CHAPTER 10

Information About Access Lists

Cisco ASA 5500 Series Adaptive Security Appliances 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 9, "Using Modular Policy Framework."

This chapter includes the following sections:

Access List Types

The adaptive security appliance 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 13, "Adding a Standard Access 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 11, "Adding an Extended Access List."
- EtherType access lists—Use one or more ACEs that specify an EtherType. For more information, see Chapter 12, "Adding an EtherType Access List."
- Webtype access lists—Used in a configuration that supports filtering for clientless SSL VPN. For more information, see Chapter 14, "Adding a Webtype Access List."

- IPv6 access lists—Determine which IPv6 traffic to block and which traffic to forward at router interfaces. For more information, see Chapter 15, "Adding an IPv6 Access List."

Table 10-1 lists the types of access lists and some common uses for them.

Table 10-1 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 37, "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 Entry (ACE). 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

Each access list has 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.

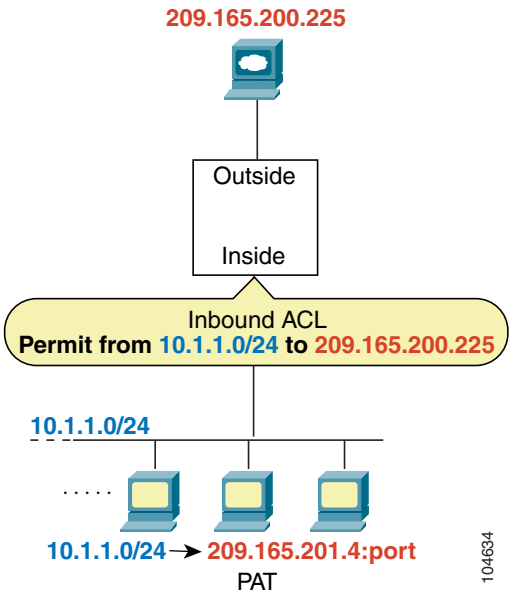
For EtherType access lists, the implicit deny at the end of the access list does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the access list does not now block any IP traffic that you previously allowed with an extended access list (or implicitly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

When you use NAT, the IP addresses that you specify for an access list depend on the interface to which the access list is attached; you need to use addresses that are valid on the network connected to the interface. This guideline applies for both inbound and outbound access lists: the direction does not determine the address used, only the interface does.

For example, if you want to apply an access list to the inbound direction of the inside interface, you configure the ASA to perform NAT on the inside source addresses when they access outside addresses. Because the access list is applied to the inside interface, the source addresses are the original untranslated addresses. Because the outside addresses are not translated, the destination address used in the access list is the real address. (See Figure 10-1.)

Figure 10-1 IP Addresses in Access Lists: NAT Used for Source Addresses

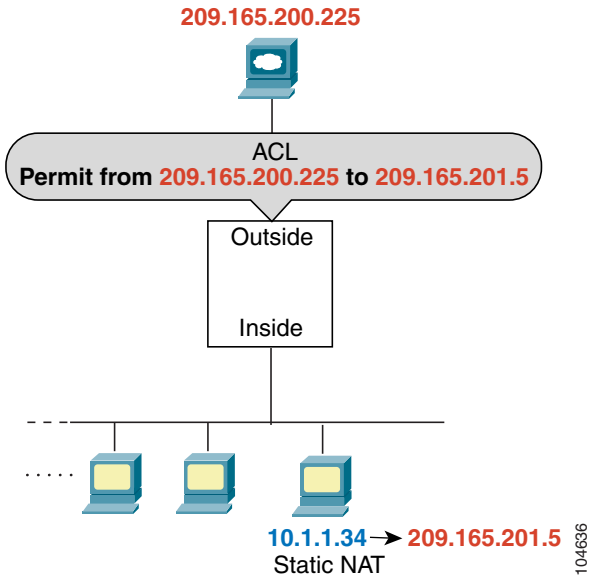


See the following commands for this example:

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
209.165.200.225
hostname(config)# access-group INSIDE in interface inside
```

If you want to allow an outside host to access an inside host, you can apply an inbound access list on the outside interface. You need to specify the translated address of the inside host in the access list because that address is the address that can be used on the outside network. (See Figure 10-2.)

Figure 10-2 IP Addresses in Access Lists: NAT Used for Destination Addresses

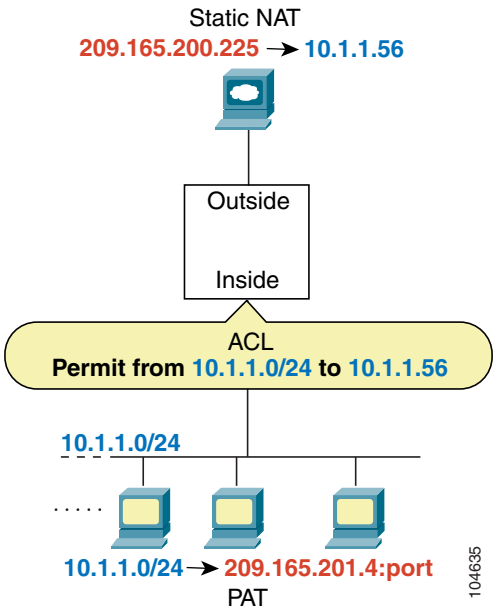


See the following commands for this example:

```
hostname(config)# access-list OUTSIDE extended permit ip host 209.165.200.225 host
209.165.201.5
hostname(config)# access-group OUTSIDE in interface outside
```

If you perform NAT on both interfaces, keep in mind the addresses that are visible to a given interface. Figure 10-3 shows an outside server that uses static NAT so that a translated address appears on the inside network.

Figure 10-3 IP Addresses in Access Lists: NAT used for Source and Destination Addresses



See the following commands for this example:

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
10.1.1.56
hostname(config)# access-group INSIDE in interface inside
```

Where to Go Next

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

- Chapter 11, “Adding an Extended Access List”
- Chapter 12, “Adding an EtherType Access List”
- Chapter 13, “Adding a Standard Access List”
- Chapter 14, “Adding a Webtype Access List”
- Chapter 15, “Adding an IPv6 Access List”