Cloud Web Security Using Cisco ASA

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:

- **Manage the Safe Use of Web-Based and Social Networking Applications for Internal Users and Guests**—All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco Cloud Web Security (CWS) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security though a cloud-based service.

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 provide Internet edge firewall security and intrusion prevention.
- 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

Remote Access VPN Technology Design Guide

Cloud Web Security Using Cisco AnyConnect Technology Design Guide

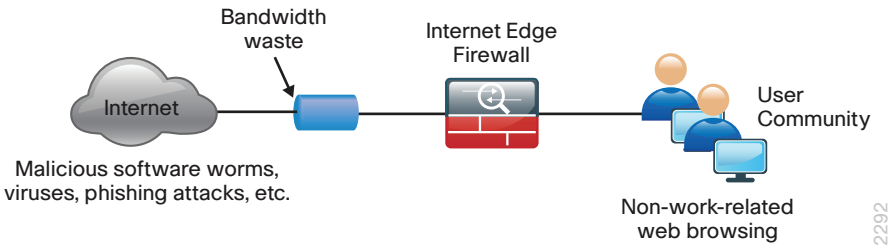
To view the related CVD guides, click the titles or visit the CVD Foundation web site.

Introduction

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access in order to ensure employees work effectively and ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

Another risk associated with Internet access for the organization is the pervasive threat that exists from accessing sites and content. As the monetary gain for malicious activities on the Internet has grown and developed, the methods used to affect these malicious and or illegal activities has grown and become more sophisticated. *Botnets*, one of the greatest threats that exists in the Internet today, are malicious Internet servers (mostly web) being used to host content that then attacks innocent user's browsers as they view the content. These types of attacks have been used very successfully by *bot herders* (originators of the attack) in order to gather millions of infected members that are subject to the whims of the people who now control their machines. Other threats include the still popular and very broad threats of viruses and *Trojans*, in which a user receives a file in some manner and is tricked into running it, and the file then executes malicious code. The third variant uses directed attacks over the network. Examples of these attacks are the Internet worms that gathered so much attention in the early to mid-2000s. These types of risks are depicted in the figure below.

Figure 1 - Business reasons for deploying Cisco Cloud Web Security



Technology Use Cases

Cisco Cloud Web Security (CWS) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.

Browsing websites can be risky, and many websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or lax security configurations. The websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the Internet in search of additional web servers that they can infect in order to continue propagating. This dynamic environment introduces significant challenges to maintain up-to-date Internet threat profiles.

Use Case: Manage the Safe Use of Web-Based and Social Networking Applications for Internal Users and Guests

All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco CWS complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security though a cloud-based service.

This design guide enables the following security capabilities:

- **Transparent redirection of user web traffic**—Through seamless integration with the Cisco ASA firewall, web traffic is transparently redirected to the Cisco CWS service. No additional hardware or software is required, and no configuration changes are required on user devices.
- **Web filtering**—Cisco CWS supports filters based on predefined content categories, and it also supports more detailed 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.
- **Malware protection**—Cisco CWS analyzes every web request in order to determine if content is malicious. CWS is powered by the Cisco Security Intelligence Operations (SIO) whose primary role is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- **Differentiated policies**—The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key of the forwarding firewall, source IP address of the web request, or the Microsoft Active Directory user and domain information of the requestor.

Design Overview

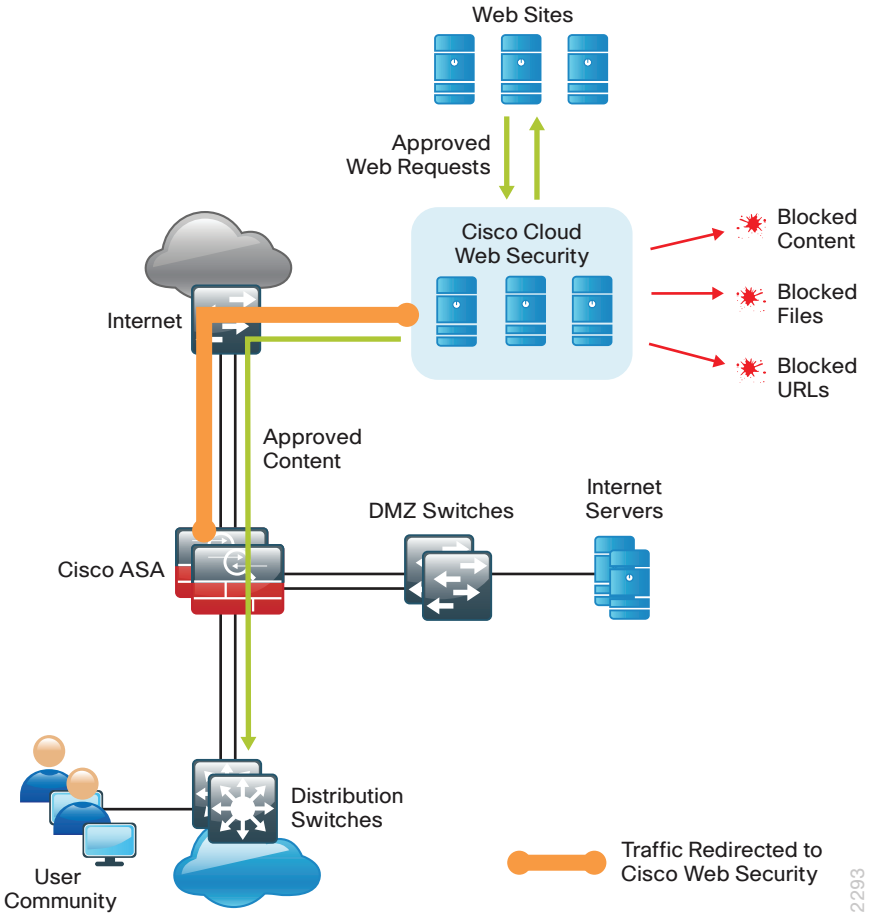
The Cisco Validated Design (CVD) Internet edge design provides the basic framework for the enhancements and additions that are discussed in this guide. A prerequisite for using this design guide is that you must have already followed the guidance in the Firewall and IPS Technology Design Guide.

Through the use of multiple techniques, Cisco CWS provides granular control over all web content that is accessed. These techniques include real-time dynamic web content classification, a URL-filtering database, and file-type and content filters. The policies enforced by Cisco CWS provide strong web security and control for an organization. Cisco CWS policies apply to all users regardless of their location and device type.

Internal users at both the primary site and at remote sites access the Internet by using the primary site's Internet-edge Cisco Adaptive Security Appliance (ASA), which provides stateful firewall and intrusion prevention capabilities. It is simple and straightforward to add Cisco CWS to a Cisco ASA appliance that is already configured and operational. This integration uses the Cloud Web Security Cloud Connector for Cisco ASA and requires no additional hardware.

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 CWS Cloud Connector for Cisco ASA provides users with transparent access to a cloud service and is classified as an embedded cloud connector application.

Figure 2 - Cisco Cloud Web Security deployment



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. Laptops and other devices that support the Cisco AnyConnect Secure Mobility Client with Cisco CWS are not required to send web traffic to the primary site. This solution is covered in detail in the Cloud Web Security Using Cisco AnyConnect Technology Design Guide. If you have an existing CWS deployment for remote-access users, the procedures are similar.

Cisco CWS using Cisco ASA also protects mobile users who are using a non-CWS-enabled Cisco AnyConnect Secure Mobility Client that connects through remote-access VPN, as detailed in the Remote Access VPN Technology Design Guide.

Cisco CWS is a cloud-based method of implementing web security that is similar in function to the Cisco Web Security Appliance (WSA), which uses an on-premise appliance for web security. This guide is focused on the deployment of Cisco CWS on Cisco ASA. For more information about using Cisco WSA, see the Web Security Using Cisco WSA Technology Design Guide.

Some key differences between Cisco CWS and Cisco WSA include the items listed in the following table.

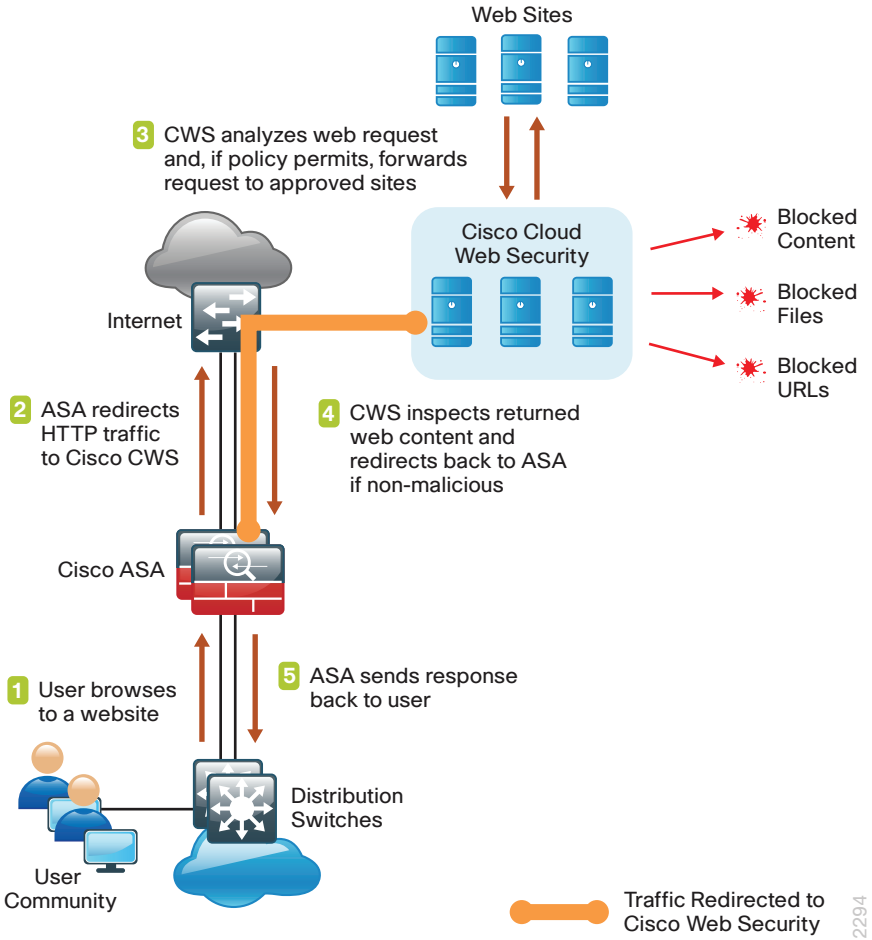
Table 1 - Cisco Web Security solution comparison

	Cisco CWS	Cisco WSA
Web/URL filtering	Yes	Yes
Supported protocols	HTTP and HTTPS	HTTP and HTTPS, FTP
Outbreak Intelligence (zero-day malware)	Yes (multiple scanners for malware)	Yes (URL/IP reputation filtering, Multiple scanners for malware)
Remote user security	Direct to cloud using Cisco AnyConnect	VPN backhaul
Remote user security (mobile devices)	VPN backhaul	VPN backhaul
Deployment	Redirect to cloud service	On-premises redirect
Policy and reporting	Web portal (cloud)	On premises

Many organizations provide guest access by using wireless LAN and enforce an acceptable use policy and provide additional security for guest users by using Cisco CWS. This guide includes a section on how to deploy CWS for wireless guest users without requiring any configuration changes to Cisco ASA.

