Cloud Web Security Using AnyConnect

Technology Design Guide

August 2014 Series

CISCO VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Secure Remote Worker Web Traffic**—All web traffic to the Internet from remote-access VPN users accesses the Internet through the Cisco Cloud Web Security service, which provides granular control over all web content that is accessed.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Cisco ASA 5500-X Series Adaptive Security Appliances for client-based remote-access VPN
- Cisco AnyConnect Secure Mobility Client for remote users who require full network connectivity
- Cisco Cloud Web Security provides granular control over all web content that is accessed

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks
- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

Related CVD Guides

- Firewall and IPS Technology Design Guide
- Device Management Using ACS Technology Design Guide
- Remote Access VPN Technology Design Guide
- Cloud Web Security Using Cisco ASA Technology Design Guide

To view the related CVD guides, click the titles or visit the CVD Foundation web site.

Introduction

One of the most profound advances in modern networks is the degree of mobility those networks support. Users can move around wirelessly inside the campus and enjoy the same degree of connectivity as if they were plugged in using cables in their offices. Users can leave their primary networks completely and work from a home-office environment that offers the same connectivity and user experience as they would get in their offices. Users also have the option of being truly mobile and connecting from any place that offers Internet access. With smartphones and tablets, this mobility now commonly includes connecting while travelling down the highway or on a train. This guide applies primarily to the truly mobile users who use a laptop, smartphone, or tablet device to connect through infrastructure that is not provided by their organizations. The guide does not cover use cases related to campus wireless access or home teleworker solutions.

Technology Use Cases

As users move outside the boundaries of the traditional network, their requirements for access to job-related data, such as email, calendars, and more, don't change. In order for people to be productive, organizations need to allow them access to the network from wherever they are and to whatever data they need, using any device the organization allows. At the same time, organizations must ensure that all access to the network is secure and appropriate and that it follows organizational guidelines.

Mobile, remote users connect to the network by using devices that can generally be broken down into two categories: laptop computers and other mobile devices, such as smartphones and tablets. Networks have handled laptops for years, but integrating the other mobile devices continues to challenge network design and administration.

An organization's network must meet many requirements today that are sometimes contradictory. The network must be secure and prevent unauthorized access while being open enough to allow users to do their jobs regardless of where they are. As the mobility of users has increased, the requirements the network must meet have increased. In the past, a worker might have needed laptop connectivity while at the office or at home. Today, a worker needs access to the network from a smartphone while traveling, from a laptop while on site at a customer's or partner's office, or from both while sitting in the local coffee shop. Although providing this access is the primary requirement for the network, other requirements, such as ease of use and security, have not been relaxed.

Because these mobile users are outside the traditional perimeter (or physical border) of the network, their devices are exposed to potentially more malicious activity than a device that is located inside the protection of the network. So protection of the end device and the data being accessed and stored is critical. The mobile user's device needs to have protection from threats such as malware and viruses. Ideally, this protection occurs even if the device is not connected to the headquarters' network or if such a connection isn't possible. Because many mobile devices are smaller and are used much more often than a laptop, they are also more easily lost or stolen. These devices potentially carry the same information that a laptop might, so there is a need to protect the data on the devices and prevent unauthorized users from retrieving it.

As a standard part of their processes and guidelines, many organizations are required to control what sites users access on the Internet while they are using organizational resources. Providing this level of control for mobile users who do not reside within the boundaries of the network is challenging. In order to provide a complete solution, the network enforces standard access guidelines on the device, whether the device resides inside the headquarters or is connecting from a coffee shop. End users should have similar experiences inside or outside the traditional network perimeter, as well as the same protection from malware.

Use Case: Secure Remote Worker Web Traffic

As more users move outside the boundaries of the network, a corresponding increase in network load occurs on the organization's Internet connection. This load increase can raise costs. Intelligent routing of traffic is a priority to control which traffic from a user has to go through the Internet edge component of the organization's network and which traffic can be kept out on the Internet. Reducing security on this traffic is not an option that is readily available. Traffic destined for the Internet that has to be brought back to the Internet edge for security inspection increases bandwidth usage and load on the Internet edge design, while increasing latency on user connections.

It is suboptimal to force all user traffic to the central site when using a remote-access VPN. This central-tunneling approach adds increased latency to Internet bound user traffic and unnecessarily congests the central site's Internet link. Enabling the Cisco AnyConnect Cloud Web Security (CWS) module allows an organization to use a split-tunneling approach. Only traffic destined to the organization is sent to the central site. All web traffic to the Internet from remote-access VPN users accesses the Internet through the cloud-based CWS service.

This design guide enables the following security capabilities:

- **Redirect web traffic**—The CWS module can be installed along with the Cisco AnyConnect client, allowing web traffic to be transparently redirected to the Cisco CWS service. The CWS module is administered centrally on the remote access VPN (RAVPN) firewall and requires no additional hardware. Once installed, the CWS module continues to provide web security even when disconnected from the RAVPN firewall.
- **Filter web content**—Cisco CWS supports filters based on predefined content categories, as well as custom filters that can specify application, domain, content type, or file type. The filtering rules can be configured to block or warn based on the specific web usage policies of an organization.
- **Protect against malware**—Cisco CWS analyzes every web request to determine if the content is malicious. CWS is powered by the Cisco Security Intelligence Operations (SIO), the primary role of which is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- **Apply differentiated policies**—The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key assigned within the Cisco AnyConnect CWS profile on the RAVPN firewall.

Design Overview

The CVD Internet edge design provides the basic framework for the enhancements and additions that will be discussed in this guide. A prerequisite for using this design guide is that you must have already followed the guidance in the Remote Access VPN Technology Design Guide, which itself builds upon the Firewall and IPS Technology Design Guide.

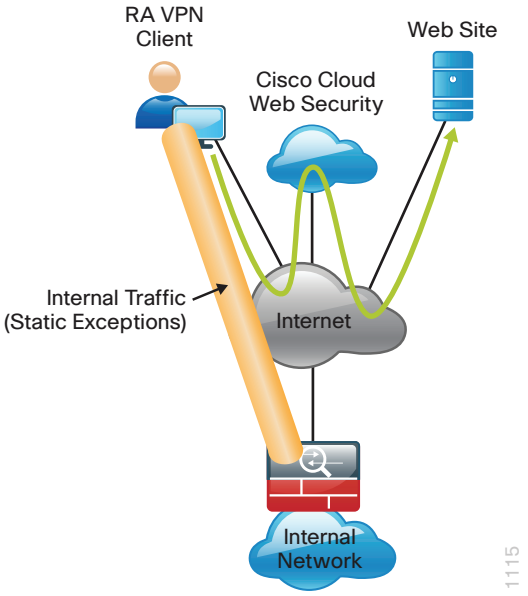
Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ.

The Internet edge design covers RAVPN for laptops running the Cisco AnyConnect Secure Mobility Solution client (for SSL VPN or IP Security [IPsec] connections). A feature built into the Cisco AnyConnect 3.1 client is the cloud connector for Cisco Cloud Web Security (CWS) service, formerly known as *Cisco ScanSafe Cloud Web Security*. Cisco CWS is a web security service that provides threat protection and control for organizations delivered through the cloud.

Cloud connectors are software components embedded in, hosted on, or integrated with platforms in order to enable or enhance a cloud service. The native integration of the Cisco AnyConnect CWS module with the AnyConnect client, which provides remote users with transparent access to a cloud service, is classified as an embedded cloud connector application.

This cloud connector, known as the Cisco AnyConnect Cloud Web Security Module, gives the AnyConnect client the ability to let Internet web traffic go out through a CWS proxy directly to the destination without forcing it through the organization's headend. Without Cisco CWS, the traffic must be routed down the VPN tunnel, inspected at the campus Internet edge, and then redirected to the original destination; this process consumes bandwidth and potentially increases user latency. With Cisco CWS, the connection can be proxied through the Cisco CWS cloud and never has to traverse the VPN tunnel.

Figure 1 - Cisco CWS traffic flow using the Cisco AnyConnect CWS Module



Mobile devices such as the iPhone and iPad and some Android devices have access to the Cisco AnyConnect 3.1 client, which allows Secure Sockets Layer (SSL) VPN connectivity (check the app store for the device in question for availability). Using Cisco AnyConnect to connect the device to the corporate network provides full access to the internal network.

Only the Cisco AnyConnect 3.1 client for Windows and Mac OS X include support for the Cisco AnyConnect CWS Module. Other types of mobile devices must connect to their primary site RAVPN firewall and secure their web traffic with resources located at the primary site. The use of CWS at the primary site is covered in the Cloud Web Security for Cisco ASA Technology Design Guide.

This document covers the additional configuration for remote access VPN for the Cisco AnyConnect 3.1 client that is required to activate Cisco CWS. It also covers interaction with the Cisco CWS management tool, ScanCenter.

Deployment Details

This section describes how to configure the components needed to enable Cisco CWS service for Cisco AnyConnect 3.1 users who connect to an organization's network with laptop devices.

PROCESS

Configuring Cloud Web Security for Remote Laptop Devices

1. Enable CWS security configuration
2. Configure ACL for trusted server
3. Configure Policies for AnyConnect Cloud Web Security Module
4. Configure ASA AnyConnect group policies
5. Install certificate on the client
6. Add RAVPN firewalls as trusted sites on the client
7. Test the AnyConnect configuration
8. Test Cloud Web Security
9. Synchronize the profiles to failover ASA

Procedure 1 Enable CWS security configuration

This guide assumes you have purchased a Cisco CWS license and created an administrative CWS account that allows a user to log in and manage the account.

If you want to apply specific policies based on user identity, you must have groups built in Active Directory (AD) in order to allow differentiation based on group membership.

