Working with ScanSafe Web Security

Security Manager provides integration with ScanSafe Web Security. ScanSafe Web Security is a cloud-based SaaS (Security as a Service) function that makes available its web security data centers at various locations worldwide. When ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to ScanSafe Cloud for content scanning and for malware detection by other means. Also, you can use ScanSafe Web Security to provide differentiated services to particular users, user groups, and IPs.

Invoking ScanSafe Web Security from Security Manager, you can define policies and settings in the following areas:

- Content scanning settings
- Content scanning policies
- AAA server settings
- AAA policies

With ScanSafe Web Security integration in Security Manager you can copy and share most policies and framework-based policy features. The following table details the scope of support for scanning and AAA policy types.

Supported Type	Example
Content Scan Settings	Primary server IP, secondary server IP, server timeouts
Content Scan Policies	Global allow list policies Include/exclude user groups, default user configuration, default user group configuration Interfaces that must have content scanning enabled
AAA Server Settings	Identity policy object used in http-basic and NTLM policy Http-basic and NTLM related timeouts Order of occurrence for proxy, http-basic, and NTLM LDAP server and LDAP attribute map configuration for IOS **Note** Radius and TACAS servers are also supported. Per interface AAA list
AAA Policies	Http-basic and NTLM admission rule support (authentication methods) now join the previously available Auth-Proxy method

Security Manager does *not* support the following features:

- PAM configuration when inspect or ZBF rules for http/https are not present
- Auth-proxy using LDAP on older IOS versions. (That is, only IOS versions that support ScanSafe Web Security)
- Identity policy with auth-proxy as AAA method. (Support only for NTLM and http-basic.)
- Validation of Virtual Template number for identity policy creation
- Validation of the Secure Trust Point for LDAP server
- Inheritance of content scanning rules
- AD browsing of user groups and users
- Tool support for newer policies (such as policy query)
- Control tag policy

For more information on the ScanSafe Web Security product, go to http://www.cisco.com/en/US/partner/products/ps11720/index.html.

Related Topics

- ScanSafe Web Security Page, page 20-4
- ScanSafe Web Security Settings Page, page 20-6
- Configuring ScanSafe Web Security, page 20-2
- Add and Edit Default User Groups Dialog Box, page 20-6

This chapter contains the following topics:

Configuring ScanSafe Web Security

Use the ScanSafe Web Security Settings page to define the settings for the default user group. As with other settings policies, you can share the default user group policy settings.

Related Topics

- ScanSafe Web Security Page, page 20-4
- ScanSafe Web Security Settings Page, page 20-6
- Chapter 20, “Working with ScanSafe Web Security”
- Add and Edit Default User Groups Dialog Box, page 20-6
- AAA Rules Page, page 15-10

Note All steps are shown as performed from the Policy view.

To configure ScanSafe Web Security, perform the following steps:

Step 1 From the Policy Types selector, select Firewall > ScanSafe Web Security.

The ScanSafe Web Security page appears with the Interfaces tab selected.

Step 2 Enable those interfaces by which web requests are to be forwarded to the ScanSafe Web Security server by selecting them from the list in the **Available Interfaces** column and moving them to the **Selected Interfaces** column.

Step 3 Select the **WhiteListing Regular Expressions** tab.

Step 4 Select the **Notify Tower** checkbox to send notifications to the ScanSafe Web Security server regarding the allowed list. It is applicable to all allowed list except that which is IP-based.

(ScanSafe Web Security receives a warning when no regular expression is specified for white listing.)

Step 5 In the HTTP Host area specify the regular expressions to be allowed (using regular expression matching) by selecting them from the list in the **Available Regular Expressions** column and moving them to the **Selected Regular Expressions** column.

Step 6 In the HTTP User Agent area specify the regular expressions to be allowed by selecting them from the list in the **Available Regular Expressions** column and moving them to the **Selected Regular Expressions** column.

Step 7 Select the **WhiteListing ACLs** tab.

Step 8 Specify the type of ACLs to operate upon by selecting either **Extended** or **Standard** from the Type list.

Step 9 Specify the ACLs to be allowed by selecting them from the list in the column on the left and moving them to the **Selected items** column.

Step 10 Select the **User Groups** tab.

Tip You can use the User Groups page to define user groups, specify both the default user and default user group, and to include or exclude user groups. You can also edit or delete entries in all three of these lists.

Step 11 Specify a default user by entering the user name in the **Default User** field (optional).

