CISCO SYSTEMS

IPv6 Filtering

ISP/IXP Workshops

IPv6 Standard Access Control Lists

- **IPv6 access-lists (ACL) are used to filter traffic and restrict access to the router**

- **IPv6 prefix-lists are used to filter routing protocol updates.**

- **IPv6 Standard ACL (Permit/Deny)**

  IPv6 source/destination addresses

  IPv6 prefix-lists

  On Inbound and Outbound interfaces

IPv6 Extended ACL

- **Adds support for IPv6 option header and upper layer filtering**

- **Only named access-lists are supported for IPv6**

- **IPv6 and IPv4 ACL functionality**

    Implicit deny any any as final rule in each ACL.

    A reference to an empty ACL will permit any any.

    ACLs are NEVER applied to self-originated traffic.

IPv6 Extended ACL overview

- **CLI mirrors IPv4 extended ACL CLI**
- **Implicit permit rules, enable neighbor discovery**
- **ULP, DSCP, flow-label,… matches**
- **Logging**
- **Time-based**
- **Reflexive**
- **CEFv6 and dCEFv6 ACL feature support**

IPv6 ACL Implicit Rules

- ## Implicit permit rules, enable neighbor discovery

  The following implicit rules exist at the end of each IPv6 ACL to allow ICMPv6 neighbor discovery:

  ```
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any
  ```

IPv6 Extended ACL Match

- **TCP/UDP/SCTP and ports (eq, lt, gt, neq, range)**

- **ICMPv6 code and type**

- **Fragments**

- **Routing Header**

- **Undetermined transport**

    The first unknown NH can be matched against (numerically rather than by name).

    Since an unknown NH cannot be traversed, the ULP cannot be determined.

IPv6 Extended ACL

- ## Logging

  ```
  (conf-ipv6-acl)# permit tcp any any log-input
  (conf-ipv6-acl)# permit ipv6 any any log
  ```

- ## Time based

  ```
  (conf)# time-range bar
  (conf-trange)# periodic daily 10:00 to 13:00
  (conf-trange)# ipv6 access-list tin
  (conf-ipv6-acl)# deny tcp any any eq www time-range bar
  (conf-ipv6-acl)# permit ipv6 any any
  ```

IPv6 ACL Reflexive

- ## Reflect

  A reflexive ACL is created dynamically, when traffic matches a permit entry containing the reflect keyword.

  The reflexive ACL mirrors the permit entry and times out (by default after 3 mins), unless further traffic matches the entry (or a FIN is detected for TCP traffic).

  The timeout keyword allows setting a higher or lower timeout value.

  Reflexive ACLs can be applied to TCP, UDP, SCTP and ICMPv6.

- ## Evaluate

  Apply the packet against a reflexive ACL.

  Multiple evaluate statements are allowed per ACL.

  The implicit deny any any rule does not apply at the end of a reflexive ACL; matching continues after the evaluate in this case.

Cisco IOS IPv6 ACL CLI (1)

- **Entering address-family sub-mode**

  [no] ipv6 access-list <name>

  Add or delete an ACL.

- **IPv6 address-family sub-mode**

  [no] permit | deny ipv6 | <protocol> any | host <src> | src/len [sport] any | host <dest> | dest/len [dport] [reflect <name> [timeout <secs>]] [fragments] [routing] [dscp <val>] [flow-label <val>][time-range <name>] [log | log-input] [sequence <num>]

  Permit or deny rule defining the acl entry. Individual entries can be inserted or removed by specifying the sequence number.

  Protocol is one of TCP, UDP, SCTP, ICMPv6 or NH value.

Cisco IOS IPv6 ACL CLI (2)

[no] evaluate

Evaluate the dynamically created acl via the permit reflect keyword.

[no] remark

User description of an ACL.

- **Leaving the sub-mode**

  exit

- **Showing the IPv6 ACL configuration**

  # show ipv6 access-list [name]
  # show access-list [name]

- **Clearing the IPv6 ACL match count**
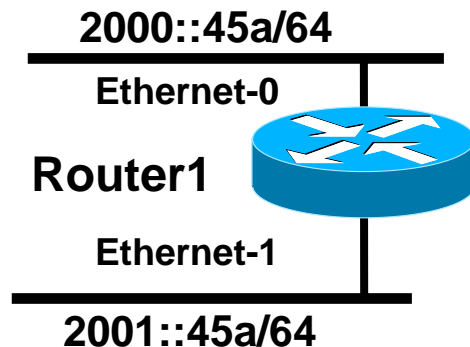
  # clear ipv6 access-list [name]
  # clear access-list [name]

Cisco IOS IPv6 ACL CLI (3)

- **Applying an ACL to an interface**

    (config-int)# ipv6 traffic-filter <acl_name> in | out

- **Restricting access to the router**

    (config-access-class)# ipv6 access-class <acl_name> in | out

- **Applying an ACL to filter debug traffic**

    (Router)# debug ipv6 packet [access-list <acl_name>] [detail]

