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 ACL to 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.

Note 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.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>/*
```

- The **access-list webtype** command is used to configure clientless SSL VPN filtering. The URL specified may be full or partial (no file specified), may include wildcards for the server, or may specify a port. See the "Adding Webtype ACLs with a URL String" section on page 22-4 for information about using wildcard characters in the URL string.
- Valid protocol identifiers are http, https, cifs, ica, imap4, pop3, and smtp. The RL may also contain the keyword **any** to refer to any URL. An asterisk may be used to refer to a subcomponent of a DNS name.
- Dynamic ACLs have been extended to support IPv6 ACLs. If you configure both an IPv4 ACL and an IPv6 ACL, they are converted to dynamic ACLs.
- If you use the Access Control Server (ACS), you must configure IPv6 ACLs using the cisco-av-pair attribute; downloadable ACLs are not supported in the ACS GUI.

- 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 22-1 lists the default settings for Webtype ACLs parameters.

Table 22-1 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 22-3.
- Apply the ACL to an interface. See the Configuring Access Rules section in the firewall configuration guide for more information.

Adding Webtype ACLs with a URL String

To add an ACL to the configuration that supports filtering for clientless SSL VPN, enter the following command:

Command	Purpose
access-list *access_list_name* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]] **Example:** `ciscoasa(config)# access-list acl_company webtype deny url http://*.cisco.example`	Adds an ACL to the configuration that supports filtering for clientless SSL VPN. The *url_string* option specifies the URL to be filtered. You can use the following wildcard characters to define more than one wildcard in the Webtype ACE: • Enter an asterisk "*" to match no characters or any number of characters. • Enter a question mark "?" to match any one character exactly. • Enter square brackets "[]" to create a range operator that matches any one character in a range. **Note** To match any HTTP URL, you must enter **http://*/*** instead of the former method of entering http://*. • The **any** keyword specifies all URLs. The **interval** option specifies the time interval at which to generate system log message 106100; valid values are from 1 to 600 seconds. The **log** [[**disable** | **default**] | *level*] option specifies that system log message 106100 is generated for the ACE. When the log optional keyword is specified, the default level for system log message 106100 is 6 (informational). See the **log** command for more information. The **time_range** *name* option specifies a keyword for attaching the time-range option to this access list entry. To remove an ACL, use the **no** form of this command with the complete syntax string as it appears in the configuration.

Adding Webtype ACLs with an IP Address

To add an ACL to the configuration that supports filtering for clientless SSL VPN, enter the following command:

Command	Purpose
access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** [*dest_address_argument*] [**eq** *port*] [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]] **Example:** `ciscoasa(config)# access-list acl_company webtype permit tcp any`	Adds an ACL to the configuration that supports filtering for WebVPN. The *dest_address_argument* specifies the IP address to which the packet is being sent: • **host** *ip_address*—Specifies an IPv4 host address. • *dest_ip_address mask*—Specifies an IPv4 network address and subnet mask. • *ipv6-address/prefix-length*—Specifies an IPv6 host or network address and prefix. • **any**, **any4**, and **any6**—**any** specifies both IPv4 and IPv6 traffic; **any4** specifies only IPv4 traffic; and **any6** specifies only IPv6 traffic. The **eq** *port* can be one of the following ports: **http**, **https**, **cifs**, **imap4**, **pop3**, and **smtp**. The **interval** option specifies the time interval at which to generate system log message 106100; valid values are from 1 to 600 seconds. The **log** [[**disable** | **default**]| *level*] option specifies that system log message 106100 is generated for the ACE. The default level is 6 (informational). The **time_range** *name* option specifies a keyword for attaching the time-range option to this access list entry. To remove an ACL, use the **no** form of this command with the complete syntax string as it appears in the configuration.

Adding Remarks to ACLs

You can include remarks about entries in any ACL, including extended, EtherType, IPv6, standard, and Webtype ACLs. The remarks make the ACL easier to understand.

To add a remark after the last **access-list** command you entered, enter the following command:

Command	Purpose
access-list *access_list_name* **remark** *text* **Example:** `ciscoasa(config)# access-list OUT remark - this is the inside admin address`	Adds a remark after the last access-list command you entered. The text can be up to 100 characters in length. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored. If you enter the remark before any **access-list** command, then the remark is the first line in the ACL. If you delete an ACL using the **no access-list** *access_list_name* command, then all the remarks are also removed.

Example

You can add a remark before each ACE, and the remarks appear in the ACL in these locations. Entering a dash (-) at the beginning of a remark helps set it apart from an ACE.

```
ciscoasa(config)# access-list OUT remark - this is the inside admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.3 any
ciscoasa(config)# access-list OUT remark - this is the hr admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

What to Do Next

Apply the ACL to an interface. See the Configuring Access Rules section in the firewall configuration guide for more information.

Monitoring Webtype ACLs

To monitor webtype ACLs, enter the following command:

Command	Purpose
show running-config access-list	Displays the access-list configuration running on the ASA.
debug webvpn url	Debug webtype ACL related issues.

Configuration Examples for Webtype ACLs

The following example shows how to deny access to a specific company URL:

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

The following example shows how to deny access to a specific file:

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

The following example shows how to deny HTTP access to any URL through port 8080:

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

The following examples show how to use wildcards in Webtype ACLs.

- The following example matches URLs such as http://www.example.com/layouts/1033:

  ```
  access-list VPN-Group webtype permit url http://www. example.com/*
  ```

- The following example matches URLs such as http://www.example.com/ and http://www.example.net/:

  ```
  access-list test webtype permit url http://www.**ample.com/
  ```

- The following example matches URLs such as http://www.cisco.com and ftp://wwz.example.com:

  ```
  access-list test webtype permit url *://ww?.c*co*/
  ```

- The following example matches URLs such as http://www.cisco.com:80 and https://www.cisco.com:81:

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

  The range operator "[]" in the preceding example specifies that either character **0** or **1** can occur.

- The following example matches URLs such as http://www.example.com and http://www.example.net:

```
access-list test webtype permit url http://www.[a-z]ample?*/
```

  The range operator "[]" in the preceding example specifies that any character in the range from **a** to **z** can occur.

- The following example matches URLs such as http://www.cisco.com/anything/crazy/url/ddtscgiz:

```
access-list test webtype permit url htt*://*/*cgi?*
```

Note To match any http URL, you must enter **http://*/*** instead of the former method of entering http://*.

The following example shows how to enforce a webtype ACL to disable access to specific CIFS shares.

In this scenario we have a root folder named "shares" that contains two sub-folders named "Marketing_Reports" and "Sales_Reports." We want to specifically deny access to the "shares/Marketing_Reports" folder.

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

However, due to the implicit "deny all," the above ACL makes all of the sub-folders inaccessible ("shares/Sales_Reports" and "shares/Marketing_Reports"), including the root folder ("shares").

To fix the problem, add a new ACL to allow access to the root folder and the remaining sub-folders:

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

Feature History for Webtype ACLs

Table 22-2 lists the release history for this feature.

Table 22-2 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 and the following command: **access-list webtype**.
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 commands: **access-list extended**, **access-list webtype**. We removed the following commands: **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**
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 commands.