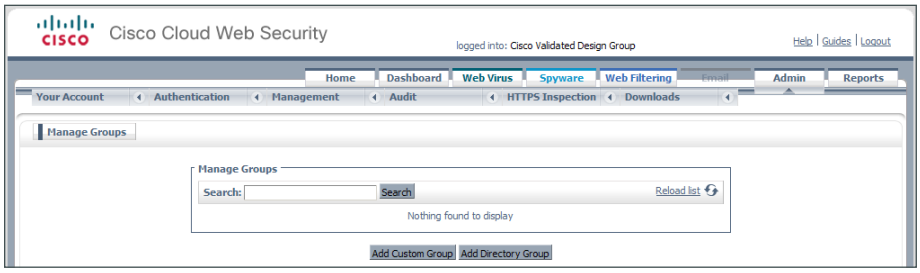
Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to **Admin > Management** > **Groups**.

Tech Tip

Policy can differ based on group assignment. The simplest method for assigning group membership is to generate a unique key for a group and use that key during deployment to group members. If more granular policies are required, other methods for group assignment include IP address range or mapping to an Active Directory group.



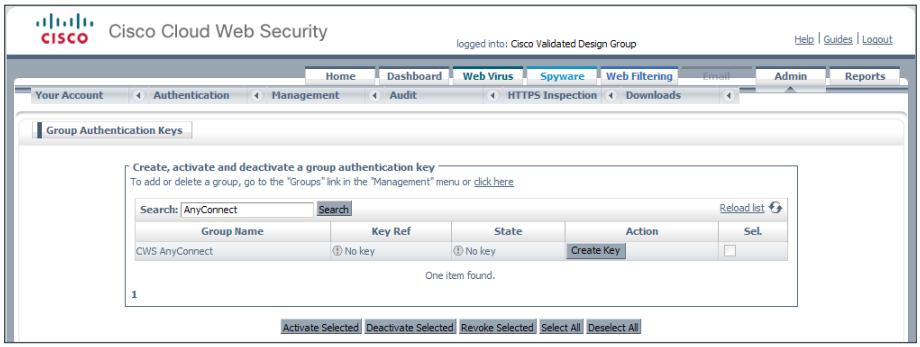
Step 3: Click **Add Custom Group**.

Step 4: On the Add New Custom Group pane, enter the group name (Example: CWS AnyConnect), and then click **Save**.

A group-specific authentication license key is generated for use in the Cisco ASA VPN configuration.

Step 5: Navigate to **Authentication > Group Keys**.

Step 6: For the group created in Step 4, click **Create Key**. ScanCenter generates a key that it sends to an email address of your choosing.



Step 7: Store a copy of this key by copying and pasting it into a secure file because it cannot be rebuilt and can only be replaced with a new key. After it is displayed the first time (on generation) and sent in email, you can no longer view it in ScanCenter. After this key is generated, the page options change to **Deactivate** or **Revoke**.

Step 8: Navigate to **Web Filtering > Management > Filters**.

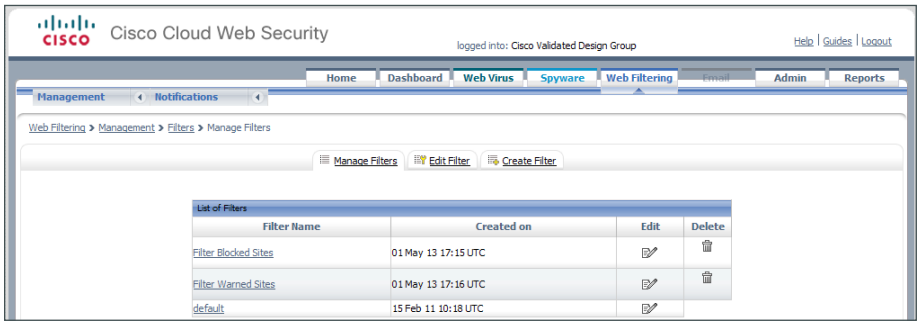
> **Tech Tip**
>
> The filtering policy in this guide is an example only. The actual policy implemented should align with the organization's security policy and business requirements.

Step 9: Click **Create Filter**.

Step 10: Assign a name to the filter (Example: Filter Blocked Sites), select the categories blocked by your organization's policy (Examples: Pornography and Hate Speech), and then click **Save**. Access to these categories is completely restricted.

Step 11: Click **Create Filter**.

Step 12: Assign a name to the filter (Example: Filter Warned Sites), select the categories that are considered inappropriate by your organization's policy (Example: Gambling), and then click **Save**. Access to these categories is permitted, but only after accepting a warning message.



Step 13: Navigate to **Web Filtering > Management > Policy**.

Step 14: Select the Rule name **Default**, change the rule action to **Allow**, and then click **Save.**

Step 15: Click **Create Rule**.

Step 16: Assign a name to the rule (Example: Block_Blocked_Sites), and then select **Active**.

Step 17: From the rule action list, choose **Block**.

Step 18: In the Define Group pane, click **Add group**.

Step 19: In the dialog box, in the **Search** box, enter the name of the group created in Step 4, and then click **Go**.

Step 20: Click **Select**, and then click **Confirm Selection**.

Step 21: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 10 (Example: Filter Blocked Sites), and then click **Add**.

Step 22: Click **Create rule**. The policy rule has now been created.

Next, create a new rule.

Step 23: Click **Create Rule**.

Step 24: Assign a name to the rule (Example: Warn_Warned_Sites), and then select **Active**.

Step 25: From the **Rule Action** list, choose **Warn**.

Step 26: In the Define Group pane, click **Add group**.

Step 27: In the dialog box, in the search box, enter the name of the group created in Step 4, and then click **Go**.

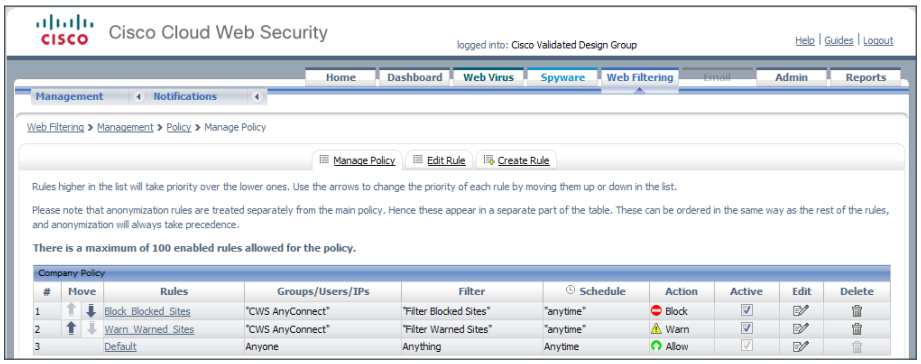
Step 28: Click **Select**, and then click **Confirm Selection**.

Step 29: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 12 (Example: Filter Warned Sites), and then click **Add**.

Step 30: Click **Create rule**. The policy rule has now been created.

Because all rules are evaluated on a first-hit rule, the following is the correct order for the rules in this example:

1. Block Blocked Sites (which blocks access to restricted categories)
2. Warn Warned Sites (which allows access to sites but with a warning)
3. Default (which permits all other sites to all groups)



Procedure 2 Configure ACL for trusted server

The Trusted Network Detection (TND) feature of Cisco CWS determines whether a host is connected directly to a *trusted network*, in this guide referring to a LAN or WLAN at an organization's primary or remote sites. Conversely, if a host connects to an organization through a remote access VPN, then the host is considered to be on an *untrusted network*.

The TND configuration requires a trusted server that is reachable for all hosts on the internal network but is unreachable for remote-access VPN users. The trusted server is required to support HTTPS connections and the fully qualified hostname must be resolvable in the Domain Name Service (DNS) for your organization.

Step 1: If a trusted server does not exist, deploy a server with an HTTP server and enable HTTPS. Ports other than TCP 443 may be used if necessary. (Example: CWS-Trusted-Host.cisco.local, 10.4.48.11:443)

Tech Tip

Access to the trusted server is blocked for remote access VPN users. Choose a trusted server that does not support applications required for these users.

Step 2: From a client on the internal network, navigate to the RAVPN firewall's inside IP address, and then launch the Cisco ASA Security Device Manager. (Example: https://10.4.24.24)

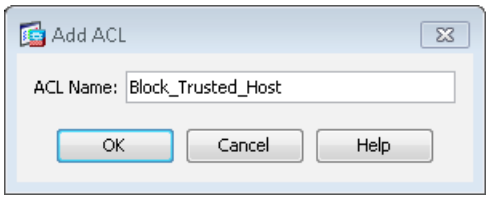
Step 3: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, select **GroupPolicy_Employee**, and then click **Edit**.

Step 4: On the Edit Internal Group Policy dialog box, click the two down arrows. The More options pane expands.

Step 5: For Filter, clear **Inherit**, and then click **Manage**.

Step 6: On the ACL Manager dialog box, click the **Extended ACL** tab, and then click **Add > Add ACL**.

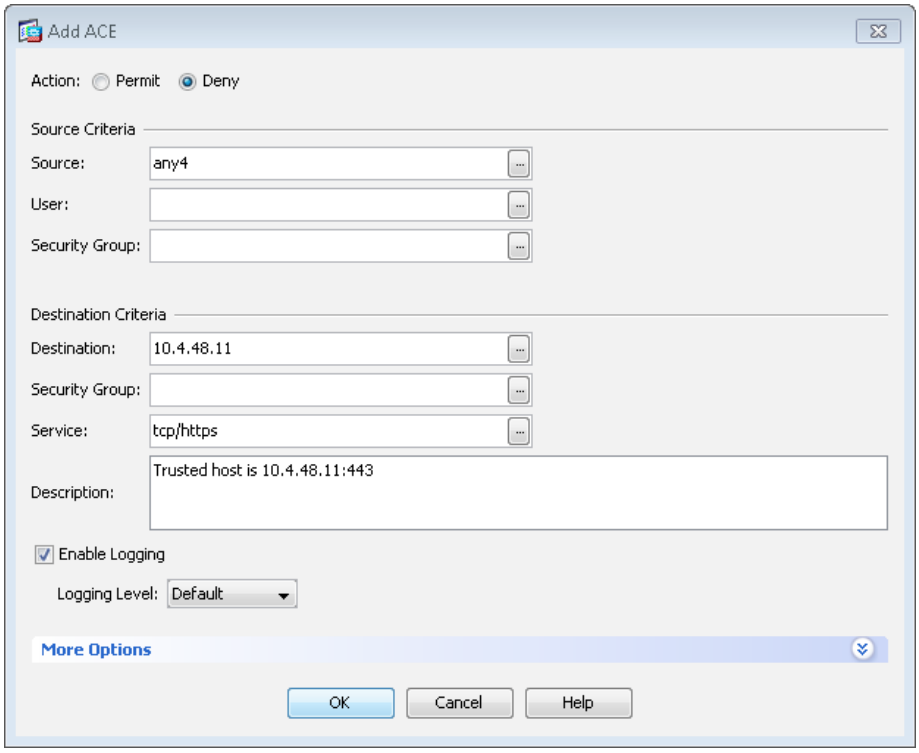
Step 7: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example Block_Trusted_Host)



Step 8: Click **Add > Add ACE**.

