Fundamentals of Cisco ASA Security Appliance Access-Control Lists

By Don R. Crawley, CCNA Security, Linux+

This document is from the book "The Accidental Administrator: Cisco ASA Security Appliance", available on Amazon.com and based on Cisco ASA Training: 2-Day Hands-On Workshop. A companion video is available: www.youtube.com/soundtraining.

Understanding Access Control Lists

Access Control Lists (ACLs) are lists of permit and deny conditions applied to traffic flows and based on various criteria including protocol type source IP address, destination IP address, source port number, and/or destination port number.

ACLs can be used to filter traffic for various purposes including security, monitoring, route selection, and network address translation. ACLs are comprised of one or more Access Control Entries (ACEs). Each ACE is an individual line within an ACL.

Rules for Access-Control Lists

- Packets are evaluated against entries in an ACL in sequential order.
- Once a packet matches an entry, no further evaluation is done.
- There is an implicit "deny any" at the end of every ACL, so any packet not explicitly permitted is implicitly denied. In other words, if a packet does not match any entry in an ACL, that packet is dropped.

soundthinking point: Order of entries in an ACL is important

When building ACLs, put entries in order from most specific to most general.

Types of Access-Control Lists

There are fundamentally two types of access-control lists: standard ACLs and extended ACLs. Standard ACLs filter based only on the source IP address of a packet. Extended ACLs filter based on the source and/or destination IP address, protocol type such as IP, TCP, UDP, ICMP, and others, and source and/or destination TCP/UDP port numbers.

ACL Syntax

ACLs on a Cisco ASA Security Appliance are similar to those on a Cisco router, but not identical. Firewalls use real subnet masks instead of the inverted mask used on a router. ACLs on a firewall are named instead of numbered and assumed to be an extended list.

The syntax of an ACE is relatively straight-forward, as you can see on the following page:

ciscoasa(config)#**access-list***name* [**line***number*] [extended] {**permit** | **deny**} *protocolsource_IP_address source_netmask [operator source_port] destination_IP_address destination_netmask [operator destination_port]* [**log** [[**disable** | **default**] | [*level*]] [**interval***seconds*]] [**time-range***name*] [**inactive**]


```
asa03(config)# access-list demo1 permit tcp 10.1.0.0 255.255.255.0 any eq www
asa03(config)# access-list demo1 permit tcp 10.1.0.0 255.255.255.0 any eq 443
asa03(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list demo1; 2 elements
access-list demo1 line 1 extended permit tcp 10.1.0.0 255.255.255.0 any eq www (hitcnt=0)
0x3f8412a5
access-list demo1 line 2 extended permit tcp 10.1.0.0 255.255.255.0 any eq https (hitcnt=0
) 0xf420b1e8
asa03(config)#
```

Creating an access control list (ACL)

In the above example, an ACL called “demo1” is created in which the first ACE permits TCP traffic originating on the 10.1.0.0 subnet to go to any destination IP address with the destination port of 80 (www). In the second ACE, the same traffic flow is permitted for destination port 443. Notice in the output of the *show access-list*that line numbers are displayed and the *extended* parameter is also included, even though neither was included in the configuration statements.

You can deactivate an ACE without deleting it by appending the *inactive* option to the end of the line.

As with Cisco routers, there is an implicit “deny any” at the end of every ACL. Any traffic that is not explicitly permitted is implicitly denied.