The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security. The design uses Cisco ASA to implement a service policy that matches specified traffic and redirects the traffic to the Cisco CWS cloud for inspection by using a cloud connector. This method is considered a transparent proxy, and no configuration changes are required to web browsers on user devices.

Figure 3 - Cisco Cloud Web Security detailed traffic flow



The easiest way to apply the service policy is to modify the existing global service policy to add Cisco CWS inspection. The global policy applies to traffic received on any interface, so the same service policy applies to the following:

- Internal users at the primary site or at remote sites
- Wireless guest users connected to a demilitarized zone (DMZ) network
- Remote-access VPN users using a non-CWS-enabled Cisco AnyConnect client connecting with either the integrated firewall and VPN model or standalone VPN model

The various traffic flows for each of these user types are shown in the following figures.

Figure 4 - Cisco Cloud Web Security with internal and guest users

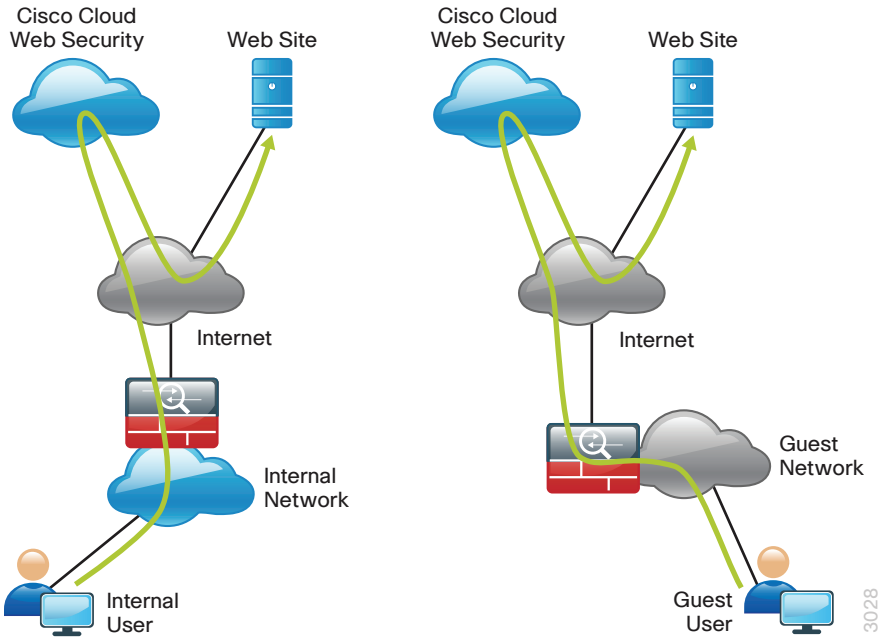
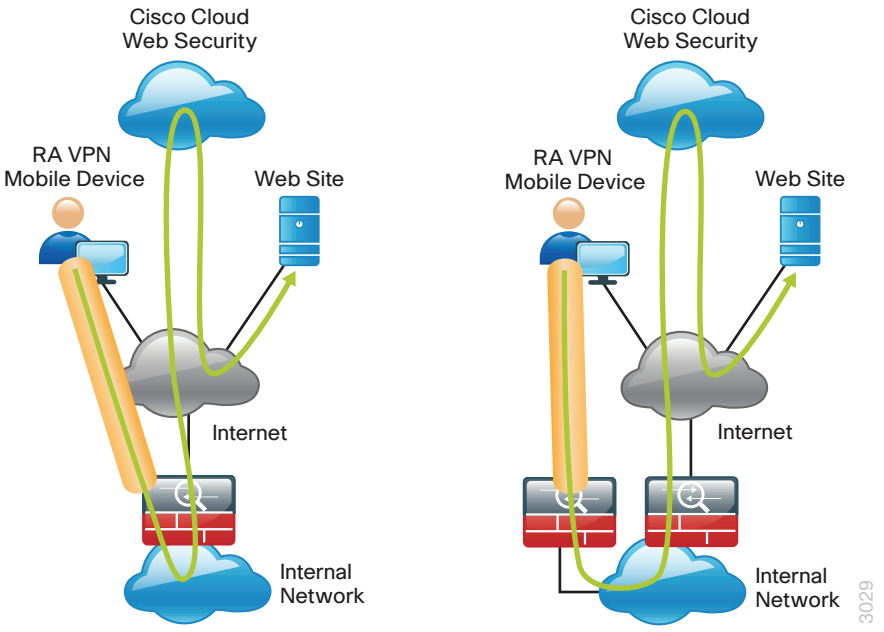


Figure 5 - Cisco Cloud Web Security for mobile devices using remote-access VPN



Certain source and destination pairs should be exempted from the service policy, such as remote-access VPN users accessing internal networks or internal users accessing DMZ networks. The creation of these exemptions is shown in the “Deployment Details” chapter of this guide.

The Cisco CWS cloud is accessed through a network of proxy servers, which have a broad geographic distribution in order to support a globally diverse set of customers. Cisco ASA is configured with a primary and secondary proxy server in order to provide high availability. Specific details for which proxy servers to use are provided by Cisco and based on the location and size of the deployment.

Cisco CWS is administered by using the CWS ScanCenter web portal. This includes creating filters and rules for policies, creating groups, activating keys, and viewing reports. All required CWS administration tasks are covered in this guide.

Deployment Details

The first part of this chapter describes how to configure the components in order to enable Cisco CWS service for internal users who access the Internet through the Internet-edge Cisco ASA, including users at the primary site and remote sites. Additionally, if internal users are using remote-access VPN from mobile devices, they are also protected with Cisco CWS. The second part of this chapter describes how to configure CWS for guest users, who may require a different policy than internal users.

PROCESS

Configuring Cisco CWS Policies for Internal Users

1. Enable Cisco CWS security configuration

Procedure 1 Enable Cisco 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.

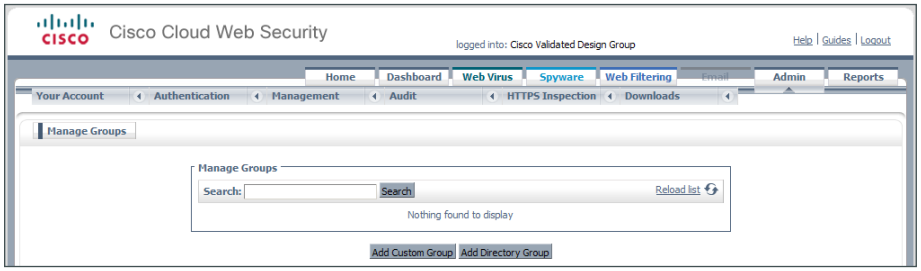
Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

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.



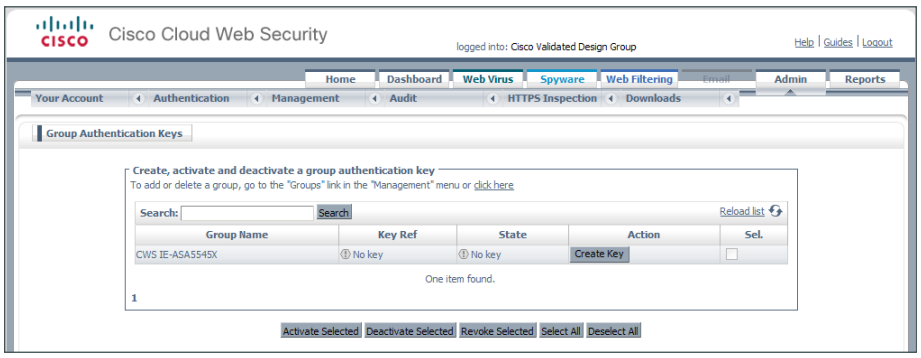
Step 3: Click **Add Custom Group**.

Step 4: In the Add New Custom Group pane, enter the group name (Example: CWS IE-ASA5545X), and then click **Save**.

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

Step 5: Navigate to **Admin > 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 the key 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**.

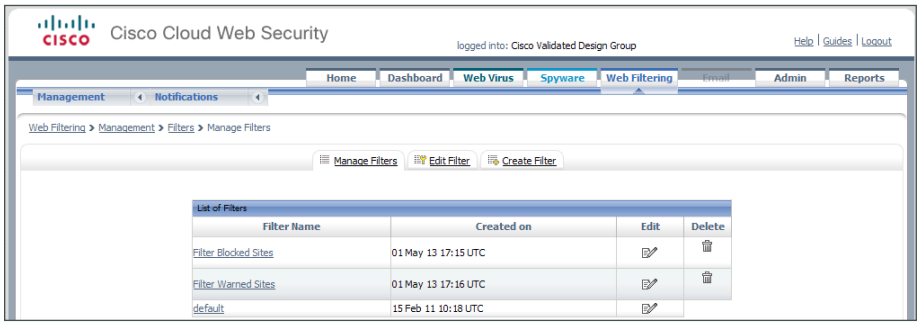
> **Tech Tip**
>
> The filtering policy in this guide is an example only. The actual policy implemented should align with the organization's security policy and business requirements.

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**.