Step 9: On the Add ACE dialog box, configure the following values, and then click **OK**.

- Action–**Deny**
- Source–**any4**
- Destination–**10.4.48.11**
- Service–**tcp/https**
- Description–**Trusted host is 10.4.48.11:443**



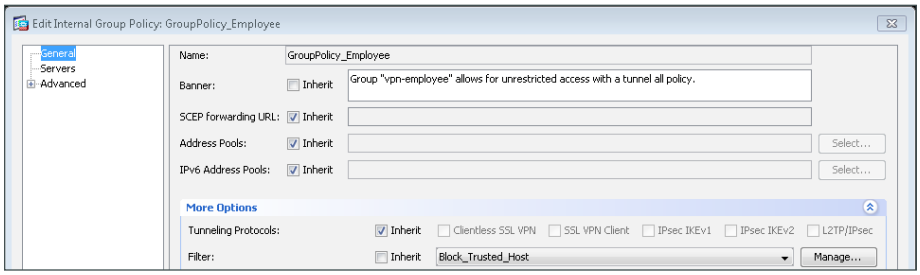
Step 10: Click **Add > Insert After**.

Step 11: On the Add ACE dialog box, configure the following values, and then click **OK**.

- Action–**Permit**
- Source–**any4**
- Destination–**any4**
- Service–**ip**
- Description–**Permit all other traffic**

Step 12: On the ACL Manager dialog box, click **OK**.

Step 13: On the Add Internal Group Policy dialog box, click **OK**.



Step 14: In the Group Policies pane, click **Apply**.

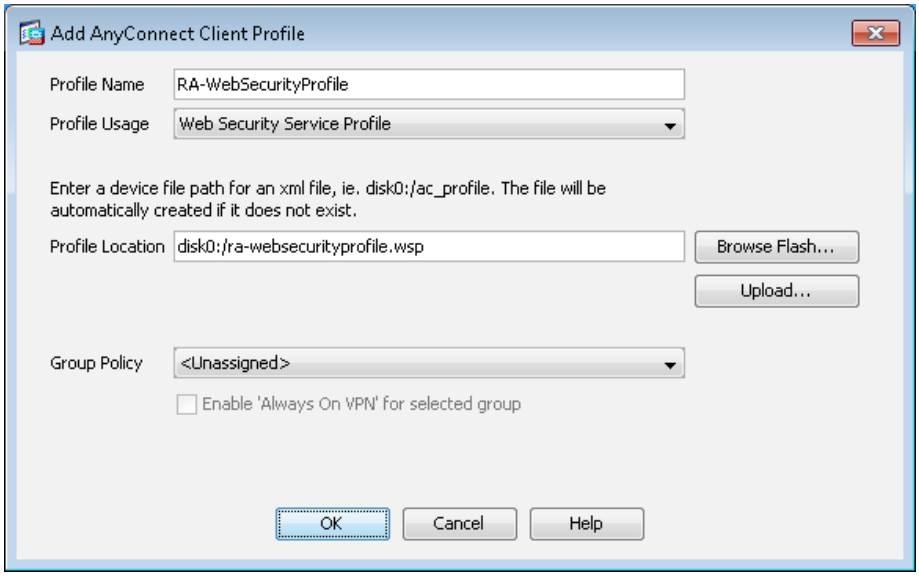
Procedure 3 Configure Policies for AnyConnect Cloud Web Security Module

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, select **Add**.

Step 2: On the Add AnyConnect Client Profile dialog box, in the Profile Name box, enter **RA-WebSecurityProfile**.

Step 3: In the **Profile Usage** list, choose **Web Security Service Profile**, click **OK**, and then click **Apply**.

> **Tech Tip**
>
> You must click Apply before you proceed to the next step. This ensures that the two required files are created before they are edited in Step 4.



Step 4: Select the newly created RA-WebSecurityProfile profile, and then click **Edit**.

A scanning proxy is a Cisco Cloud Web Security proxy server on which Cisco Cloud Web Security analyzes the Web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which Cisco Cloud Web Security scanning proxies the AnyConnect Web Security module redirects web traffic.

Step 5: In **Web Security > Scanning Proxy**, if the status is "Scanning Proxy list is currently up-to-date.", then skip to Step 6. If the status is "Updates to the Scanning Proxy list are now available.", then click **Update Proxies**. The Scanning Proxy list is updated.

Step 6: In the drop-down list, choose a default proxy location that best matches your location.

Add a list of individual IP addresses or IP address ranges in Classless Inter-Domain Routing (CIDR) notation for which traffic should bypass CWS. In the list, include the Internet facing public IP addresses of your RAVPN firewalls.

Step 7: In **Web Security > Exceptions**, review the list exceptions for internal networks. All of the RFC-1918 networks are already preconfigured as Static Exceptions.

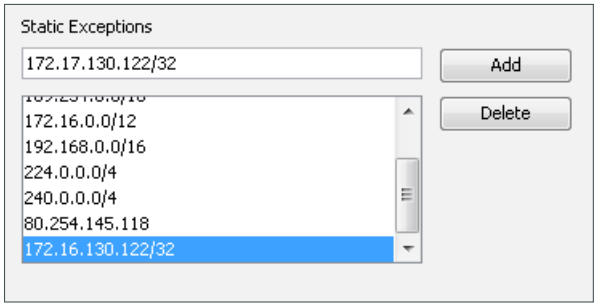
Table 1 - List of Static Exceptions

Default list of networks	Description
10.0.0.0/8	Private Network (RFC-1918)
172.16.0.0/12	Private Network (RFC-1918)
192.168.0.0/16	Private Network (RFC-1918)
127.0.0.0/8	Loopback (RFC-5735)
169.254.0.0/15	Link Local (RFC 3927)
224.0.0.0/4	IP multicast (RFC 5771)
240.0.0.0/4	Reserved (RFC 1700)
80.254.145.118	Cisco CWS (ScanSafe)

Tech Tip

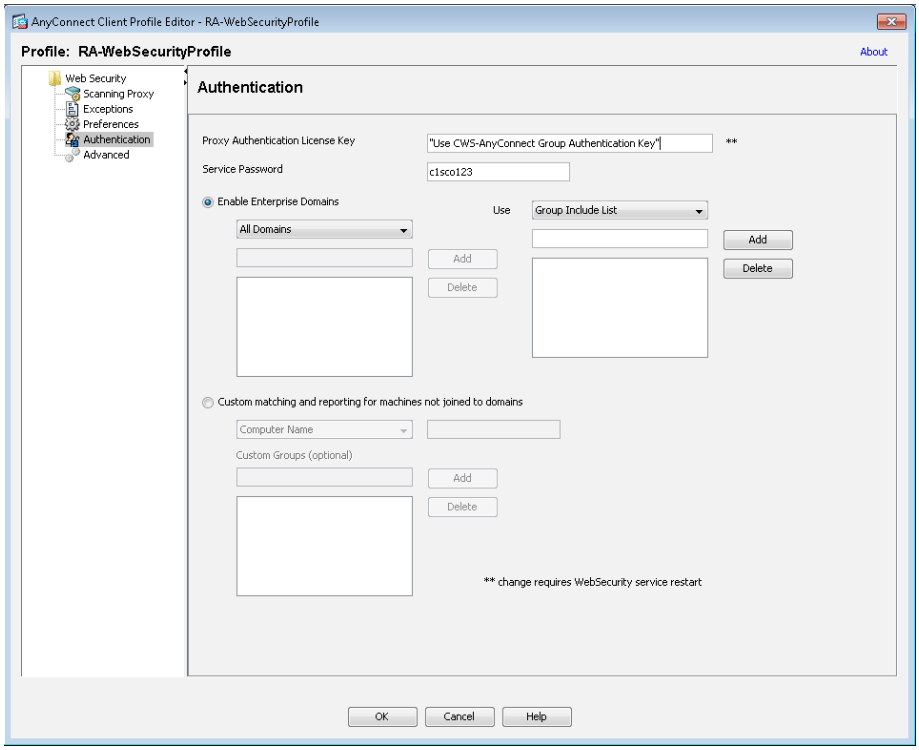
Make sure to add the IP address of your RAVPN firewall to the Static Exceptions list. If you have a resilient topology, then both the primary and backup addresses must be added to the list. Note, the addresses shown in the example (**172.16.130.22/32** and **172.17.130.122/32**) are already included within the RFC-1918 ranges but are shown as a reference.

Step 8: If you want to add other internal networks to the list of exceptions, in the Static Exceptions box, enter the network number in the format N.N.N.N/x, and then click **Add**. Repeat this step for all additional exceptions.



