其第一个命令时，即开始存储这些记录。记录按日期以升序排序。如果数据大小超过允许的最大值 (2 MB)，则最早的记录会被覆盖。除非您擦除设备配置，否则整个数据始终不会被清除。

  auditLog.log 文件中每个记录的结构如下：

  <dd>-<MM>-<yyyy> <hh>:<mm>:<ss> <事件描述>

  示例：

  2009 年 6 月 12 日 19:16:11 命令：用户 radware 通过控制台“注销”
- HTTPFLD.tar - 包含 HTTP 泛洪的数据。
- NTFLD.tar - 包含网络泛洪的数据。

要使用 CLI 在终端上生成并显示技术支持文件的输出

> 请输入以下命令：

manage support display

故障排除

要使用 CLI 生成技术支持文件并将其发送到 TFTP 服务器

> 请输入以下命令：

manage support tftp put <文件名> <TFTP 服务器 IP 地址> [-v]

其中：

-v 也可以显示命令输出。

要使用基于 Web 的管理来生成和下载技术支持文件

1. 依次选择**文件 (File) > 支持 (Support)**。系统会显示*下载技术支持信息文件 (Download Tech Support Info File)* 窗格。
2. 点击**设置 (Set)**。随后会打开*文件下载 (File Download)* 对话框。
3. 点击**打开 (Open)** 或**保存 (Save)** 并指定所需信息。

附录 F - 术语表

此术语表是用于 Radware 技术环境中的术语和定义的列表。某些词汇属于公共域，而某些则为 Radware 特定词汇，但所有这些词汇均用于 Radware 文档之中。

Radware 术语表旨在作为 Radware 技术环境中所用的专有词汇及其定义的列表。某些词汇属于公共域，而某些则为 Radware 特定词汇，但所有这些词汇均用于印刷版和在线版的 Radware 文档之中。

表 173：术语表

术语	定义
DDoS	DNS 服务器上的分布式拒绝服务攻击。典型的攻击涉及发送欺骗性域名请求到 DNS 服务器的大量受危害的僵尸系统（僵尸网络），处理“合法”请求并向受欺骗的受害者发送应答。 当 DNS 服务器配置为提供递归查询时，如果被请求的域名本地不可用，则 DNS 服务器将查询 IP 地址的根域名服务器。接着，流量会穿越 Internet 主干，影响互联网服务提供商以及任何上游提供商达到预定目标。 Radware 的基于适应行为的 DoS 保护获知 DNS 流量的特征，并重新建立正常的流量行为基准。基于模糊逻辑的嵌入式决策引擎会持续分析 DNS 流量，并检测何时发生偏离正常基准。检测时，系统会执行可疑 DNS 数据包的深度分析，以便识别数据包报头和负载中参数的反常表现。
DoS	拒绝服务是一种攻击，目的在于消耗系统资源并制造暂时性服务丧失。
IP 接口	DefensePro 中的 IP 接口由两个组件构成：IP 地址和关联的接口。关联的接口可以是物理接口或虚拟接口 (VLAN)。IP 路由在 DefensePro IP 接口之间执行，而桥接则在包含 IP 地址（与 VLAN 关联）的 IP 接口内执行。 DefensePro 被设计为拦截 HTTP 请求，并将这些请求重定向至内容检测服务器群。设计 DefensePro 网络的首个设想是 DefensePro 设备处于客户端与互联网以及内容检测服务器之间的路径上。这之所以必要，是因为 DefensePro 需要拦截客户端发往互联网的请求，并处理从内容检测服务器返回到客户端的数据包。 除使用本地三角测量时，所有流量必须确实通过 DefensePro 设备。这包括从用户去往互联网的流量以及从内容检测服务器群返回到用户的流量。 如果用户被静态配置为使用内容检测服务器，则用户应配置到 DefensePro 虚拟地址。此地址为内容检测服务器的访问 IP 地址。此地址仅用于经静态配置的用户。
NHR	下一跳路由器 (NHR) 是具有 IP 地址的网络元素，流量通过它进行路由。

