CHAPTER 35

Permitting or Denying Network Access

This chapter describes how to control network access through the security appliance by applying an access list to an interface, and it includes the following sections:

Information About Inbound and Outbound Access Rules

Because all traffic from a higher-security interface to a lower-security interface is allowed, access lists enable you to either allow traffic from lower-security interfaces or restrict traffic from higher-security interfaces.

The ASA supports two types of access lists:

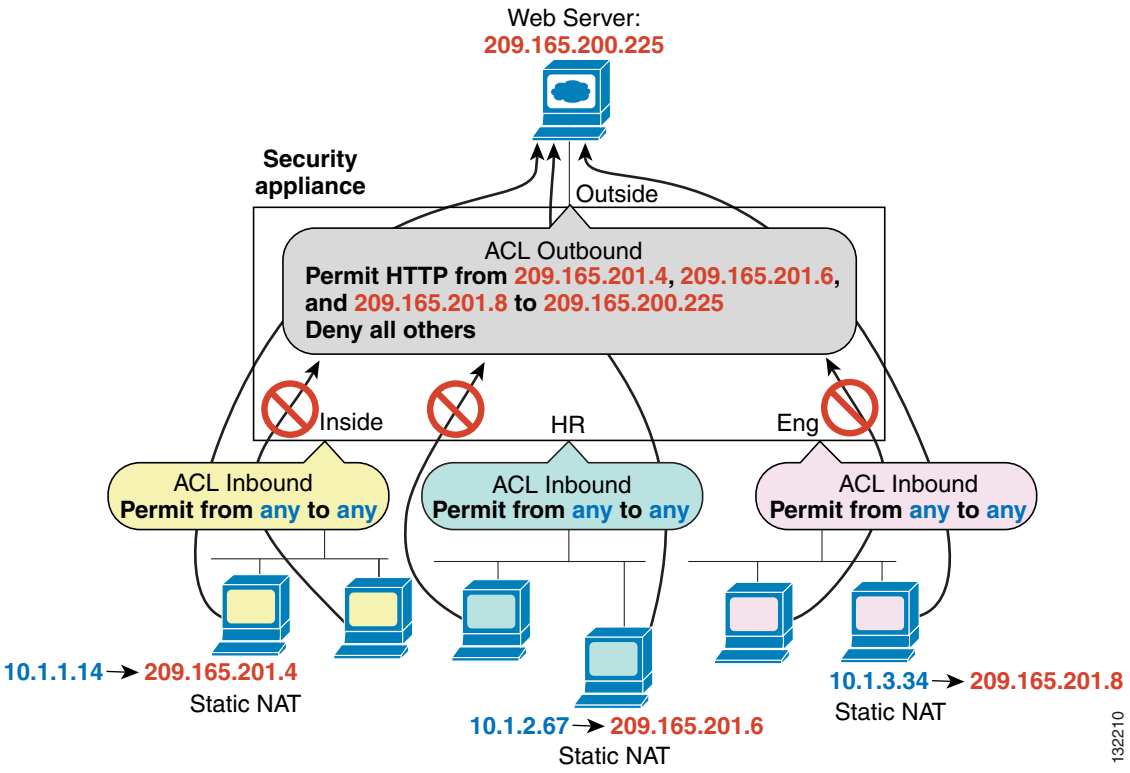
- Inbound—Inbound access lists apply to traffic as it enters an interface.
- Outbound—Outbound access lists apply to traffic as it exits an interface.

Note The terms “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 35-1.) See the "IP Addresses Used for Access Lists When You Use NAT" section on page 10-3 for information about NAT and IP addresses. The outbound access list prevents any other hosts from reaching the outside network.