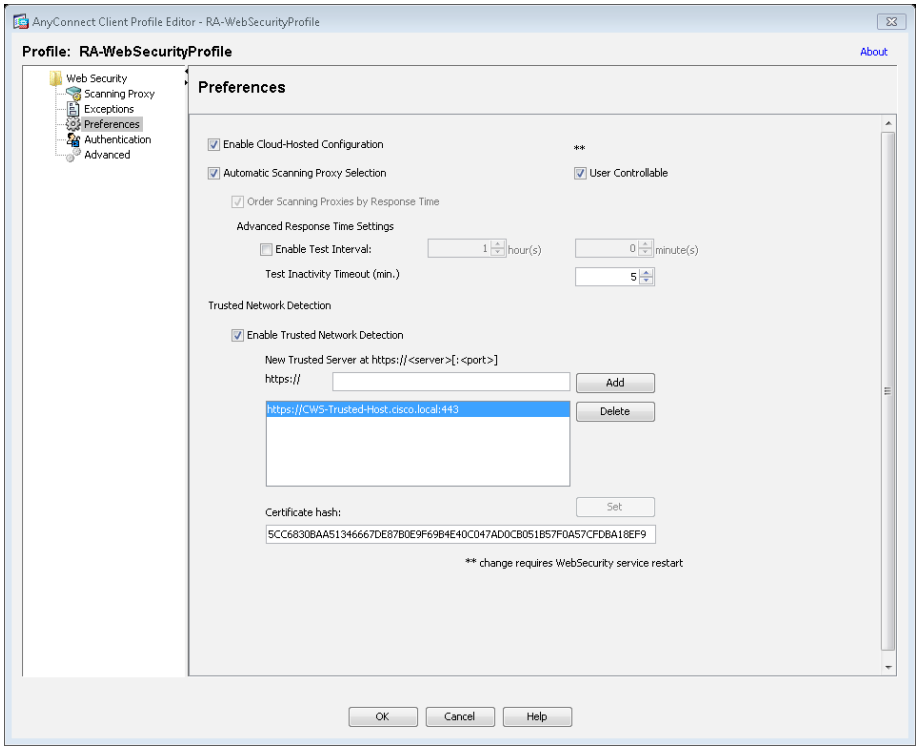
Step 9: In **Web Security > Authentication**, in the Proxy Authentication License Key box, enter the group key created in Step 6 of Procedure 1, "Enable CWS security configuration."

Step 10: In the Service Password box, enter a new password that will be associated with the Web Security service when the service is running on the end host. (Example: c1sco123)



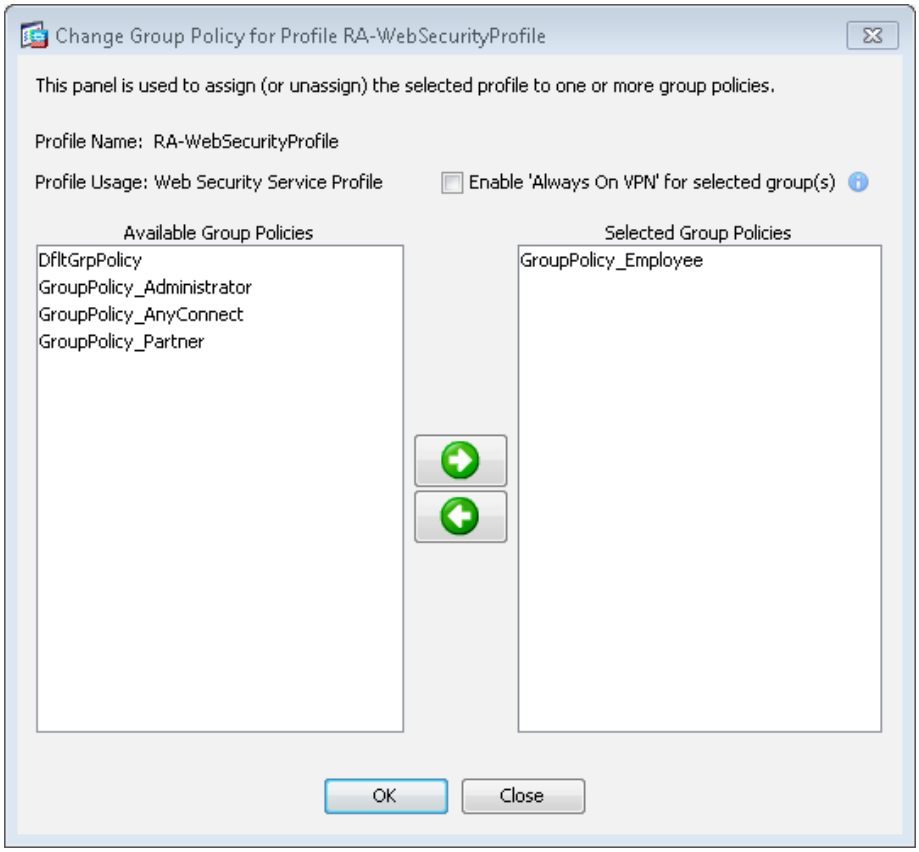
Step 11: In **Web Security > Preferences**, do the following:

- Select **Automatic Scanning Proxy Selection**.
- If your organization allows users to control use of web security functions, select **User Controllable**.
- In the Trusted Network Detection section, select **Enable Trusted Network Detection**.
- For New Trusted Server, enter the fully qualified domain name (FQDN) for the server (Example: CWS-Trusted-Host.cisco.local) configured in Procedure 2, "Configure ACL for trusted server," and then click **Add**.



Step 12: On the **Add AnyConnect Client Profile Editor** dialog box, click **OK**.

Step 13: Click **Change Group Policy**, select the group policy **GroupPolicy_Employee**, and then add it to the **Selected Group Policies** pane by clicking the right arrow, and then clicking **OK**.



Step 14: On the AnyConnect Client Profile screen, click **Apply**.

> **Tech Tip**
>
> Modifications to the AnyConnect Web Security Service Profile do not take effect on a client machine until after the next RAVPN connection, followed by a restart of the AnyConnect Web Security Agent service. A workstation reboot is the easiest way to restart this service.

Procedure 4 Configure ASA AnyConnect group policies

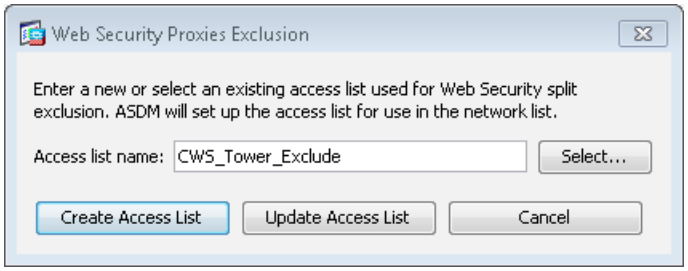
Step 1: In Cisco Adaptive Security Device Manager (ASDM), navigate to **Configuration > Remote Access VPN > Network Client Access > Group Policies**, select the **GroupPolicy_Employee** policy, and then click **Edit**.

Step 2: Under **Advanced**, select **Split Tunneling**.

Step 3: Next to **Policy**, clear the **Inherit** check box, and then choose **Exclude Network List Below**.

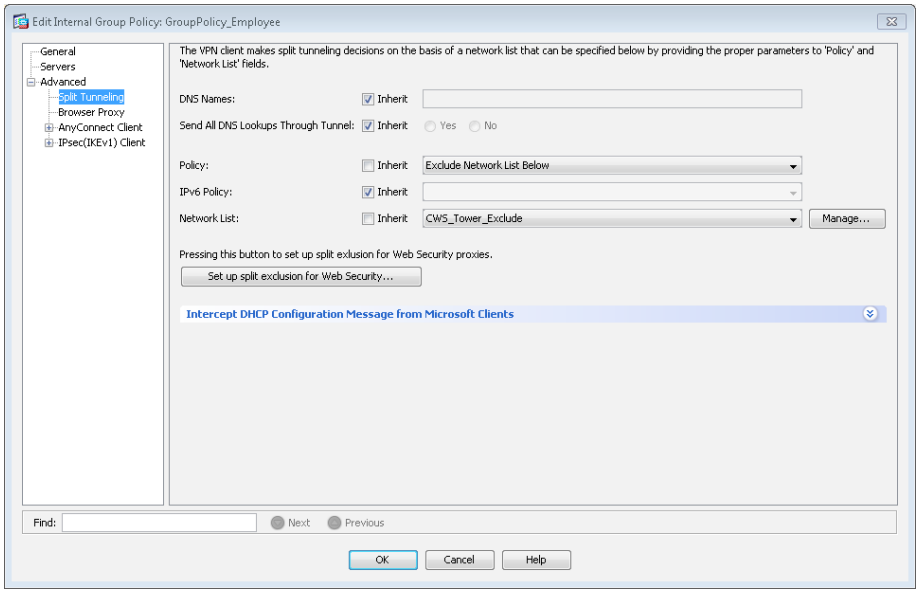
Step 4: Click **Set up split exclusion for Web Security**.

Step 5: On the Web Security Proxies Exclusion dialog box, in the **Access list name** box, enter **CWS_Tower_Exclude**, and then click **Create Access List**.



Step 6: On the Access List Result dialog box, review the list of proxies added to the access list, and then click **Close**.

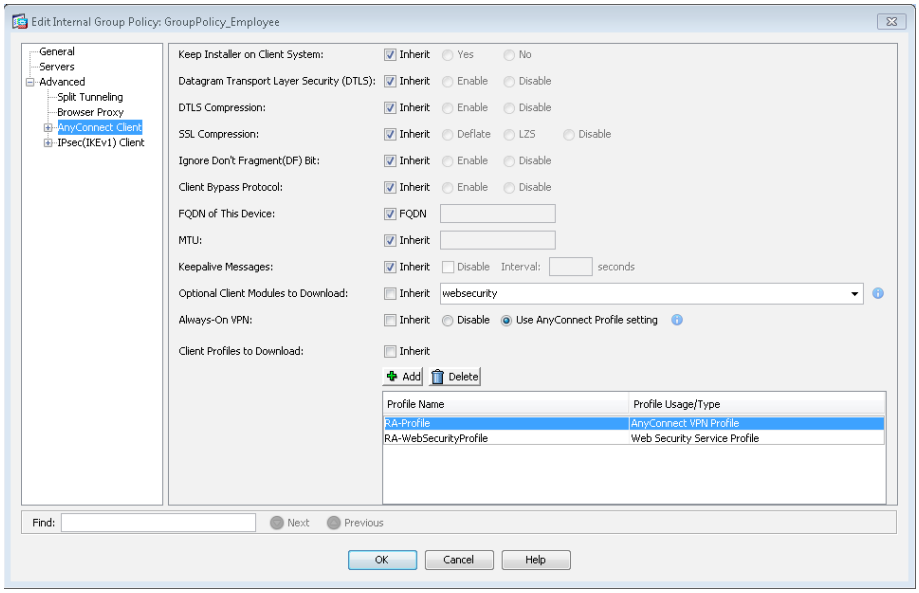
Step 7: Next to **Network List**, clear the **Inherit** check box, and then choose **CWS_Tower_Exclude**.