Cisco IOS IPv6 Reflexive ACL

2000::45a/64

Ethernet-0

Router1

Ethernet-1

2001::45a/64

Allow www traffic via a Reflexive ACL, based on time of day

```
Router1#
interface ethernet-0
  ipv6 address 2000::45a/64
  ipv6 traffic-filter In in
  ipv6 traffic-filter Out out

interface ethernet-1
  ipv6 address 2001::45a/64
  ipv6 traffic-filter Ext-out out

ipv6 access-list In
  permit tcp host 2000::1 eq www host 2001::2 time-range
tim reflect myp
  permit icmp any any router-solicitation

ipv6 access-list Out
  evaluate myp
  evaluate another

time-range tim
  periodic daily 16:00 to 21:00
```
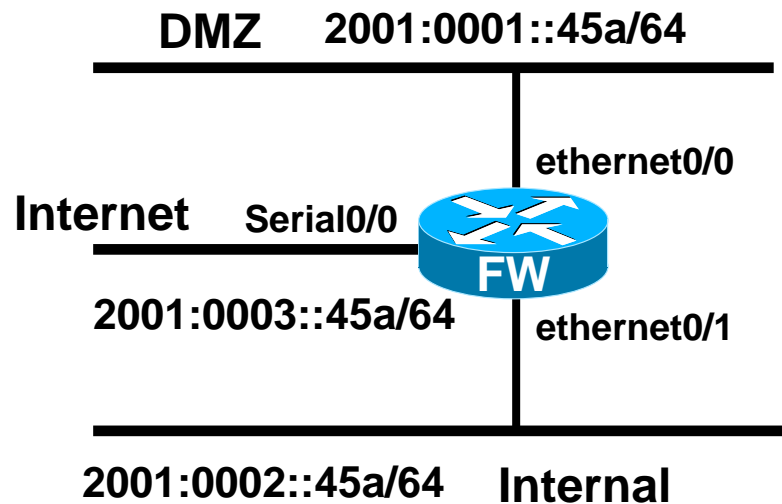
Cisco IOS IPv6 ACL Display

```
brum-45c#show ipv6 access-list
IPv6 access list In
    permit tcp host 2000::1 eq www host 2001::2 time-range tim (active)
reflect myp (1 match)

IPv6 access list Out
    evaluate myp
    evaluate another

IPv6 access list myp (Reflexive)
    permit tcp host 2001::2 2432 host 2000::1 eq www (timeout 180)
```

Cisco IOS IPv6 Firewall (1)

DMZ   **2001:0001::45a/64**

Internet   **Serial0/0**   **ethernet0/0**

2001:0003::45a/64   **ethernet0/1**

2001:0002::45a/64   **Internal**

IPv6 Firewall

```
FW#
  interface ethernet0/0
   ipv6 address 2001:0001::45a/64
   ipv6 traffic-filter dmz-in6 in
  interface ethernet0/1
   ipv6 address 2001:0002::45a/64
   ipv6 traffic-filter internal-in6 in
   ipv6 traffic-filter internal-out6 out
  interface serial0/0
   ipv6 address 2001:0003::45a/64
   ipv6 traffic-filter exterior-in6 in
   ipv6 traffic-filter exterior-out6 out

  ipv6 access-list vty
   deny ipv6 any any log-input

  line vty 0 4
   ipv6 access-class vty in

  ipv6 access-list dmz-in6
   permit ipv6 host 2001:0001::100 any
```

Cisco IOS IPv6 Firewall (2)

```
ipv6 access-list internal-in6
    permit tcp 2001:0002::/64 any reflect internal-tcp
    permit udp 2001:0002::/64 any reflect internal-udp
    permit icmp 2001:0002::/64 any
    permit icmp any any router-solicitation
ipv6 access-list internal-out6
    evaluate internal-tcp
    evaluate internal-udp
    permit icmp any 2001:0002::/64 echo-reply
ipv6 access-list exterior-in6
    evaluate exterior-tcp
    evaluate exterior-udp
    remark Allow access to ftp/http server on the DMZ
    permit tcp any host 2001:0001::100 eq ftp
    permit tcp any host 2001:0001::100 eq www
    permit tcp any host 2001:0001::100 range 49152 65535
    permit icmp any any echo-reply
    permit icmp any any unreachable
    deny ipv6 any any log-input
ipv6 access-list exterior-out6
    permit tcp 2001:0002::/64 any reflect exterior-tcp
    permit udp 2001:0002:;/64 any reflect exterior-udp
```

Cisco IOS IPv6 ACL Behaviour

- **Common ACL name space.**

    ACL names cannot begin with a numeric.

- **IPv6 access-lists are used to filter traffic and restrict access to the router.**

    IPv6 prefix-lists are used to filter routing protocol updates.

- **Non-consecutive bit match patterns are not allowed**

Cisco IOS IPv6 ACL Troubleshooting

- ***sh ipv6 access-list [<name>]***

    Hit count for matching entries.

    (In)active time-based entries.

- ***clear ipv6 access-list [<aclname>]*** **to reset the hit counts for an ACL.**

- **Configure logging for an ACL entry.**

- ***debug ipv6 packet detail*** **to determine which packets are being dropped by an ACL.**

IPv6 Filtering

ISP/IXP Workshops