Cisco AnyConnect Secure Mobility Solution Guide

This document contains the following information:

Cisco AnyConnect Secure Mobility Overview

Users and their devices are increasingly more mobile, connecting to the Internet from several locations, such as the office, home, airports, or cafes. Traditionally, users inside the network were protected from security threats, and users outside the traditional network boundary had no acceptable use policy enforcement, minimal protection against malware, and are at a higher risk of data loss.

Employers want to create flexible working environments where employees and partners can work anywhere on any device, but they also want to protect corporate interests and assets from Internet-based threats at all times (always-on security).

Traditional network and content security solutions are ideal for protecting users and assets behind the network firewall, but they are ineffective when users or devices are not connected to the network, or when data is not routed through the security solutions.

Cisco offers AnyConnect Secure Mobility to extend the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. Cisco AnyConnect Secure Mobility provides an innovative new way to protect mobile users on computer-based or smart-phone platforms, providing a more seamless, always-protected experience for end users and comprehensive policy enforcement for IT administrators.

You might want to use AnyConnect Secure Mobility if your organization has users who must access resources on the Internet in order to do their work, but who work on different types of mobile devices outside of a traditional office location.

AnyConnect Secure Mobility is a collection of features across the following Cisco products:

- Cisco IronPort Web Security appliance (WSA)
- Cisco ASA 5500 series adaptive security appliance (ASA)
- Cisco AnyConnect client

Cisco AnyConnect Secure Mobility addresses the challenges of a mobile workforce by offering the following features:

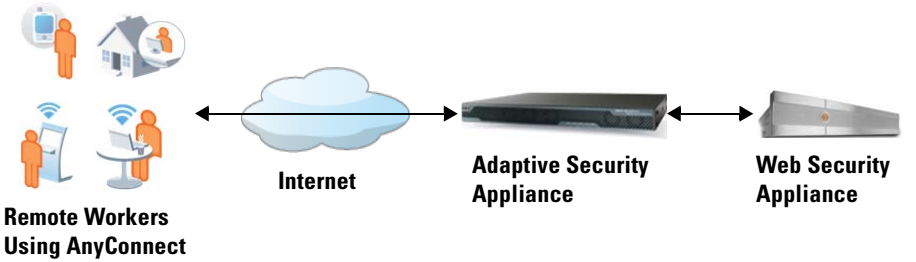
- **Secure, persistent connectivity.** Cisco AnyConnect (with the adaptive security appliances at the headend) provides the remote access connectivity portion of AnyConnect Secure Mobility. The connection is secure because both the user and device must be authenticated and validated prior to being provided access to the network. The connection is persistent because AnyConnect is typically configured to be always-on even when roaming between networks. Although AnyConnect is always-on, it is also flexible enough to apply different policies based on location, allowing users access to the Internet in a “captive portal” situation, when users must accept terms of agreement before accessing the Internet.
- **Persistent security and policy enforcement.** The Web Security appliance applies context-aware policies, including enforcing acceptable use policies and protection from malware for all users, including mobile (remote) users. The Web Security appliance also accepts user authentication information

from the adaptive security appliance based on its authentication of the AnyConnect client, providing an automatic authentication step for the user to access web content.

Understanding How AnyConnect Secure Mobility Works

Cisco AnyConnect Secure Mobility is a collection of features across multiple Cisco products that extends control and security into borderless networks. The products that work together to provide AnyConnect Secure Mobility are the Web Security appliance, adaptive security appliance, and Cisco AnyConnect client.

The following figure shows how these Cisco products work together to provide AnyConnect Secure Mobility.



Remote and mobile users use the Cisco AnyConnect Secure VPN client to establish VPN sessions with the adaptive security appliance. The adaptive security appliance sends web traffic to the Web Security appliance along with information identifying the user by IP address and user name. The Web Security appliance scans the traffic, enforces acceptable use policies, and protects the user from security threats. The adaptive security appliance returns all traffic deemed safe and acceptable to the user.

All Internet traffic scanning is done by the Web Security appliance, not the client on the mobile device. This improves overall performance by not burdening the mobile device, some of which have limited processing power. In addition, by scanning Internet traffic on the network, you can more easily and quickly update security updates and acceptable use policies since you do not have to wait days, weeks, or even months to push the updates to the client.