Step 8: Navigate to **Advanced > AnyConnect Client**. Under **Optional Client Modules to Download**, clear the **Inherit** check box**,** choose **AnyConnect Web Security** from the list, and then click **OK**.

Step 9: In the Always-On VPN section, clear the **Inherit** check box, and then select **Use AnyConnect Profile setting**.

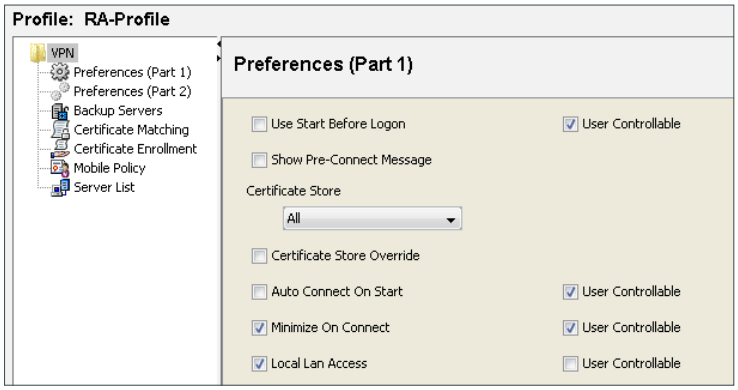
Step 10: In the Client Profiles to Download section, click **Add**, under Profile Name, choose **RA-WebSecurityProfile**, and then click **OK**.



Step 11: Click **OK**, and then click **Apply**.

Step 12: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, select the AnyConnect VPN Profile (Example: RA-Profile), and then click **Edit**.

Step 13: In **VPN > Preferences (Part 1)**, select **Local LAN Access**, which is required for a split tunnel exclude policy. Clear **User Controllable** for **Local LAN Access**.



Step 14: Click **OK**, and then click **Apply**.

Procedure 5 Install certificate on the client

(Optional)

This procedure is optional and only required if a self-signed certificate is generated and applied to Cisco ASA outside interfaces. Because of the untrusted nature of self-signed certificates, all clients generate an error until the certificate is manually added to the trusted certificates. Certificates signed by a trusted certificate authority (CA) don't need to be manually added.

Because some of the features configured later in this guide involve automatic certificate checking, it isn't acceptable to have the errors show up when self-signed certificates are used. This procedure solves the error problems.

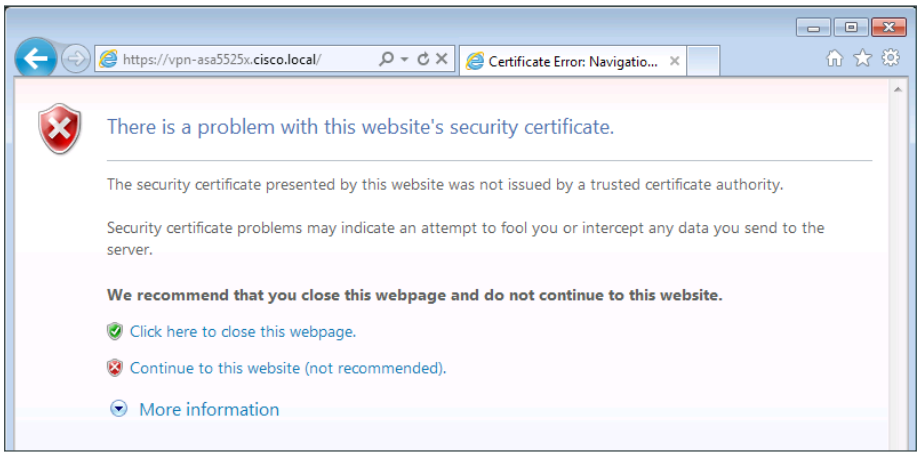
Trusted certificates do not have these issues and are easier to use in practice.

Tech Tip

It is essential that the DNS Fully Qualified Domain Name (FQDN) for the Cisco ASA can be resolved and that the interface certificates on the RAVPN Cisco ASA match properly.

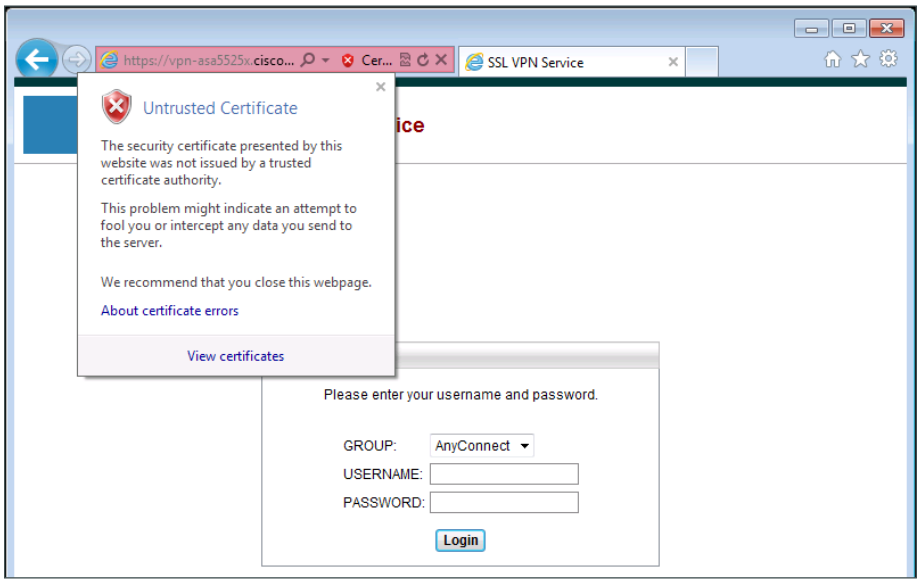
Step 1: On a client located outside the network, open a web browser (this procedure details the process for Internet Explorer), and go to the Cisco ASA address:
https://**vpn-asa5525x.cisco.local**

The first page reports a problem with the certificate.



Step 2: Click **Continue to this website**.

Step 3: On the next page, in the URL bar, click **Certificate Error**.



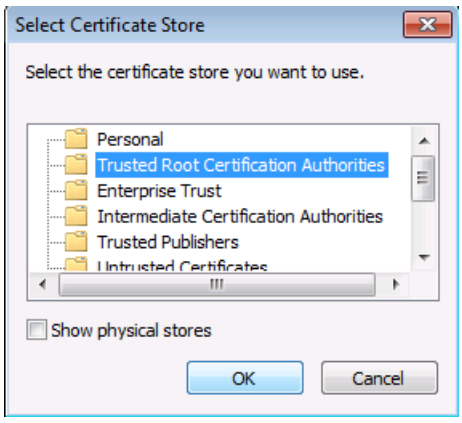
Step 4: Select **View Certificate**.

Step 5: At the bottom of the Certificate page, select **Install Certificate**. When the Certificate Import Wizard opens, click **Next**.

> **Tech Tip**
>
> If the Install Certificate option is not available, close the browser and reopen it with the **Run as administrator** option, and then restart this procedure from Step 1.

Step 6: Select **Place all Certificates in the following store**, and then click **Browse.**

Step 7: Select **Trusted Root Certification Authorities**, and then click **OK.**



Step 8: Click **Next**, and then click **Finish.**

Step 9: Accept the security warning and install the certificate.

Tech Tip

When outside a lab environment, be very careful when installing certificates; after they are installed, they are implicitly trusted by the client. Certificates issued by trusted certificate authorities do not have to be manually trusted.

Step 10: On the Certificate Import Wizard dialog box, click **OK**.

Step 11: In the **Certificate** window, click **OK**.

Step 12: Close and reopen the browser, and then navigate to the following location: https://**vpn-asa5525x.cisco.local**

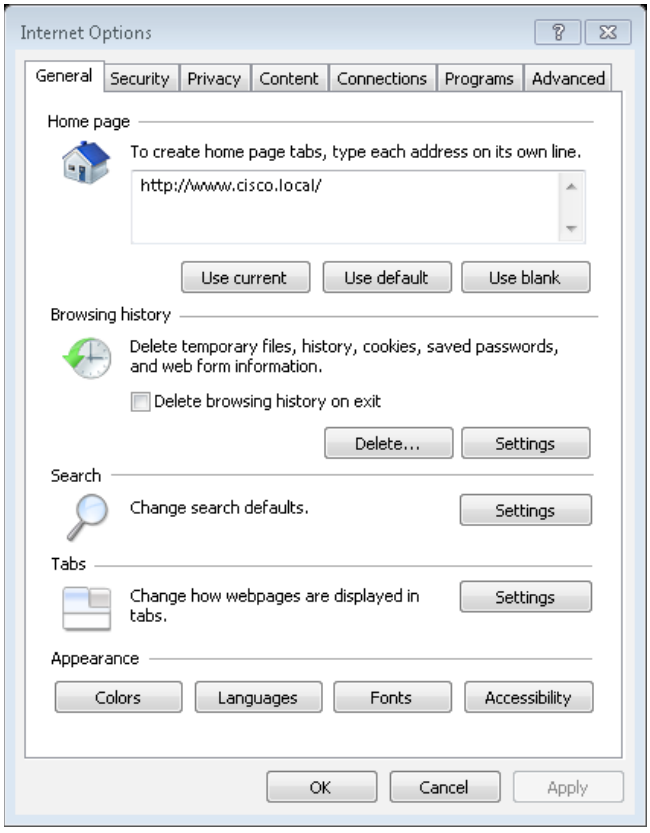
The SSL VPN Service page loads without any certificate warnings or errors.

