CHAPTER 25

Configuring the ASA for Cisco Cloud Web Security

Cisco Cloud Web Security provides web security and web filtering services through the Software-as-a-Service (SaaS) model. Enterprises with the ASA in their network can use Cloud Web Security services without having to install additional hardware.

When Cloud Web Security is enabled on the ASA, the ASA transparently redirects selected HTTP and HTTPS traffic to the Cloud Web Security proxy servers. The Cloud Web Security proxy servers then scan the content and allow, block, or send a warning about the traffic based on the policy configured in Cisco ScanCenter to enforce acceptable use and to protect users from malware.

The ASA can optionally authenticate and identify users with Identity Firewall (IDFW) and AAA rules. The ASA encrypts and includes the user credentials (including usernames and/or user groups) in the traffic it redirects to Cloud Web Security. The Cloud Web Security service then uses the user credentials to match the traffic to the policy. It also uses these credentials for user-based reporting. Without user authentication, the ASA can supply an (optional) default username and/or group, although usernames and groups are not required for the Cloud Web Security service to apply policy.

You can customize the traffic you want to send to Cloud Web Security when you create your service policy rules. You can also configure a "whitelist" so that a subset of web traffic that matches the service policy rule instead goes directly to the originally requested web server and is not scanned by Cloud Web Security.

You can configure a primary and a backup Cloud Web Security proxy server, each of which the ASA polls regularly to check for availability.

Note This feature is also called "ScanSafe," so the ScanSafe name appears in some commands.

This chapter includes the following sections:

Information About Cisco Cloud Web Security

This section includes the following topics:

Redirection of Web Traffic to Cloud Web Security

When an end user sends an HTTP or HTTPS request, the ASA receives it and optionally retrieves the user and/or group information. If the traffic matches an ASA service policy rule for Cloud Web Security, then the ASA redirects the request to the Cloud Web Security proxy servers. The ASA acts as an intermediary between the end user and the Cloud Web Security proxy server by redirecting the connection to the proxy server. The ASA changes the destination IP address and port in the client requests and adds Cloud Web Security-specific HTTP headers and then sends the modified request to the Cloud Web Security proxy server. The Cloud Web Security HTTP headers include various kinds of information, including the username and user group (if available).

User Authentication and Cloud Web Security

User identity can be used to apply policy in Cloud Web Security. User identity is also useful for Cloud Web Security reporting. User identity is not required to use Cloud Web Security. There are other methods to identify traffic for Cloud Web Security policy.

The ASA supports the following methods of determining the identity of a user, or of providing a default identity:

- AAA rules—When the ASA performs user authentication using a AAA rule, the username is retrieved from the AAA server or local database. Identity from AAA rules does not include group information. If configured, the default group is used. For information about configuring AAA rules, see Chapter 8, "Configuring AAA Rules for Network Access."
- IDFW—When the ASA uses IDFW with the Active Directory (AD), the username and group is retrieved from the AD agent when you activate a user and/or group by using an ACL in a feature such as an access rule or in your service policy, or by configuring the user identity monitor to download user identity information directly.

  For information about configuring IDFW, see Chapter 38, "Configuring the Identity Firewall," in the general operations configuration guide.
- Default username and group—Without user authentication, the ASA uses an optional default username and/or group for all users that match a service policy rule for Cloud Web Security.

Authentication Keys

Each ASA must use an authentication key that you obtain from Cloud Web Security. The authentication key lets Cloud Web Security identify the company associated with web requests and ensures that the ASA is associated with valid customer.

You can use one of two types of authentication keys for your ASA: the company key or the group key.

- Company Authentication Key, page 25-3
- Group Authentication Key, page 25-3

Company Authentication Key

A Company authentication key can be used on multiple ASAs within the same company. This key simply enables the Cloud Web Security service for your ASAs. The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter. For more information, see the Cloud Web Security documentation: http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

Group Authentication Key

A Group authentication key is a special key unique to each ASA that performs two functions:

- Enables the Cloud Web Security service for one ASA.
- Identifies all traffic from the ASA so you can create ScanCenter policy per ASA.

For information about using the Group authentication key for policy, see the "ScanCenter Policy" section on page 25-4).

The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter.

For more information, see the Cloud Web Security documentation: http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

ScanCenter Policy

In ScanCenter, traffic is matched against policy rules in order until a rule is matched. Cloud Web Security then applies the configured action for the rule. User traffic can match a policy rule in ScanCenter based on group association: a *directory group* or a *custom group*.

- Directory Groups, page 25-4
- Custom Groups, page 25-4
- How Groups and the Authentication Key Interoperate, page 25-5

Directory Groups

Directory groups define the group to which traffic belongs. The group, if present, is included in the HTTP header of the client request. The ASA includes the group in the HTTP header when you configure IDFW. If you do not use IDFW, you can configure a default group for traffic matching an ASA rule for Cloud Web Security inspection.

When you configure a directory group, you must enter the group name exactly.

- IDFW group names are sent in the following format:

  *domain-name**group-name*

  When the ASA learns the IDFW group name, the format on the ASA is *domain-name**group-name*. However, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation.

- The default group name is sent in the following format:

  [*domain*\]*group-name*

  On the ASA, you need to configure the optional domain name to be followed by 2 backslashes (\\); however, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation. For example, if you specify “Cisco\\Boulder1,” the ASA modifies the group name to be “Cisco\Boulder1” with only one backslash (\) when sending the group name to Cloud Web Security.

Custom Groups

Custom groups are defined using one or more of the following criteria:

- ScanCenter Group authentication key—You can generate a Group authentication key for a custom group. Then, if you identify this group key when you configure the ASA, all traffic from the ASA is tagged with the Group key.
- Source IP address—You can identify source IP addresses in the custom group. Note that the ASA service policy is based on source IP address, so you might want to configure any IP address-based policy on the ASA instead.
- Username—You can identify usernames in the custom group.
  - IDFW usernames are sent in the following format:

    *domain-name**username*

- AAA usernames, when using RADIUS or TACACS+, are sent in the following format:

  LOCAL*username*

- AAA usernames, when using LDAP, are sent in the following format:

  *domain-name**username*

- For the default username, it is sent in the following format:

  [*domain-name*\]*username*

  For example, if you configure the default username to be "Guest," then the ASA sends "Guest." If you configure the default username to be "Cisco\Guest," then the ASA sends "Cisco\Guest."

How Groups and the Authentication Key Interoperate

Unless you need the per-ASA policy that a custom group+group key provides, you will likely use a company key. Note that not all custom groups are associated with a group key. Non-keyed custom groups can be used to identify IP addresses or usernames, and can be used in your policy along with rules that use directory groups.

Even if you do want per-ASA policy and are using a group key, you can also use the matching capability provided by directory groups and non-keyed custom groups. In this case, you might want an ASA-based policy, with some exceptions based on group membership, IP address, or username. For example, if you want to exempt users in the America\Management group across all ASAs:

1. Add a directory group for America\Management.
2. Add an exempt rule for this group.
3. Add rules for each custom group+group key after the exempt rule to apply policy per-ASA.
4. Traffic from users in America\Management will match the exempt rule, while all other traffic will match the rule for the ASA from which it originated.

Many combinations of keys, groups, and policy rules are possible.

Cloud Web Security Actions

After applying the configured policies, Cloud Web Security either blocks, allows, or sends a warning about the user request:

- Allows—When Cloud Web Security allows the client request, it contacts the originally requested server and retrieves the data. It forwards the server response to the ASA, which then forwards it to the user.
- Blocks—When Cloud Web Security blocks the client request, it notifies the user that access has been blocked. It sends an HTTP 302 "Moved Temporarily" response that redirects the client application to a web page hosted by the Cloud Web Security proxy server showing the blocked error message. The ASA forwards the 302 response to the client.
- Warns—When the Cloud Web Security proxy server determines that a site may be in breach of the acceptable use policy, it displays a warning page about the site. You can choose to heed the warning and drop the request to connect, or you can click through the warning and proceed to the requested site.

You can also choose how the ASA handles web traffic when it cannot reach either the primary or backup Cloud Web Security proxy server. It can block or allow all web traffic. By default, it blocks web traffic.

Bypassing Scanning with Whitelists

If you use AAA rules or IDFW, you can configure the ASA so that web traffic from specific users or groups that otherwise match the service policy rule is not redirected to the Cloud Web Security proxy server for scanning. When you bypass Cloud Web Security scanning, the ASA retrieves the content directly from the originally requested web server without contacting the proxy server. When it receives the response from the web server, it sends the data to the client. This process is called "whitelisting" traffic.

Although you can achieve the same results of exempting traffic based on user or group when you configure the class of traffic using ACLs to send to Cloud Web Security, you might find it more straightforward to use a whitelist instead. Note that the whitelist feature is only based on user and group, not on IP address.