The Web Security appliance tracks the requests it receives and applies policies configured for remote users to traffic received from remote users. For information on how it identifies remote users, see Communication Between the ASA and WSA, page 4.

Depending on how you configure the Web Security appliance, the AnyConnect client may use a VPN connection to an adaptive security appliance to communicate directly with the Web Security appliance. For more information, see Communication from the Client, page 5.

Communication Between the ASA and WSA

Whether the Web Security appliance interacts and communicates with the adaptive security appliance depends on how the Web Security appliance is configured to identify remote users. The Web Security appliance keeps track of the traffic it receives and applies policies configured for remote users to traffic received from remote users. It identifies remote users using one of the following methods:

- **Associate by IP address.** The Web Security appliance administrator specifies a range of IP addresses that it considers as assigned to remote devices. Typically, the adaptive security appliance assigns these IP addresses to devices that connect using VPN functionality. When the Web Security appliance receives a transaction from one of the configured IP addresses, it considers the user as a remote user. With this configuration, the Web Security appliance does not communicate with any adaptive security appliance.
- **Integrate with a Cisco ASA.** The Web Security appliance administrator configures the Web Security appliance to communicate with one or more adaptive security appliances. The adaptive security appliance maintains an IP address-to-user mapping and communicates that information to the Web Security appliance. When the Web Security appliance receives a transaction, it obtains the IP address and checks the IP address-to-user mapping to determine the user name. When you integrate with an adaptive security appliance, you can enable single sign-on for remote users. With this configuration, the Web Security appliance communicates with the adaptive security appliance.

When the Web Security appliance is configured to integrate with an adaptive security appliance, it tries to establish an HTTPS connection with all configured adaptive security appliances when it first starts up. Once the connection is

established, the Web Security appliance authenticates with the adaptive security appliance using the configured ASA access password. After successful authentication, the adaptive security appliance sends the IP address-to-user mapping to the Web Security appliance. The connection remains open, and the adaptive security appliance updates the IP address-to-user mapping as necessary. For example, when a new VPN connection is made, it adds a new user to the mapping, and when a VPN connection is closed, it deletes the user from the mapping.

Note If the connection between the Web Security appliance and an adaptive security appliance is lost, the Web Security appliance tries to reestablish the connection every 60 seconds by default. You can configure this time interval on the Web Security appliance.

Communication from the Client

When a user opens a VPN session using Cisco AnyConnect, the AnyConnect client connects to the adaptive security appliance using SSL. The client authenticates with the adaptive security appliance and is assigned an internal IP address on the network.

When the Web Security appliance is configured to integrate with the adaptive security appliance, the adaptive security appliance instructs the client to directly contact the Web Security appliance to test its connection. The client and Web Security appliance use the VPN session to exchange some information, such as copyright status.

Note The client periodically checks connectivity to the Web Security appliance by sending a request to a fictitious host. By default, the fictitious host URL is mus.cisco.com. When AnyConnect Secure Mobility is enabled, the Web Security appliance intercepts requests destined for the fictitious host and replies to the client.

Supported Architectures

Enterprise network infrastructures are dynamic and unique, and there is an array of architectures to consider when implementing the AnyConnect Secure Mobility solution. In addition to AnyConnect remote access connectivity, the minimum requirements for a successful Secure Mobility implementation consist of an adaptive security appliance, Web security appliance, and in many cases, a WCCP (Web Cache Communication Protocol) enabled router. However, there are design requirements that could expand these architectures to include additional appliances and routers.

The WCCP router allows the network to transparently redirect web traffic to the WSA so that client applications are unaware of the presence of a proxy server on the network. Most architectures included in this document require at least one WCCP router. The WCCP router is necessary in most of these cases due to a limitation in the WCCP implementation on the adaptive security appliance.

Note Consider all adaptive security appliance feature requirements your organization needs when setting up the network for AnyConnect Secure Mobility. For example, depending on where the adaptive security appliance is placed in the network, some features may or may not work, such as IPS.

Table 5-1 describes some example architectures to consider when deploying AnyConnect Secure Mobility in your network.

