Chapter 32

Configuring Access Rules

This chapter describes how to control network access through the ASA using access rules and includes the following sections:

- Information About Access Rules, page 32-1
- Licensing Requirements for Access Rules, page 32-6
- Prerequisites, page 32-7
- Guidelines and Limitations, page 32-7
- Default Settings, page 32-7
- Configuring Access Rules, page 32-7
- Monitoring Access Rules, page 32-9
- Configuration Examples for Permitting or Denying Network Access, page 32-9
- Feature History for Access Rules, page 32-10

Note
You use access rules to control network access in both routed and transparent firewall modes. In transparent mode, you can use both access rules (for Layer 3 traffic) and EtherType rules (for Layer 2 traffic).

To access the ASA interface for management access, you do not also need an access rule allowing the host IP address. You only need to configure management access according to Chapter 37, “Configuring Management Access.”

Information About Access Rules

You create an access rule by applying an extended or EtherType access list to an interface or globally for all interfaces. You can use access rules in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally the source and destination ports.

For transparent mode only, an EtherType rule controls network access for non-IP traffic. An EtherType rule permits or denies traffic based on the EtherType.

This section includes the following topics:

- General Information About Rules, page 32-2
- Information About Extended Access Rules, page 32-4
General Information About Rules

This section describes information for both access rules and EtherType rules, and it includes the following topics:

- Implicit Permits, page 32-2
- Using Access Rules and EtherType Rules on the Same Interface, page 32-2
- Implicit Deny, page 32-3
- Inbound and Outbound Rules, page 32-3

Implicit Permits

For routed mode, the following types of traffic are allowed through by default:

- Unicast IPv4 traffic from a higher security interface to a lower security interface.
- Unicast IPv6 traffic from a higher security interface to a lower security interface.

For transparent mode, the following types of traffic are allowed through by default:

- Unicast IPv4 traffic from a higher security interface to a lower security interface.
- Unicast IPv6 traffic from a higher security interface to a lower security interface.
- ARPs in both directions.

Note

ARP traffic can be controlled by ARP inspection, but cannot be controlled by an access rule.

- BPDUs in both directions.

For other traffic, you need to use either an extended access rule (IPv4 and IPv6) or an EtherType rule (non-IPv4/IPv6).

Information About Interface Access Rules and Global Access Rules

You can apply an access rule to a specific interface, or you can apply an access rule globally to all interfaces. You can configure global access rules in conjunction with interface access rules, in which case, the specific interface access rules are always processed before the general global access rules.

Note

Global access rules apply only to inbound traffic. See the “Inbound and Outbound Rules” section on page 32-3.

Using Access Rules and EtherType Rules on the Same Interface

You can apply one access rule and one EtherType rule to each direction of an interface.
Implicit Deny

Access lists have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the ASA except for particular addresses, then you need to deny the particular addresses and then permit all others.

For EtherType access lists, the implicit deny at the end of the access list does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the access list does not now block any IP traffic that you previously allowed with an extended access list (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.

If you configure a global access rule, then the implicit deny comes after the global rule is processed. See the following order of operations:

1. Interface access rule.
2. Global access rule.
3. Implicit deny.

Inbound and Outbound Rules

The ASA supports two types of access rules:

- Inbound—Inbound access rules apply to traffic as it enters an interface. Global access rules are always inbound.
- Outbound—Outbound access rules apply to traffic as it exits an interface.

Note

“Inbound” and “outbound” refer to the application of an access list on an interface, either to traffic entering the ASA on an interface or traffic exiting the ASA on an interface. These terms do not refer to the movement of traffic from a lower security interface to a higher security interface, commonly known as inbound, or from a higher to lower interface, commonly known as outbound.

