Cisco Systems
Networking Academy

Cisco.com

Network Security 1

Module 9 – Configure Filtering on a PIX Security Appliance

CCNA CISCO CERTIFIED

Högskolan Halmstad

Cisco Systems Networking Academy

Cisco.com

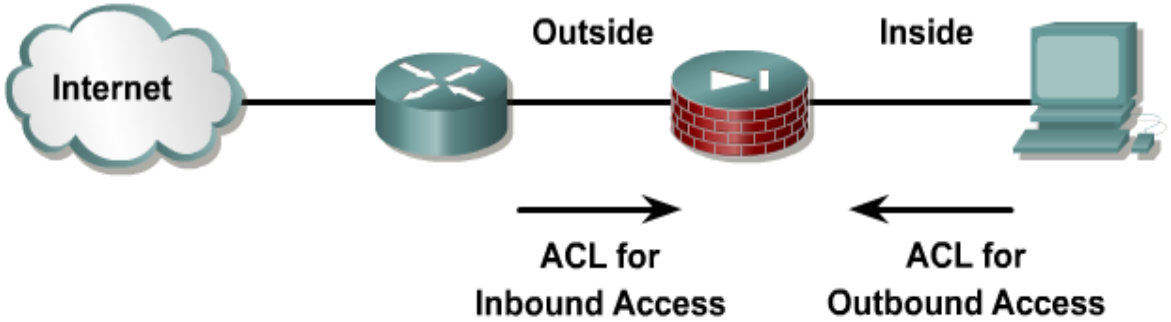
Module 9 – Configure Filtering on a PIX Security Appliance

9.1 Configure ACLs and Content Filters

CCNA CISCO CERTIFIED

Högskolan Halmstad

PIX Security Appliance ACLs



No ACL

- Outbound permitted by default
- Inbound denied by default

Firewall appliance access-control policy is interface dependant.

- Interface ACL permits or denies the initial packet incoming on that interface.
- ACL needs to describe only the initial packet of the application; no need to think about return traffic.
- If no ACL is attached to an interface, the following ASA policy applies:
  - Outbound packet is permitted by default.
  - Inbound packet is denied by default.

access-list command

Cisco.com

Mode	Command	Description
pixfirewall (config)#	**access-list** ***acl_ID*** **deny | permit** ***protocol source_addr source_mask*** [***operator port***[port]] ***destination_addr destination_mask operator port*** [port]	The access-list command is used to create an ACL

```
pixfirewall(config)# access-list DMZ1 deny tcp
192.168.1.0 255.255.255.0 host 192.168.0.1 lt 1025
```

- Denies access from the 192.168.1.0 network to TCP ports less than 1025 on host 192.168.0.1.

access-group command

Mode	Command	Description
pixfirewall (config)#	**access-group *acl_ID* in interface *interface_name***	Binds an ACL to an interface

```
pixfirewall(config)# access-group DMZ1 in
interface dmz
```

- Binds ACL DMZ1 to interface dmz

nat 0 access-list command

Mode	Command	Description
pixfirewall (config)#	**nat [(*if_name*)] 0 access-list *acl_name* [outside]**	Exempt traffic that is matched by an **access-list** command statement from NAT

```
pixfirewall(config)# access-list NONAT permit ip host
10.0.0.11 host 10.2.1.3
pixfirewall(config)# nat (inside) 0 access-list NONAT
```

ACL Line Numbers

Cisco.com

```
pixfirewall(config)# show access-list
access-list aclout line 2 extended permittcp any host 192.168.0.7 eq
   www (hitcnt=0)
access-list aclout line 3 extended permittcp any host 192.168.0.8 eq
   www (hitcnt=0)
access-list aclout line 4 extended permittcp any host 192.168.0.10 eq
   www (hitcnt=0)
access-list aclout line 5 extended permittcp any host 192.168.0.11 eq
   www (hitcnt=0)
```

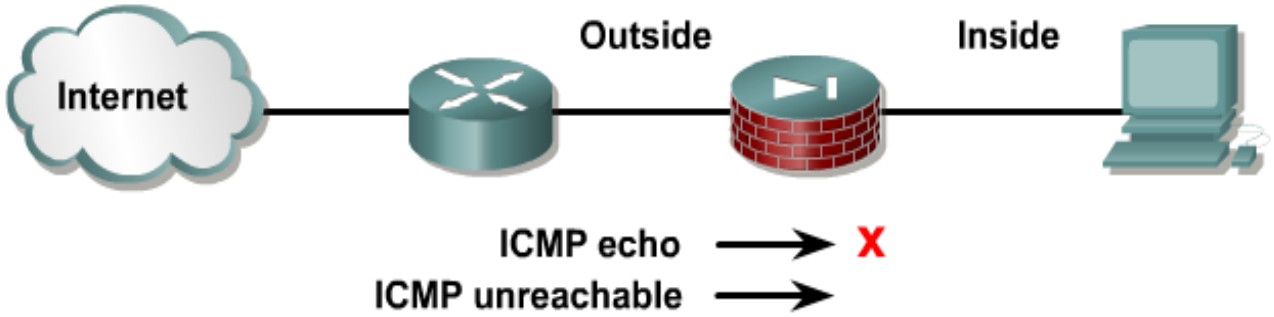
Insert

```
access-list id [line line-number] [extended] {deny | permit} {object-
group network_obj_grp_id | tcp | udp} source_address mask [operator
port] dest_address mask [operator port]
```