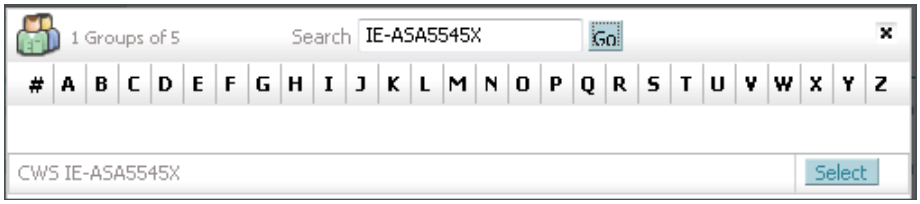
Step 15: Click **Create Rule**.

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

Step 17: In the **Rule Action** list, choose **Block**.

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

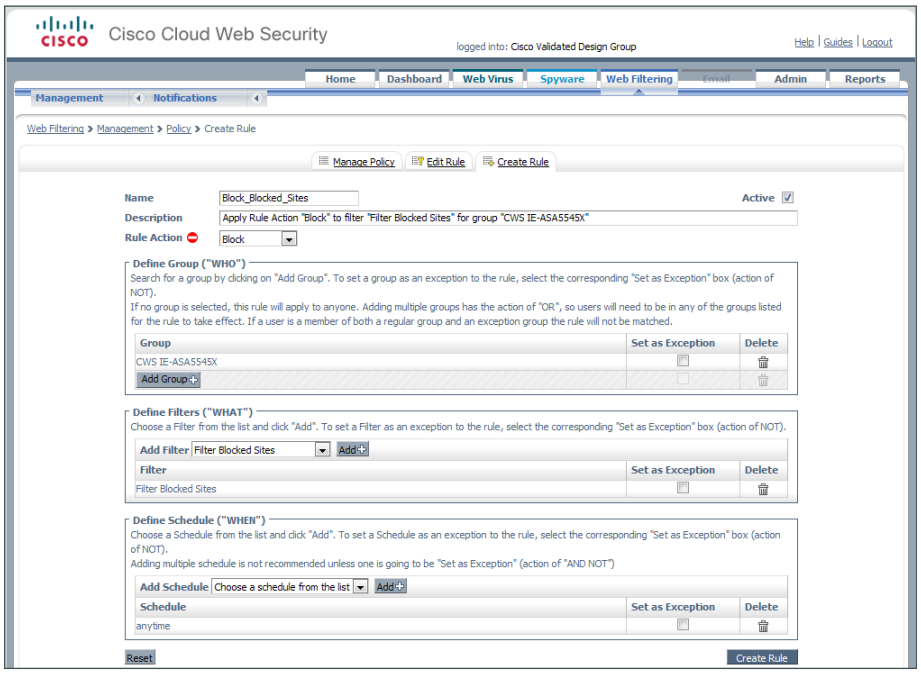
Step 19: On the dialog box, in the **Search** box, enter the name of the group created in Step 4, and then click **Go**.



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: In the **Rule Action** list, choose **Warn**.

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

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

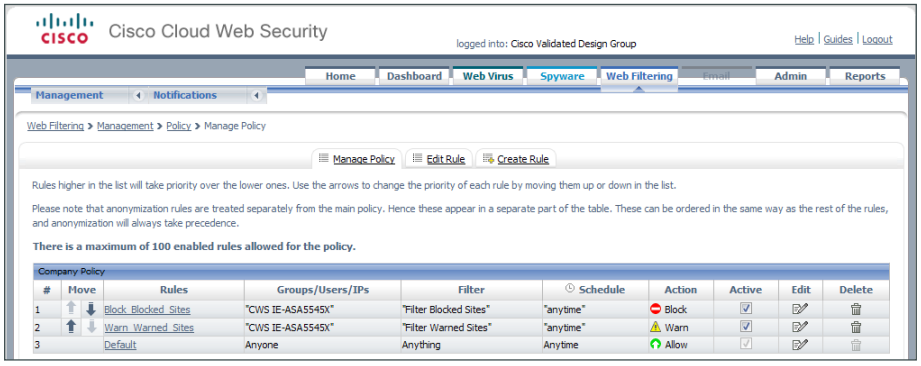
Step 28: Click **Select**, and then click **Confirm Selection**.

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)



PROCESS

Configuring Policy Exceptions for Apple Wireless Devices

1. Create exceptions to bypass Captive Network Assistant

Procedure 1 Create exceptions to bypass Captive Network Assistant

When an Apple iDevice (such as an iPad, iPod, or iPhone) or an Apple Mac OS X machine connects to a wireless network, it sends an HTTP request to one of a variety of destinations to help determine if a captive portal is blocking access to the Internet.

If the success page is returned, the device assumes it has network connectivity and no action is taken.

If the success page is not returned, an Apple feature called the Captive Network Assistant (CNA) assumes there is a captive portal present. CNA then launches a browser to prompt the user with the login page from the captive portal. The CNA browser is limited in function and is used only to authenticate with a captive portal.

Table 2 - Known sites used to trigger Apple Captive Network Assistant

Website	CWS category
.apple.com	Computers and Internet
.apple.com.edgekey.net	Computers and Internet
.akamaiedge.net	currently unclassified
.akamaitechnologies.com	SaaS and B2B
www.airport.us	Computers and Internet
www.appleiphonecell.com	Mobile Phones
www.ibook.info	Science and Technology
www.itools.info	Computers and Internet
www.thinkdifferent.us	Business and Industry

If you have implemented a CWS block or Warn policy that blocks access to the known sites listed in the previous table, then the CNA may be invoked.

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 **Web Filtering > Management > Filters**.

Step 3: Click **Create Filter**.

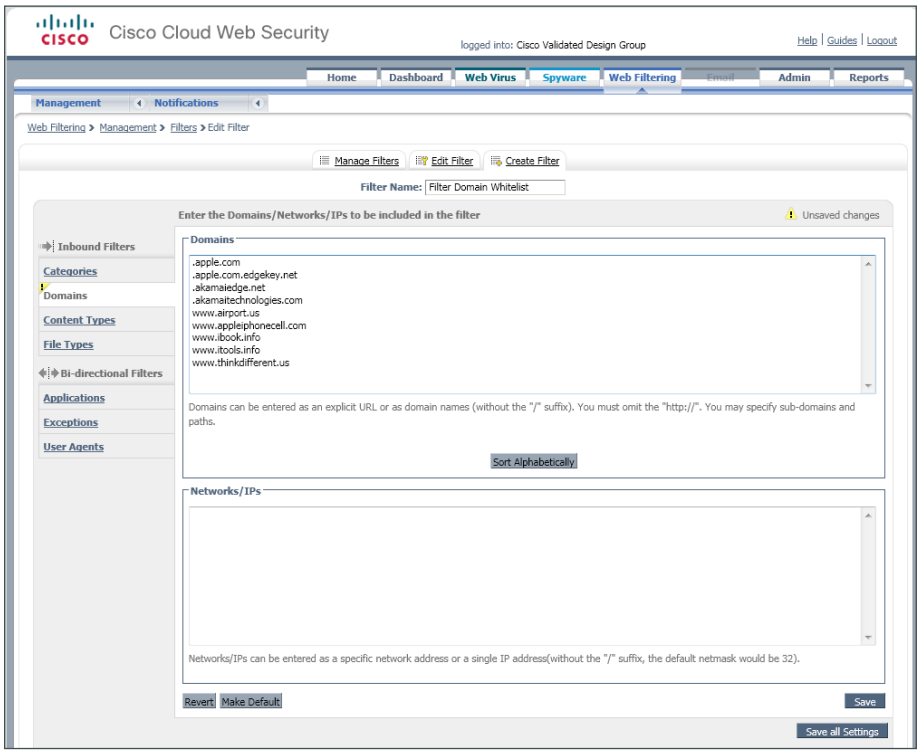
Step 4: Assign a name to the filter (Example: Filter Domain Whitelist), and then in the Inbound Filters pane, click **Domains**.

Step 5: In the domain pane, enter the full list of websites listed in Table 2, and then click **Save all Settings**.

Tech Tip

If a website begins with a ".", it will match anything that ends with that suffix. The entry ".apple.com" will match "www.apple.com" and "store.apple.com".

When you save the list, the ScanCenter portal automatically alphabetizes it.



Step 6: Navigate to **Web Filtering > Management > Policy**.

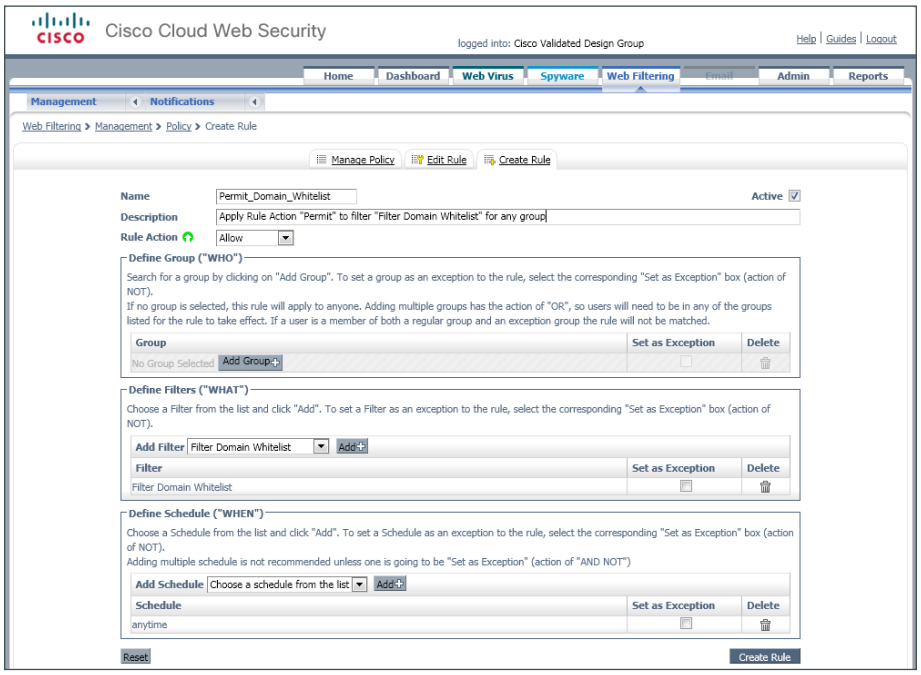
Step 7: Click **Create Rule**.

Step 8: Assign a name to the rule (Example: Permit_Domain_Whitelist), and then select **Active**.

Step 9: In the **Rule Action** list, choose **Allow**.