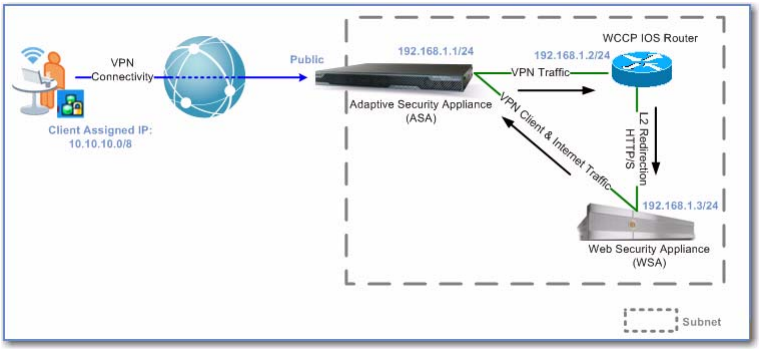
Table 5-1 Summary of Architecture Scenarios

Architecture Scenario	Description
Architecture Scenario 1, Single Subnet, page 8	This architecture has the following characteristics: • Web transactions are transparently redirected to the Web Security appliance, and those transactions are redirected by a WCCP enabled router. • The adaptive security appliance, WCCP router, and Web Security appliance reside on the same subnet.
Architecture Scenario 2, Multiple Subnets, page 10	This architecture is similar to Architecture Scenario 1, Single Subnet except that the Web Security appliance resides on a different subnet than the adaptive security appliance and WCCP router.
Architecture Scenario 3, Explicit Forward Proxy, page 12	This architecture is similar to Architecture Scenario 1, Single Subnet except that client applications are configured to explicitly forward web traffic to the Web Security appliance as a Web Proxy. There is no need for a WCCP enabled router.
Architecture Scenario 4, Non-WCCP Router, page 15	This architecture uses a router, but the router is not WCCP enabled. Instead, the ASA (which is WCCP enabled) uses WCCP to redirect web traffic to the WSA. You might want to use this architecture if you do not have a router that is WCCP enabled.

Architecture Scenario 1, Single Subnet

Figure 1 illustrates the architecture described in this section.

Figure 1 Single Site and Subnet



The deployment scenario in Figure 1 depicts a layer 2 (L2) topology which includes an ASA acting as a remote access and Internet gateway. In addition, this topology includes a WCCP router for L2 redirection of web traffic. All command examples included below refer to the example in Figure 1. The traffic flow for this deployment scenario consists of the following:

- The AnyConnect client establishes an SSL VPN session to the ASA headend and forwards all its traffic over the session. In some cases, security administrators might define VPN policies that exclude specific traffic from the VPN session. For example, administrators might enable local printing for the connected end-user.
- The ASA is configured with a tunnel default gateway (`route inside 0.0.0.0 0.0.0.0 192.168.1.2 255.255.255.0 Tunneled`) which forwards all VPN traffic from the tunnel to the WCCP router (`192.168.1.2/24`).
- The WCCP router forwards only web traffic to the WSA. It forwards all non-web traffic destined for the Internet to its default route (`ip route 0.0.0.0 0.0.0.0 192.168.1.1`), which in this case is the ASA, or to a predefined static route if destined for the enterprise network. On the WCCP router, the command syntax `ip wccp [port] redirect in` (as opposed to `ip wccp [port] redirect out`) must be applied to the interface configured for L2 redirection. This command enables web traffic inbound to the interface to successfully be redirected to the WSA.

- The WSA receives web traffic redirected from the WCCP router and enforces its policies on the traffic received from the AnyConnect client. If the WSA grants access to the web request, it rewrites the traffic prior to forwarding it to the Internet via its default route, the ASA. This will enable the ASA to return the traffic back to the WSA for scanning and policy enforcement. You must ensure that the WSA has a route to return successfully scanned traffic back to the AnyConnect client. For example, you could add a static route to the WSA to send all traffic destined for the client IP address pool (`10.10.10.0/8`) back to the ASA.

Note Non-web traffic sent from the Internet back to the ASA will be dropped if the source and destination of that traffic is in the AnyConnect client IP address pool (`10.10.10.0/8`). To prevent this, you can configure a static route (`route inside 10.10.10.0 255.0.0.0 192.168.1.2`) on the ASA to enable it to forward the traffic back to the AnyConnect client IP address pool.