表 173：术语表（续）

术语	定义
SYN cookie	SYN cookies 是 TCP 服务器对初始 TCP 序列号的特定选择。服务器的初始序列号与客户端的初始序列号之间的差异在于： ● 前 5 位：t mod 32，其中 t 为每 64 秒增加一次的 32 位计时器。 ● 下 3 位：由服务器选择的 MSS 编码以响应客户端的 MSS。 ● 最后 24 位：客户端 IP 地址和端口号、服务器 IP 地址和端口号，以及 t 的由服务器选择的密钥功能。 选择这种序列号符合序列号缓慢增加的基本 TCP 要求；相比客户端的初始序列号，服务器的初始序列号增加略快。 使用 SYN cookie 的服务器在其 SYN 队列已满时不需要丢弃连接。相反，它会发回 SYN+ACK，就像是 SYN 队列曾经更大。（例外情况：服务器必须拒绝例如大窗口的 TCP 选项，并且必须使用其可编码的八个 MSS 值之一。）当服务器收到 ACK 时，其会检查密钥功能是否对 t 的最近值有效，接着从编码的 MSS 重建 SYN 查询条目。 SYN 泛洪只是来自伪造 IP 地址的一系列 SYN 数据包。IP 地址是随机选择的，不会提供攻击者所在位置的任何提示。SYN 泛洪使服务器的 SYN 队列保持已满状态。通常这会强制服务器丢弃连接。但使用 SYN cookie 的服务器将继续正常运行。SYN 泛洪的最大影响是禁用大窗口。
SYN 泛洪	SYN 攻击/泛洪是 DoS（拒绝服务）攻击的一种类型。通过发送 SYN 数据包但不完成 TCP 三次握手而执行 SYN 泛洪攻击，称为单包攻击。或者，虽然完成 TCP 三次握手，但之后并未发送任何数据包。此类攻击也称为连接泛洪攻击。 SYN 数据包会通知服务器存在新连接。接着，服务器会分配一些内存以便处理传入连接，发回确认信息，然后等待客户端完成连接并开始发送数据。通过欺骗大量 SYN 请求，攻击者可以耗尽服务器内存，而服务器则在等待更多无法达到的数据。一旦内存耗尽，服务器就无法接受来自合法客户端的连接。这会有效地禁用服务器。要点：SYN 泛洪会利用 TCP/IP 技术本身的核心缺陷。针对此攻击并无完备的防御。但是存在部分防御手段。服务器可以配置为保留更多内存，并减少其等待连接完成的时间。 同样地，路由器和防火墙可以过滤出某些受欺骗的 SYN 数据包。最后，某些技术（例如“SYN cookie”）可以巧妙运用协议以协助区分良好 SYN 和不良 SYN。
SYN-ACK 反射攻击防御	SYN-ACK 反射攻击防御旨在防范 SYN 攻击的反射，并减少为响应 DoS 攻击而创建的 SYN-ACK 数据包风暴。 当设备遭受 SYN 攻击时，其会发送带有嵌入式 Cookie 的 SYN-ACK 数据包，以便提示客户端继续会话。
病毒	病毒是一种恶意程序代码，其编写目的在于损害计算机系统，并对自身进行复制以扩大可能的损害范围。
服务	提供防御一系列攻击的功能。
服务器，报告	报告服务器是负责运行必需服务以将向最终用户显示报告的组件。它可以包含 Web 服务器并同时为 Eclipse 和网络界面提供服务。
攻击	以大写字母“A”表示的攻击是威胁的实现形式，是针对网络、主机或服务器而采取的恶意行为。
攻击列表	攻击列表是“签名数据库”(Signatures Database) 中定义的已知攻击者的数据库。
攻击签名数据库	Radware 的攻击签名数据库包含已知攻击的签名。 这些签名包括在由 Radware 提供的预定义组和配置文件中，以便在“连接和保护表”(Connect and Protect Table) 中创建策略。每个攻击组包括具有常规特征的攻击签名，旨在保护特定应用或 IP 地址范围。