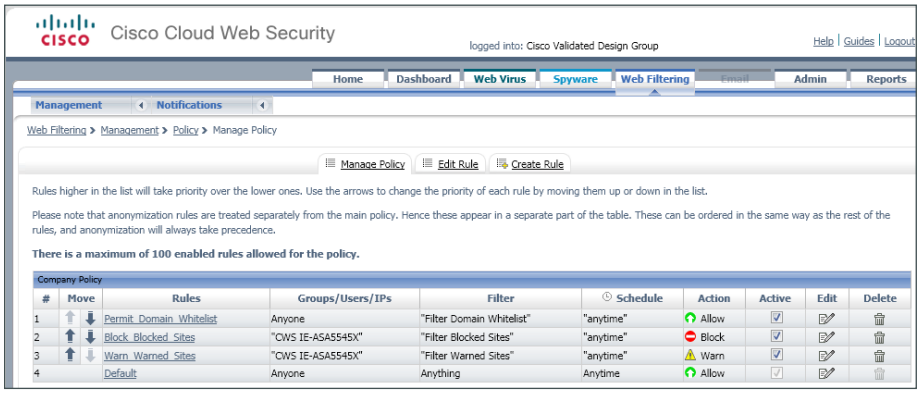
Step 10: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 3 (Example: Filter Domain Whitelist), and then click **Add**.

Step 11: Click **Create rule**. The policy rule has now been created.



Because all rules are evaluated on a first-hit rule, the Permit Domain Whitelist rule must be listed first.

Step 12: Click the Up arrow next to the Permit_Domain_Whitelist rule until it is listed first.



Step 13: Click **Apply Changes**.

PROCESS

Configuring Cisco ASA for Cisco Cloud Web Security

1. Configure Cisco CWS servers
2. Configure Cisco ASA firewall objects
3. Configure Cisco ASA service policy
4. Test Cisco Cloud Web Security

Procedure 1 Configure Cisco CWS servers

Cisco ASA is configured with a primary and backup server. You will receive a provisioning email after purchasing your Cisco CWS license. This email includes the primary and backup server address that you use for configuring Cisco ASA. An example email is included in Appendix C: Provisioning Email Example.

Table 3 - Example of Cisco CWS primary and secondary proxy servers from a provisioning email

Primary web services proxy address	proxyXXXX.scansafe.net
Web services proxy port	8080
Secondary web services proxy address	proxyXXXX.scansafe.net
Web services proxy port	8080

Tech Tip

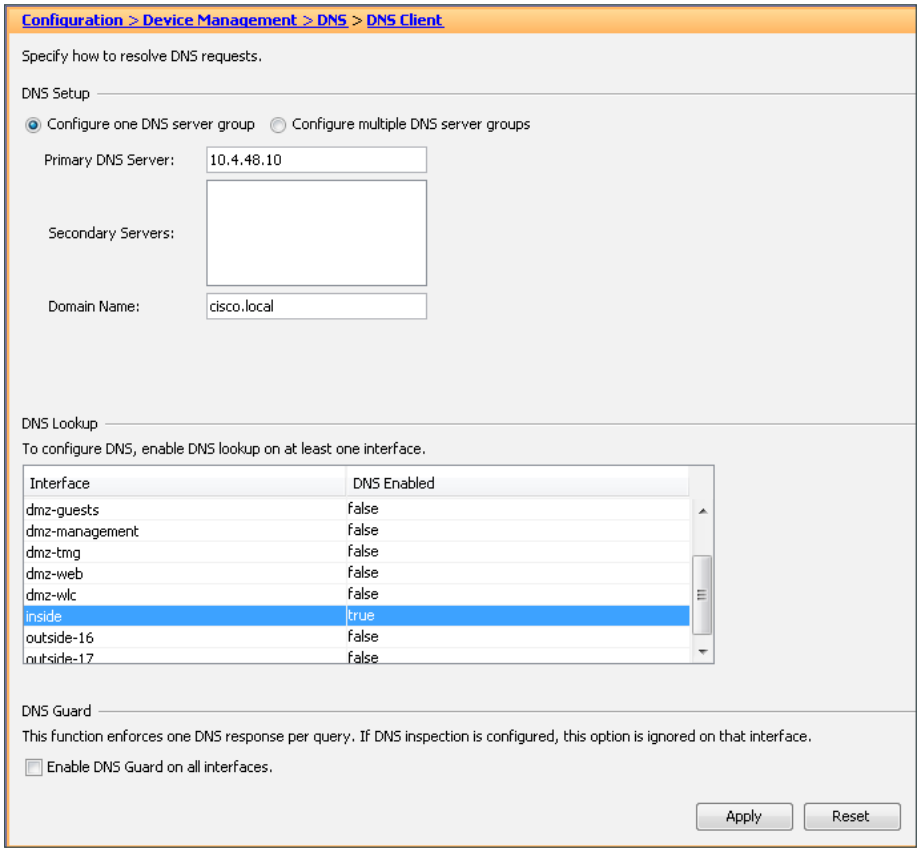
Domain Name Service (DNS) is required to resolve the Fully Qualified Domain Name (FQDN) of a Cisco CWS web services proxy server.

Step 1: From a client on the internal network, navigate to the Internet-edge firewall's inside IP address, and then launch Cisco ASA Security Device Manager. (Example: https://10.4.24.30)

Step 2: If the firewall is not configured to use DNS resolution, navigate to **Configuration > Device Management > DNS > DNS Client**, and then configure it as follows:

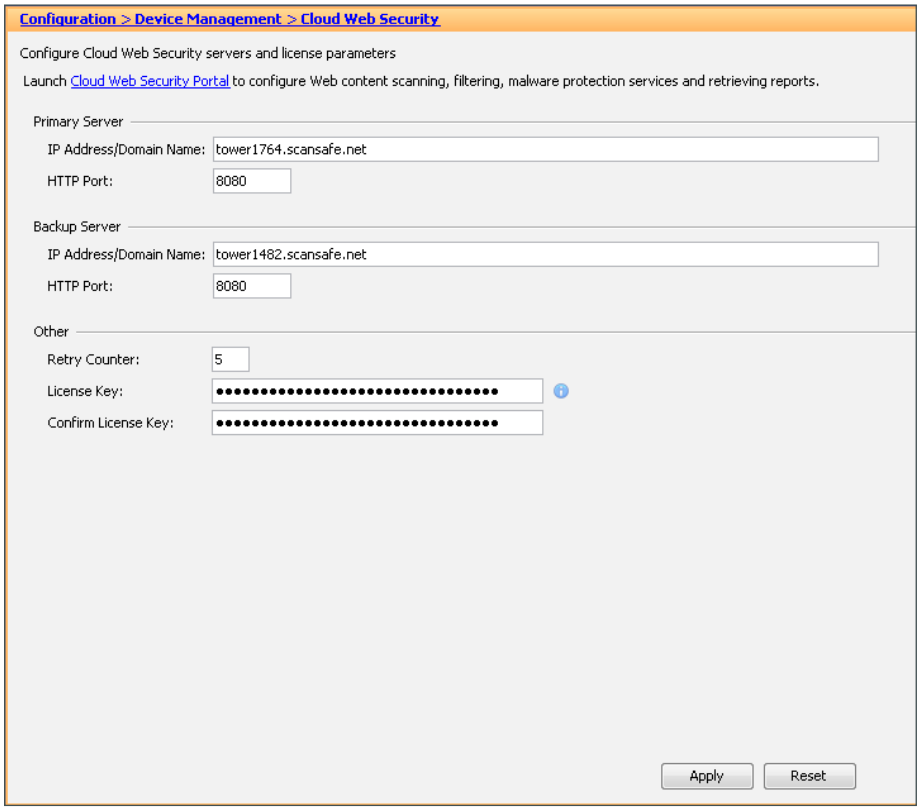
- Primary DNS Server–**10.4.48.10**
- Domain Name–**cisco.local**

Step 3: In the DNS Lookup pane, scroll to view the **Interface** list, click in the **DNS Enabled** column for the interface that is used to reach the DNS server (Example: inside), choose **True**, and then click **Apply**.

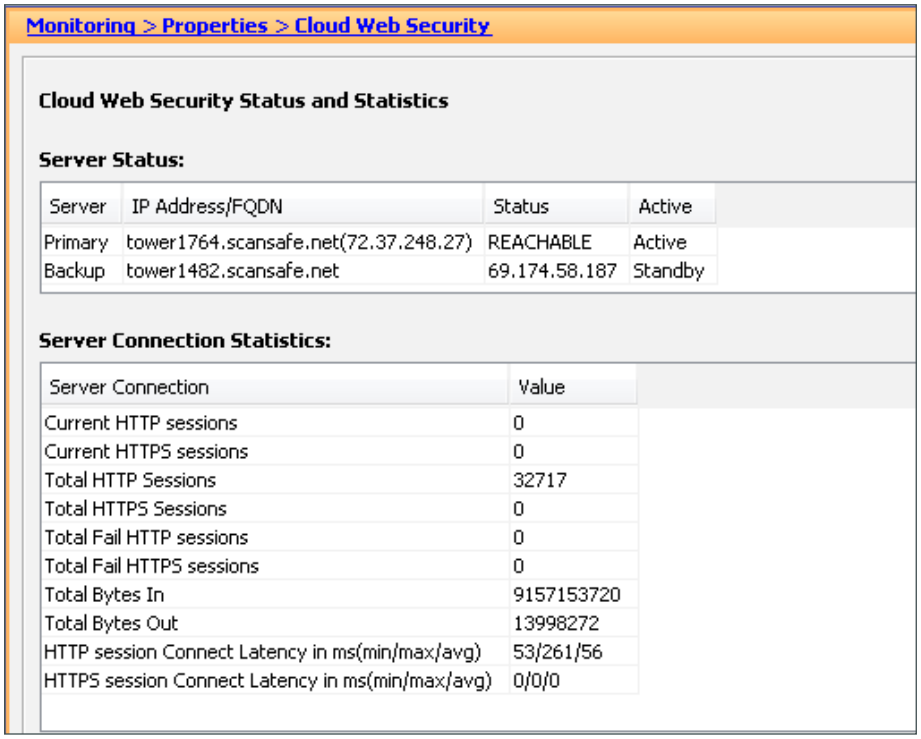


Step 4: In **Configuration > Device Management > Cloud Web Security**, configure the following values from Table 3, and then click **Apply**.