Figure 35-1 Outbound Access List



See the following commands for this example:

```
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.4
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.6
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.8
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

Licensing Requirements for Access Rules

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Prerequisites

Permitting and denying network access has the following prerequisites:

Before you can apply an access list to an you need to have created the access list with access list entries. See Chapter 11, "Adding an Extended 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

Additional Guidelines and Limitations

The following guidelines and limitations apply to permitting or denying network access:

- By default, all IP traffic from a higher-security interface to a lower-security interface is allowed. Access lists enable you to either allow traffic from lower-security interfaces or restrict traffic from higher-security interfaces.
- You use access lists to control network access in both routed and transparent firewall modes. In transparent mode, you can use both extended access lists (for Layer 3 traffic) and EtherType access lists (for Layer 2 traffic). For information about creating extended access lists, see Chapter 11, "Adding an Extended Access List," For information about creating EtherType access lists, see Chapter 12, "Adding an EtherType Access List."
- To access the ASA interface for management access, you do not need an access list allowing the host IP address. You only need to configure management access by following the instructions in Chapter 37, "Configuring Management Access."
- For connectionless protocols, you need to apply the access list to the source and destination interfaces if you want traffic to pass in both directions. For example, you can allow BGP in an EtherType access list in transparent mode, and you need to apply the access list to both interfaces.
- At the time a packet arrives, if there is no per-user access list associated with the packet, the interface access list will be applied.
- The per-user access list is governed by the timeout value specified by the **uauth** option of the **timeout** command, but it can be overridden by the AAA per-user session timeout value.
- If user traffic is denied because of a per-user access list, syslog message 109025 will be logged. If user traffic is permitted, no syslog message is generated. The log option in the per-user access-list will have no effect.
- Always use the **access-list** command with the **access-group** command.

- If all of the functional entries (the permit and deny statements) are removed from an access list that is referenced by one or more **access-group** commands, the **access-group** commands are automatically removed from the configuration. The **access-group** command cannot reference empty access lists or access lists that contain only a remark.
- The **no access-group** command unbinds the access list from the interface *interface_name*.
- The show running config access-group command displays the current access list bound to the interfaces.
- The **clear configure access-group** command removes all the access lists from the interfaces.
- Access control rules for to-the-box management traffic (defined by such commands as **http**, **ssh**, or **telnet**) have higher precedence than an access list 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.

Default Settings

Table 35-1 lists the default settings for Permitting or Denying Network Access parameters.

Table 35-1 Default Parameters for Permitting or Denying Network Access

Parameters	Default
—	No default behavior or values.

Applying an Access List to an Interface

You can apply an extended access list to the inbound or outbound direction of an interface. You can apply one access list of each type (extended and EtherType) to both directions of the interface. You can also apply an IPv4 and an IPv6 access list to an interface at the same time and in the same direction. See the "Information About Inbound and Outbound Access Rules" section on page 35-1 for more information about access list directions.

To apply an access list to the inbound or outbound direction of an interface, enter the following command.

Command	Purpose
access-group *access_list* {**in** | **out**} **interface** *interface_name* [**per-user-override**] **Example:** hostname(config)# access-group acl_out in interface outside	Binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in the **access-list** command statement, the security appliance continues to process the packet. If you enter the deny option in the **access-list** command statement, the security appliance discards the packet and generates a syslog message. The **in** keyword applies the access list to the traffic on the specified interface. The **out** keyword applies the access list to the outbound traffic. The **per-user-override** keyword 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 **vpn-filter** applied in the group policy and whether you set the **per-user-override** option: • No **per-user-override**, no **vpn-filter**—Traffic is matched against the interface ACL (per the default **no sysopt connection permit-vpn** command). • No **per-user-override**, **vpn-filter**—Traffic is matched first against the interface ACL, then against the VPN filter. • **per-user-override**, **vpn-filter**—Traffic is matched against the VPN filter only. See the "Configuring RADIUS Authorization" section on page 38-9 for more information about per-user access lists. **Note** The optional **per-user-override** keyword is only available for inbound access lists. If the **per-user-override** optional argument is not present, the security appliance preserves the existing filtering behavior. (For additional information about command options, see the **access-group** command in the *Cisco Security Appliance Command Reference*.)

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

```
hostname(config)# static (inside,outside) 209.165.201.3 10.1.1.3
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 **static** command provides a global address of 209.165.201.3 for the web server at 10.1.1.3. 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 Permitting or Denying Network Access

To monitor network access, perform one of the following tasks:

Command	Purpose
show running-config access-group	Displays the current access list bound to the interfaces.

Configuration Examples for Permitting or Denying Network Access

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

The following example illustrates the commands required to enable access to an inside web server with the IP address 209.165.201.12. (This IP address is the address visible on the outside interface after NAT.)

```
hostname(config)# access-list OUTSIDE-ACL extended permit tcp any host 209.165.201.12 eq
www
hostname(config)# access-group OUTSIDE-ACL in interface outside
```

You also need to configure NAT for the web server.

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
hostname(config)# access-group ETHER in interface outside
```

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:

```
!
hostname (config)# object-group service myaclog
```

```
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

Feature History for Permitting or Denying Network Access

Table 35-2 lists the release history for this feature.

Table 35-2 Feature History for Permitting or Denying Network Access

Feature Name	Releases	Feature Information
Permitting or denying network access	7.0	Controlling network access through the security appliance using access lists. The following command was introduced or modified: **access-group**.