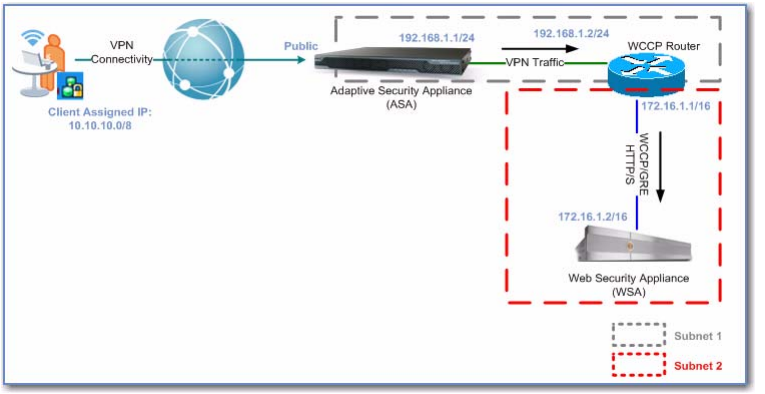
All Secure Mobility components reside on a flat network, allowing the WCCP router to use layer 2 redirection instead of Generic Routing Encapsulation (GRE). GRE adds traffic overhead, works at layer 3, and is required when the WCCP router and the WSA are on different subnets.

When the ASA acts as both the remote access and Internet gateway as shown in Figure 1 on page 8, Network Address Translation (NAT) or Port Address Translation (PAT) must be configured on the ASA to route non-web traffic or traffic from the private IP address space to the Internet. In addition, to prevent traffic sent from the enterprise network back to the AnyConnect client from being subjected to the NAT or PAT command, you must configure a NAT Exemption rule for the defined AnyConnect client IP address pool.

Architecture Scenario 2, Multiple Subnets

Figure 2 illustrates the architecture described in this section.

Figure 2 Single Site and Multiple Subnets



The deployment scenario in Figure 2 depicts an architecture similar to Figure 1 on page 8. However, this architecture introduces WCCP with Generic Routing Encapsulation (GRE) redirection which is required when the WSA is on a different subnet than the WCCP router. Like the architecture depicted in Figure 1, the traffic flow is essentially the same. Nevertheless, you must consider Layer 3 (L3) redirection which includes GRE as the redirection method. In addition, you must consider alternative routing entries on the WSA to route traffic back to the ASA.

You might want to use the architecture in Figure 2 instead of Figure 1 if your network topology prevents you from placing the WSA on the same subnet as the WCCP router or if you want all web traffic to enter the WCCP router from a separate subnet as other network traffic. Isolating traffic destined for the Internet like this can allow network administrators to more easily monitor and report on web traffic. Additionally, you can create firewall policies to block web traffic from all users unless their traffic goes through the WSA Web Proxy.

The WCCP router automatically negotiates the redirection method with the WSA, encapsulates the web traffic in a GRE header, and routes it to the WSA based on its routing table. Non-web traffic destined for the Internet is forwarded to its default route (`ip route 0.0.0.0 0.0.0.0 192.168.1.1`), which in this case is

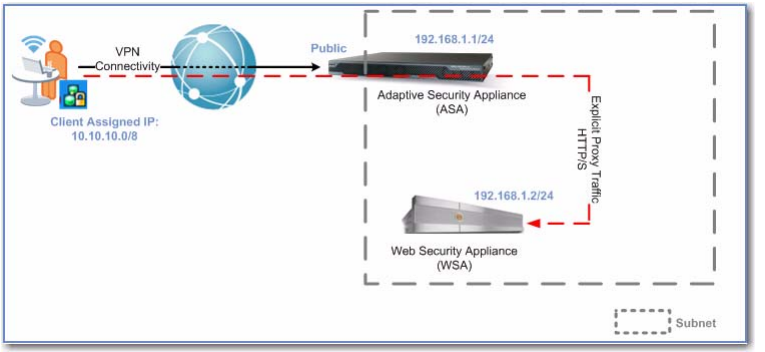
the ASA, or to a predefined static route if destined for the enterprise network. On the WCCP router, you must still apply the command syntax `ip wccp [port] redirect in` on the interface configured for redirection. This command enables web traffic inbound to the interface to be redirected to the WSA. The WSA decapsulates the GRE packet and enforces its security policies.

Like the architecture in Figure 1 on page 8, the WSA must be configured with the appropriate route (`route 10.10.10.0/8 x.x.x.x`) back to the ASA in an effort to return scanned traffic back to the AnyConnect client. The router in this case is generally a router residing on the distribution or aggregation layer of the routing infrastructure.

Architecture Scenario 3, Explicit Forward Proxy

Figure 3 illustrates the architecture described in this section.