- Primary Server IP Address/Domain Name–**[FQDN of primary web services proxy from provisioning email]**
- Backup Server IP Address/Domain Name–**[FQDN of secondary web services proxy from provisioning email]**
- License Key–**[Group key from Step 6 of Procedure 1, "Enable Cisco CWS security configuration"]**



Step 5: In **Monitoring > Properties > Cloud Web Security**, verify the Cisco CWS server status. Your primary server should show a status of REACHABLE.



Monitoring > Properties > Cloud Web Security

Cloud Web Security Status and Statistics

Server Status:

Server	IP Address/FQDN	Status	Active
Primary	tower1764.scansafe.net(72.37.248.27)	REACHABLE	Active
Backup	tower1482.scansafe.net	69.174.58.187	Standby

Server Connection Statistics:

Server Connection	Value
Current HTTP sessions	0
Current HTTPS sessions	0
Total HTTP Sessions	32717
Total HTTPS Sessions	0
Total Fail HTTP sessions	0
Total Fail HTTPS sessions	0
Total Bytes In	9157153720
Total Bytes Out	13998272
HTTP session Connect Latency in ms(min/max/avg)	53/261/56
HTTPS session Connect Latency in ms(min/max/avg)	0/0/0

Procedure 2 Configure Cisco ASA firewall objects

In this procedure, you create the network objects listed in the following table.

Table 4 - Firewall network objects

Network object name	IP address	Netmask
internal-network	10.4.0.0/15	255.254.0.0
dmz-networks	192.168.16.0/21	255.255.248.0

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

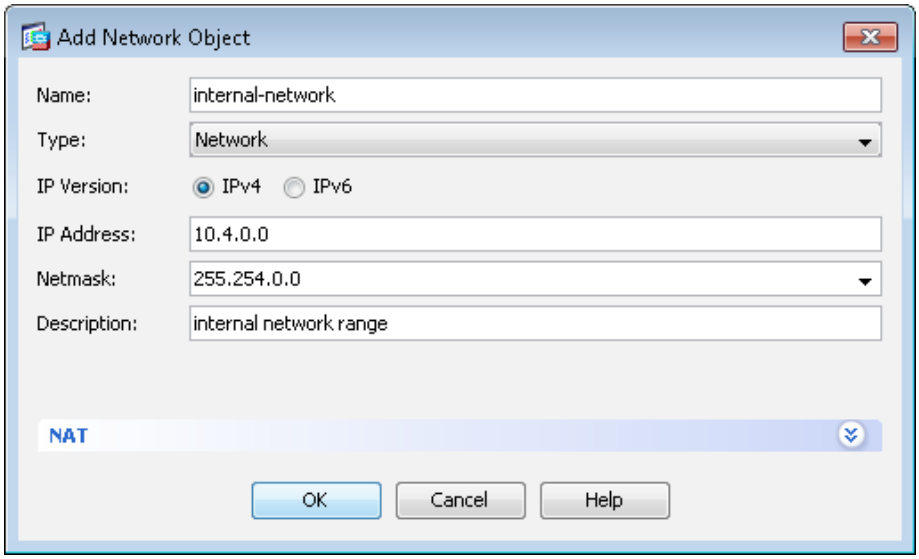
Step 2: Click **Add > Network Object**.

Step 3: On the Add Network Object dialog box, in the **Name** box, enter the Network object name from Table 4. (Example: internal-network)

Step 4: In the **Type** list, choose **Network**.

Step 5: In the **IP Address** box, enter the IP address of the object from Table 4. (Example: 10.4.0.0)

Step 6: In the **Netmask** box, enter the netmask of the object from Table 4, and then click **OK**. (Example: 255.254.0.0)



Step 7: Repeat Step 2 through Step 6 for all objects listed in Table 4. If the object already exists, then skip to the next object listed in the table.

Step 8: After adding all of the objects listed in Table 4, in the Network Objects/Groups pane, click **Apply**.

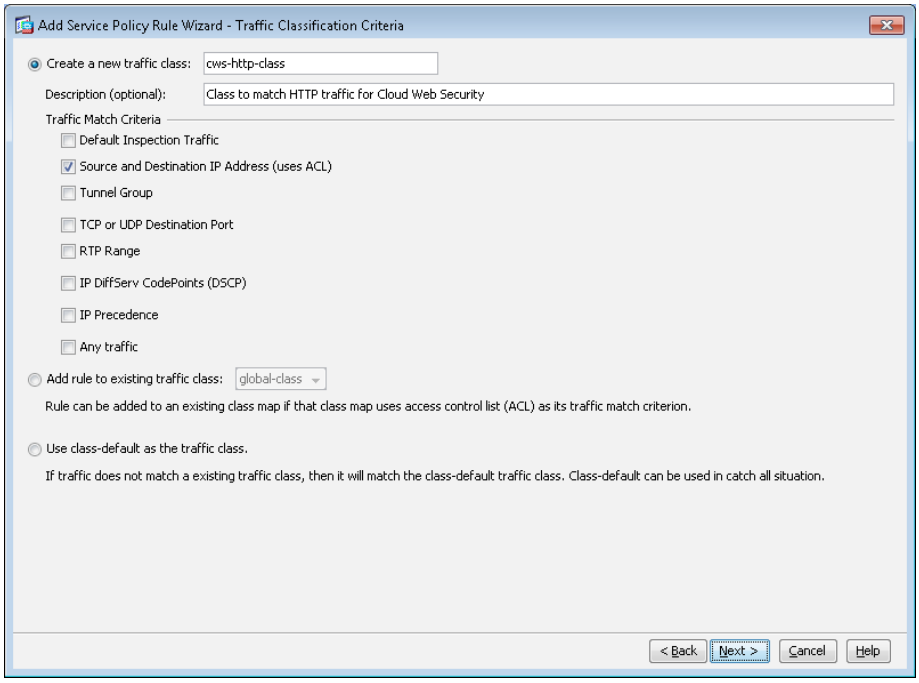
Procedure 3 Configure Cisco ASA service policy

The existing global service policy is modified to enable Cisco CWS. The global service policy applies to all interfaces on the firewall, so this procedure enables CWS on all interfaces.

Step 1: In **Configuration > Firewall > Service Policy Rules**, select **Add > Add Service Policy Rule**.

Step 2: Skip the Add Service Policy Rule Wizard – Service Policy dialog box by clicking **Next**.

Step 3: On the Add Service Policy Rule Wizard – Traffic Classification Criteria dialog box, in the **Create a new traffic class** box, enter **cws-http-class**, for Traffic Match Criteria, select **Source and Destination IP Address**, and then click **Next**.



Next, create the single global policy for Cisco CWS in order to match traffic on all interfaces. Because this policy may be used by internal users and remote-access VPN users, certain source and destination traffic pairs are exempted from the CWS policy by using **Do not match** as the action, as shown in the following table. The final policy rule matches all other source and destination pairs.

Table 5 - Example policy for Cisco Cloud Web Security

Action	Source object	Destination object	Service	Description
Do not match	any4	internal-network	ip	Do not match any to internal networks
Do not match	any4	dmz-networks	ip	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

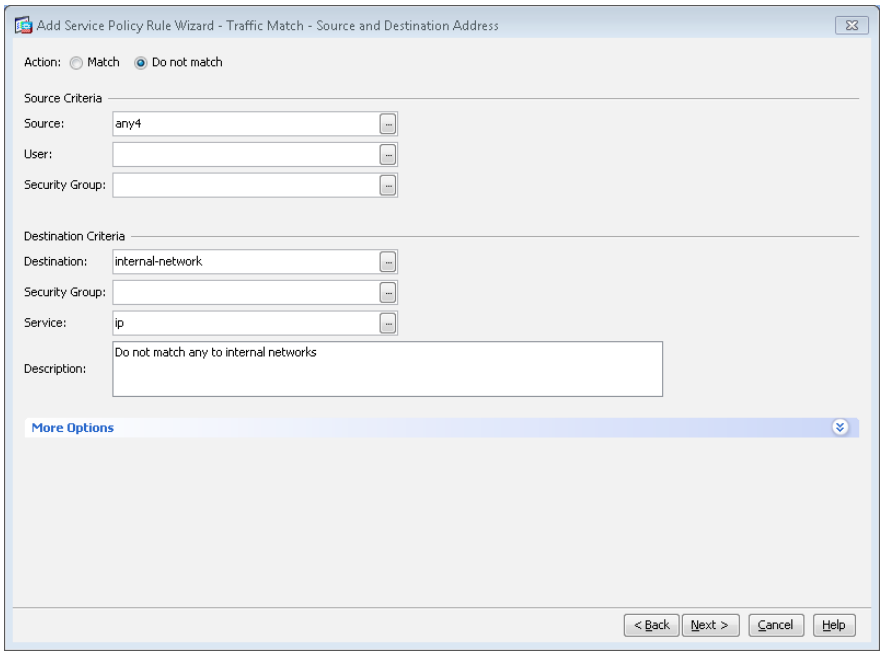
The Add Service Policy Rule Wizard allows only a simple policy containing a single match entry, so the following steps are used to configure only the first entry in Table 5. You configure the remaining entries in Table 5 after you complete the first pass of the wizard.

Step 4: On the Add Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in the first row of Table 5. (Example: Do not match)

Step 5: In the **Source** box, enter the source object listed in the first row of Table 5. (Example: any4)

Step 6: In the **Destination** box, enter the destination object listed in the first row of Table 5. (Example: internal-network)

Step 7: In the **Service** box, enter the service listed in the first row of Table 5. (Example: ip), and then click **Next**.