表 173：术语表（续）

术语	定义
行为 DoS (BDoS)	行为 DoS (行为拒绝服务) 保护为网络防御零日网络泛洪攻击，这种攻击会使用具有欺骗性的流量阻塞可用的网络带宽，拒绝合法用户使用网络资源。 BDoS 配置文件可通过识别异常流量的足迹来达成此目的。网络泛洪保护类型包括： ● SYN 泛洪 ● TCP 泛洪，包括 TCP Fin + Ack 泛洪、TCP 重置泛洪 ● TCP Syn + Ack 泛洪、TCP 分段泛洪 ● UDP 泛洪 ● ICMP 泛洪 ● IGMP 泛洪
检测端口	检测端口是您可对其配置以接收、检测和传输流量的 DefensePro 设备上的端口。
零日攻击	零日攻击 (0day) 是一种漏洞攻击，除发现者外没有人了解这种漏洞。 零日漏洞是针对非公开的未知漏洞的攻击。由于不存在已知的签名，零日漏洞攻击能够穿透任何基于签名的安全防御。如果漏洞攻击通过常见端口且无其他防御（例如基于行为或基于影响的技术），那么这种漏洞攻击就难以阻止。
漏洞	漏洞是利用软件漏洞的程序或技术。 这种程序可以用于破坏安全或其他方式攻击网络上的主机。
欺骗	欺骗是指一个系统实体冒充或承担其他实体的身份。
启发式分析	启发式分析是基于行为的分析，旨在提供可阻止异常现象的过滤器。 启发式分析是病毒扫描程序的功能，通过分析程序的行为而不是查找已知的病毒签名来识别潜在的病毒。
签名	签名是基于模式的分析，用于搜索由已知攻击工具生成的数据包。
蠕虫	蠕虫是一种计算机病毒，利用互联网或本地网络通过将自身的副本发送到其他主机来进行扩散。
入侵	入侵是以未经授权的方式尝试性地或成功地访问系统资源。
入侵防御	入侵防御是一种安全服务，扫描、检测和防范危害系统安全的实时尝试。
入侵检测系统 (IDS)	Radware 的入侵检测系统 (IDS) 应用了最新的安全或攻击专业知识，从数量更多的合法活动中过滤出潜在的破坏性/恶意事件。 存在两种系统监控方法： ● NIDS - 基于网络的 IDS - 监控安装代理的网段上传输的所有网络流量，对可疑的异常活动和基于签名的活动发挥作用。 ● HIDS - 基于主机的 IDS - 限于本地主机，并可详细地监控活动，例如，命令执行、文件访问或系统调用。 组织通常会选择根据已知漏洞结合使用这些方法。

表 173：术语表（续）

术语	定义
深度数据包检测	与仅检测数据包报头不同，会检测数据包负载。这可使安全设备在应用级别执行检测。
特洛伊木马	特洛伊木马（也称为*木马 (Trojan)*）一种计算机程序，看似良性，但其实际上被设计为损害或危害系统。 通常，木马被设计为绕过安全监控和审计策略，提供对内部系统不受限制的访问。
威胁	互联网安全术语中的威胁是指对资产构成危害的个人、事物、事件或想法。 最基本的威胁可以是以下任何内容：信息泄露、拒绝服务、完整性遭破坏以及非法使用。
异常	异常是流量模式或协议的反常或意外行为。

Radware Ltd. 最终用户许可协议

通过接受此最终用户许可协议（以下简称“许可协议”），您同意 Radware Ltd.（以下简称“Radware”）销售人员与您取得联系。

如果您希望收到的许可权利不同于下文所授予的权利，或者希望获得的保修或支持服务超出本协议所规定的范围（如果有），请联系 Radware 的销售团队。

针对 RADWARE 开发和/或分销的所有软件以及在许可授予期间向您提供的软件的所有升级、修正版本、更新、添加和副本（以下简称“软件”），您对上述内容的使用均适用本许可协议。无论软件是作为 RADWARE 产品（以下简称“产品”）的嵌入组件，还是作为独立软件产品提供给您的，均将适用本许可协议。为避免疑义，特此明确如下：本许可协议适用于 RADWARE 开发的、能够将 RADWARE 产品连接或集成到第三方产品的插件、连接器或扩展件和相似的软件组件（以下统称“连接器”），上述组件可以提供、停用、管理、配置或监控 RADWARE 产品。无论这些连接器是由 RADWARE 还是第三方产品供应商分销给您，本许可协议均将进行适用。如果连接器是根据您与第三方产品供应商之间协议的条款而由该供应商分销给您的，那么就 RADWARE 和您而言，如果在本许可协议条款以及您与和第三方产品供应商签订的协议条款之间存在任何的差异或不一致，那么将适用本许可协议的条款，并以之为准。在打开 RADWARE 产品包之前，或者在下载、安装、复制或以其他方式使用 RADWARE 的独立软件之前（如果适用），请仔细阅读本许可协议中的条款和条件。本软件为许可版本（不供销售）。如果您打开 RADWARE 产品包，或下载、安装、复制或使用软件（如适用），即表明您确认已经阅读并了解本许可协议，并且同意受本许可协议条款的约束。此外，如果您主张上文中所表明的接受行为并不相当于（或被认为）对本许可协议的有效签字，那么您在此放弃由此而可能享有的所有索赔或权利。如果您不愿受到本许可协议条款的约束，您应及时返还尚未打开的产品包，或者您不应下载、安装、复制或以其他方式使用本软件（如果适用）。本许可协议代表您和 RADWARE 之间就本软件所签订的全部协议，并取代双方之前所有的建议书、声明或谅解书。“您”是指同意接受本许可协议约束的自然人或实体，以及他们的员工和第三方承包商。如果上述员工和第三方承包商未遵守本许可协议的条款，您应当对上述所有的违约行为承担责任。