IPv4 and IPv6 Support

Cloud Web Security currently supports only IPv4 addresses. If you use IPv6 internally, NAT 64 must be performed for any IPv6 flows that need to be sent to Cloud Web Security.

The following table shows the class map traffic that is supported by Cloud Web Security redirection:

Class Map Traffic	Cloud Web Security Inspection
From IPv4 to IPv4	Supported
From IPv6 to IPv4 (using NAT64)	Supported
From IPv4 to IPv6	Not Supported
From IPv6 to IPv6	Not Supported

Failover from Primary to Backup Proxy Server

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 miniutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active.

If a client or the ASA can reach the server at least twice consecutively before the retry count is reached, the polling stops and the tower is determined to be reachable.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

Licensing Requirements for Cisco Cloud Web Security

Model	License Requirement
All models	Strong Encryption (3DES/AES) License to encrypt traffic between the security appliance and the Cloud Web Security server.

On the Cloud Web Security side, you must purchase a Cisco Cloud Web Security license and identify the number of users that the ASA handles. Then log into ScanCenter, and generate your authentication keys.

Prerequisites for Cloud Web Security

(Optional) User Authentication Prerequisites

To send user identity information to Cloud Web Security, configure one of the following on the ASA:

- AAA rules (username only)—See Chapter 8, "Configuring AAA Rules for Network Access."
- IDFW (username and group)—See Chapter 38, "Configuring the Identity Firewall," in the general operations configuration guide.

(Optional) Fully Qualified Domain Name Prerequisites

If you use FQDNs in ACLs for your service policy rule, or for the Cloud Web Security server, you must configure a DNS server for the ASA according to the "Configuring the DNS Server" section on page 16-17 in the general operations configuration guide.

Guidelines and Limitations

Context Mode Guidelines

Supported in single and multiple context modes.

In multiple context mode, the server configuration is allowed only in the system, and the service policy rule configuration is allowed only in the security contexts.

Each context can have its own authentication key, if desired.

Firewall Mode Guidelines

Supported in routed firewall mode only. Does not support transparent firewall mode.

IPv6 Guidelines

Does not support IPv6. See the "IPv4 and IPv6 Support" section on page 25-6.

Additional Guidelines

- Cloud Web Security is not supported with ASA clustering.
- Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security.

- When an interface to the Cloud Web Security proxy servers goes down, output from the **show scansafe server** command shows both servers up for approximately 15-25 minutes. This condition may occur because the polling mechanism is based on the active connection, and because that interface is down, it shows zero connection, and it takes the longest poll time approach.
- Cloud Web Security is not supported with the ASA CX module. If you configure both the ASA CX action and Cloud Web Security inspection for the same traffic, the ASA only performs the ASA CX action.
- Cloud Web Security inspection is compatibile with HTTP inspection for the same traffic. HTTP inspection is enabled by default as part of the default global policy.
- Cloud Web Security is not supported with extended PAT or any application that can potentially use the same source port and IP address for separate connections. For example, if two different connections (targeted to separate servers) use extended PAT, the ASA might reuse the same source IP and source port for both connection translations because they are differentiated by the separate destinations. When the ASA redirects these connections to the Cloud Web Security server, it replaces the destination with the Cloud Web Security server IP address and port (8080 by default). As a result, both connections now appear to belong to the same flow (same source IP/port and destination IP/port), and return traffic cannot be untranslated properly.
- The Default Inspection Traffic traffic class does not include the default ports for the Cloud Web Security inspection (80 and 443).

Default Settings

By default, Cisco Cloud Web Security is not enabled.

Configuring Cisco Cloud Web Security

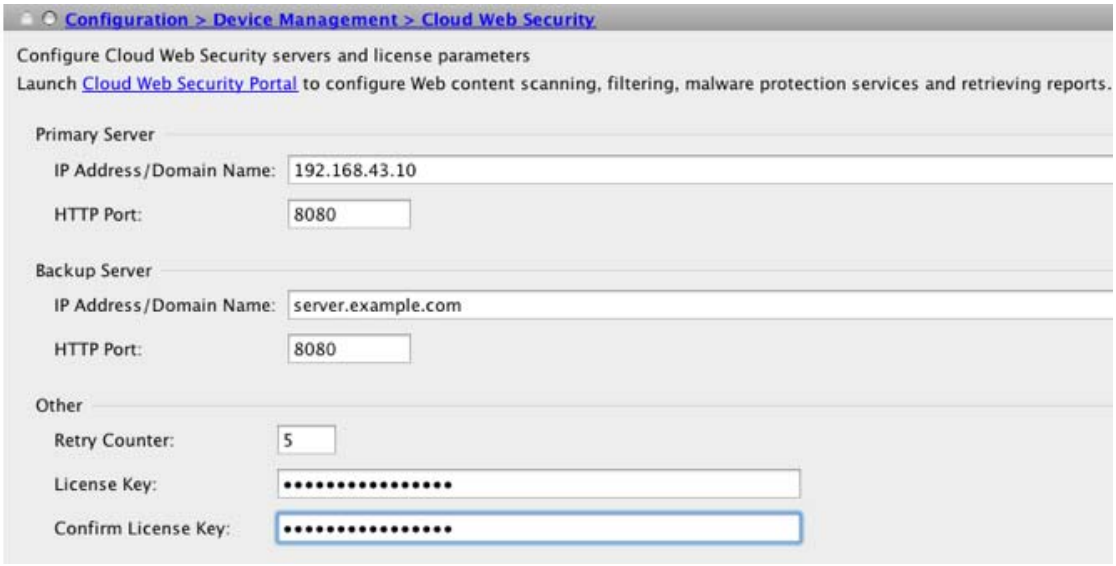
Configuring Communication with the Cloud Web Security Proxy Server

Guidelines

The public key is embedded in the ASA software, so there is no need for you to configure it.

Detailed Steps

Step 1 Choose **Configuration > Device Management > Cloud Web Security**.



Step 2 In the Primary Server area, enter the following:

- IP Address/Domain Name—Enter the IPv4 address or FQDN of the primary server.
- HTTP Port—Enter the HTTP port of the primary server (port to which traffic must be redirected). By default the port is 8080; do not change this value unless directed to do so.

Step 3 In the Backup Server area, enter the following:

- IP Address/Domain Name—Enter the IPv4 address or FQDN of the backup server.
- HTTP Port—Enter the HTTP port of the backup server (port to which traffic must be redirected). By default the port is 8080. Valid values are from 1 to 65535.

Step 4 In the Other area, enter the following:

- Retry Counter—Enter the value for the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable. Polls are performed every 30 seconds. Valid values are from 2 to 100, and the default is 5.
- License Key—Configure the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexidecimal number. See the "Authentication Keys" section on page 25-3.
- Confirm License Key—Confirm the authentication key.

Step 5 Click **Apply**.

(Multiple Context Mode) Allowing Cloud Web Security Per Security Context

In multiple context mode, you must allow Cloud Web Security per context. See the "Configuring a Security Context" section on page 8-21 in the general operations configuration guide.

Note You must configure a route pointing to the Scansafe towers in both; the admin context and the specific context. This ensures that the Scansafe tower does not become unreachable in the Active/Active failover scenario.

Configuring a Service Policy to Send Traffic to Cloud Web Security

Your service policy consists of multiple service policy rules, applied globally, or applied to each interface. Each service policy rule can either send traffic to Cloud Web Security (Match) or exempt traffic from Cloud Web Security (Do Not Match). Create rules for traffic destined for the Internet. The order of these rules is important. When the ASA decides whether to forward or exempt a packet, the ASA tests the packet with each rule in the order in which the rules are listed. After a match is found, no more rules are checked. For example, if you create a rule at the beginning of a policy that explicitly Matches all traffic, no further statements are ever checked. You can reorder the rules as needed after you add them.

See Chapter 1, "Configuring a Service Policy," for more information about service policy rules.

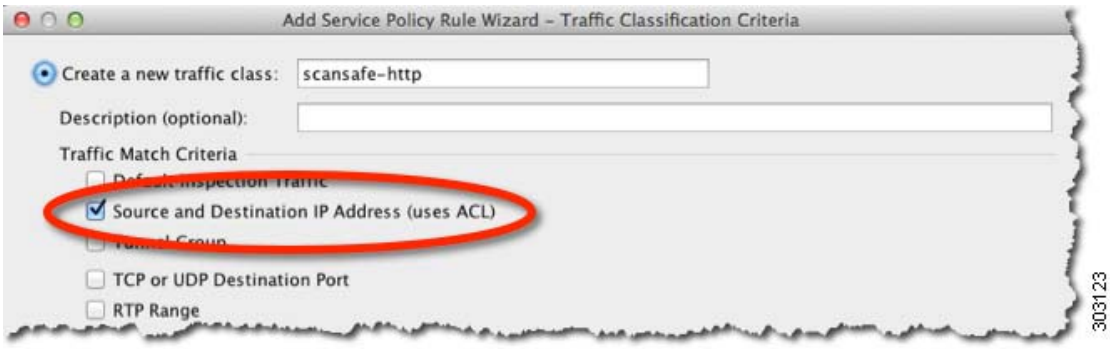
Prerequisites

(Optional) If you need to use a whitelist to exempt some traffic from being sent to Cloud Web Security, first create the whitelist according to the "(Optional) Configuring Whitelisted Traffic" section on page 25-23 so you can refer to the whitelist in your service policy rule.