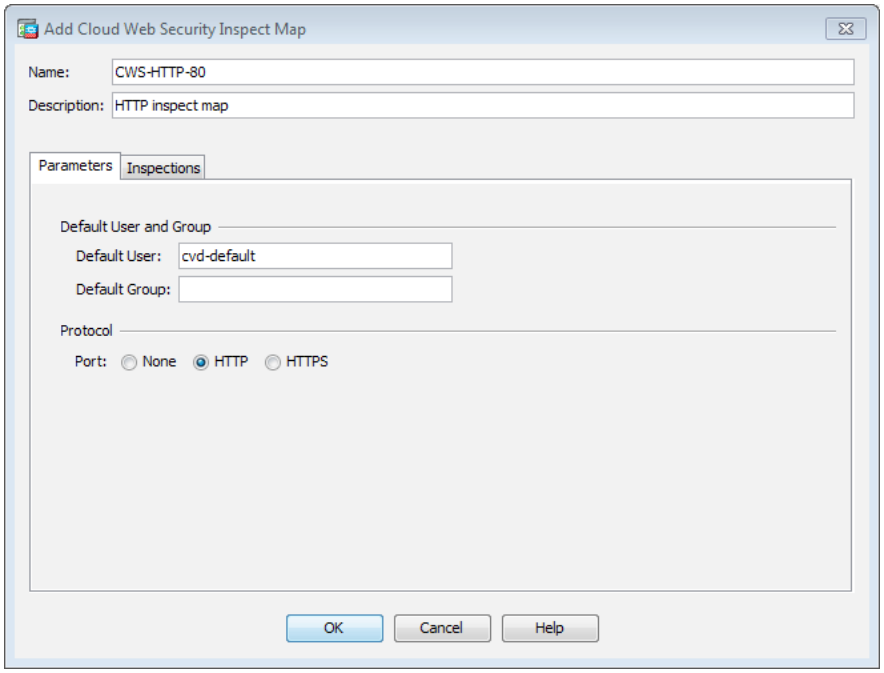


Step 8: On the Add Service Policy Rule Wizard – Rule Actions dialog box, click the **Protocol Inspection** tab, select **Cloud Web Security**, and then click **Configure**.

Step 9: On the Select Cloud Web Security Inspect Map dialog box, click **Add**.

Step 10: On the Add Cloud Web Security Inspect Map dialog box, enter a name (Example: CWS-HTTP-80). On the Parameters tab, in the **Default User** box, enter a username that will be used by default (Example: cvd-default).

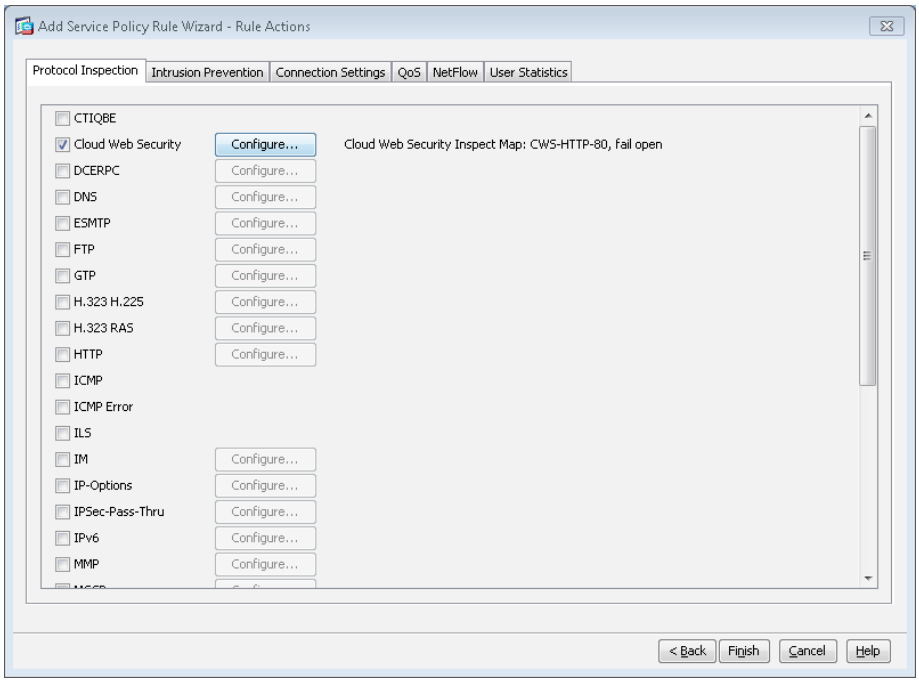
Step 11: Select protocol **HTTP**, and then click **OK**.



Step 12: On the Select Cloud Web Security Inspect Map dialog box, select the inspect map you created in Step 10, for Cloud Web Security Traffic Action, select **Fail Open**, and then click **OK**.

> **Tech Tip**
>
> A *fail open* or *fail closed* condition, in a security context, refers to the default behavior when a service is unavailable. If *fail open* is configured and the Cisco CWS service is unavailable, the firewall allows user web traffic to pass without restriction. Conversely, if *fail closed* is configured and the Cisco CWS service is unavailable, the firewall blocks user web traffic.

Step 13: On the Add Service Policy Rule Wizard – Rule Actions dialog box, click **Finish**.

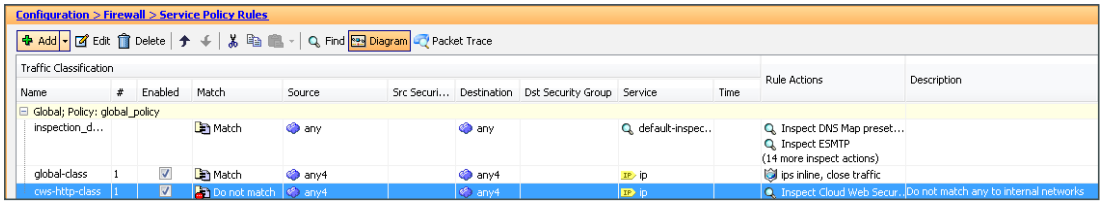


Because the Add Service Policy Rule Wizard allowed only a simple policy containing a single match entry, use the following steps in order to configure the remaining entries from Table 5, which are replicated in Table 6.

Table 6 - Example policy for Cisco Cloud Web Security (remaining entries from Table 5)

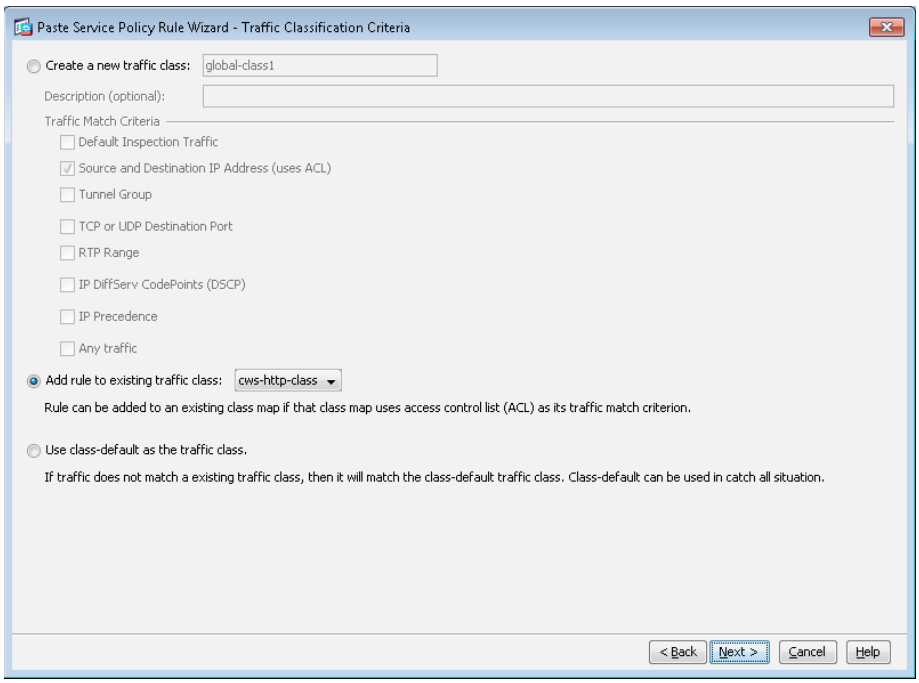
Action	Source object	Destination object	Service	Description
Do not match	any4	dmz-networks	ip	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

Step 14: In **Configuration > Firewall > Service Policy Rules**, select the highest numbered rule for the Cisco CWS policy (Example: cws-http-class). Right-click to Copy, and then right-click to Paste After.



Step 15: Skip the Paste Service Policy Rule Wizard – Service Policy dialog box by clicking **Next**.

Step 16: On the Paste Service Policy Rule Wizard – Traffic Classification Criteria dialog box, select **Add rule to existing traffic class**, and then from list of classes, choose the class created in Step 3 (Example: cws-http-class). Click **Next**.

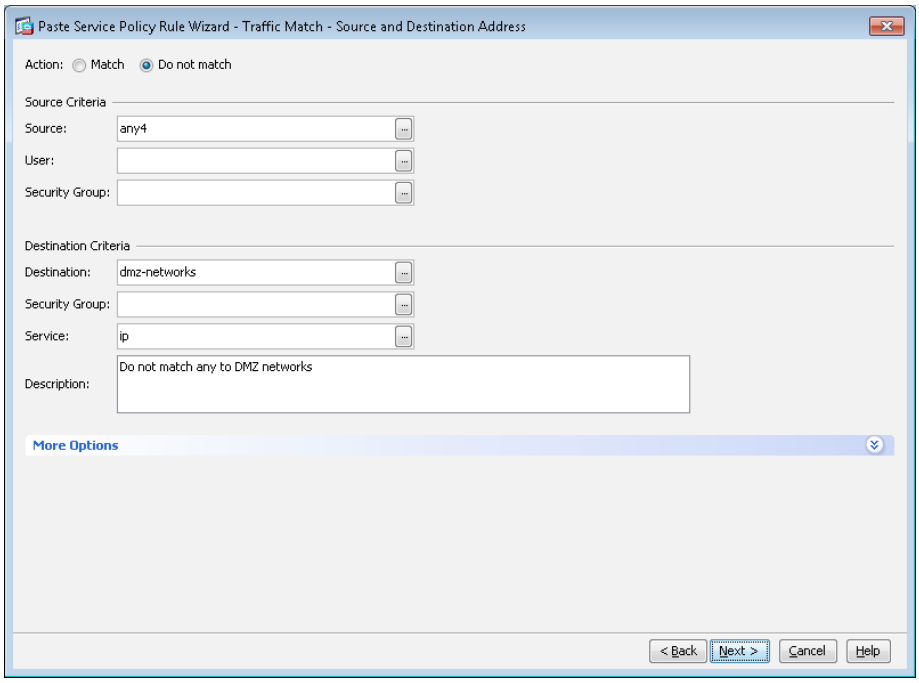


Step 17: On the Paste Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in Table 6. (Example: Do not match)

Step 18: In the **Source** box, enter the source object listed in Table 6. (Example: any4)

Step 19: In the **Destination** box, enter the destination object listed in Table 6. (Example: dmz-networks)

Step 20: In the **Service** box, enter the service listed in Table 6 (Example: ip), and then click **Next**.