Figure 3 Explicit Mode Policy Enforcement



In the deployment scenario depicted in Figure 3, client web traffic is configured to explicitly use the WSA for web traffic instead of the web traffic being transparently redirected to the WSA. Client applications, such as web browsers, are configured to explicitly use the WSA as a proxy server (`address: 192.168.1.2, port: 80/443`). This is different than the deployments described in Figure 1 and Figure 2, where a WCCP router transparently redirects web traffic to the WSA, and the clients are unaware their web traffic is going through a proxy server.

Note Browser proxy settings can either be defined manually by the end user or dynamically by the ASA during VPN establishment. You can use the Adaptive Security Device Manager (ASDM) to configure dynamic proxy configuration settings under Configuration > Remote Access VPN > Network (Client) Access > Group Policies > *Group Name* > Edit > Advanced > Browser Proxy in the predefined internal Group Policy on the ASA.

Both web and non-web traffic is forwarded to the ASA over the VPN session. However, web traffic is explicitly sent to the WSA as defined in the browser proxy settings, and non-web traffic is routed based on the routing table of the ASA.

Note You can only dynamically deploy proxy configuration settings using the ASA to Internet Explorer on Windows and Safari on Mac OS connected AnyConnect clients. Other browsers must be manually configured on the client machine in order to explicitly use the WSA as a proxy. Transparently redirecting web traffic to the WSA creates a better user experience for end users; however, explicitly configuring client browsers to use the WSA can be deployed in any network architecture as long as the AnyConnect client can successfully route web traffic from its VPN session to the WSA.

When users are remote and client applications are configured to explicitly use the WSA for web traffic, consider the following information when configuring client applications to use a proxy server:

- **Proxy settings used before the VPN connection is established.** When Internet Explorer is configured to use a proxy, AnyConnect uses those proxy settings to connect to the ASA. If these proxy settings point to the WSA inside your enterprise LAN, AnyConnect will fail to connect to the ASA. To prevent this, you must perform one of the following actions:
  - Modify the browser proxy settings to add an exception for the ASAs.
  - Using an AnyConnect profile, set the ProxySettings attribute to IgnoreProxy. For more information, see Configuring the ProxySettings Attribute, page 13.
- **Proxy settings used after the VPN connection is established.** To ensure that the web traffic is sent to the WSA, you have the following options:
  - Keep the current browser proxy settings (with the exception for ASAs as recommended above).
  - Use ASDM to dynamically set proxy settings in the browser.

Configuring the ProxySettings Attribute

To configure the ProxySettings attribute to IgnoreProxy for an AnyConnect profile, use ASDM. Follow the instructions in the “Configuring the Client to Ignore Browser Proxy Settings” section in the “Configuring AnyConnect Features” chapter of the *Cisco AnyConnect Secure Mobility Client Administrator Guide*.

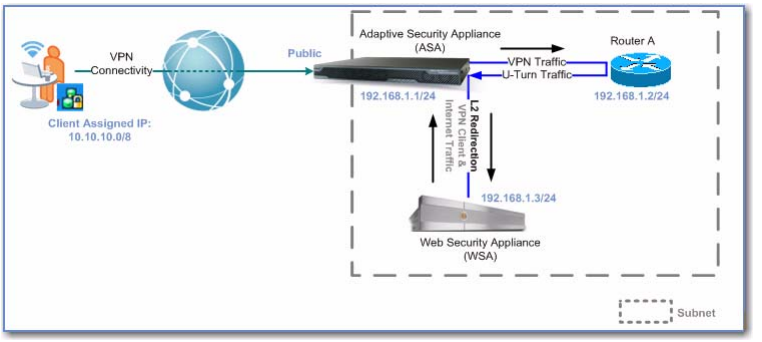
For more information on accessing Cisco documentation, see Additional Documentation, page 22.

Note AnyConnect profile settings, such as IgnoreProxy, only apply when the AnyConnect client connects to the ASA. The client does not use these settings after it establishes a tunnel with the ASA.

Architecture Scenario 4, Non-WCCP Router

Figure 4 illustrates the architecture described in this section.