1. **许可授予**。在符合本协议条款规定的情况下，Radware 特此授予您（同时您接受）一项有限、非独占、不可转让的许可，以便您只能出于自身内部业务目的以及仅以机器可读、目标代码的形式安装和使用本软件（以下简称“商业许可”）。如果向您发布本软件的同时随附软件开发套件 （“SDK”），那么仅仅就 SDK 而言，上文的商业许可也包括一项有限、非独占、不可转让的许可，以便您只能在贵组织内部的电脑上安装和使用 SDK，并且只能通过您自身所有的、由您许可和/或控制的软件或硬件产品，仅出于您内部开发目的而将本软件和/或其他 Radware 产品进行集成或实现交互操作（“SDK 目的”）。如果向您发布 SDK 的同时还以源码的格式向您提供代码样本（以下简称“代码样本”），旨在向您说明和教授如何对本软件和/或任何其他 Radware 产品进行配置、监控和/或控制，则上文的本商业许可进一步包括一项有限、非独占、不可转让的许可，以便仅出于 SDK 目的以及仅在贵组织内部的电脑上复制和修改本代码样本，并据此制作衍生品。出于本许可协议的全部目的，均应将 SDK 视为术语“软件”的一部分。您同意，您不会根据本许可协议销售、分配、许可、再许可、转让、质押、租用、租赁或共享您的权利，也不会分销本软件的副本或其中的任何部分。此处未经明确授予的权利，即为明确禁止。
2. **评估用途**。即便本许可协议有任何相反的规定，如果如您的采购订单或销售收据所表明，向您提供本软件是出于评估目的，并且在您下载软件的网站上，向您提供任何的限时评估许可密钥，从而可以激活软件，那么您仅仅可以出于内部评估之目的（“评估使用”）使用本软件，使用时间最长为 30 天，或者在上述期间内，根据 Radware 的全权决定，以书面列明的方式使用该软件。在评估期间届满后，包含相关功能的软件评估副本将自动禁用。您同意不会禁用、破坏或删除软件的相关功能，并且，任何试图执行上述操作的行为均会严重违反本许可协议。在评估期期内（或评估期间结束时），您可以联系 Radware 销售团队以购买一份商业许可从而根据本许可协议条款继续使用本软件。如果您决定不购买商业许可，那么您同意停止使用本软件，并且将您所收到的，在评估期间届满时处于您占有或控制下的所有计算机上的评估副本进行删除。无论如何，在评估期间届满之后如果您继续使用本软件（如可能），那么将视为您基于本许可协议的条款接受本软件的商业许可，并且您同意就任何适用的许可费，按照 Radware 当时的价目表向 Radware 支付所有应付的金额。
3. **订用软件**。如果您在订用的基础上获得软件的许可，那么对软件的使用权利只限于订用期间。您可选择延长您的订用期间。如果您延长订用期间，那么您可以继续使用本软件，直到延长的订用期间届满。如果您在您的订用期间届满后，您未延长订用期间，那么您就负有相应的法律义务以停止使用本软件并将其从您的系统中彻底删除。

4. **反馈**。您向 Radware 提供的有关软件的所有反馈，包括但不限于发现潜在错误和改进，推荐更改或建议（以下简称“反馈”），将由 Radware 专属拥有并视为 Radware 的机密信息。向 Radware 提供反馈，即表明您将上述任何反馈里的所有权利、所有权和利益（包括其中所有的知识产权）均转让给 Radware。如果根据适用的法律，上述反馈中存在不能转让给 Radware 的权利，那么针对上述所有权利，您在此不可撤销地为 Radware 放弃这些权利，并且基于反馈里的上述权利，授予 Radware 一项世界范围的、永久性免版税、不可撤销、可以再许可的和非独占性的许可，从而可以无限制地使用、复制、公布、再许可、修改、制作、允许他人制作、分销、销售，代销、展示、执行、制作衍生作品以及通过其他方式进行利用。在本协议终止或到期后第 4 部分的条款仍将继续有效。

