Information About Access Lists

Cisco ASAs provide basic traffic filtering capabilities with access lists, which control access in your network by preventing certain traffic from entering or exiting. This chapter describes access lists and shows how to add them to your network configuration.

Access lists are made up of one or more access control entries (ACEs). An ACE is a single entry in an access list that specifies a permit or deny rule (to forward or drop the packet) and is applied to a protocol, to a source and destination IP address or network, and, optionally, to the source and destination ports.

Access lists can be configured for all routed and network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

Access lists are used in a variety of features. If your feature uses Modular Policy Framework, you can use an access list to identify traffic within a traffic class map. For more information on Modular Policy Framework, see Chapter 1, "Configuring a Service Policy Using the Modular Policy Framework."

This chapter includes the following sections:

Access List Types

The ASA uses five types of access control lists:

- Standard access lists—Identify the destination IP addresses of OSPF routes and can be used in a route map for OSPF redistribution. Standard access lists cannot be applied to interfaces to control traffic. For more information, see Chapter 1, "Adding a Standard Access Control List."
- Extended access lists—Use one or more access control entries (ACE) in which you can specify the line number to insert the ACE, the source and destination addresses, and, depending upon the ACE type, the protocol, the ports (for TCP or UDP), or the IPCMP type (for ICMP). For more information, see Chapter 1, "Adding an Extended Access Control List."
- EtherType access lists—Use one or more ACEs that specify an EtherType. For more information, see Chapter 1, "Adding an EtherType Access List."
- Webtype access lists—Used in a configuration that supports filtering for clientless SSL VPN. For more information, see Chapter 1, "Adding a Webtype Access Control List."

Table 1-1 lists the types of access lists and some common uses for them.

Table 1-1 Access List Types and Common Uses

Access List Use	Access List Type	Description
Control network access for IP traffic (routed and transparent mode)	Extended	The ASA does not allow any traffic from a lower security interface to a higher security interface unless it is explicitly permitted by an extended access list. **Note** To access the ASA interface for management access, you do not also need an access list allowing the host IP address. You only need to configure management access according to Chapter 1, "Configuring Management Access."
Identify traffic for AAA rules	Extended	AAA rules use access lists to identify traffic.
Control network access for IP traffic for a given user	Extended, downloaded from a AAA server per user	You can configure the RADIUS server to download a dynamic access list to be applied to the user, or the server can send the name of an access list that you already configured on the ASA.
Identify addresses for NAT (policy NAT and NAT exemption)	Extended	Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses in an extended access list.
Establish VPN access	Extended	You can use an extended access list in VPN commands.
Identify traffic in a traffic class map for Modular Policy Framework	Extended EtherType	Access lists can be used to identify traffic in a class map, which is used for features that support Modular Policy Framework. Features that support Modular Policy Framework include TCP and general connection settings, and inspection.
For transparent firewall mode, control network access for non-IP traffic	EtherType	You can configure an access list that controls traffic based on its EtherType.
Identify OSPF route redistribution	Standard	Standard access lists include only the destination address. You can use a standard access list to control the redistribution of OSPF routes.
Filtering for WebVPN	Webtype	You can configure a Webtype access list to filter URLs.
Control network access for IPV6 networks	IPv6	You can add and apply access lists to control traffic in IPv6 networks.

Access Control Entry Order

An access list is made up of one or more access control entries (ACEs). Each ACE that you enter for a given access list name is appended to the end of the access list. Depending on the access list type, you can specify the source and destination addresses, the protocol, the ports (for TCP or UDP), the ICMP type (for ICMP), or the EtherType.

The order of ACEs is important. When the ASA decides whether to forward or to drop a packet, the ASA tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are checked, and the packet is forwarded.

Access Control Implicit Deny

All access lists have an implicit deny statement at the end, so unless you explicitly permit traffic to pass, it will be denied. For example, if you want to allow all users to access a network through the ASA except for one or more particular addresses, then you need to deny those 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.

IP Addresses Used for Access Lists When You Use NAT

For the following features, you should always use the *real* IP address in the access list when you use NAT, even if the address as seen on an interface is the mapped address:

- **access-group** command
- Modular Policy Framework **match access-list** command
- Botnet Traffic Filter **dynamic-filter enable classify-list** command
- AAA **aaa ... match** commands
- WCCP **wccp redirect-list group-list** command

The following features use access lists, but these access lists use the *mapped* values as seen on an interface:

- IPsec access lists
- capture command access lists
- Per-user access lists
- Routing protocols
- All other features...

Where to Go Next

For information about implementing access lists, see the following chapters in this guide:

- *Chapter 1, "Adding an Extended Access Control List"*
- Chapter 1, "Adding an EtherType Access List"
- Chapter 1, "Adding a Standard Access Control List"
- Chapter 1, "Adding a Webtype Access Control List"
- Chapter 1, "Configuring Access Rules"