An outbound access list is useful, for example, if you want to allow only certain hosts on the inside networks to access a web server on the outside network. Rather than creating multiple inbound access lists to restrict access, you can create a single outbound access list that allows only the specified hosts. (See Figure 32-1.) The outbound access list prevents any other hosts from reaching the outside network.
Information About Access Rules

Figure 32-1  Outbound Access List

See the following commands for this example:

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

Information About Extended Access Rules

This section describes information about extended access rules and includes the following topics:

- Access Rules for Returning Traffic, page 32-4
- Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules, page 32-5
- Management Access Rules, page 32-5

Access Rules for Returning Traffic

For TCP and UDP connections for both routed and transparent mode, you do not need an access rule to allow returning traffic because the ASA allows all returning traffic for established, bidirectional connections.
For connectionless protocols such as ICMP, however, the ASA establishes unidirectional sessions, so you either need access rules to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections. To control ping, specify `echo-reply (0)` (ASA to host) or `echo (8)` (host to ASA).

### Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules

In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Transparent firewall mode can allow any IP traffic through.

Note: Because these special types of traffic are connectionless, you need to apply an extended access list to both interfaces, so returning traffic is allowed through.

Table 32-1 lists common traffic types that you can allow through the transparent firewall.

#### Table 32-1: Transparent Firewall Special Traffic

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Protocol or Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>UDP ports 67 and 68</td>
<td>If you enable the DHCP server, then the ASA does not pass DHCP packets.</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Protocol 88</td>
<td>—</td>
</tr>
<tr>
<td>OSPF</td>
<td>Protocol 89</td>
<td>—</td>
</tr>
<tr>
<td>Multicast streams</td>
<td>The UDP ports vary depending on the application.</td>
<td>Multicast streams are always destined to a Class D address (224.0.0.0 to 239.x.x.x).</td>
</tr>
<tr>
<td>RIP (v1 or v2)</td>
<td>UDP port 520</td>
<td>—</td>
</tr>
</tbody>
</table>

### Management Access Rules

You can configure access rules that control management traffic destined to the ASA. Access control rules for to-the-box management traffic (defined by such commands as `http`, `ssh`, or `telnet`) have higher precedence than an management access rule applied with the `control-plane` option. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box access list.

### Information About EtherType Rules

This section describes EtherType rules and includes the following topics:

- Supported EtherTypes and Other Traffic, page 32-6
- Access Rules for Returning Traffic, page 32-6
- Allowing MPLS, page 32-6
Supported EtherTypes and Other Traffic

An EtherType rule controls the following:

- EtherType identified by a 16-bit hexadecimal number, including common types IPX and MPLS unicast or multicast.
- Ethernet V2 frames.
- BPDUs, which are permitted by default. BPDUs are SNAP-encapsulated, and the ASA is designed to specifically handle BPDUs.
- Trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the ASA modifies the payload with the outgoing VLAN if you allow BPDUs.
- IS-IS (supported in Version 8.4(5) only).

The following types of traffic are not supported:

- 802.3-formatted frames—These frames are not handled by the rule because they use a length field as opposed to a type field.

Access Rules for Returning Traffic

Because EtherTypes are connectionless, you need to apply the rule to both interfaces if you want traffic to pass in both directions.

Allowing MPLS

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the ASA by configuring both MPLS routers connected to the ASA to use the IP address on the ASA interface as the router-id for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

On Cisco IOS routers, enter the appropriate command for your protocol, LDP or TDP. The interface is the interface connected to the ASA.

```
hostname(config)# mpls ldp router-id interface force
```

Or

```
hostname(config)# tag-switching tdp router-id interface force
```

Licensing Requirements for Access Rules

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>
Prerequisites

Before you can create an access rule, create the access list. See Chapter 15, “Adding an Extended Access List,” and Chapter 16, “Adding an EtherType Access List,” for more information.

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 modes.

IPv6 Guidelines
Supports IPv6.

Per-User Access List Guidelines
• If there is no per-user access list associated with a packet, the interface access rule is applied.
• The per-user access list uses the value in the timeout uauth command, but it can be overridden by the AAA per-user session timeout value.
• If traffic is denied because of a per-user access list, syslog message 109025 is logged. If traffic is permitted, no syslog message is generated. The log option in the per-user access list has no effect.

Default Settings

See the “Implicit Permits” section on page 32-2.