Editing ACLs and ACEs

New ACEs are appended to the end of the ACL. If you want, however, to insert the new ACE at a particular location within the ACL, you can add the line number parameter to the ACE:

```
asa03(config)# show access-list demo1
access-list demo1; 2 elements
access-list demo1 line 1 extended permit tcp 10.1.0.0 255.255.255.0 any eq www
access-list demo1 line 2 extended permit tcp 10.1.0.0 255.255.255.0 any eq https
asa03(config)# access-list demo1 line 2 deny tcp host 10.1.0.2 any eq https
asa03(config)# show access-list demo1
access-list demo1; 3 elements
access-list demo1 line 1 extended permit tcp 10.1.0.0 255.255.255.0 any eq www
access-list demo1 line 2 extended deny tcp host 10.1.0.2 any eq https
access-list demo1 line 3 extended permit tcp 10.1.0.0 255.255.255.0 any eq https
asa03(config)#
```

Editing an access control list

Notice in the fifth line of the example above that an ACE is added at line two in the ACL. Notice in the output from the *show access-list demo1* command that the new entry is added in the second position in the ACL and the former second entry becomes line number three.

You can remove an ACE from an ACL by preceding the ACE configuration statement with the modifier *no*, as in the following example:

```
asa03(config)#
asa03(config)# no access-list demo1 deny tcp host 10.1.0.2 any eq https
asa03(config)#
```


Removing an entry from an ACL

Time ranges can be used with ACEs to enable the ACE during specific time parameters. Configuring time ranges is a two-part process. Part one is naming and creating the time range. Part two is configuring the ACE with the time range.

Time-ranges permit the use of both periodic ranges, such as every week day, or absolute ranges, such as February 1 through February 14.

Use the following syntax for naming and creating the time-range:

Periodic

```
ciscoasa(config)#time-range name
ciscoasa(config-time-range)#periodic days-of-the-week time
to time
```

Absolute

```
ciscoasa(config)#time-range name
ciscoasa(config-time-range)#absolute start time date [end
time date]
```

The time is expressed in 24:00 time and the date is expressed in day, month, year.

```
(config)# time-range workweek
(config-time-range)# periodic weekdays 08:00 to 17:00
(config-time-range)# access-list www_restrict deny tcp any any eq www time-range workweek
(config)#
```

Configuring a time-range

ACLs can be renamed with the following simple command:

```
(config)# access-list www_restrict rename web_restrict
```

Renaming an access-list

In the above example, the ACL *www_restrict* is renamed to *web_restrict*.

Object Groups

Object Groups simplify ACL management by grouping similar components together for inclusion in an ACE. There are five types of object groups available on the ASA:

- Network object group: One or more IP addresses
- Protocol object group: One or more IP protocols

- ICMP object group: One or more ICMP types
- Basic service object group: One or more TCP or UDP port numbers
- Enhanced service object group: Mix of protocols, ICMP types, UDP/TCP ports

In the following example, a network object group is created with the name *Accounting*. Note the use of the description command to document the object group's purpose. This particular object group identifies a single host at 10.1.0.1 and the subnet 10.2.0.0/24.

```
asa03(config)# object-group network Accounting
asa03(config-network)# description Accounting and Finance
asa03(config-network)# network-object host 10.1.0.1
asa03(config-network)# network-object 10.2.0.0 255.255.255.0
asa03(config-network)# exit
asa03(config)#
```

Configuring an object group

The object group can be applied to an ACE as follows:

```
asa03(config)# access-list demo2 permit tcp object-group Accounting any eq www
asa03(config)# access-list demo2 permit tcp object-group Accounting any eq 443
```

Using an object group in an access-list

Notice how the ACL demo2 permits hosts identified in the object-group *Accounting* to access port 80 and 443 on any host.

Using Access-Control Lists

In order for an ACL to have any effect, it must be applied to an interface or a function. In the following example, the ACL is designed to permit inside hosts to ping hosts on an outside network such as the public Internet.

The first four lines in the example identify and permit the traffic flows. The last line applies the list to inbound traffic on the outside interface. Note the use of the "access-group 101" statement which applies access-list 101 to the interface.

```
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any source-quench
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-group 101 in interface outside
```

This document is from the book "The Accidental Administrator: Cisco ASA Security Appliance", available on Amazon.com and based on Cisco ASA Training: Two-Day Hands-On Workshop. A companion video is at www.youtube.com/soundtraining.