Adding a Webtype Access Control List

Webtype ACLs are added to a configuration that supports filtering for clientless SSL VPN. This chapter describes how to add an ACLto the configuration that supports filtering for WebVPN.

This chapter includes the following sections:

Licensing Requirements for Webtype ACLs

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature:

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

The following guidelines and limitations apply to Webtype ACLs:

- There are two types of webtype ACLs; URL based ACLs and TCP based ACLs. URL based ACLs are used to allow or deny URLs with the format -protocol://ip-address/path, these ACLs are for filtering based on clientless features. TCP based ACLs are used to allow or deny ip-address and port.
- Permitting one type of an ACL creates an implicit deny for the other type of ACL.
- A duplicate ACE refers to ACEs with URLs that are equivalent after normalization. A duplicate ACE found during upgrade, will be removed after the upgrade.

Note URL normalization is an additional security feature that includes path normalization, case normalization and scheme normalization. URLs specified in an ACE and portal address bar are normalized before comparison; for making decisions on webvpn traffic filtering.

- If an upgrade is followed by a downgrade, duplicate ACEs will not be present in the downgraded version, if a **write memory** operation is performed after upgrade. To preserve the old configuration, you must save the running configuration to a disk, before the upgrade.
- To permit any http/https based website and all the paths within the site, www.cisco.com use the format:

```
access-list <ACL-NAME> webtype permit url http://www.cisco.com/*
```

- To permit RDP plugin protocol over clientless VPN use the format:

```
access-list <ACL-NAME> webtype permit url rdp://<host-name>/*
```

- To permit SSH plugin protocol over clientless VPN use the format:

```
access-list <ACL-NAME> webtype permit url ssh://<host-name>/*
```

- To permit telnet plugin protocol over clientless VPN use the format:

```
access-list <ACL-NAME> webtype permit url telnet://<host-name>/*
```

- To permit ica plugin protocol over clientless VPN use:

```
access-list <ACL-NAME> webtype permit url ica://<host-name>/*
```

- Smart tunnel ACEs filter on a per-server basis only, so you cannot create smart tunnel ACEs to permit or deny access to directories or to permit or deny access to specific smart tunnel-enabled applications.
- If you add descriptive remarks about your ACL with non-English characters on one platform (such as Windows) then try to remove them from another platform (such as Linux), you might not be able to edit or delete them because the original characters might not be correctly recognized. This limitation is due to an underlying platform dependency that encodes different language characters in different ways.

- Smart tunnel and ica plug-ins are not affected by an ACL with ‘permit url any’ because they match smart-tunnel:// and ica:// types.
- ‘Permit url any' will allow all the urls that have format protocol://server-ip/path and will block traffic that does not match any of the protocol://address/path such as port-forwarding; the ASA admin should explicitly set an ACE to allow connection to the required port (port 1494 in case of citrix) so that an implicit deny does not occur.

Default Settings

Table 23-1 lists the default settings for Webtype ACLs parameters.

Table 23-1 Default Webtype ACL Parameters

Parameters	Default
deny	The ASA denies all packets on the originating interface unless you specifically permit access.
log	ACL logging generates system log message 106023 for denied packets. Deny packets must be present to log denied packets.

Using Webtype ACLs

This section includes the following topics:

Task Flow for Configuring Webtype ACLs

Use the following guidelines to create and implement an ACL:

- Create an ACL by adding an ACE and applying an ACL name. See the “Using Webtype ACLs” section on page 23-3.
- Apply the ACL to an interface. See the Configuring Access Rules section in the firewall configuration guide for more information.

Adding a Webtype ACL and ACE

You must first create the webtype ACL and then add an ACE to the ACL.

Note Smart tunnel ACEs filter on a per-server basis only, so you cannot create smart tunnel ACEs to permit or deny access to directories or to permit or deny access to specific smart tunnel-enabled applications.

To configure a webtype ACL, perform the following steps:

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

Step 2 Click **Add**, and choose one of the following ACL types to add:

- **Add ACL**
- **Add IPv6 ACL**

The Add ACL dialog box appears.

Step 3 Enter a name for the ACL (with no spaces), and click **OK**.

Step 4 To add an entry to the list that you just created, click **Add**, and choose **Add ACE** from the drop-down list.

Step 5 In the Action field, click the radio button next to the desired action:

- Permit—Permits access if the conditions are matched.
- Deny—Denies access if the conditions are matched.

Note The end of every ACL has an implicit deny rule.