Detailed Steps

Step 1 Choose **Configuration > Firewall > Service Policy Rules**, and click **Add > Service Policy Rule** to add a service policy rule.

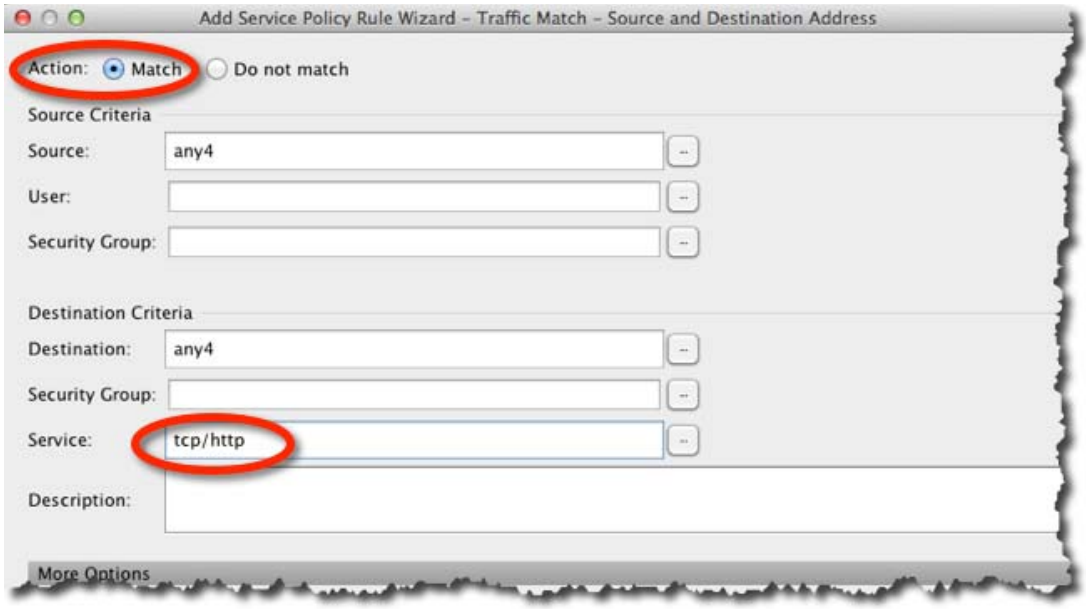
Step 2 On the Service Policy dialog box, you can configure Cloud Web Security as part of a new service policy, or you can edit an existing service policy. Click **Next**.



Step 3 On the Traffic Classification Criteria dialog box, name the traffic class (or accept the default name), keep the **Create a new traffic class** option selected, and click **Source and Destination IP address (Uses ACL)**, then click **Next**.

When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** on the Traffic Classification dialog box.

The Traffic Match - Source and Destination dialog box appears.



a. Click **Match** or **Do Not Match**.

   Match specifies that traffic matching the source and destination is sent to Cloud Web Security. **Do Not Match** exempts matching traffic from Cloud Web Security. You can later add additional rules to match or not match other traffic.

   When creating your rules, consider how you can match appropriate traffic that is destined for the Internet, but not match traffic that is destined for other internal networks. For example, to prevent inside traffic from being sent to Cloud Web Security when the destination is an internal server on the DMZ, be sure to add a deny ACE to the ACL that exempts traffic to the DMZ.

b. In the Source Criteria area, enter or browse for a Source IP address or network object, an optional IDFW Username or group, and an optional TrustSec Security Group.

c. In the Destination Criteria area, enter or browse for a Destination IP address or network object, and an optional TrustSec Security Group.

   FQDN network objects might be useful in matching or exempting traffic to specific servers.

d. In the Service field, enter **http** or **https**, and click **Next**.

   Note Cloud Web Security only operates on HTTP and HTTPS traffic. Each type of traffic is treated separately by the ASA. Therefore, you need to create HTTP-only rules and HTTPS-only rules.

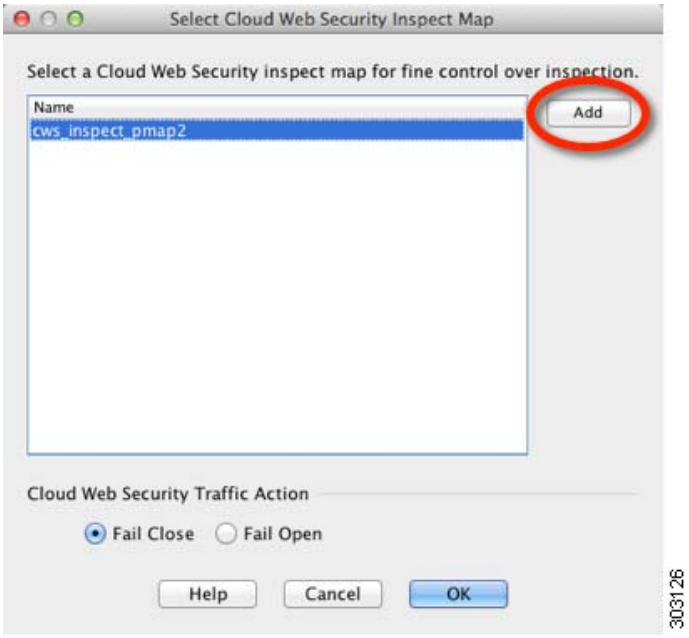
   The Rule Actions dialog box appears.

Step 4 On the Protocol Inspection tab, check the **Cloud Web Security** check box.

Step 5 Click **Configure** to set the traffic action (fail open or fail close) and add the inspection policy map.

The inspection policy map configures essential parameters for the rule and also optionally identifies the whitelist. An inspection policy map is required for each class of traffic that you want to send to Cloud Web Security. You can also pre-configure inspection policy maps from the Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security pane.

The Select Cloud Web Security Inspect Map dialog box appears.

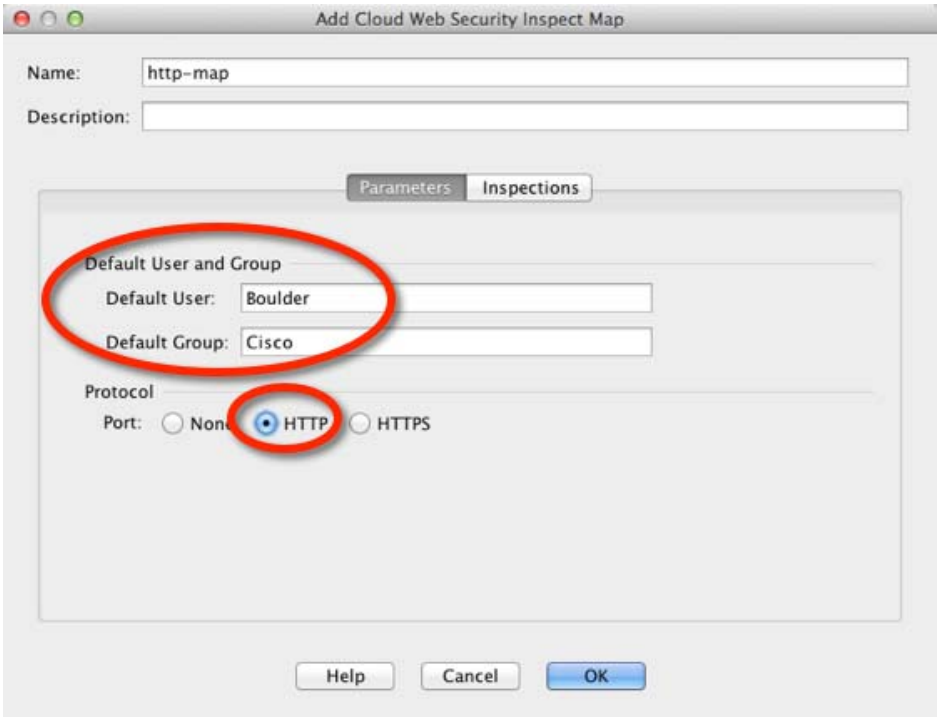


a. For the Cloud Web Security Traffic Action, choose one:
   - **Fail Close**—Drops all traffic if the Cloud Web Security servers are unavailable.
   - **Fail Open**—Allows traffic to pass through the ASA if the Cloud Web Security servers are unavailable.

b. Choose an existing inspection policy map, or add one using the **Add** button.

c. Click **Add** to add a new inspection policy map.

   The Add Cloud Web Security Inspect Map dialog box appears.