Step 12 Specify a default user group by entering the user group name in the **Default User Group** field.

Step 13 Include a user group by selecting the interface and then adding the user group to the Include list.

Step 14 Exclude a user group by selecting the interface and then adding the user group to the Exclude list.

Step 15 Select **Policy > Firewall > Settings > ScanSafe Web Security** from the policy selector.

Step 16 With the **Details** tab selected, specify the Primary ScanSafe Server by entering the following values:

- IP Address/Name
- HTTP Port (default 8080)
- HTTPS Port (default 8080)

Step 17 With the **Details** tab selected, specify the Secondary ScanSafe Server by entering the following values:

- IP Address/Name (only a valid IP address or FQDN).
- HTTP Port (default 8080)
- HTTPS Port (default 8080)

Step 18 Specify the **Server Timeout** period in seconds (default 300).

Step 19 Specify the **Session Idle Timeout** period in seconds (default 300).

Step 20 Specify the source address by doing *one* of the following:

- Click the **IP Address** button and then enter the IP address.

- Click the **Interface** button, and then click the **Select** button and browse the Interface Selector to select an interface.

Note A valid source IP or interface must be one of the interfaces on which ScanSafe Web Security is enabled (on the Firewall > ScanSafe Web Security page > Interface tab.

Step 21 Enter the **License** and select the checkbox if it is encrypted.

Tip If Encrypted is not selected, the value entered must be 32 hexadecimal characters.

Step 22 If desired, select the **Enable Logging** checkbox.

ScanSafe Web Security Page

Security Manager provides integration with ScanSafe Web Security. ScanSafe Web Security is a cloud-based SaaS (Security as a Service) function that makes available its web security data centers at various locations worldwide. When ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to ScanSafe Cloud for content scanning and for malware detection by other means. Also, you can use ScanSafe Web Security to provide differentiated services to particular users, user groups, and IPs.

Using ScanSafe Web Security in Security Manager, you can define settings and policies in the following areas:

- Content scanning settings
- Content scanning policies
- AAA server settings
- AAA policies

With ScanSafe Web Security integration in Security Manager you can copy and share most policies and framework-based policy features.

For information on how best to configure the ScanSafe Web Security Page for your particular purposes, see Working with ScanSafe Web Security.

Navigation Path

(Policy view) Select Firewall and open Settings from the Policy Type selector. Then click ScanSafe Web Security to open the ScanSafe Web Security Settings Page.

Note Configuration of the ScanSafe Web Security policies and settings is also possible by way of the Map view.

Related Topics

- Chapter 20, “Working with ScanSafe Web Security”
- Configuring ScanSafe Web Security, page 20-2
- ScanSafe Web Security Settings Page, page 20-6

- Add and Edit Default User Groups Dialog Box, page 20-6
- AAA Rules Page, page 15-10

Field Reference

Element	Description
Interfaces Tab	
—Filter	Details on using filters in Security Manager are found at Filtering Tables, page 1-48.
Interfaces	This tab allows you to select interfaces and Security Manager-defined interface roles on which web requests will be forwarded to the ScanSafe Web Security server for content scanning.
—Available Interfaces	Interfaces that are available to be selected for ScanSafe Web Security.
—Selected Interfaces	Interfaces selected must be facing the WAN on which hosts' requests for web services are forwarded to ScanSafe Web Security server
-	-
Whitelisting Regular Expressions Tab	
—Notify Tower	This checkbox, when selected, specifies that the ScanSafe Web Security tower must be notified regarding the allowed list. It is applicable to all ACL-based allowed list variants except IP based allowed list. The default behavior is that the notification is not sent.
—Available Regular Expressions (HTTP Host)	Lists the regular expressions available and considered for delivery to the ScanSafe Web Security server.
——Filter (HTTP Host)	Enables the administrator to filter allowed regular expressions sent to ScanSafe Web Security server by specifying include and exclude user group list. It operates on a match-all or match-any basis.
—Selected Regular Expressions (HTTP Host)	A host that matches the selected regular expressions is allowed, and is not redirected to the ScanSafe Web Security server.
—Available Regular Expressions (HTTP User Agent)	An agent that matches the available regular expressions is allowed, and is not redirected to the ScanSafe Web Security server.
—Selected Regular Expressions (HTTP User Agent)	When configured, only regular expressions that are in the Selected Regular Expressions list are sent to ScanSafe Cloud.
Whitelisting ACLs Tab	
—ACL Type	Specifies the type of ACL allowed list, either standard or extended. **Note** Standard ACLs used for allowed list are discovered as extended ACLs. A prefix of "CSM_EXT_" is added to the ACL name. Standard ACls are converted to extended ACLs as extended ACLs are complete and recommended
—Selected ACLS	When configured, only regular expressions that are in the Selected Regular Expressions list are sent to ScanSafe Cloud.