- Insert ACE into existing ACL

```
pixfirewall(config)# access-list aclout line 4 permit tcp any host
192.168.0.9 eq www
```

icmp command



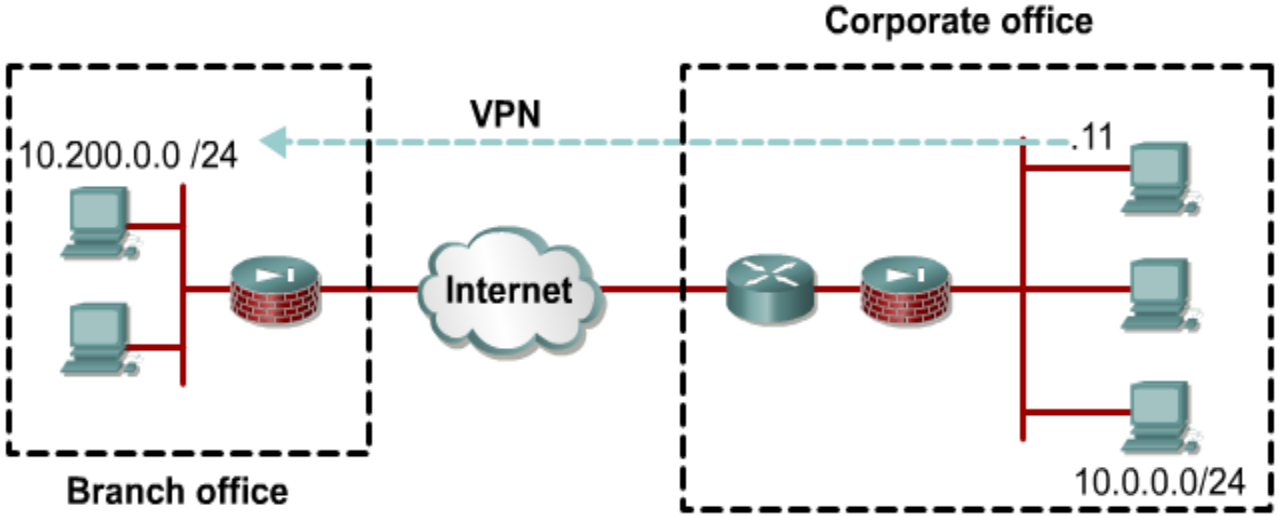
pixfirewall(config)#

```
icmp {permit | deny} src_addr src_mask [icmp-type] if_name
```

- Enables or disables pinging to an interface
- All ping requests denied at the outside interface, and all unreachable messages permitted at the outside interface

```
pixfirewall(config)# icmp deny any echo outside
pixfirewall(config)# icmp permit any unreachable outside
```

NAT 0 ACLs

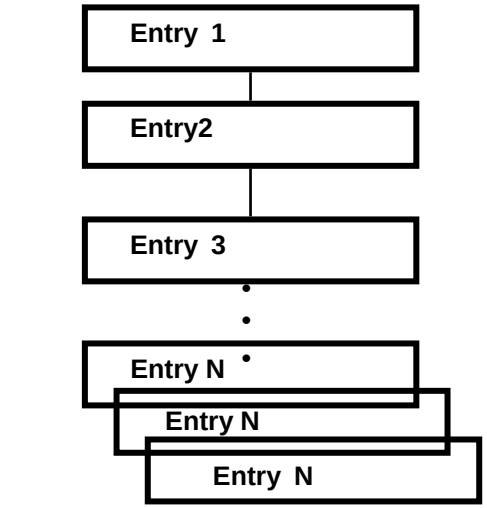


The NAT 0 access control list statement turns on identity NAT only for connections that match a permit statement of a specified access control list, such as branch office to corporate office.