Figure 4 Using WCCP on the ASA



The deployment scenario in Figure 4 illustrates using WCCP on the ASA to redirect web traffic to the WSA instead of using a WCCP router for traffic redirection. In the deployment scenarios documented previously, a WCCP router is used to transparently redirect web traffic to the WSA. You might want to use this architecture if you do not have a router that is WCCP enabled. Instead, you can use the WCCP functionality in the ASA to redirect web traffic to the WSA. You can use any router in this deployment scenario.

With the deployment scenario in Figure 4, the ASA forwards all VPN traffic to its tunnel default gateway, router A (`route inside 0.0.0.0 0.0.0.0 192.168.1.2 255.255.255.0 Tunneled`). Router A then returns VPN web traffic back to the ASA (`ip route 0.0.0.0 0.0.0.0 192.168.1.1`), and forwards non-web traffic based on its routing table. The ASA then uses WCCP to redirect web traffic to the WSA for scanning.

Like the architectures discussed previously, the WSA must be configured with a default route to the Internet gateway to enforce its policies. In addition, the WSA must be configured with a route (`route 10.10.10.0/8 192.168.1.1`) back to the ASA to return scanned traffic back to the AnyConnect client.

Note Version 8.3 of the ASA can only use WCCP to redirect web traffic when the traffic enters the ASA on the same interface where WCCP is enabled. However, the AnyConnect client traffic does not enter the ASA on the same interface where WCCP is enabled (which is the same interface connected to the WSA). To work around this, you must connect a router off the WCCP enabled interface to direct all traffic to the router and then return it to the ASA on the WCCP enabled interface. This allows the ASA to use WCCP to redirect web traffic to the WSA for scanning. In Figure 4, Router A returns all traffic back to the ASA on the same interface as the WSA, the inside interface.

Note When using this architecture with the Web Security appliance proxy bypass list feature, only local users are able to successfully reach websites listed in the proxy bypass list. When a remote user tries to access a website listed in the proxy bypass list, the connection fails.

Configuring AnyConnect Secure Mobility

To achieve secure mobility for users connecting to the network using VPN, you must configure the following products:

- **Cisco IronPort Web Security appliance.** For more information, see Configuring WSA Support for AnyConnect Secure Mobility, page 17.
- **Cisco adaptive security appliance.** For more information, see Configuring ASA Support for AnyConnect Secure Mobility, page 18.
- **Cisco AnyConnect secure mobility client.** For more information, see Configuring AnyConnect Support for AnyConnect Secure Mobility, page 19.

To integrate a Web Security appliance and an adaptive security appliance, you need the following information:

- IP address for each adaptive security appliance
- Port number of each adaptive security appliance
- IP address for each Web Security appliance
- Port number of each Web Security appliance

- A single access password that you configure on each adaptive security appliance and Web Security appliance

To use secure mobility, you must use the following Cisco product versions:

- Cisco adaptive security appliance release 8.3.1.6 or higher
- Cisco adaptive security device manager (ASDM) Release 6.3 or later
- Cisco IronPort Web Security appliance version 7.0 or later

Configuring WSA Support for AnyConnect Secure Mobility

When AnyConnect Secure Mobility is enabled on the Web Security appliance, you can distinguish remote users from local users and create separate policies for remote and local users. For example, you can create Access Policies that allow access to arts and entertainment sites when users are outside the office (remote users), but block access when users are in the office (local users).

AsyncOS for Web version 7.0 or later supports AnyConnect Secure Mobility.

To configure the Web Security appliance to work with AnyConnect Secure Mobility, perform the following tasks:

1. **Enable the AnyConnect Secure Mobility feature on the Web Security appliance.** Enable the feature on the Security Services > Mobile User Security page. When you enable the AnyConnect Secure Mobility feature, you choose how to identify remote users, either by associating with particular IP addresses or by integrating with a Cisco adaptive security appliance. When users are identified by IP address, the Web Security appliance does not communicate with the adaptive security appliance.

Note If multiple adaptive security appliances are configured in a cluster, you configure the Web Security appliance to communicate with each adaptive security appliance in the cluster. If two adaptive security appliances are configured for high availability, you configure the Web Security appliance to communicate with the active adaptive security appliance only.

2. **Create one or more Identity policies that applies to remote users.** You can choose whether or not authentication is required for the Identity:

- **No authentication required.** Configure the Identity to not use authentication. Users are identified by IP address.
- **Authentication required.** Configure the Identity to apply to remote users only and to transparently identify users by integrating with the Cisco adaptive security appliance. Users are identified by the user name using the IP address to user name mapping from the adaptive security appliance.