5. **使用限制**。您同意不将：(a) 基于本软件复制、修改、转换、改编或制作任何衍生作品；或 (b) 对软件进行再许可或转让，或者将本软件或其任何部分纳入任何产品中；或 (c) 全部或部分地对本软件进行反向组合、反汇编、反编译、反向工程或尝试获取源码（或基础创意、算法、结构、组织），另外如果在法律允许实施的上述任何行为的所有实例里，在您知晓上述行为得到批准和许可的至少九十 (90) 天内向 Radware 提供书面通知，从而为 Radware 提供相关的机会以评估根据法律的要求是否有必要实施上述行为；或 (d) 以违反软件技术限制的方式，创建、开发、许可、安装、使用或部署任何软件或服务从而避免、启用、修改或提供访问、许可或权利；或 (e) 如果软件是作为另一个 Radware 产品的嵌入组件或捆绑组件而提供的，则除了将其作为组合产品的一部分（和处于组合的产品的既定目的）进行使用以外，您不得以其他方式使用本软件；(f) 从软件中删除所有的版权声明、识别或其他任何专有通知，包括第三方软件（定义见下文）的任何通知；或 (g) 将软件复制到在任何公共或分布式网络上，或者在分时式、外包的服务中心、应用运营商或托管服务提供商环境里（或作为此种机构）运行该软件。尽管有第 5 部分 (e) 的规定，但是如果您为客户提供托管或云计算服务，那么您有权在提供服务的 IT 基础设施里使用和纳入本软件。在此申明，对 Radware 提供的所有软件进行修改或基于此制作衍生作品的禁止性规定，无论该软件系在计算机里或者以用户可读的形式而提供的均将适用此项规定。在此确认，如果以用户可读的形式提供示例，则用户可以对其进行修改。

6. **知识产权**。您确认并同意，本许可协议除了向您转让使用本软件的有限权利之外，未将本软件里的任何利益转让给您，并且本软件的所有权利、所有权和利益（包括所有相关的知识产权）属于（并将继续属于） Radware 或其第三方授权人。您进一步确认并同意，本软件是 Radware 和/或其许可人的专有产品，并且受到适用的版权法的保护。

7. **无保证**。本软件和所有随附的软件、文件、库、数据和材料，均由 Radware 或第三方许可人（如适用）按照“原样”分销和提供，并且没有任何形式（无论明示或暗示）的保证，包括但不限于不侵权保证、适销性保证或适用于特定用途的保证。就软件的所有权、软件的使用或是由结果，Radware 及其附属公司或许可人均未保证、担保或做出任何声明。Radware 及其任何附属公司、许可人均未保证，软件的运行不会遭到中断或不发生错误，或者任何密码、许可密钥和/或加密功能能够有效防止任何文件里包含的信息免受无意的披露。您确认，良好的数据处理过程要求，在任何依赖于它采取行动之前，必须使用非关键数据来对程序（包括本软件）进行全面的测试，并且针对所有的本许可覆盖下的软件副本之使用，您将对此承担所有的风险。针对第三方供应商或其他软件组件提供的，与本软件兼容的所有操作系统、数据库、迁移工具或其他任何软件组件，Radware 不做出任何声明或担保，亦不承担任何责任或义务，或提供任何许可或技术维护和支持。

   此项保证的免责声明是本许可的重要和实质性的组成部分。

   除了上述对保证的免责声明之外，如果基于任何保证条款，Radware 附有责任，但是引致责任的原因是软件遭到滥用、疏忽、意外或不正确的安装，或者通过 Radware 授权服务人员以外的其他人进行维修或修复，那么 Radware 对此不承担任何责任。

8. **责任限制**。除非适用的制定法明确进行禁止，否则在任何情况下 Radware 及其负责人、股东、高级管理人员、员工、子公司、许可人、承包商、附属公司或母组织（以下统称“Radware 方”），针对与软件的使用或无法使用有关的或者您和 Radware 或任何 Radware 方之间的关系而相关的任何事项（包括但不限于数据或信息丢失或披露，和/或利润、收入、商机或业务优势的丧失，和/或业务中断）所导致的任何直接、间接、偶然、必然、特殊或惩罚性损害赔偿，上述人员均不承担责任，而无论相关的损害赔偿是基于合同、保证、过失、严格责任、责任分担、赔偿或其他任何法理或诉因（即便是通知过可能发生该损害赔偿）而产生的。如果根据任何适用的法律，除了本条下的明确提出的免责声明和责任限制之外，任何 Radware 方需要向您或任何第三方承担责任，那么 Radware 方所承担的任何责任将完全限制于退还您向 Radware 支付的任何许可、注册或订用费用。

