Information About Access Control Lists

Access control lists (ACLs) identify traffic flows by one or more characteristics, including source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the type of ACL. ACLs are used in a variety of features. ACLs are made up of one or more access control entries (ACEs). An ACE is a single entry in an ACL that specifies a permit or deny rule.

ACL Types

The ASA uses five types of ACLs:

- Standard ACLs—Identify the destination IP addresses of OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic. For more information, see Chapter 23, “Standard Access Control Lists.”
- Extended ACLs—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 21, “Extended Access Control Lists.”
- EtherType ACLs—Use one or more ACEs that specify an EtherType. For more information, see Chapter 22, “EtherType Access Control Lists.”
- Webtype ACLs—Used in a configuration that supports filtering for clientless SSL VPN. For more information, see Chapter 24, “Webtype Access Control Lists.”

Table 20-1 lists the types of ACLs and some common uses for them.

Table 20-1 ACL Types and Common Uses

ACL Use	ACL 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 ACL. **Note** To access the ASA interface for management access, you do not also need an ACL allowing the host IP address. You only need to configure management access according to Chapter 43, "Management Access."
Identify traffic for AAA rules	Extended	AAA rules use ACLs 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 ACL to be applied to the user, or the server can send the name of an ACL 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 ACL.
Establish VPN access	Extended	You can use an extended ACL in VPN commands.
Identify traffic in a traffic class map for Modular Policy Framework	Extended EtherType	ACLs 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 ACL that controls traffic based on its EtherType.
Identify route redistribution	Standard	Standard ACLs include only the destination address. You can use a standard ACL to control the redistribution of routes.
Filtering for clientless SSL VPN	Webtype	You can configure a Webtype ACL to filter URLs.

Access Control Entry Order

An ACL is made up of one or more access control entries (ACEs). Each ACE that you enter for a given ACL name is appended to the end of the ACL. Depending on the ACL 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 ACL that explicitly permits all traffic, no further statements are checked, and the packet is forwarded.

Access Control Implicit Deny

All ACLs 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 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.

IP Addresses Used for ACLs When You Use NAT

For the following features, you should always use the *real* IP address in the ACL 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 ACLs, but these ACLs use the *mapped* values as seen on an interface:

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

Where to Go Next

For information about implementing ACLs, see the following chapters:

- Chapter 21, “Extended Access Control Lists”
- Chapter 22, “EtherType Access Control Lists”
- Chapter 23, “Standard Access Control Lists”
- Chapter 24, “Webtype Access Control Lists”