3. **Create other policies that use an Identity configured for remote users.** Configure all settings as business needs dictate. No particular policy configurations are necessary for AnyConnect Secure Mobility.

For more information on enabling AnyConnect Secure Mobility and working with remote users, see the "Achieving Secure Mobility" chapter in the *IronPort AsyncOS for Web User Guide* for version 7.0 and later. You can access the *IronPort AsyncOS for Web User Guide* in the online help from the Web Security appliance web interface. You can also access the *IronPort AsyncOS for Web User Guide* on cisco.com. For more information on accessing Cisco documentation, see Additional Documentation, page 22.

Once AnyConnect Secure Mobility is enabled and policies are created for remote users, you can view reports on the Web Security appliance for remote traffic.

Configuring ASA Support for AnyConnect Secure Mobility

To enable AnyConnect Secure Mobility on the adaptive security appliance, you need information for accessing the Web Security appliance. Once the adaptive security appliance and the Web Security appliance are configured to communicate with each other, the adaptive security appliance can send traffic from AnyConnect secure mobility clients to the Web Security appliance for scanning. The client periodically checks to ensure that Web Security appliance protection is enabled.

Enable and configure AnyConnect Secure Mobility by using the Mobile User Security (MUS) dialog box at Configuration > Remote Access VPN > Network (Client) Access > Mobile User Security.

To configure the adaptive security appliance to support AnyConnect Secure Mobility:

1. Upgrade the adaptive security appliance to Release 8.3.1.6 or later.
2. Upgrade ASDM to Release 6.3 or later.

3. In the Mobile User Security window in ASDM, add one or more Web Security appliances that the adaptive security appliance communicates with. After you choose Add or Edit, you can specify the Interface Name, IP address, and mask of the host.
4. Enable the Mobile User Security feature on the adaptive security appliance. This enables the adaptive security appliance to communicate with the Web Security appliance using a secure HTTPS connection for passing user credentials to the Web Security appliance for single sign-on functionality. When enabled, you must enter the access password used by the Web Security appliance when contacting the adaptive security appliance. You must also enter a port number for the service to use. If no Web Security appliance is present, the status is disabled.
5. Change Password. Enables you to configure and change the Web Security appliance access password required for authentication between the adaptive security appliance and Web Security appliance. This password must match the corresponding password configured on the Web Security appliance.
6. (Optional) View session information of Web Security appliances connected to the adaptive security appliance and the duration of the connection.

For more information on configuring the adaptive security appliance, read the documentation. See Additional Documentation, page 22 for the location.

Configuring AnyConnect Support for AnyConnect Secure Mobility

When you use AnyConnect Secure Mobility with the AnyConnect client, users are easily and seamlessly protected from security threats and their web transactions are subject to acceptable use policy enforcement configured by their IT administrators. AnyConnect client users are usually not aware that their traffic is scanned by the Web Security appliance except that they can see a status message in the AnyConnect client that AnyConnect Secure Mobility is enabled.

To allow the AnyConnect client to work with AnyConnect Secure Mobility, perform the following tasks:

1. Upgrade the adaptive security appliance to Release 8.3.1.6 or later.
2. Upgrade ASDM to Release 6.3 or later.

3. Load the AnyConnect Secure Mobility client package Release 2.5 or later onto the adaptive security appliance.
4. Using ASDM, configure the adaptive security appliance to support Network (Client) Access as usual.
5. In ASDM, consider configuring the VPN profile to be always on. You might want to configure this feature for when the user is in an untrusted network. When you configure the VPN profile to be always on, you must also enable Trusted Network Detection (TND).

   The always on feature lets AnyConnect automatically establish a VPN session after the user logs onto a computer. The VPN session remains up until the user logs off of the computer. If the physical connection is lost, the session remains up, and AnyConnect continually attempts to reestablish the physical connection with the adaptive security appliance to resume the VPN session.