Configuring Access Rules

To apply an access rule, perform the following steps.
Configuring Access Rules

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`access-group access_list {{in</td>
<td>out} interface interface_name [per-user-override</td>
</tr>
<tr>
<td>hostname(config)# access-group acl_out in interface outside</td>
<td>The <code>in</code> keyword applies the access list to inbound traffic. The <code>out</code> keyword applies the access list to the outbound traffic.</td>
</tr>
<tr>
<td></td>
<td>• Specify the <code>interface</code> name.</td>
</tr>
<tr>
<td></td>
<td>• The <code>per-user-override</code> keyword (for inbound access lists only) allows dynamic user access lists that are downloaded for user authorization to override the access list assigned to the interface. For example, if the interface access list denies all traffic from 10.0.0.0, but the dynamic access list permits all traffic from 10.0.0.0, then the dynamic access list overrides the interface access list for that user. For VPN remote access traffic, the behavior depends on whether there is a <code>vpn-filter</code> applied in the group policy and whether you set the <code>per-user-override</code> option:</td>
</tr>
<tr>
<td></td>
<td>– No <code>per-user-override</code>, no <code>vpn-filter</code>—Traffic is matched against the interface ACL (per the default <code>no sysopt connection permit-vpn</code> command).</td>
</tr>
<tr>
<td></td>
<td>– No <code>per-user-override</code>, <code>vpn-filter</code>—Traffic is matched first against the interface ACL, then against the VPN filter.</td>
</tr>
<tr>
<td></td>
<td>– <code>per-user-override</code>, <code>vpn-filter</code>—Traffic is matched against the VPN filter only.</td>
</tr>
<tr>
<td></td>
<td>See the “Configuring RADIUS Authorization” section on page 38-14 for more information about per-user access lists. See also the “Per-User Access List Guidelines” section on page 32-7.</td>
</tr>
<tr>
<td></td>
<td>• The <code>control-plane</code> keyword specifies if the rule is for to-the-box traffic.</td>
</tr>
<tr>
<td></td>
<td>For a global rule, specify the <code>global</code> keyword to apply the access list to the inbound direction of all interfaces.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to use the `access-group` command:

```
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

The `access-list` command lets any host access the global address using port 80. The `access-group` command specifies that the `access-list` command applies to traffic entering the outside interface.
Monitoring Access Rules

To monitor network access, enter the following command:

```
show running-config access-group
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config access-group</td>
<td>Displays the current access list bound to the interfaces.</td>
</tr>
</tbody>
</table>

Configuration Examples for Permitting or Denying Network Access

This section includes typical configuration examples for permitting or denying network access.

The following example adds a network object for inside server 1, performs static NAT for the server, and enables access to from the outside for inside server 1.

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12
hostname(config)# access-list outside_access extended permit tcp any object inside-server1 eq www
hostname(config)# access-group outside_access in interface outside
```

The following example allows all hosts to communicate between the inside and hr networks but only specific hosts to access the outside network:

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

For example, the following sample access list allows common EtherTypes originating on the inside interface:

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

The following example allows some EtherTypes through the ASA, but it denies all others:

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

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

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

The following example uses object groups to permit specific traffic on the inside interface:
### Feature History for Access Rules

Table 32-2 lists each feature change and the platform release in which it was implemented.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface access rules</td>
<td>7.0(1)</td>
<td>Controlling network access through the ASA using access lists. We introduced the following command: <strong>access-group</strong>.</td>
</tr>
<tr>
<td>Global access rules</td>
<td>8.3(1)</td>
<td>Global access rules were introduced. We modified the following command: <strong>access-group</strong>.</td>
</tr>
<tr>
<td>Support for Identity Firewall</td>
<td>8.4(2)</td>
<td>You can now use identity firewall users and groups for the source and destination. You can use an identity firewall ACL with access rules, AAA rules, and for VPN authentication. We modified the following commands: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>EtherType ACL support for IS-IS traffic</td>
<td>8.4(5)</td>
<td>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</td>
</tr>
<tr>
<td>(transparent firewall mode)</td>
<td></td>
<td><em>Not available in Version 8.5(1), 8.6(1), 9.0(1), or 9.1(1).</em></td>
</tr>
</tbody>
</table>