- PIX/ASA Access Control Lists -

Basics of Access Control Lists (ACLs)

Access control lists (ACLs) can be used for two purposes on Cisco devices:

- To **filter** traffic
- To **identify** traffic

Access lists are a set of rules, organized in a rule table. Each rule or line in an access-list provides a condition, either **permit** or **deny**:

- When using an access-list to filter traffic, a *permit* statement is used to "allow" traffic, while a *deny* statement is used to "block" traffic.
- Similarly, when using an access list to identify traffic, a *permit* statement is used to "include" traffic, while a *deny* statement states that the traffic should "not" be included. It is thus interpreted as a **true/false** statement.

Filtering traffic is the primary use of access lists. However, there are several instances when it is necessary to identify traffic using ACLs, including:

- Identifying interesting traffic to bring up an ISDN link or VPN tunnel
- Identifying routes to filter or allow in routing updates
- Identifying traffic for QoS purposes

When filtering traffic, access lists are applied on interfaces. As a packet passes through a device, the top line of the rule list is checked first, and the device continues to go down the list until a match is made. Once a match is made, the packet is either permitted or denied.

There is an implicit 'deny all' at the end of all access lists. You don't create it, and you can't delete it. Thus, access lists that contain **only deny statements** will **prevent all traffic**.

* * *

ACLs on a PIX/ASA Firewall

Recall that Cisco security appliances protect **trusted** zones from **untrusted** zones.

Like most firewalls, a Cisco PIX/ASA will **permit** traffic from the *trusted* interface to the *untrusted* interface, **without** any explicit configuration. However, traffic from the *untrusted* interface to the *trusted* interface must be **explicitly permitted.**

Thus, any traffic that is not explicitly permitted from the untrusted to trusted interface will be **implicitly denied.**

To control the *trust* value of each interface, each firewall interface is assigned a **security level**, which is represented as a **numerical value** between **0 – 100** on the Cisco PIX/ASA. A **higher** security level is *more trusted*, whereas a **lower** security level is *less trusted***.**

To explicitly allow a *less trusted* interface to communicate with a *more trusted* interface, an **access control list (ACL)** *must* be used.

ACL Syntax on a Cisco PIX/ASA Firewall

To configure an ACL on a Cisco PIX/ASA device:

pixfirewall(config)# *access-list MYLIST permit ip any 150.80.0.0 255.255.0.0*

The above command creates an *access-list* named *MYLIST*, which *permit*s IP traffic from *any* source to the *158.80.0.0/16* network.

The syntax is nearly identical to a Cisco IOS ACL - with two critical differences:

- *Names* are used instead of *numbers* to identify access-lists.
- *Subnet Masks* are used instead of *wildcard masks*.

A common practice is to **capitalize the name** of access control lists (and other user-defined names), for simplified reference in configuration files.

* * *

ACL Syntax on a Cisco PIX/ASA Firewall (continued)

Removing an entire ACL is simple:

pixfirewall(config)# *no access-list MYLIST*

To remove a *specific* line from an ACL:

pixfirewall(config)# *no access-list MYLIST permit ip any 150.80.0.0 255.255.0.0*

Additionally, as of PIX OS 6.3, individual lines can now be inserted, edited, or deleted in an ACL by including **line numbers:**

pixfirewall(config)# *no access-list MYLIST line 4 permit ip any host 10.1.1.1*
pixfirewall(config)# *no access-list MYLIST line 5 permit ip any host 10.1.1.2*

To apply a configured ACL to an interface:

pixfirewall(config)# *access-group MYLIST in interface outside*

The above command applies the ACL named *MYLIST* to all *in*coming traffic on the *interface* named *outside.*

To remove a configured ACL from an interface:

pixfirewall(config)# *no access-group MYLIST in interface outside*

Note: When an access-list is completely deleted, the associated *access-group* statement is removed as well.

To view all configured ACLs:

pixfirewall(config)# *show access-list*

Enabling ICMP on PIX/ASA Interfaces

To configure a specific PIX/ASA interface to respond to ping requests:

pixfirewall(config)# *icmp permit any outside*

To allow a specific ICMP type:

pixfirewall(config)# *icmp permit any echo outside*

ICMP is **disabled** on all interfaces in current versions of the PIX OS.

(Reference: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094e8a.shtml)

* * *