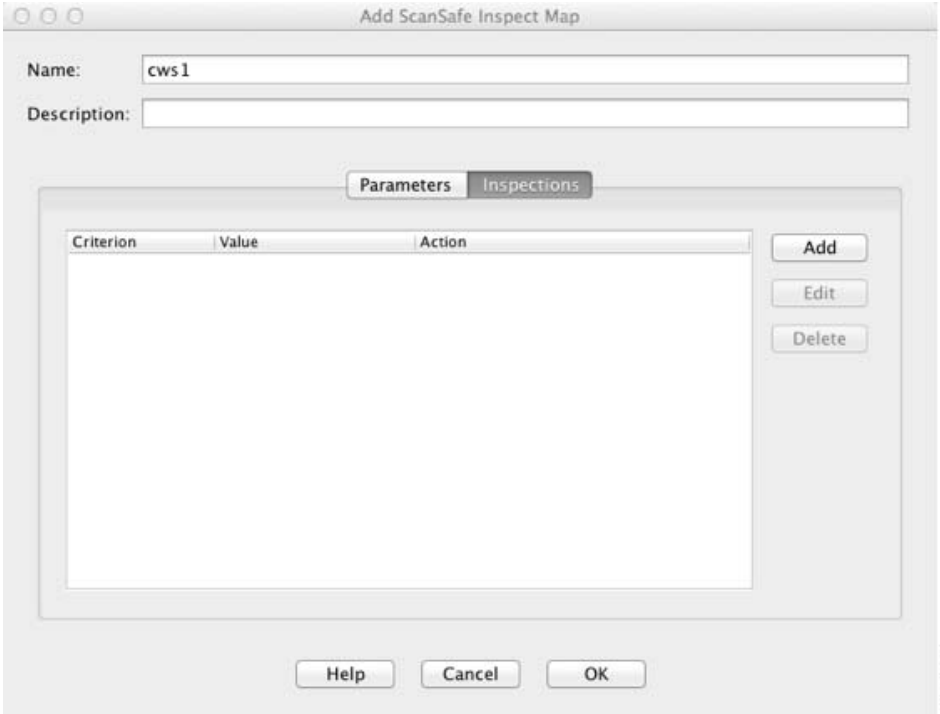
d. In the Name field, specify a name for the inspection policy map, up to 40 characters in length.

e. (Optional) Enter a description.

f. (Optional) On the Parameters tab, specify a Default User and/or a Default Group. If the ASA cannot determine the identity of the user coming into the ASA, then the default user and/or group is applied.

g. For the Protocol, click **HTTP** or **HTTPS**, to match the service you set in Step 3d. Cloud Web Security treats each type of traffic separately.

h. (Optional) To identify a whitelist, click the **Inspections** tab.



- Click **Add** to choose the inspection class map you created in the "(Optional) Configuring Whitelisted Traffic" section on page 25-23.

  The Add Cloud Web Security Match Criterion dialog box appears.
- From the Cloud Web Security Traffic Class drop-down menu, choose an inspection class map.

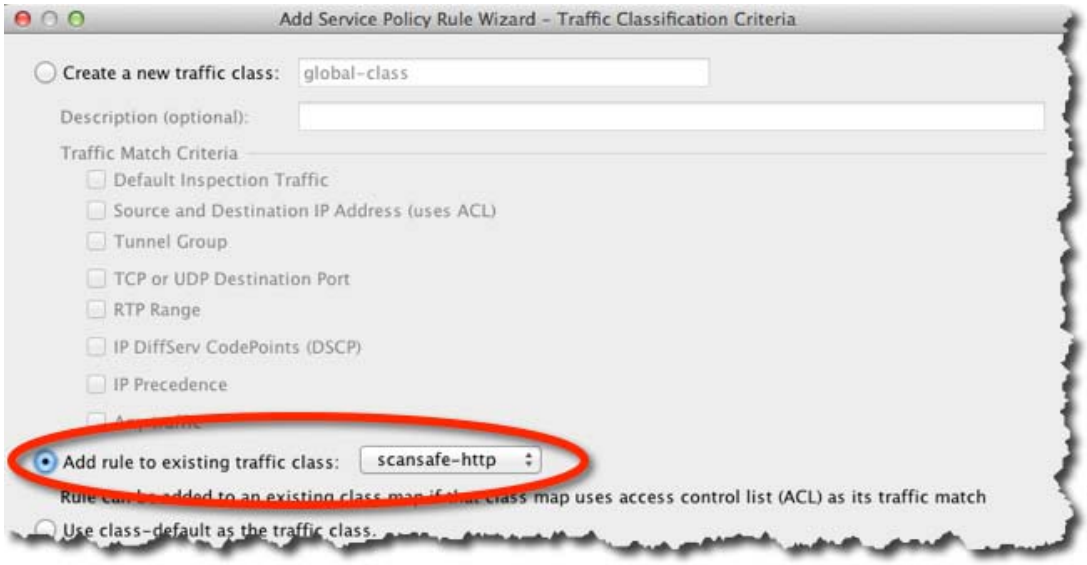
  To add or edit a class map, click **Manage**.
- For the Action, click **Whitelist**.
- Click **OK** to add the whitelist to the policy map.
- Click **OK**.

Step 6 Click **Finish**. The rule is added to the Service Policy Rules table.

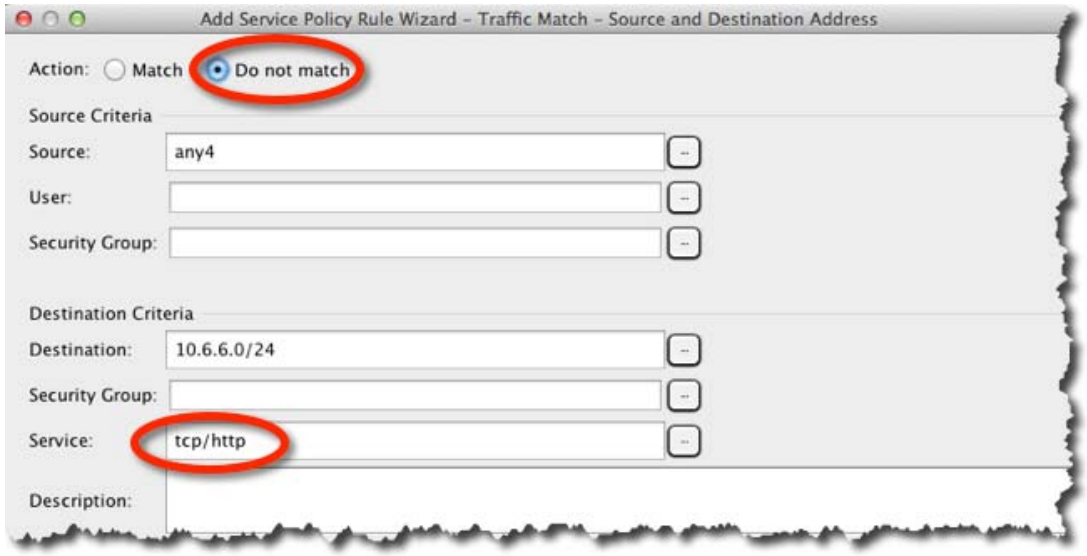
Step 7 To add additional sub-rules (ACEs) for this traffic class, to match or exempt additional traffic:

a. Choose **Configuration > Firewall > Service Policy Rules**, and click **Add > Service Policy Rule**.

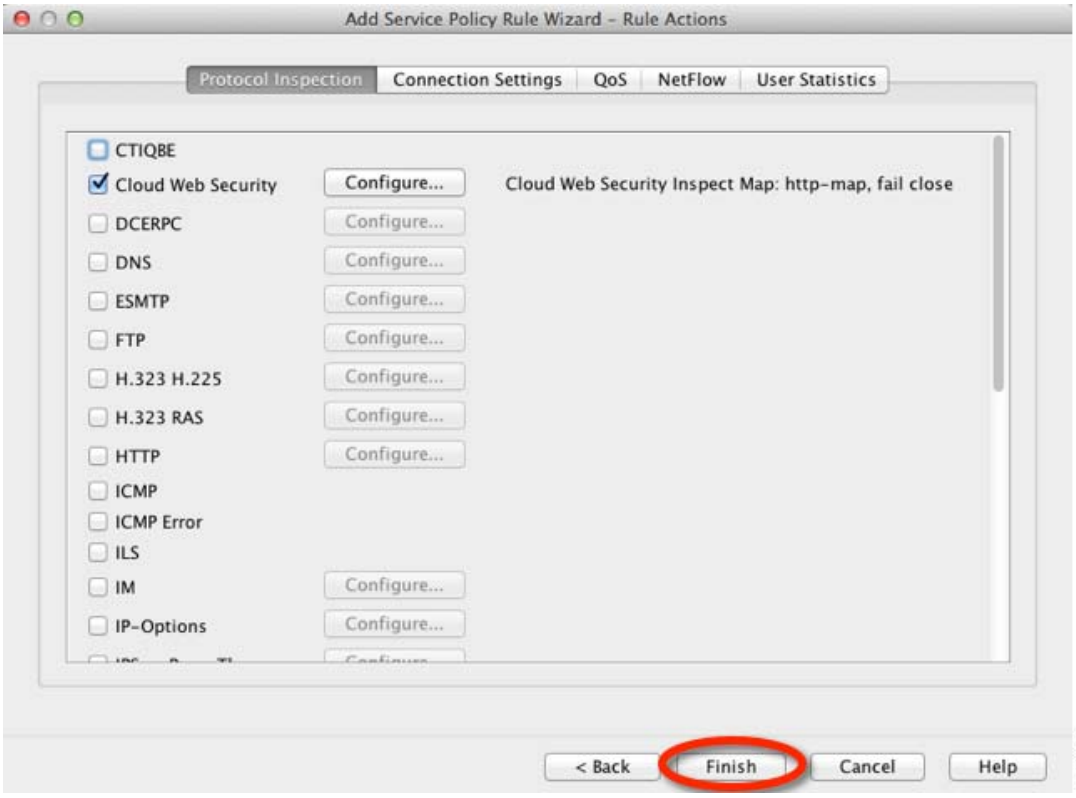
b. Choose the same service policy as Step 2. Click **Next**.