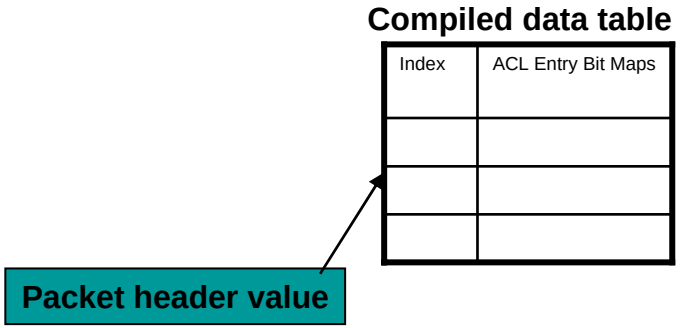
Turbo ACLs

Cisco.com

Regular ACL processing



Turbo ACL processing



- ACLs organized internally as linked lists.
- Linear search to find matching entry to deny or permit packet.
- Increased search time when ACL A contains large number of entries, which leads to performance degradation.

- **ACLs compiled into sets of lookup data tables.**
- **Improved search time for large ACLs.**
- **Required minimum of 2.1 MB of memory.**

Turbo ACL

Cisco.com

pixfirewall(config)#

```
access-list compiled
```

- **Enables the Turbo ACL feature on all ACLs.**
- **Turbo compiles all ACLs with 19 or more entries.**

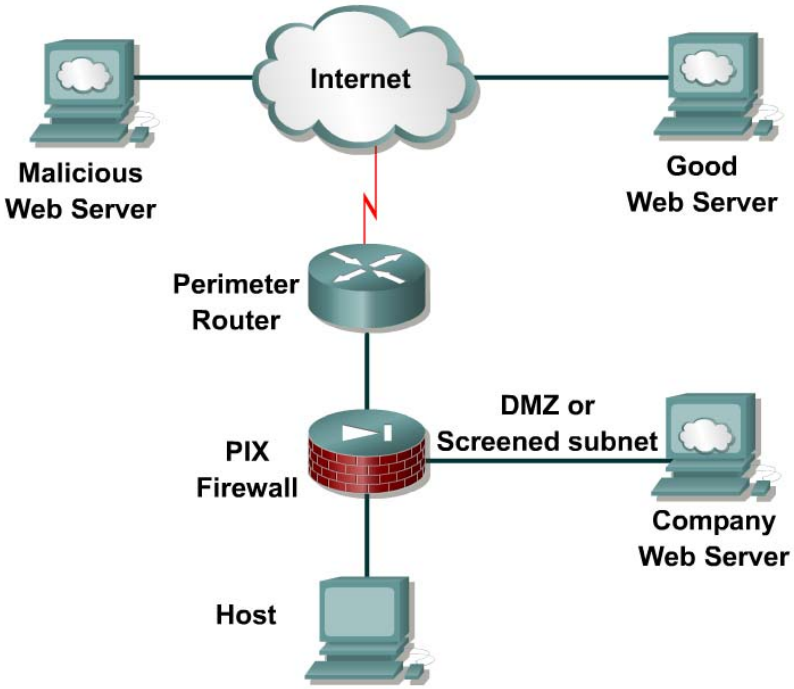
pixfirewall(config)#

```
access-list acl_ID compiled
```

- **Enables the Turbo ACL feature for a specific ACL.**

Java Applet Filtering

- Java applet filtering enables an administrator to prevent the downloading of Java applets by an inside system.
- Java programs can provide a vehicle through which an inside system can be invaded.
- Java applets are executable programs that are banned within some security policies.



ActiveX Blocking

- ActiveX controls are applets that can be inserted in web pages or other applications.
- ActiveX controls can provide a way for someone to attack servers.
- The PIX Security Appliance can be used to block ActiveX controls.

filter activex | *java* Command

pixfirewall(config)#

```
filter activex | java port [-port]
  local_ip mask foreign_ip mask
```

- Filters out ActiveX usage from outbound packets.
- Filters out Java applets that return to the PIX Security Appliance from an outbound connection.

Designate the URL-Filtering Server

pixfirewall(config)#

```
url-server [(if_name)] [vendor websense] host
  local_ip [timeout seconds] [protocol TCP | UDP
  version [1 | 4]]
```

– Designates a server that runs a Websense URL-filtering application.

pixfirewall(config)#

```
url-server [(if_name)] vendor n2h2 host local_ip
  [port number][timeout seconds][protocol TCP |
  UDP]
```

- **Designates a server that runs an N2H2 URL-filtering application.**

```
pixfirewall(config)# url-server (dmz) host
  172.16.0.3 protocol TCP version 4
```

– The URL-filtering host is on the DMZ interface at IP address 172.16.0.3. The PIX Security Appliance performs a username lookup and then the URL-filtering server handles URL filtering and username logging.

Configure the PIX Security Appliance to Work with a URL-Filtering Server

Cisco.com

pixfirewall(config)#

```
filter url port[-port] | except local_ip local_mask
  foreign_ip foreign_mask [allow] [proxy-block]
  [longurl-truncate | longurl-deny][cgi-truncate]
```

- Prevents outbound users from accessing URLs that are designated with the URL-filtering application.

```
pixfirewall(config)# filter url http 0 0 0 0 allow
```

- **Tells the PIX Security Appliance how to filter requests.**