   TND gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).
6. When you configure always-on VPN, you can optionally choose to enable any of the following options that affect the mobile user's experience:
   - **Connect Failure Policy.** When AnyConnect fails to initiate or maintain a VPN session in accordance with the always on feature, the connect failure policy determines whether the user can establish network connectivity using a service or domain that is not configured as trusted. You can configure the VPN profile to fail open or fail close.
   - **Allow Captive Portal Remediation.** This is the process of satisfying the requirements of a captive portal hot spot to obtain network access. When a facility offering Internet access requires users to accept terms and conditions before gaining access, users enter a captive portal environment. By default, captive portals prevent AnyConnect from connecting to the VPN. You might want to enable Allow Captive Portal Remediation to give users a few minutes to satisfy the terms and conditions to gain access, thus allowing AnyConnect to connect to the VPN.
   - **Apply Last VPN Local Resource Rules.** When the Connect Failure Policy is set to fail closed, this feature allows users to print locally and synchronize tethered devices. To allow that, you must also configure the appropriate firewall rules.

For more information on configuring the Cisco AnyConnect secure mobility client, read the *Cisco AnyConnect Secure Mobility Client Administrator Guide*. See Additional Documentation, page 22 for the location.

Troubleshooting

Web Security appliance:

- AnyConnect Secure Mobility events are included in the User Discovery Service (UDS) log.
- The Web Security appliance web interface has a button to test connectivity to the configured adaptive security appliances.
- Use the `musstatus` CLI command to view adaptive security appliance to Web Security appliance connections and statistics.

Adaptive security appliance:

- `mus server enable <port>` command can be verified using `show config | include mus`
- `debug webvpn mus <1-255>` enables additional AnyConnect Secure Mobility debug information.
- Logs are available via syslog.

ASDM:

- `Monitoring -> VPN -> WSA Sessions` show host and uptime statistics.

AnyConnect Secure Mobility client:

- DART collects endpoint event logs, install logs, system information, dump files, profile, preferences, and more.
- Produces a zip file.
- Can be dynamically installed from adaptive security appliance or using a standalone installer.
- Can be launched from the Start menu or client using a Troubleshoot button.

Additional Documentation

This document is intended to serve as an overview of the entire AnyConnect Secure Mobility solution. It does not include detailed steps on configuring each component of the product, nor does it list all potential interactions with other features of each component. For detailed information on how to install, configure, and upgrade each component in the solution, see the release notes and user guides for each product.

Cisco adaptive security appliance (ASA) documentation home page:

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Cisco AnyConnect documentation home page:

http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco AnyConnect Secure Mobility Client documentation home page:

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

Cisco Adaptive Security Device Manager (ASDM) documentation home page:

http://www.cisco.com/en/US/products/ps6121/products_installation_and_configuration_guides_list.html

Cisco IronPort Web Security Appliance documentation home page:

http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

Introduction to the Cisco AnyConnect Secure Mobility Solution:

http://www.cisco.com/en/US/netsol/ns1049/index.html

Contacting Support

Because the Cisco AnyConnect Secure Mobility solution covers multiple Cisco products, you might need to contact a different support group for help resolving issues related to AnyConnect Secure Mobility. Each AnyConnect Secure Mobility product is supported by a different product support team which is located in either Cisco TAC (Technical Assistance Center) or Cisco IronPort Customer Support.

Both Cisco TAC and Cisco IronPort Customer Support have communication measures in place to work with each other to resolve AnyConnect Secure Mobility related issues. However, when you encounter an AnyConnect Secure Mobility issue, apply your best judgment to identify where the problem might exist and contact the appropriate support team when possible. This can help decrease the time required to resolve the issue.

- For problems related to the adaptive security appliance or AnyConnect client, open a case with Cisco TAC at the following location:
  `http://tools.cisco.com/ServiceRequestTool/create/launch.do`
  Use “Security - Adaptive Security Appliance (ASA) and PIX” for the technology field and “WebVPN/SSLVPN - Anyconnect Client issue” for the subtechnology field.
- For problems related to the Web Security appliance, open a case with Cisco IronPort Customer support using the built in support request functionality on the Web Security appliance. From the CLI, use the `supportrequest` command. From the web interface, go to Support and Help > Open A Support Case. Or, you can open a case from the web at the following location:
  `http://www.cisco.com/web/ironport/index.html`.

To help discern which AnyConnect Secure Mobility product currently has a problem, use any of the troubleshooting tips in Troubleshooting, page 21. In particular, consider the following approaches:

- If the solution worked before, investigate where the last changes were made.
- Test basic network connectivity between devices. For example, ping from the client to the adaptive security appliance, and from the adaptive security appliance to the router, and from the router to the Web Security appliance. Between which connections did the ping fail?
- Check the adaptive security appliance syslog messages for error or warning messages.