c. On the Traffic Classification Criteria dialog box, choose **Add Rule to Existing Traffic Class**, and choose the name you created in Step 3. Click **Next**.



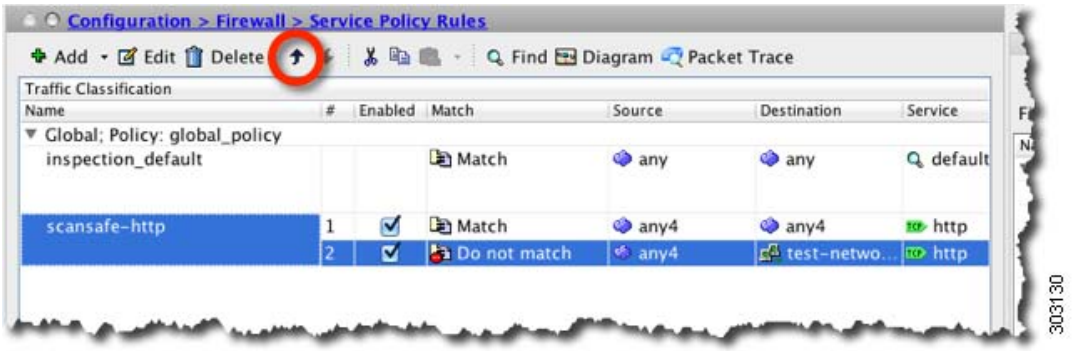
d. In the Traffic Match - Source and Destination dialog box, choose **Match** to add inspect additional traffic, or **Do Not Match** to exempt traffic from Cloud Web Security inspections. Be sure to set the service to match the previous rules in this class (HTTP or HTTPS); you cannot mix HTTP and HTTPS in the same traffic class for Cloud Web Security. Click **Next**.

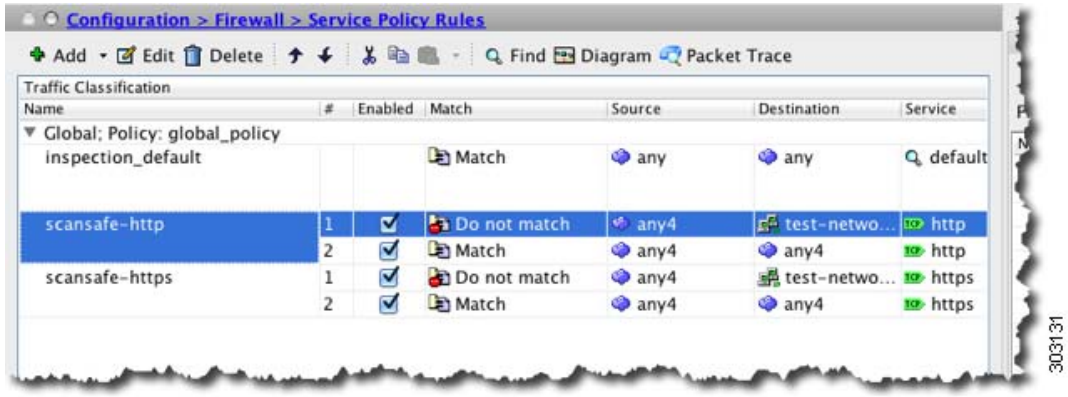


e. On the Rule Actions dialog box, do not make any changes; click **Finish**. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs, so the previously-specified actions are inherited.

Step 8 Repeat this entire procedure to create an additional traffic class, for example for HTTPS traffic. You can create as many rules and sub-rules as needed.

Step 9 Arrange the order of Cloud Web Security rules and sub-rules on the Service Policy Rules pane. See the "Managing the Order of Service Policy Rules" section on page 1-15 for information about changing the order of ACEs.



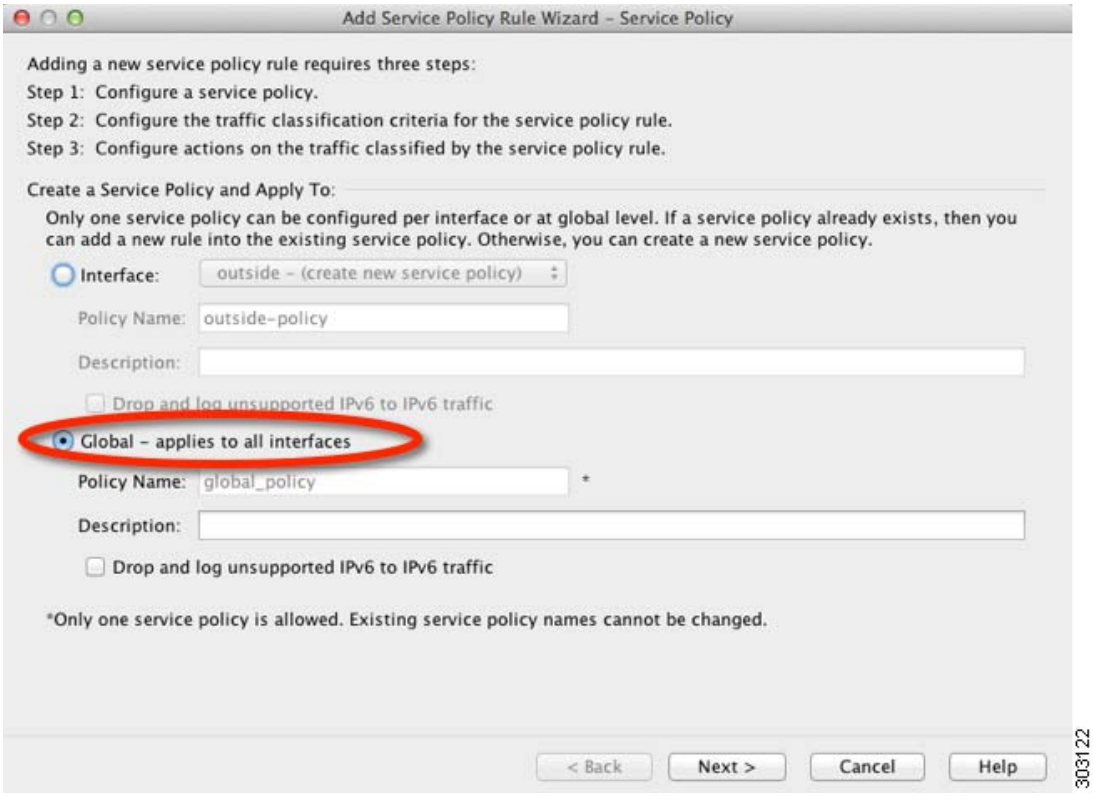


Step 10 Click **Apply**.