Step 21: On the Paste Service Policy Rule Wizard – Rule Actions dialog box, click **Finish**.

Step 22: Repeat Step 14 through Step 21 for all of the entries in Table 6.

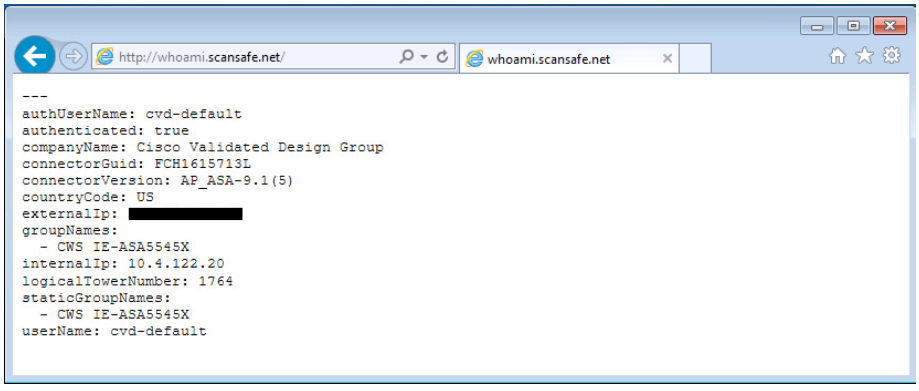
Step 23: Verify that your service policy rules match the following figure, and then click **Apply**.

Procedure 4 Test Cisco Cloud Web Security

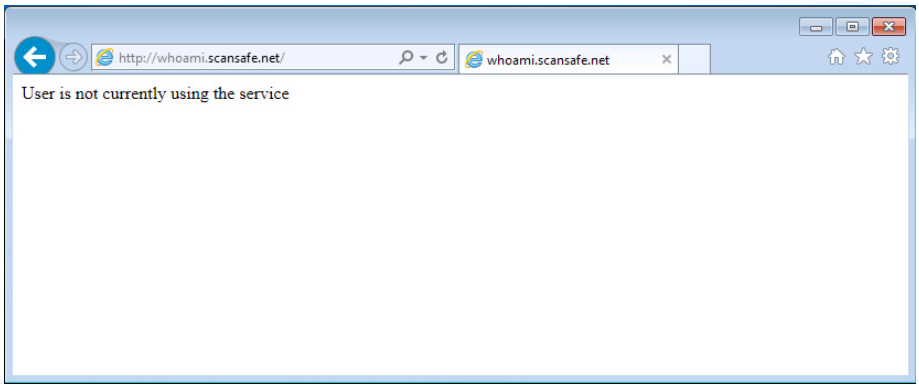
Step 1: From a client machine on the internal network, open a web browser to the following website:

http://whoami.scansafe.net

This website returns diagnostic information from the Cisco CWS service.



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



PROCESS

Configuring Cisco CWS Policies for Guest Users

1. Enable Cisco CWS security configuration
2. Test Cisco Cloud Web Security

This is an optional process that is only required if you want to apply a different Cisco CWS policy for guest users. Otherwise, the same policy created for internal users is applied.

Reader Tip

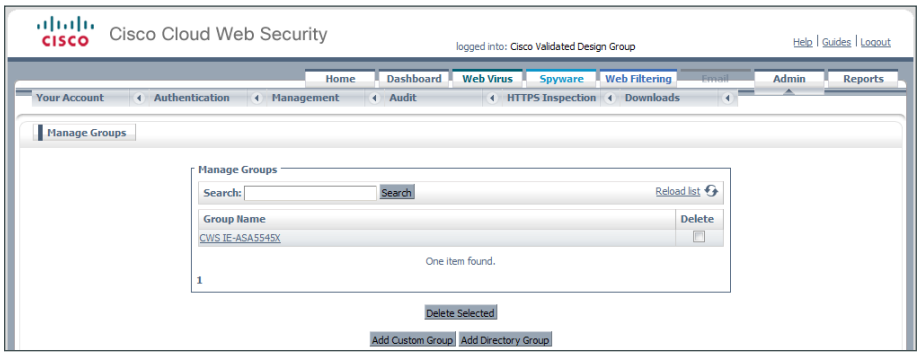
This process assumes that wireless LAN guest access has already been configured following the guidance in the Campus Wireless LAN Technology Design Guide. Only the procedures required to enable Cisco CWS for an existing guest user deployment are included.

Procedure 1 Enable Cisco CWS security configuration

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**.

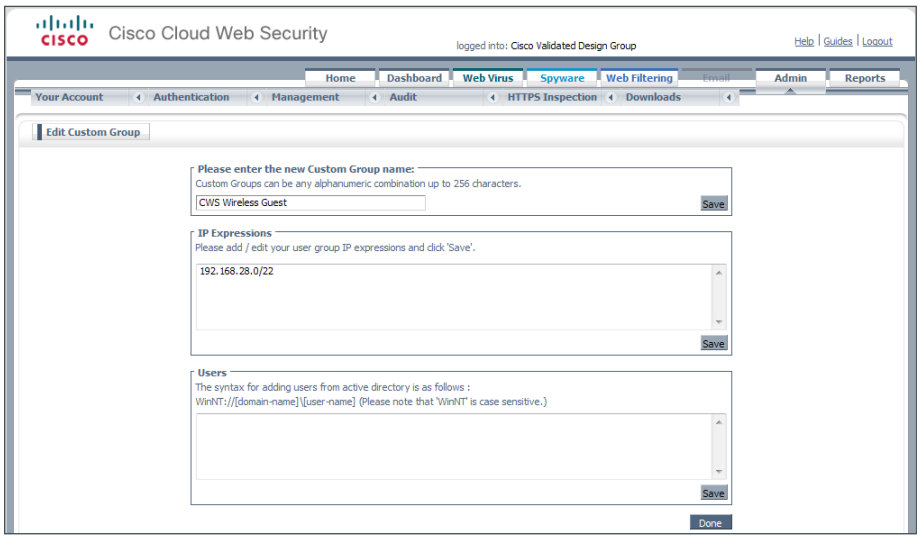


Step 3: Click **Add Custom Group**.

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

Step 5: On the **Admin > Management > Groups** page, click the link for the group created in Step 4.

Step 6: In the IP Expressions pane, add the IP subnet range that corresponds to the wireless guest DMZ configuration in the Campus Wireless LAN Technology Design Guide, click **Save**, and then click **Done**.



Step 7: 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. This example uses a whitelist policy and uses filters that initially select all categories for blocking or warning. Only specifically selected categories are exempt.

If you make the whitelist too limited, web browsing to many common websites may be restricted.

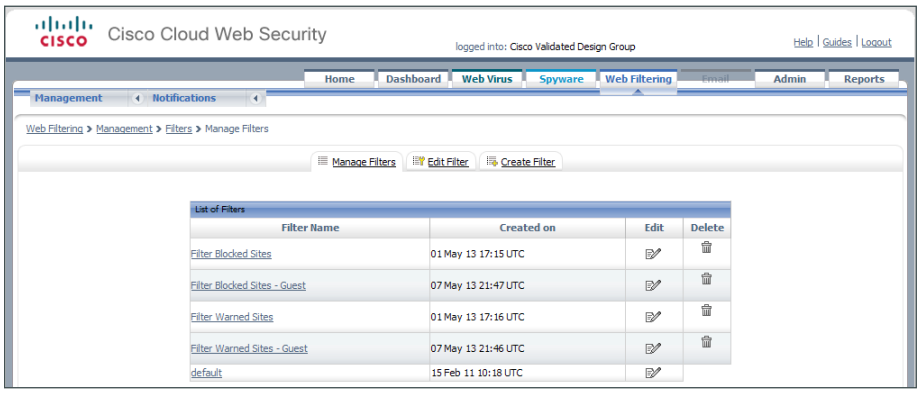
If your policy uses both a block list and a warn list as suggested in this example, all permitted categories must be contained in both lists.

Step 8: Click **Create Filter**.

Step 9: Assign a name to the filter (Example: Filter Warned Sites - Guest), click **Select All**, clear the categories that are considered appropriate by your organization's policy that do not require a warning (Example: News, Shopping, Entertainment and Social Networking), and then click **Save**. Access to all other categories is permitted, but only after accepting a warning message.

Step 10: Click **Create Filter**.

Step 11: Assign a name to the filter (Example: Filter Blocked Sites - Guest), click **Select All**, clear all of the categories that were selected in Step 9. Then clear additional categories that require a warning according to your organization's policy (Examples: Tobacco), and then click **Save**. Access to all other categories is completely restricted.



Step 12: Navigate to **Web Filtering > Management > Policy**.

Step 13: Click **Create Rule**.

Step 14: Assign a name to the rule (Example: Block_Blocked_Sites_Guest), and then select **Active**.

Step 15: In the **Rule Action** list, choose **Block**.

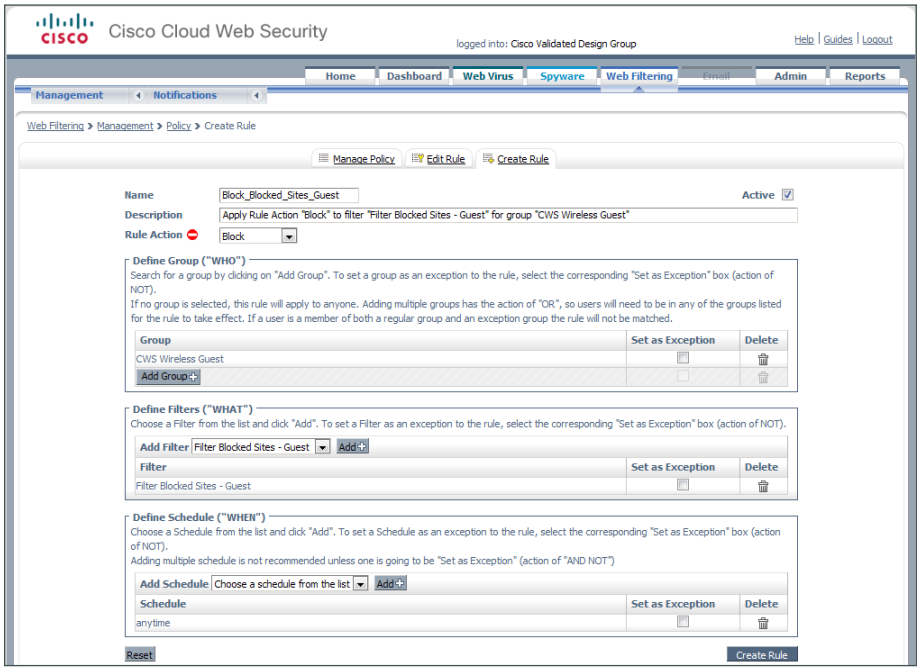
Step 16: In the Define Group pane, click **Add group**.