Step 13: If you are using a resilient Internet connection, the RAVPN firewall has two outside interfaces, each with a different IP address and DNS name. Repeat Step 1 through Step 11 for the secondary outside interface using the Cisco ASA address: https://vpn-asa5525x-fo.cisco.local

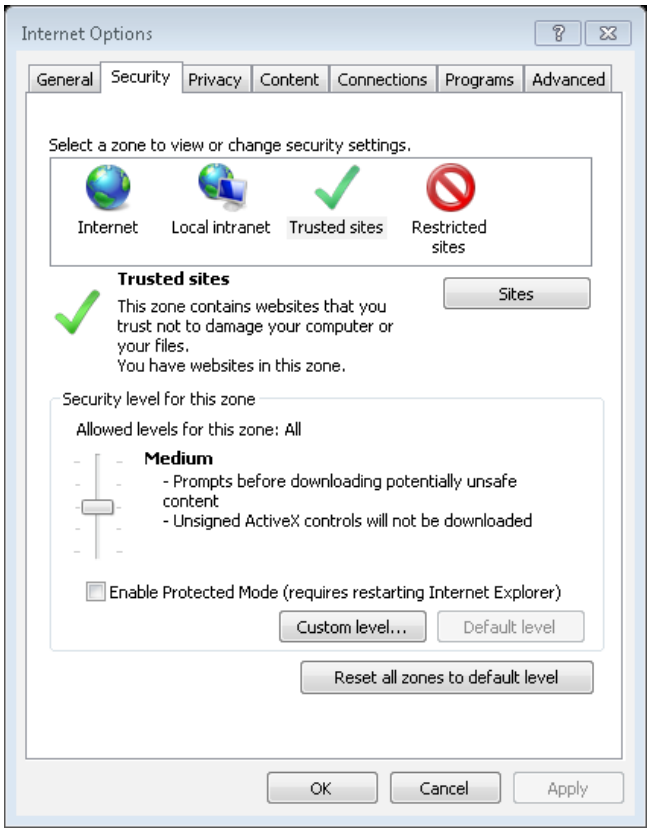
Procedure 6 Add RAVPN firewalls as trusted sites on the client

The weblaunch installer for the AnyConnect client may require that the RAVPN firewall be added to the list of trusted sites for Internet Explorer.

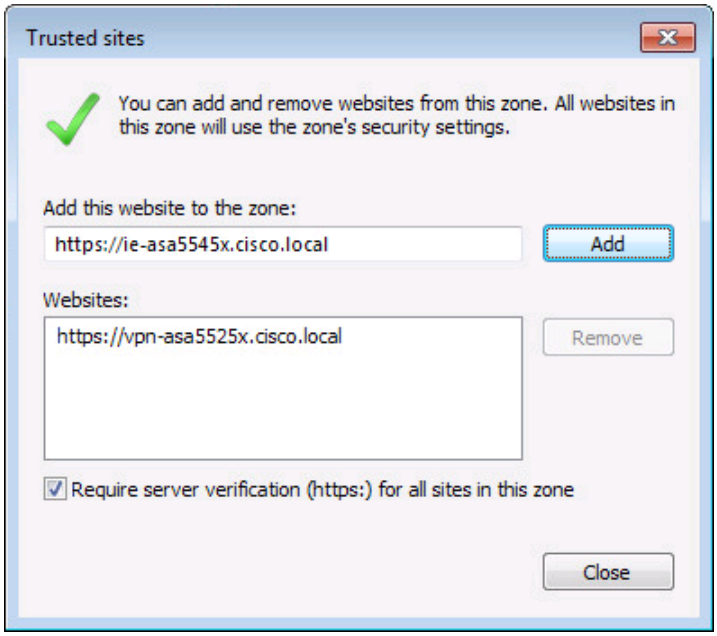
Step 1: Launch Internet Explorer, and then access the Internet Options screen by typing **Alt-X** and then clicking **Internet Options**.



Step 2: Click the **Security** tab, click the **Trusted sites** zone to select, and then click **Sites**.



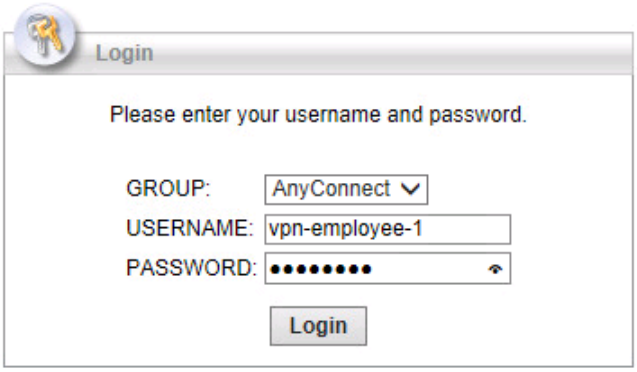
Step 3: Add RAVPN firewall(s) as trusted sites by entering the fully qualified URL (Example: https://vpn-asa5525x.cisco.local), and then clicking **Add**. Repeat for any additional RAVPN firewalls, and then click **Close**.



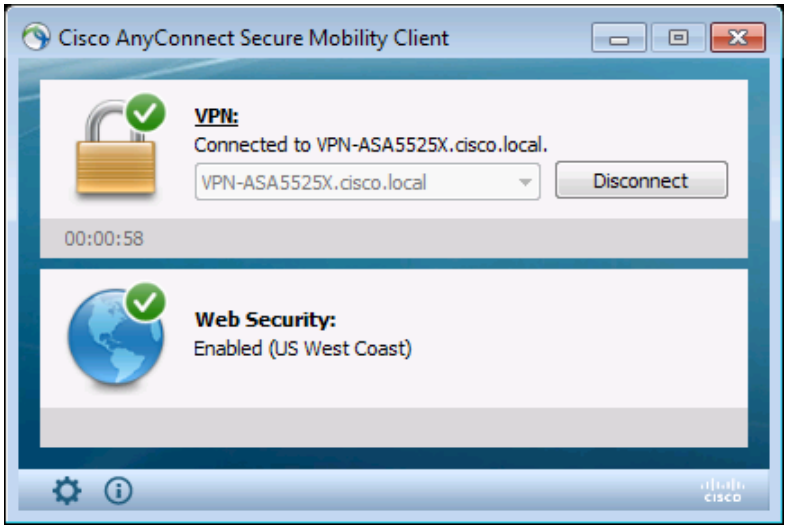
Step 4: In the Internet Options window, click **OK**.

Procedure 7 Test the AnyConnect configuration

Step 1: Log in using a known username and password that is part of the vpn-employee group in Windows AD. If Cisco AnyConnect 3.1 is not installed, the client software is downloaded and installed. If necessary, accept installation warnings.

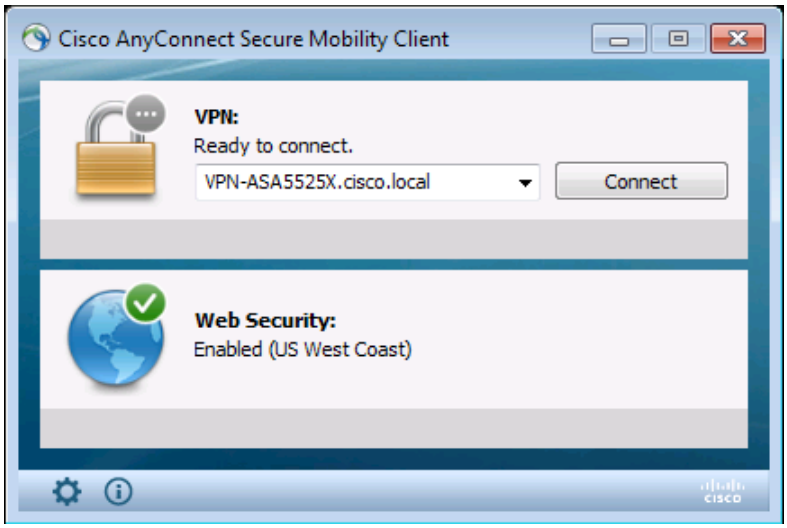


Step 2: After you are connected, click the Cisco AnyConnect taskbar icon. This displays the client information panel.



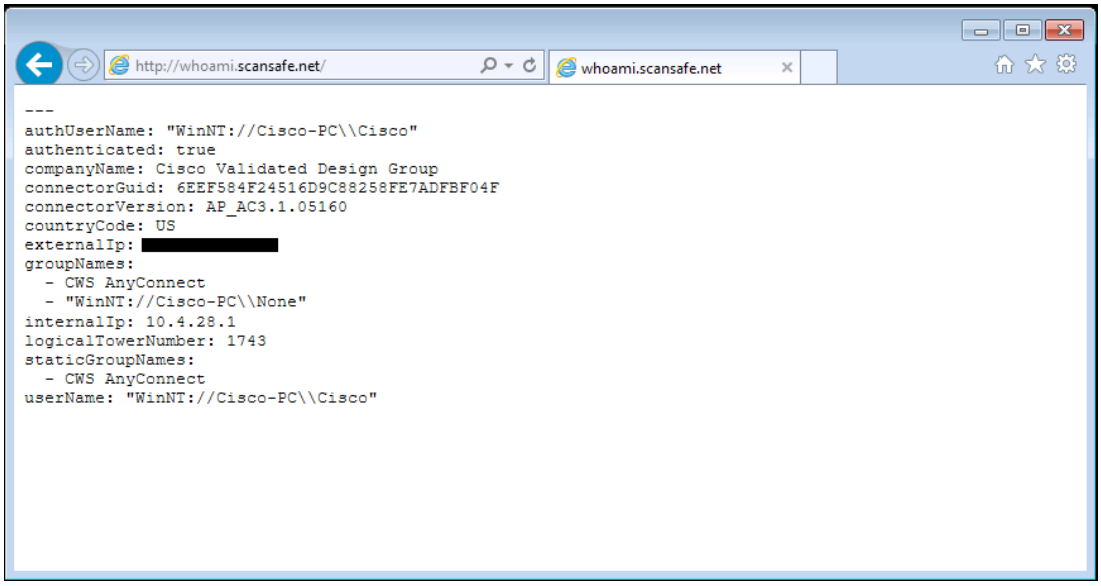
Step 3: Verify there is a green check for both VPN and Web Security.