Examples

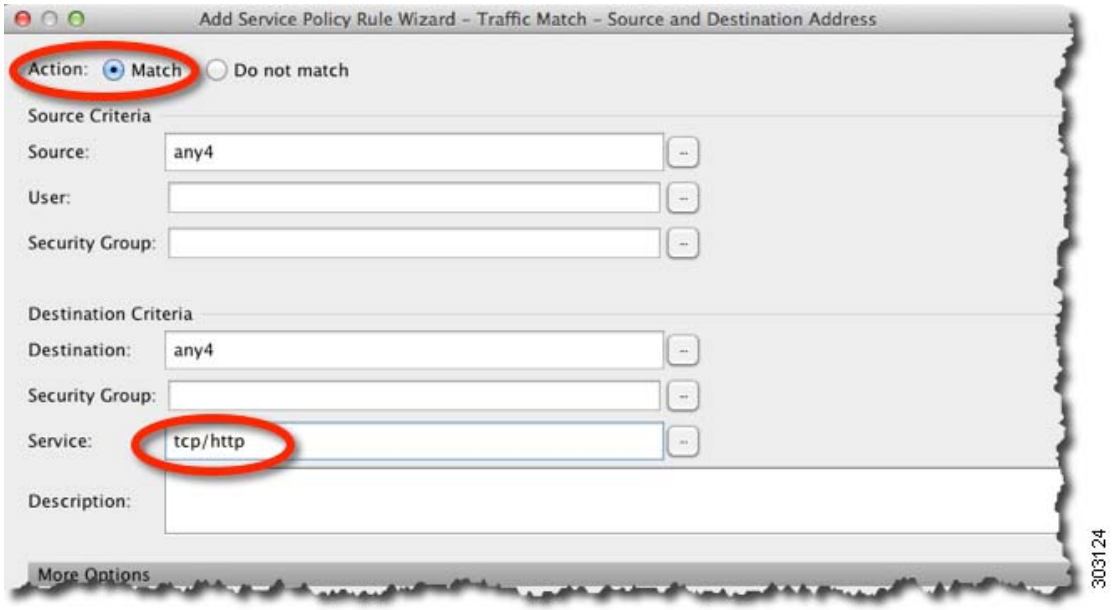
The following example exempts all IPv4 HTTP and HTTPS traffic going to the 10.6.6.0/24 (test_network), and sends all other HTTPS and HTTPS traffic to Cloud Web Security, and applies this service policy rule to all interfaces as part of the existing global policy. If the Cloud Web Security server is unreachable, the ASA drops all matching traffic (fail close). If a user is not have user identity information, the default user Boulder and group Cisco is used.

Step 1 Choose **Configuration > Firewall > Service Policy Rules**, and click **Add > Service Policy Rule**. Add this rule to the default global_policy:



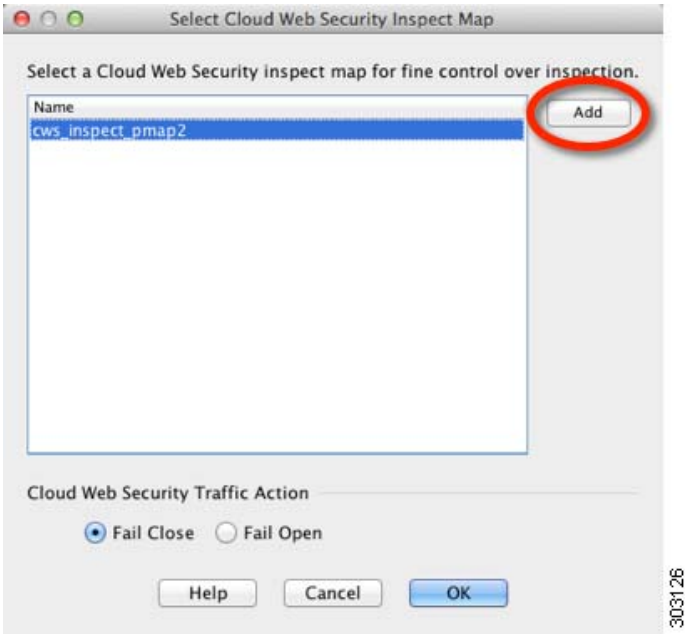
Step 2 Add a new traffic class called “scansafe-http,” and specify an ACL for traffic matching:

Step 3 Choose **Match**, and specify **any4** for the Source and Destination. Specify **tcp/http** for the Service.

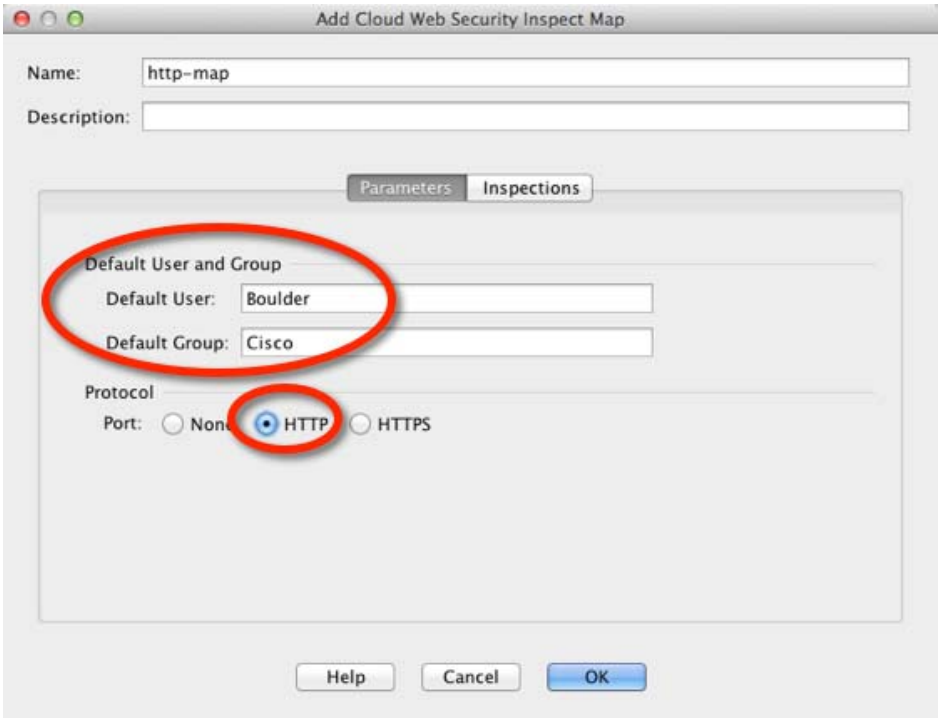


Step 4 Check **Cloud Web Security** and click **Configure**.

Step 5 Accept the default Fail Close action, and click **Add**.

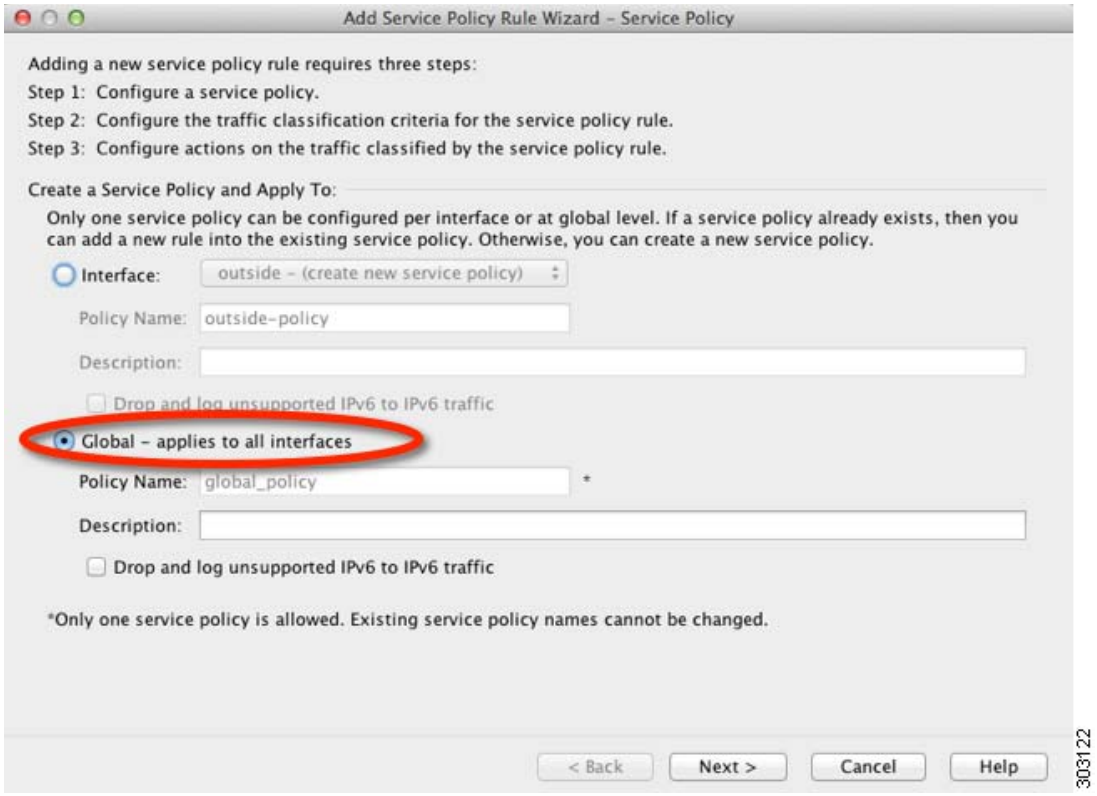


Step 6 Name the inspection policy map "http-map," set the Default User to Boulder and the default group to Cisco. Choose **HTTP**.