Element	Description
User Groups Tab	
—Default User	A global name that is sent to the ScanSafe Web Security server when there is no content-scan-session specific user name. Use it when you want the same content scan policy for all users in a branch office (for example).
—Default User Group	A global name that is sent to the ScanSafe Web Security server when there is no content-scan-session specific user name. Use it when you want the same content scan policy for all user groups in a branch office (for example).
—Interface Specific Default User Groups	Lists default user group for each interface.
—Include/Exclude	You can use the Include and Exclude lists to specify the particular user groups to be included or excluded.

Add and Edit Default User Groups Dialog Box

Use the Default User Groups dialog box to specify the default user group for a particular interface.

This dialog box is only useful when the ISR cannot determine user credentials, but would like to assign the users (that is, the IP addresses) to a user group so that other group-based policies in the ISR can be enforced. Only one group can be configured on an interface.

For details on these ScanSafe Web Security server configuration settings, see the ScanSafe Web Security Settings Page.

Related Topics

- ScanSafe Web Security Page, page 20-4
- ScanSafe Web Security Settings Page, page 20-6
- Chapter 20, “Working with ScanSafe Web Security”
- Configuring ScanSafe Web Security, page 20-2
- AAA Rules Page, page 15-10

Navigation Path

(Policy view) Select Firewall and open the ScanSafe Web Security Page. Then click on the User Groups tab.

ScanSafe Web Security Settings Page

Related Topics

- ScanSafe Web Security Page, page 20-4
- Chapter 20, “Working with ScanSafe Web Security”
- Configuring ScanSafe Web Security, page 20-2
- Add and Edit Default User Groups Dialog Box, page 20-6

- AAA Rules Page, page 15-10

Navigation Path

(Policy view) Select Firewall and open Settings from the Policy Type selector. Then click ScanSafe Web Security to open the ScanSafe Web Security Settings Page.

(Device view) Select Firewall and open Settings from the Policy Type selector. Then click ScanSafe Web Security to open the ScanSafe Web Security Settings Page.

Field Reference

Table 20-1 ScanSafe Web Security Settings

Element	Description	Usage
IP Address|Name (Primary ScanSafe Server)	The primary FQDN or IP address of the server configured to operate ScanSafe Web Security.	Both
HTTP Port (Primary ScanSafe Server)	Default primary port for proxied HTTP traffic (default=8080).	Both
HTTPS Port (Primary ScanSafe Server)	Default primary port for proxied HTTPS traffic (default=8080).	Both
IP Address/Name (Backup ScanSafe Server)	The secondary FQDN or IP address of the server configured to operate ScanSafe Web Security.	Both
HTTP Port (Backup ScanSafe Server)	Default secondary port for proxied HTTP traffic (default=8080).	Both
HTTPS Port (Secondary ScanSafe Server)	Default secondary port for proxied HTTPS traffic (default=8080).	Both
Server Timeout	Polling timeout when checking the availability of the ScanSafe Web Security server.	IOS Only
Session Idle Timeout	Inactivity timeout of the ScanSafe Web Security server (default=300 seconds). Used to remove the session if it is found inactive.	IOS Only
On Failure	Determines the action to be taken (Drop all Traffic or Allow All Traffic) when both primary and secondary ScanSafe Web Security servers are found inactive.	IOS Only
IP Address (Source Address)	IP address from which a packet to the ScanSafe Web Security server originates from the router.	IOS Only
Interface (Source Address)	Interface address from which a packet to the ScanSafe Web Security server originates from the router.	IOS Only
License	The license sent to the ScanSafe Web Security server (32 hexadecimal characters).	Both
Encrypted	When selected, enables the encryption. ASA does not accept encrypted license text to be configured.	IOS Only
Enable Logging Checkbox	Enables IOS syslogs (default=not enabled).	IOS Only
Public Key File	Name of the public key file	ASA Only

Table 20-1 ScanSafe Web Security Settings (continued)

Element	Description	Usage
Connection Retry Count	Number of times that the system should retry connecting.	ASA Only