9. **第三方软件。**软件包括第三方所开发和拥有的软件部分（以下简称“第三方软件”）。就本许可协议所有的意图和目的而言，均应将第三方软件视为本软件的一部分；但是，如果第三方软件的源码适用于开源软件许可协议，那么当本许可协议条款和上述任何开源许可协议之间存在任何差异或不一致性时（包括但不限于 开源许可协议许可权比上述第 1 部分所规定的许可权的范围更广，和/或开源许可协议对上文第 5 部分规定的行为没有限制），将适用上述任何的开源许可协议条款并以此为准。开源许可协议的条款和版权声明（第三方软件据此许可给 Radware 或相关的链路）包含在软件文档或软件的报头或自述文件里。第三方许可人和供应商保留第三方软件及其所有副本的所有权利、所有权和利益，包括与此相关的所有版权和其他知识产权。除了根据第 5 部分适用于第三方软件的使用限制之外，您同意并保证，根据本许可协议，不会将第三方软件作为通用 SQL 服务器、独立应用程序或者除了本软件外与其他应用程序进行使用。

10. **期限和终止**。当您第一次打开产品包，购买、下载、安装、复制或使用软件或其任何部分时，本许可协议即发生效力，并在期限届满前持续有效。但是，即便本许可协议出现任何终止，第 4-14 部分仍将继续有效。不可对本许可协议授予的许可进行转让，本许可在下列情况下将终止：(i) 本许可协议终止，或 (ii) 转让软件，或 (iii) 如果本软件是作为另一 Radware 产品的嵌入组件或捆绑组件而提供的，那么当软件从上述产品中分离或者非作为上述产品的一部分而以其他方式进行使用。如果基于订用的基础得到软件的使用许可，那么在订用期间到期后，如果订用期间未得到延长，那么本协议在此时将自动终止。

11. **出口**。根据适用的出口/入口管制法律和法规的规定（包括美国和以色列的此类法律和法规），本软件或其任何部分可能会受到出口和入口管制。您同意遵守这些法律和法规，并且同意，在未获得必需的政府授权或许可之前，不会故意地出口、再出口、进口、再进口或转让产品。此外，您在此约定并同意，确保您对软件的使用符合其他所有外国、联邦、州和当地法律和法规（包括但不限于与隐私权和数据保护有关的所有法律和法规）。出于提供所有服务之目的，您将拥有适当的隐私政策，并且为使用 cookie 和处理用户数据，可以根据适用法律而获得所有的权限、授权和同意（如果适用，包括但不限于根据欧盟指令 95/46/EC、2002/58/EC 和 2009/136/EC）。

12. **美国政府**。如果您是美国政府或其任何行政机关或机构，那么您确认并同意，根据适用的法规，本软件属于“商业计算机软件”和“商业计算机软件文档”，您对本软件的使用应适用本许可协议的条款。

13. **适用法律**。本协议应适用以色列国法律并据此进行解释。

14. **其他条款**。如果根据做出的司法判决，本许可协议里的任何条款属于不合理、非法或不可执行，那么该条款仅在上述司法判决认定该条款不合理、非法或不可执行的范围内无效，并且本许可协议的其他部分仍然继续产生法律效果并具备完全的效力。在任何情况下，如果一方违反或涉嫌违反本许可协议，另一方除了可以采取其他的救济措施之外，还有权申请禁制令。本许可协议组成各方之间达成的完整协议，并将取代双方在此之前就标的事项达成的所有协议。任何一方如果未要求对方履行本许可协议的任何条款，那么在任何方面均不会影响其执行该条款的权利。任何一方对任何条款所做出的弃权或对违反本许可协议任何条款的任何违约行为的弃权，均不应视为（或解释为）对上述任何条款或违约行为的进一步或持续的弃权，或者作为对其他任何条款（或对本协议其他任何条款的违约行为）的弃权。

如果您不同意本许可的条款，您必须将您拥有的任何设备上的软件删除，并立即停止使用本软件。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。