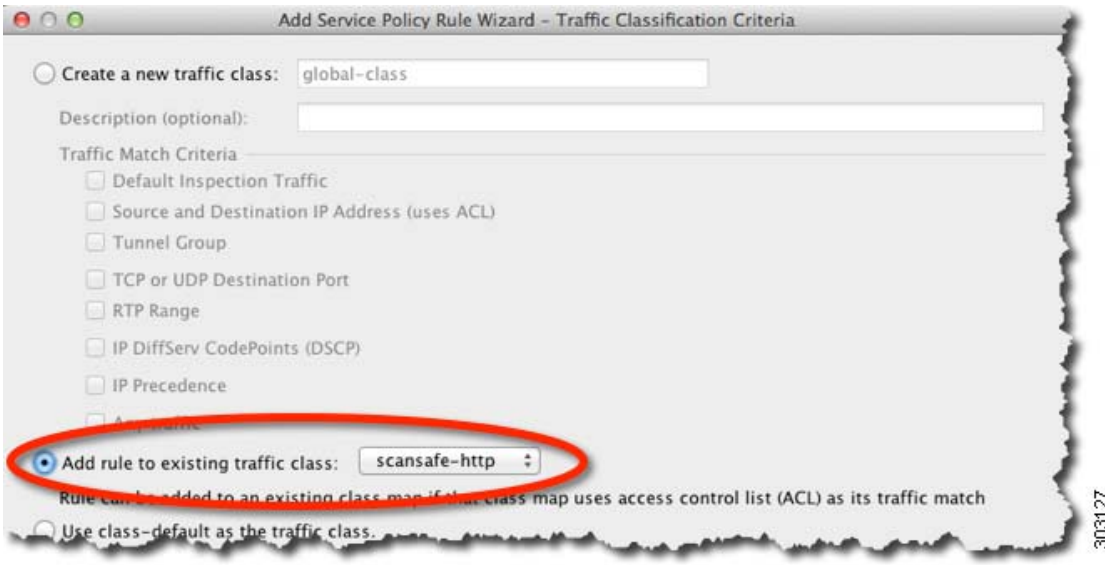


Step 7 Click **OK**, **OK**, and then **Finish**. The rule is added to the Service Policy Rules table.

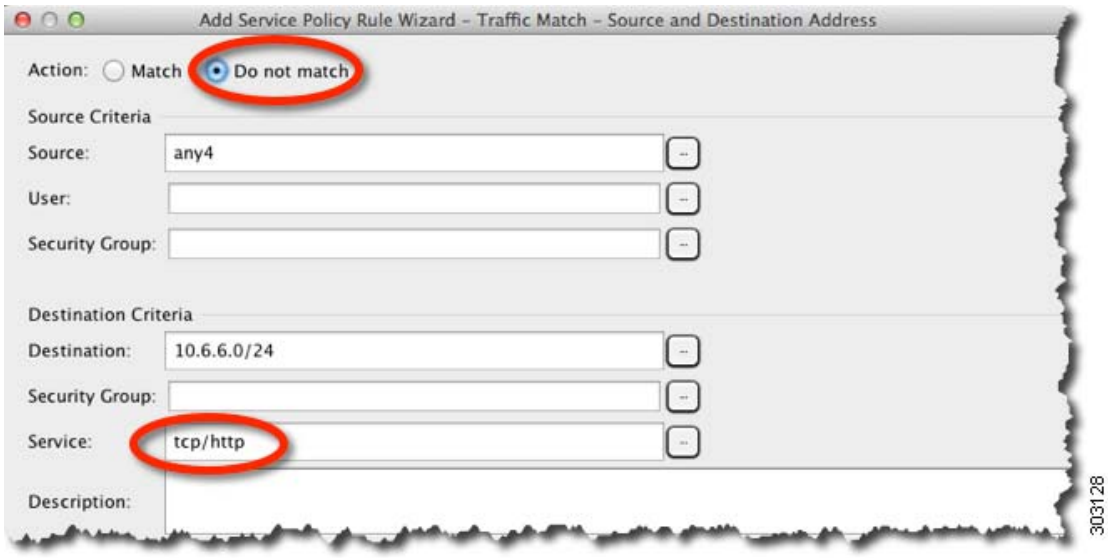
Step 8 Choose **Configuration > Firewall > Service Policy Rules**, and click **Add > Service Policy Rule**. Add the new rule to the default global_policy:



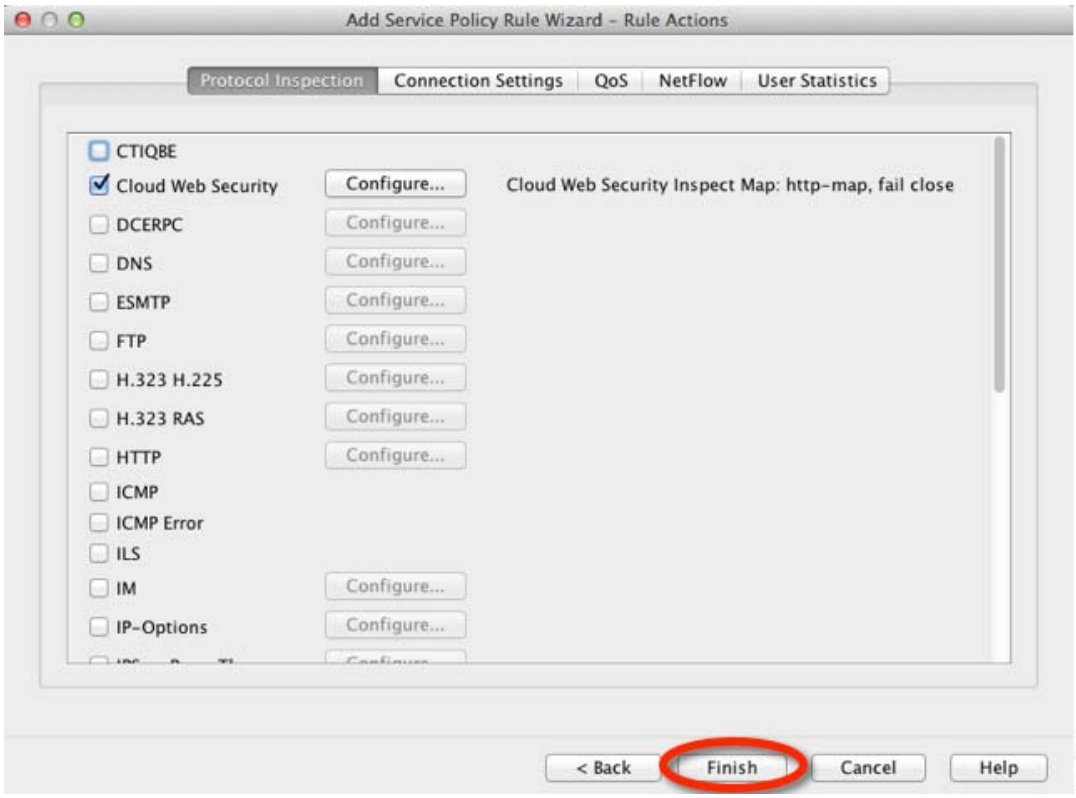
Step 9 Click **Add rule to existing traffic class**, and choose **scansafe-http**.



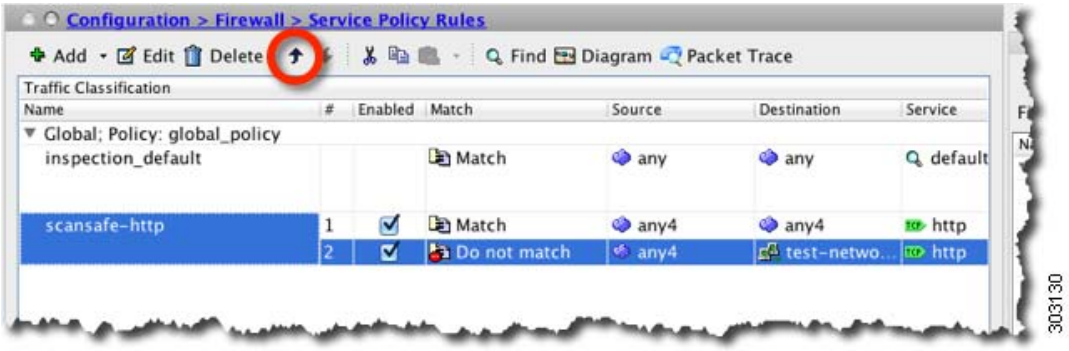
Step 10 Choose **Do not match**, set **any4** as the Source, and **10.6.6.0/24** as the Destination. Set the Service to **tcp/http**.



Step 11 Click **Finish**.

