Adding an EtherType Access Control List

This chapter describes how to configure EtherType ACLs and includes the following sections:

Information About EtherType ACLs

An EtherType ACL is made up of one or more Access Control Entries (ACEs) that specify an EtherType. An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number, as well as selected traffic types. See the Supported EtherTypes and Other Traffic section in the firewall configuration guide for more information.

For information about creating an access rule with the EtherType ACL, see Chapter 6, “Configuring Access Rules,” in the firewall configuration guide.

Licensing Requirements for EtherType 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

Available in single and multiple context modes.

Firewall Mode Guidelines

Supported in transparent firewall mode only.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

The following guidelines and limitations apply to EtherType ACLs:

- For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (or implicitly allowed from a high security interface to a low security interface). However, if you *explicitly* deny all traffic with an EtherType ACE, then IP and ARP traffic is denied.
- 802.3-formatted frames are not handled by the ACL because they use a length field as opposed to a type field.
- See the Supported EtherTypes and Other Traffic section in the firewall configuration guide for more information about supported traffic.

Default Settings

ACL logging generates system log message 106023 for denied packets. Deny packets must be present to log denied packets.

When you configure logging for the ACL, the default severity level for system log message 106100 is 6 (informational).

Configuring EtherType ACLs

This section includes the following topics:

Task Flow for Configuring EtherType ACLs

Use the following guidelines to create and implement an ACL:

Step 1 Create an ACL by adding an ACE and applying an ACL name, as shown in the "Adding EtherType ACLs" section on page 20-3.

Step 2 Apply the ACL to an interface. (See the Configuring Access Rules section in the firewall configuration guide for more information.)

Adding EtherType ACLs

To configure an ACL that controls traffic based upon its EtherType, perform the following steps:

Detailed Steps

Command	Purpose
`access-list` *access_list_name* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **is-is** | **any** | *hex_number*} **Example:** ciscoasa(config)# ciscoasa(config)# **access-list ETHER ethertype permit ipx**	Adds an EtherType ACE. The *access_list_name* argument lists the name or number of an ACL. When you specify an ACL name, the ACE is added to the end of the ACL. Enter the *access_list_name* in upper case letters so that the name is easy to see in the configuration. You might want to name the ACL for the interface (for example, INSIDE) or for the purpose (for example, MPLS or PIX). The **permit** keyword permits access if the conditions are matched. **deny** denies access. The **ipx** keyword specifies access to IPX. The **bpdu** keyword specifies access to bridge protocol data units, which are allowed by default. The **deny** keyword denies access if the conditions are matched. If an EtherType ACL is configured to deny all, all ethernet frames are discarded. Only physical protocol traffic, such as auto-negotiation, is still allowed. The **mpls-multicast** keyword specifies access to MPLS multicast. The **mpls-unicast** keyword specifies access to MPLS unicast. The **is-is** keyword specifies access to IS-IS traffic. The **any** keyword specifies access to any traffic. The *hex_number* argument indicates any EtherType that can be identified by a 16-bit hexadecimal number greater than or equal to 0x600. (See RFC 1700, "Assigned Numbers," at http://www.ietf.org/rfc/rfc1700.txt for a list of EtherTypes.) **Note** To remove an EtherType ACE, enter the **no access-list** command with the entire command syntax string as it appears in the configuration.

Example

The following sample ACL allows common traffic originating on the inside interface:

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

Adding Remarks to ACLs

You can include remarks about entries in any ACL, including extended, EtherType, IPv6, standard, and Webtype ACLs. The remarks make an 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 remarks are also removed.

Example

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

To monitor EtherType ACLs, enter one of the following commands:

Command	Purpose
`show access-list`	Displays the ACL entries by number.
`show running-config access-list`	Displays the current running access-list configuration.

Configuration Examples for EtherType ACLs

The following example shows how to configure EtherType ACLs:

The following ACL allows some EtherTypes through the ASA, but it denies IPX:

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
ciscoasa(config)# access-list ETHER ethertype permit 0x1234
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

The following ACL denies traffic with EtherType 0x1256, but it allows all others on both interfaces:

```
ciscoasa(config)# access-list nonIP ethertype deny 1256
ciscoasa(config)# access-list nonIP ethertype permit any
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

Feature History for EtherType ACLs

Table 20-1 lists the release history for this feature.

Table 20-1 Feature History for EtherType ACLs

Feature Name	Releases	Feature Information
EtherType ACLs	7.0(1)	EtherType ACLs control traffic based upon its EtherType. We introduced the feature and the following command: **access-list ethertype**.
EtherType ACL support for IS-IS traffic	8.4(5), 9.1(2)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**.