Step 4: Click **Disconnect**, and then verify that Web Security remains enabled.

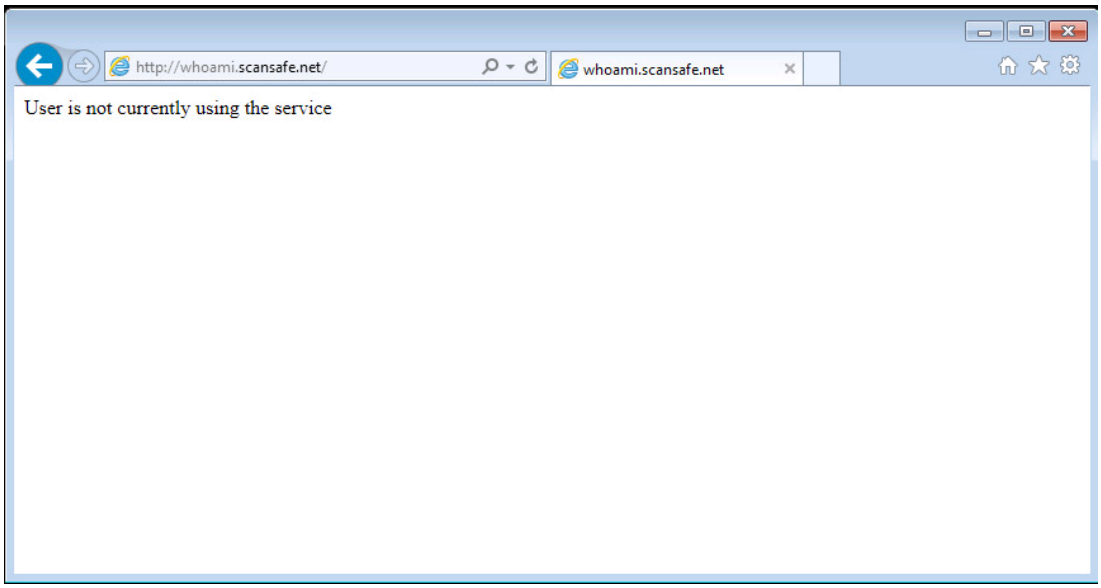


Procedure 8 Test Cloud Web Security

Step 1: Open a web browser to http://whoami.scansafe.net. This browser returns diagnostic information from the Cisco CWS service.



If the service is not active, the following information is returned.

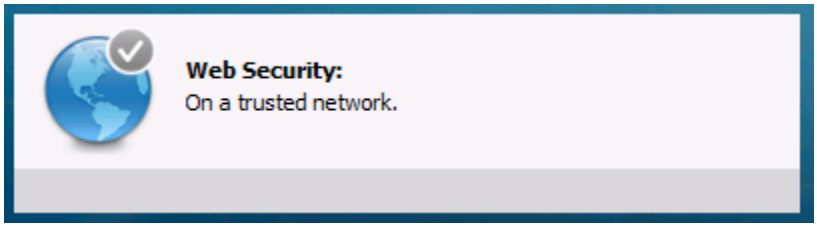


Verify Cisco CWS Trusted Network Detection by selecting a client that is connected outside the network and has the Web Security module enabled.

Step 2: Move the client to a location on the trusted network. The AnyConnect client should be in a disconnected state for this step.

When the client is on the trusted network, it should be able to reach the trusted server configured in Procedure 3, "Configure ASA VPN policy for web security," Step 11. (Example: 10.4.48.11:443)

The ability to connect to the trusted server successfully tells the Cisco AnyConnect client that it is directly connected to the internal network and that the CWS module is not necessary and should not be run because the client now resides on a trusted network. The host's web connections to external websites are now instead secured by the organization's Internet edge devices and policy. This is verified on the AnyConnect client status pane.



Procedure 9 Synchronize the profiles to failover ASA

When running an RAVPN Cisco ASA firewall pair, the Cisco AnyConnect VPN Profile file and the Web Security Service Profile files must be manually replicated to the secondary ASA firewall. All of the files listed in Table 2 must be replicated.

Tech Tip

This procedure is required after any modification to either the Cisco AnyConnect VPN Profile or the Web Security Service Profile.

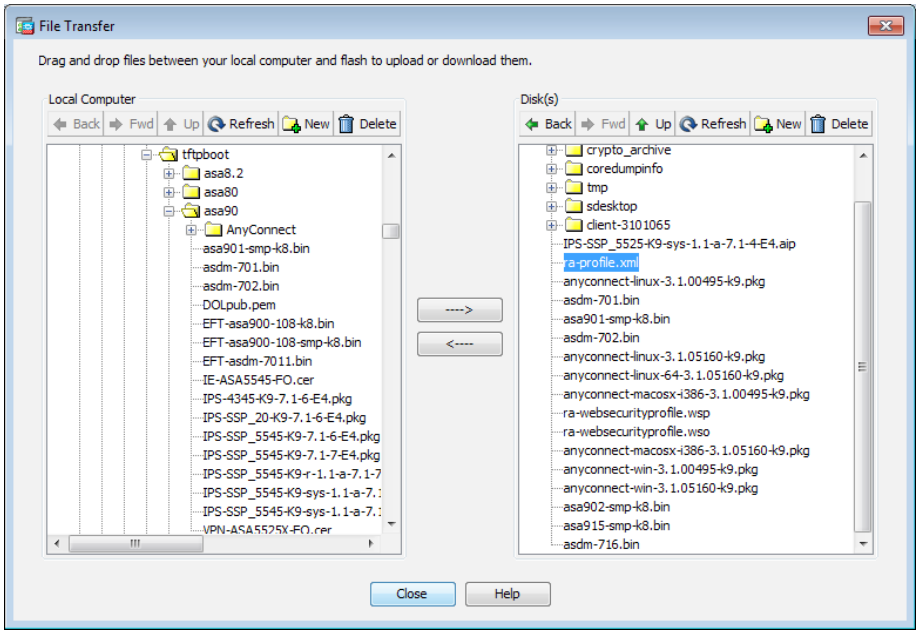
Table 2 - Cisco AnyConnect Client Profile files

Profile type	Profile name	Filename
AnyConnect VPN Profile	RA-Profile	ra-profile.xml
Web Security Service Profile	RA-WebSecurityProfile	ra-websecurityprofile.wsp
Web Security Service Profile (obscured)	RA-WebSecurityProfile	ra-websecurityprofile.wso

Step 1: Navigate to **Tools > File Management.**

Step 2: Click **File Transfer**, and then select **Between Local PC and Flash**.

Browse to a destination on your local file system and copy the AnyConnect client profile file from the Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking the left arrow.



Step 3: Repeat Step 2 for the remaining files in Table 2.

Step 4: After completing all of the file transfers, click **Close**.

Step 5: Navigate to the secondary RAVPN Cisco ASA's inside IP address, and then launch Cisco ASDM. (Example: https://10.4.24.23)

> **Tech Tip**
>
> Do not attempt to modify the firewall configuration on the standby Cisco ASA. Configuration changes are only made on the primary ASA.

Step 6: Navigate to **Tools > File Management**.

Step 7: Click **File Transfer**, and then select **Between Local PC and Flash**.

Step 8: Browse to a destination on your local file system and copy the AnyConnect client profile file to the secondary Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking the right arrow.

Step 9: Repeat Step 8 for the remaining files in Table 2.

Step 10: After completing all of the file transfers, click **Close**.

Step 11: Close Cisco ASDM on the secondary RAVPN Cisco ASA.

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.1(5) IPS 7.1(8p2)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.1(6)
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	ASA 9.1(5)
	Cisco ASA 5525-X Firewall Edition - security appliance	ASA5525-K9	
	Cisco ASA 5515-X Firewall Edition - security appliance	ASA5515-K9	
	Cisco ASA 5512-X Firewall Edition - security appliance	ASA5512-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.1(6)
AnyConnect License	AnyConnect Essentials VPN License - ASA 5545-X (2500 Users)	L-ASA-AC-E-5545	–
	AnyConnect Essentials VPN License - ASA 5525-X (750 Users)	L-ASA-AC-E-5525	
	AnyConnect Essentials VPN License - ASA 5515-X (250 Users)	L-ASA-AC-E-5515	
	AnyConnect Essentials VPN License - ASA 5512-X (250 Users)	L-ASA-AC-E-5512	
	AnyConnect Premium VPN License (2500 users)	L-ASA-SSL-2500	
	AnyConnect Premium VPN License (500 Users)	L-ASA-SSL-500	
	AnyConnect Premium VPN License (250 Users)	L-ASA-SSL-250	

VPN Client

Functional Area	Product Description	Part Numbers	Software
VPN Client	Cisco AnyConnect Secure Mobility Client (Windows)	Cisco AnyConnect Secure Mobility Client	3.1.05160
	Cisco AnyConnect Secure Mobility Client (Mac OS X)	Cisco AnyConnect Secure Mobility Client	

Web Security

Functional Area	Product Description	Part Numbers	Software
Cloud Web Security	Cisco Cloud Web Security (ScanSafe)	Cisco Cloud Web Security	–
	Cisco Cloud Web Security (ScanSafe)	Please Contact your Cisco Cloud Web Security Sales Representative for Part Numbers: scansafe-sales-questions@cisco.com	