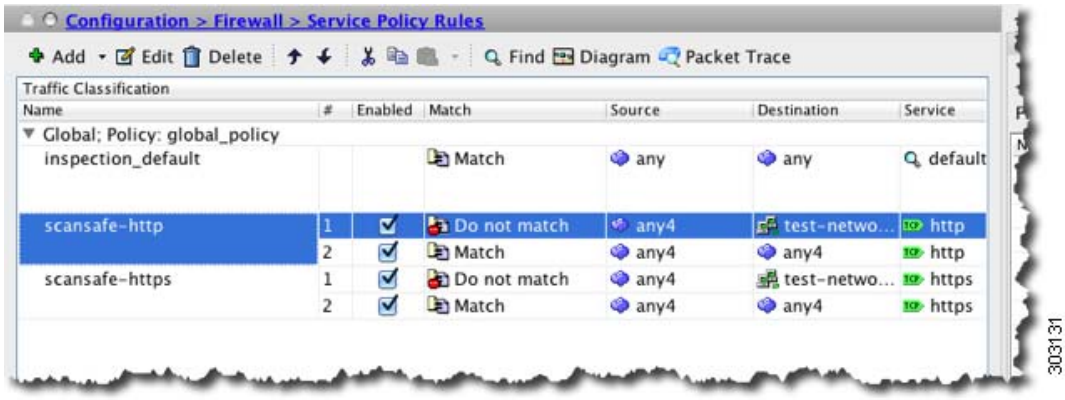


Step 12 Reorder the rules so the Do not match rule is above the Match rule.



User traffic is compared to these rules in order; if this Match rule is first in the list, then all traffic, including traffic to test_network, will match only that rule and the Do not match rule will never be hit. If you move the Do not match rule above the Match rule, then traffic to test_network will match the Do not match rule, and all other traffic will match the Match rule.

Step 13 Repeat the above steps with the following changes: add a new traffic class called "scansafe-https," and choose **HTTPS** for the inspection policy map.



Step 14 Click **Apply**.

(Optional) Configuring Whitelisted Traffic

If you use user authentication, you can exempt some traffic from being filtered by Cloud Web Security based on the username and/or groupname. When you configure your Cloud Web Security service policy rule, you can reference the whitelisting inspection class map. Both IDFW and AAA user credentials can be used with this feature.

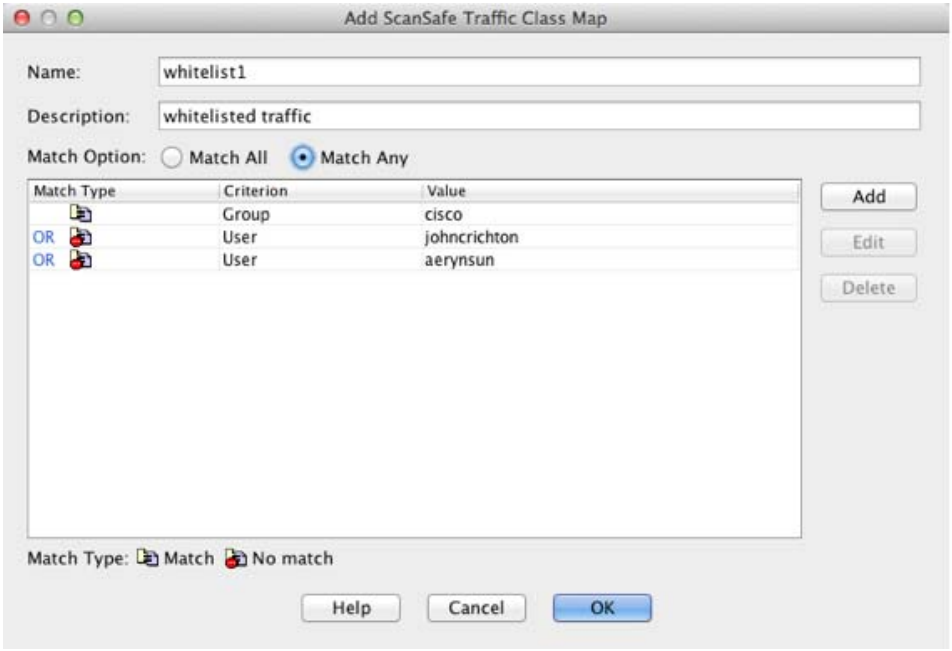
Although you can achieve the same results of exempting traffic based on user or group when you configure the service policy rule, you might find it more straightforward to use a whitelist instead. Note that the whitelist feature is only based on user and group, not on IP address.

Detailed Steps

Step 1 Choose **Configuration > Firewall > Objects > Class Maps > Cloud Web Security**.

Step 2 Click **Add** to create a new class map.

The Add Cloud Web Security Traffic Class Map screen appears.



Step 3 In the Name field, enter the name of the new class map (40 characters or less).

Step 4 In the Description field, provide a description for the class map (200 characters or less).

Step 5 Choose the Match Option for the criteria you define when you click ADD:

- Match All—Specifies that traffic must match all criteria to match the class map.
- Match Any—Specifies that the traffic matches the class map if it matches at least one of the criteria.

Step 6 Click **Add**.

The Add Cloud Web Security Match Criterion Window appears.

Step 7 Choose the Match Type:

- Match—Specifies the user and/or group that you want to whitelist.
- No Match—Specifies the user and/or group that you do *not* want to whitelist; for example, if you whitelist the group “cisco,” but you want to scan traffic from users “johncrichton” and “aerynsun,” you can specify No Match for those users.

Step 8 Choose the Match Criterion:

- User—Specifies the user.
- Group—Specifies the group.
- User and Group—Specifies a user and group.

Step 9 Click **OK**.

Step 10 Continue to add match criteria as desired.

Step 11 Click **OK** to add the class map.

Step 12 Click **Apply**.

Step 13 Use the whitelist in the Cloud Web Security policy according to the "Configuring a Service Policy to Send Traffic to Cloud Web Security" section on page 25-10.

(Optional) Configuring the User Identity Monitor

When you use IDFW, the ASA only downloads user identity information from the AD server for users and groups included in active ACLs; the ACL must be used in a feature such as an access rule, AAA rule, service policy rule, or other feature to be considered active. Because Cloud Web Security can base its policy on user identity, you may need to download groups that are not part of an active ACL to get full IDFW coverage for all your users. For example, although you can configure your Cloud Web Security service policy rule to use an ACL with users and groups, thus activating any relevant groups, it is not required; you could use an ACL based entirely on IP addresses.The user identity monitor feature lets you download group information directly from the AD agent.

Restrictions

The ASA can only monitor a maximum of 512 groups, including those configured for the user identity monitor and those monitored through active ACLs.

Detailed Steps

Step 1 Choose **Configuration > Firewall > Identity Options**, and scroll to the Cloud Web Security Configuration section.

Step 2 Click **Add**.

The Add Monitor User dialog box appears.

Step 3 To add a domain, click **Manage**, and then click **Add**. You can only monitor groups for domains you have pre-defined on the ASA.

The Configure Identity Domains dialog box appears. For detailed information about adding domains, see the "Configuring Identity Options" section on page 38-16 in the general operations configuration guide.

Step 4 When you are finished adding domains, click **OK**.

Step 5 You can either type in a group name, or you can search for groups on the AD agent per domain.

- To type in a group name directly, enter the name in the bottom field in the following format, and click **OK**:

  *domain-name**group*

- To search for a group on the AD agent:

a. Choose the domain from the Domain drop-down list.

b. In the Find field, enter a text string to match group names, and click **Find**.

The ASA downloads names from the AD agent for the specified domain.

c. Double-click the name you want to monitor; it is added to the bottom field.

d. Click **OK**.

Repeat for additional groups.

Step 6 After you add the groups you want to monitor, click **Apply**.

Configuring the Cloud Web Security Policy

After you configure the ASA service policy rules, launch the ScanCenter Portal to configure Web content scanning, filtering, malware protection services, and reports.

Detailed Steps

Go to: https://scancenter.scansafe.com/portal/admin/login.jsp.

For more information, see the Cisco ScanSafe Cloud Web Security Configuration Guides:

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Monitoring Cloud Web Security

Command	Purpose
Monitoring > Properties > Cloud Web Security	Shows the status of the server, whether it is the current active server, the backup server, or unreachable. Shows total and current HTTP(S) connections. In multiple context mode, statistics are only shown within a context.
See the following URL: http://Whoami.scansafe.net	From a client, access this web site to determine if your traffic is going to the Cloud Web Security server.

Related Documents

Related Documents	URL
Cisco ScanSafe Cloud Web Security Configuration Guides	http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Feature History for Cisco Cloud Web Security

Table 25-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 25-1 Feature History for Cloud Web Security

Feature Name	Platform Releases	Feature Information
Cloud Web Security	9.0(1)	This feature was introduced. Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. We introduced or modified the following screens: Configuration > Device Management > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit > Manage Cloud Web Security Class Maps Configuration > Firewall > Identity Options Configuration > Firewall > Service Policy Rules Monitoring > Properties > Cloud Web Security