Step 17: On the dialog box, in the **Search** box, enter the name of the group created in Step 4, and then click **Go**.

Step 18: Click **Select**, and then click **Confirm Selection**.

Step 19: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 8 (Example: Filter Blocked Sites - Guest), and then click **Add**.

Step 20: Click **Create rule**. The policy rule has now been created.



Next, create a new rule.

Step 21: Click **Create Rule**.

Step 22: Assign a name to the rule (Example: Warn_Warned_Sites_Guest), and then select **Active**.

Step 23: In the **Rule Action** list, choose **Warn**.

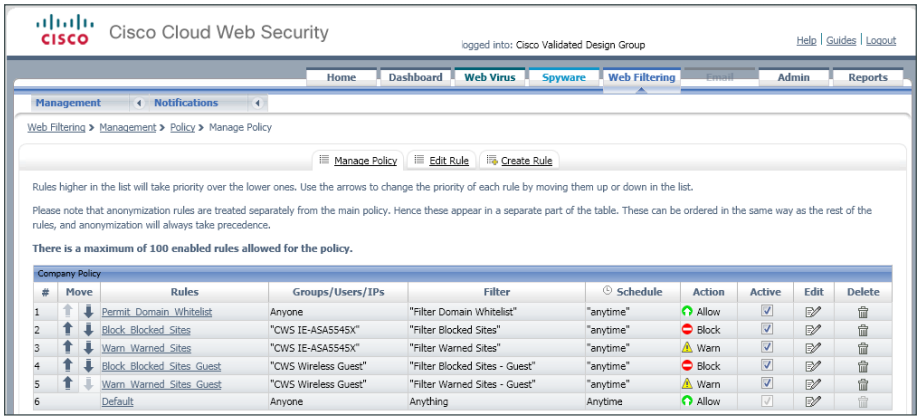
Step 24: In the Define Group pane, click **Add group**.

Step 25: On the dialog box, in the search box, enter the name of the group created in Step 4, and then click **Go**.

Step 26: Click **Select**, and then click **Confirm Selection**.

Step 27: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 9 (Example: Filter Warned Sites - Guest), and then click **Add**.

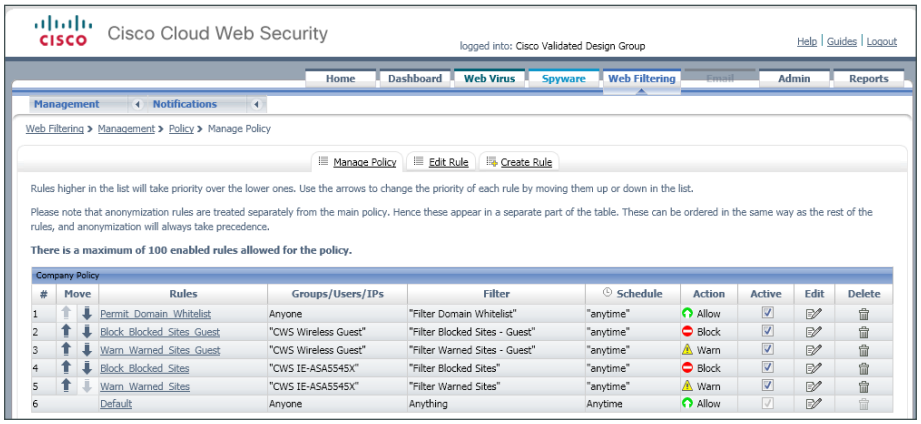
Step 28: Click **Create rule**. The policy rule has now been created.



Because the guest user traffic and internal user traffic is all redirected from the same Cisco ASA, the same group key is used. In order to properly match the guest traffic by the source IP address, the guest rules must be evaluated before the internal user rules.

Step 29: Click the Up arrow next to the Block_Blocked_Sites_Guest rule until it is listed second (after the Permit Domain Whitelist).

Step 30: Click the Up arrow next to the Warn_Warned_Sites_Guest rule until it is listed third, and then click **Apply Changes**.

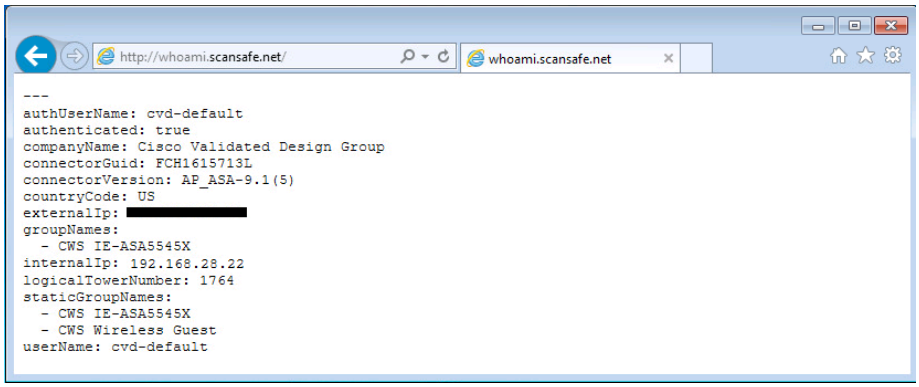


Procedure 2 Test Cisco Cloud Web Security

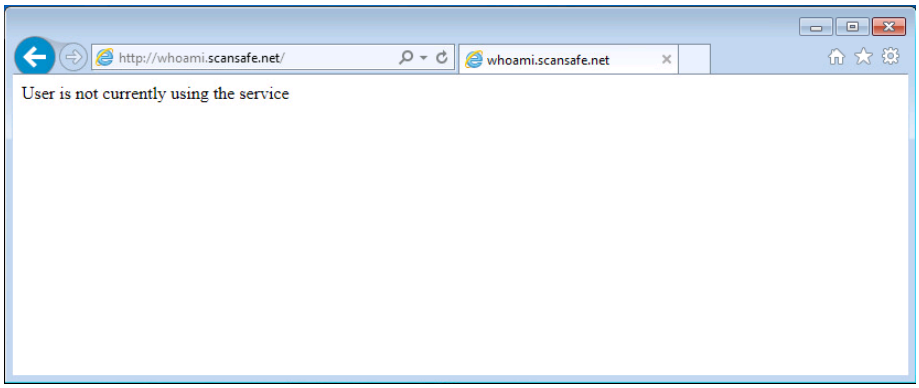
Step 1: From a client machine on the guest network, open a web browser to the following website:

http://whoami.scansafe.net

This website returns diagnostic information from the Cisco CWS service.



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



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)

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 Files

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
```

IE-ASA5545X

The Cisco ASA commands below represent the configuration added to the Cisco ASA appliance, hostname IE-ASA5545X, as configured in the Firewall and IPS Technology Design Guide. The additional configuration below enables the functionality described in this guide.

```
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 10.4.48.10
 domain-name cisco.local
!
object network internal-network
 subnet 10.4.0.0 255.254.0.0
 description The organization's internal network range
object network dmz-networks
 subnet 192.168.16.0 255.255.248.0
 description The organization's DMZ network range
!
access-list global_mpc_1 remark Do not match any to internal network
access-list global_mpc_1 extended deny ip any4 object internal-network
access-list global_mpc_1 remark Do not match any to DMZ networks
access-list global_mpc_1 extended deny ip any4 object dmz-networks
access-list global_mpc_1 remark Match HTTP to any other networks
access-list global_mpc_1 extended permit tcp any4 any4 eq www
!
scansafe general-options
```

```
 server primary ip 72.37.248.27 port 8080
 server backup ip 69.174.58.187 port 8080
 retry-count 5
 license YOURLICENSEKEYGOESHERE
!
class-map cws-http-class
 description Class to match HTTP traffic for Cloud Web Security
 match access-list global_mpc_1
!
policy-map type inspect scansafe CWS-HTTP-80
 description Cloud Web Security TCP-80
 parameters
  default user cvd-default
  http
policy-map global_policy
 class cws-http-class
  inspect scansafe CWS-HTTP-80 fail-open
!
service-policy global_policy global
```

Appendix C: Provisioning Email Example

From: ScanSafe Provisioning [mailto:provisioning@scansafe.net]
Subject: Provisioning Notification: Customer X / PO Ref:XXXXXXXX

On Day-Month-Year we completed the provisioning of the ScanSafe Web Security services for Customer X in accordance with the order details below:

Services:	Subscription Seats and Services
Term:	Subscription Months
Registered IP Addresses:	-None configured yet-
Domains:	-None configured yet-

The service is now available and you should make the necessary configuration changes described below to use the service. Please configure your system so that external Web traffic is sent via ScanSafe, using the explicit proxy setting below:

Primary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080
Secondary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080

The exact configuration changes required will vary depending in your specific existing infrastructure.

To log in to the service configuration Web portal and administer the service, please visit https://scancenter.scansafe.com/portal/admin/login.jsp and enter your email and password details below:

Email:	contact@CustomerX.com
Password :	-Not Shown-
Company ID:	XXXXXXXXXX

As part of our ongoing commitment to quality and service, a member of the ScanSafe Customer Services team will be in touch with you to ensure that the service is functioning according to your expectations.

If you require any assistance or experience any problems with the service, please do not hesitate to contact our support team.

We appreciate your choosing ScanSafe to provide Web security and look forward to a successful working partnership with you.

Customer Services
EMEA +44 (0) 207 034 9400
US + (1) 877 472 2680
support@scansafe.com

This email and any attachments are strictly confidential and intended for the addressee(s) only. If this email has been sent to you in error, please let us know by forwarding it to us at support@scansafe.com.

Neither ScanSafe nor its directors, officers or employees accepts any liability for the accuracy or completeness of this email. Unless expressly stated to the contrary, no contracts may be concluded on behalf of ScanSafe by means of e-mail communication.

Appendix D: 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 added screenshots to improve clarity.

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-0000147-1 09/14