Appendix B: Configuration Example

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

RAVPN: VPN-ASA5525X

```
ASA Version 9.1(5)
!
hostname VPN-ASA5525X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RA-pool 10.4.28.1-10.4.31.254 mask 255.255.252.0
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.122 255.255.255.0
!
interface GigabitEthernet0/3.17
 vlan 17
 nameif outside-17
 security-level 0
 ip address 172.17.130.122 255.255.255.0
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
same-security-traffic permit intra-interface
object network NETWORK_OBJ_10.4.28.0_22
 subnet 10.4.28.0 255.255.252.0
object network asdm-websecproxy-115-111-223-66
 host 115.111.223.66
object network asdm-websecproxy-122-50-127-66
 host 122.50.127.66
object network asdm-websecproxy-184-150-236-66
 host 184.150.236.66
object network asdm-websecproxy-196-26-220-66
 host 196.26.220.66
object network asdm-websecproxy-201-94-155-66
 host 201.94.155.66
object network asdm-websecproxy-202-167-250-90
 host 202.167.250.90
object network asdm-websecproxy-202-167-250-98
 host 202.167.250.98
object network asdm-websecproxy-202-177-218-66
 host 202.177.218.66
object network asdm-websecproxy-202-79-203-98
 host 202.79.203.98
object network asdm-websecproxy-46-255-40-58
 host 46.255.40.58
object network asdm-websecproxy-46-255-40-90
 host 46.255.40.90
object network asdm-websecproxy-46-255-40-98
 host 46.255.40.98
object network asdm-websecproxy-69-10-152-66
 host 69.10.152.66
object network asdm-websecproxy-69-174-58-179
 host 69.174.58.179
object network asdm-websecproxy-69-174-58-187
 host 69.174.58.187
object network asdm-websecproxy-69-174-87-131
 host 69.174.87.131
object network asdm-websecproxy-69-174-87-163
```

```
 host 69.174.87.163
object network asdm-websecproxy-69-174-87-171
 host 69.174.87.171
object network asdm-websecproxy-69-174-87-75
 host 69.174.87.75
object network asdm-websecproxy-70-39-176-115
 host 70.39.176.115
object network asdm-websecproxy-70-39-176-123
 host 70.39.176.123
object network asdm-websecproxy-70-39-176-131
 host 70.39.176.131
object network asdm-websecproxy-70-39-176-139
 host 70.39.176.139
object network asdm-websecproxy-70-39-176-35
 host 70.39.176.35
object network asdm-websecproxy-70-39-176-59
 host 70.39.176.59
object network asdm-websecproxy-70-39-177-35
 host 70.39.177.35
object network asdm-websecproxy-70-39-177-43
 host 70.39.177.43
object network asdm-websecproxy-70-39-231-107
 host 70.39.231.107
object network asdm-websecproxy-70-39-231-163
 host 70.39.231.163
object network asdm-websecproxy-70-39-231-171
 host 70.39.231.171
object network asdm-websecproxy-70-39-231-180
 host 70.39.231.180
object network asdm-websecproxy-70-39-231-182
 host 70.39.231.182
object network asdm-websecproxy-70-39-231-188
 host 70.39.231.188
object network asdm-websecproxy-70-39-231-190
 host 70.39.231.190
object network asdm-websecproxy-70-39-231-91
 host 70.39.231.91
object network asdm-websecproxy-72-37-244-163
 host 72.37.244.163
object network asdm-websecproxy-72-37-244-171
 host 72.37.244.171
object network asdm-websecproxy-72-37-248-19
 host 72.37.248.19
object network asdm-websecproxy-72-37-248-27
 host 72.37.248.27
object network asdm-websecproxy-72-37-249-139
 host 72.37.249.139
```

```
object network asdm-websecproxy-72-37-249-147
 host 72.37.249.147
object network asdm-websecproxy-72-37-249-163
 host 72.37.249.163
object network asdm-websecproxy-72-37-249-171
 host 72.37.249.171
object network asdm-websecproxy-72-37-249-195
 host 72.37.249.195
object network asdm-websecproxy-72-37-249-203
 host 72.37.249.203
object network asdm-websecproxy-80-254-147-251
 host 80.254.147.251
object network asdm-websecproxy-80-254-148-194
 host 80.254.148.194
object network asdm-websecproxy-80-254-150-66
 host 80.254.150.66
object network asdm-websecproxy-80-254-154-66
 host 80.254.154.66
object network asdm-websecproxy-80-254-154-98
 host 80.254.154.98
object network asdm-websecproxy-80-254-155-66
 host 80.254.155.66
object network asdm-websecproxy-80-254-158-147
 host 80.254.158.147
object network asdm-websecproxy-80-254-158-155
 host 80.254.158.155
object network asdm-websecproxy-80-254-158-179
 host 80.254.158.179
object network asdm-websecproxy-80-254-158-187
 host 80.254.158.187
object network asdm-websecproxy-80-254-158-211
 host 80.254.158.211
object network asdm-websecproxy-80-254-158-219
 host 80.254.158.219
object network asdm-websecproxy-80-254-158-35
 host 80.254.158.35
object network internal-network
 subnet 10.4.0.0 255.254.0.0
 description Internal Network
access-list ALL_BUT_DEFAULT standard deny host 0.0.0.0
access-list ALL_BUT_DEFAULT standard permit any4
access-list RA_PartnerACL remark Partners can access this internal host only!
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal Networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0 255.254.0.0
access-list RA_SplitTunnelACL remark DMZ Networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0 255.255.248.0
```

```
access-list Block_Trusted_Host remark Trusted Host is 10.4.48.11:443
access-list Block_Trusted_Host extended deny tcp any4 host 10.4.48.11 eq https
access-list Block_Trusted_Host remark Permit All other traffic
access-list Block_Trusted_Host extended permit ip any4 any4
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-147-251
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-155
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-147
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-179
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-187
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-211
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-219
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-148-194
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-58
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-90
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-150-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-154-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
```

```
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-154-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-155-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-196-26-220-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-201-94-155-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-184-150-236-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-10-152-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-244-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-244-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-248-19
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-248-27
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-107
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-91
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-180
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-182
any
```

```
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-188
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-190
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-58-179
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-58-187
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-59
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-115
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-123
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-131
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-139
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-139
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-147
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-195
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-203
```

```
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-177-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-177-43
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-75
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-131
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-167-250-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-167-250-90
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-115-111-223-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-122-50-127-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-79-203-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-177-218-66
any
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside-16 1500
mtu outside-17 1500
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
```

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.97 255.255.255.248 standby 10.4.24.98
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside-17) source static any any destination static NETWORK_
OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp route-lookup
nat (inside,outside-16) source static any any destination static NETWORK_
OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp route-lookup
!
router eigrp 100
 no auto-summary
 distribute-list ALL_BUT_DEFAULT out
 network 10.4.0.0 255.254.0.0
 passive-interface default
 no passive-interface inside
 redistribute static
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 50
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15
 key SecretKey
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
 timeout 5
 key SecretKey
user-identity default-domain LOCAL
```

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community cisco
no snmp-server location
no snmp-server contact
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sla monitor 16
 type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-
SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint VPN-ASA5525X-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint VPN-ASA5525X-FO-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X-FO.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=VPN-ASA5525X
```

```
 keypair foobar
 proxy-ldc-issuer
 crl configure
crypto ca trustpool policy
crypto ca certificate chain VPN-ASA5525X-Trustpoint
 certificate 196dbd50
    [certificate omitted]
  quit
crypto ca certificate chain VPN-ASA5525X-FO-Trustpoint
 certificate 1a6dbd50
    [certificate omitted]
  quit
crypto ikev1 enable outside-16
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
```

```
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
```

```
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ssl trust-point VPN-ASA5525X-FO-Trustpoint outside-17
ssl trust-point VPN-ASA5525X-Trustpoint outside-16
webvpn
 enable outside-16
 enable outside-17
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.05160-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-3.1.05160-k9.pkg 2
 anyconnect image disk0:/anyconnect-linux-3.1.05160-k9.pkg 3
 anyconnect image disk0:/anyconnect-linux-64-3.1.05160-k9.pkg 4
 anyconnect profiles RA-Profile disk0:/ra-profile.xml
 anyconnect profiles RA-WebSecurityProfile disk0:/ra-websecurityprofile.wsp
 anyconnect profiles RA-WebSecurityProfile.wso disk0:/ra-websecurityprofile.wso
 anyconnect enable
 tunnel-group-list enable
group-policy GroupPolicy_Employee internal
group-policy GroupPolicy_Employee attributes
 banner value Group "vpn-employee" allows for unrestricted access with a tunnel all
policy.
 vpn-filter value Block_Trusted_Host
 split-tunnel-policy excludespecified
 split-tunnel-network-list value CWS_Tower_Exclude
 webvpn
  anyconnect modules value websecurity
  anyconnect profiles value RA-Profile type user
  anyconnect profiles value RA-WebSecurityProfile.wso type websecurity
```

```
  always-on-vpn profile-setting
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
 wins-server none
 dns-server value 10.4.48.10
 vpn-tunnel-protocol ssl-client
 default-domain value cisco.local
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
 banner value Group "vpn-partner" allows for access control list (ACL) restricted access
with a tunnel all policy.
 vpn-filter value RA_PartnerACL
 webvpn
  anyconnect profiles value RA-Profile type user
group-policy GroupPolicy_Administrator internal
group-policy GroupPolicy_Administrator attributes
 banner value Group "vpn-administrator" allows for unrestricted access with a split
tunnel policy.
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 webvpn
  anyconnect profiles value RA-Profile type user
username admin password 7KKG/zg/Wo8c.YfN encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool RA-pool
 authentication-server-group AAA-RADIUS
 default-group-policy GroupPolicy_AnyConnect
 password-management
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyConnect enable
 group-url https://172.16.130.122/AnyConnect enable
 group-url https://172.17.130.122/AnyConnect enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
: end
```

Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We upgraded the Cisco ASA software to 9.1(5).
- We upgraded the Cisco ASDM software to 7.1(6).
- We made minor modifications to improve the clarity of this guide.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000150-1 09/14