Step 6 In the filter field, you can either filter on a URL or filter on an address and Service.

a. To filter on a URL, choose the URL prefix from the drop-down list, and enter the URL>

Wildcard characters can be used in the URL field:

- An asterisk * matches none or any number of characters.
- A question mark ? matches any one character exactly.
- Square brackets [] are range operators, matching any character in the range. For example, to match both http://www.cisco.com:80/ and http://www.cisco.com:81/, enter the following: **http://www.cisco.com:8[01]/**

b. To filter on an address and service, click the **Filter address and service** radio button, and enter the appropriate values.

Wildcard characters can be used in the with regular expression in the address field:

- An asterisk * matches none or any number of characters.
- A question mark ? matches any one character exactly.
- Square brackets [] are range operators, matching any character in the range. For example to permit a range of IP addresses from 10.2.2.20 through 10.2.2.31, enter the following: **10.2.2.[20-31]**

You can also browse for the address and service by clicking the browse buttons at the end of the fields.

Step 7 (Optional) Logging is enabled by default. You can disable logging by unchecking the check box, or you can change the logging level from the drop-down list. The default logging level is Informational.

For more information about logging options, see the Log Options section on page 21-29.

Step 8 (Optional) If you changed the logging level from the default setting, you can specify the logging interval by clicking **More Options** to expand the list.

Valid values are from 1 through 6000 seconds. The default is 300 seconds.

Step 9 (Optional) To add a time range to your access rule that specifies when traffic can be allowed or denied, click **More Options** to expand the list.

a. To the right of the Time Range drop-down list, click the browse button.

b. The Browse Time Range dialog box appears.

c. Click **Add**.

d. The Add Time Range dialog box appears.

e. In the Time Range Name field, enter a time range name, with no spaces.

f. Enter the Start Time and the End Time.

g. To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and specify the desired values.

Step 10 Click **OK** to apply the optional time range specifications.

Step 11 Click **Apply** to save the configuration.

Note After you add ACLs, you can click the following radio buttons to filter which ACLs appear in the main pane: IPv4 andIPv6, IPv4 only, or IPv6 Only.

Editing Webtype ACLs and ACEs

To edit a webtype ACL or ACT, perform the following steps:

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

Step 2 Choose the ACL type to edit by clicking one of the following radio buttons:

- **IPv4 and IPv6**— Shows ACLs that have both IPv4 and IPv6 addresses only.
- **IPv4 Only**—Shows ACLs that have IPv4 type addresses only.
- **IPv6 Only**—Shows access rules that have IPv6 type addresses only.

The main Access Rule Pane displays the available interfaces for the chosen rule type.

Step 3 Select the ACE to edit, and make any changes to the values.

For more information about specific values, see the "Adding a Webtype ACL and ACE" section on page 23-3.

Step 4 Click **OK**.

Step 5 Click **Apply** to save the changes to your configuration.

Deleting Webtype ACLs and ACEs

To delete a webtype ACE, perform the following steps:

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

Step 2 Choose the ACL type to edit by clicking one of the following radio buttons:

- **IPv4 and IPv6**— Shows ACLs that have both IPv4 and IPv6 addresses only.
- **IPv4 Only**—Shows ACLs that have IPv4 type addresses only.
- **IPv6 Only**—Shows access rules that have IPv6 type addresses only.

The main Access Rule Pane displays the available interfaces for the chosen rule type.

Step 3 Select the ACE to delete.

If you select a specific ACE, only that ACE is deleted. If you select an ACL, that ACL and all of the ACEs under it are deleted.

Step 4 Click **Delete**.

The selected items are removed from the viewing pane.

Note If you deleted an item in error and want to restore it to your configuration, click **Reset** before you click Apply. The deleted item reappears in the viewing pane.

Step 5 Click **Apply** to save the change to the configuration.

Feature History for Webtype ACLs

Table 23-2 lists the release history for this feature.

Table 23-2 Feature History for Webtype ACLs

Feature Name	Releases	Feature Information
Webtype ACLs	7.0(1)	Webtyp ACLs are ACLs that are added to a configuration that supports filtering for clientless SSL VPN. We introduced the feature.

Table 23-2 Feature History for Webtype ACLs (continued)

Feature Name	Releases	Feature Information
Unified ACL for IPv4 and IPv6	9.0(1)	ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. We modified the following screens: Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options
Webtype ACL enhancements	9.1(5)	• A duplicate ACE found during upgrade, will be removed after the upgrade. • If an upgrade is followed by a downgrade, duplicate ACEs will not be present in the downgraded version, if a **write memory** operation is performed after upgrade. To preserve the old configuration, you must save the running configuration to a disk, before the upgrade. **Note** A duplicate ACE refers to ACEs with URLs that are equivalent after normalization. We did not modify any ASDM screens.