



# Cisco IOS IPv6 Access Control Lists

**ITD Product Management**  
**Cisco Systems**

# Cisco IOS IPv6 Standard Access Control Lists

- **Cisco IOS IPv6 access-lists 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**

# Cisco IOS IPv6 Standard Access Control Lists (Cont.)

- **Minimum Cisco IOS Software releases are available from Cisco IPv6 start here manual**

[www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_configuration\\_guide\\_chapter09186a00801d65ed.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html)

**Also supported on IOS-XR**

# Cisco IOS 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**

# Cisco IOS IPv6 Extended ACL (Cont.)

- **Minimum Cisco IOS releases are available from Cisco IPv6 start here manual**

[www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_configuration\\_guide\\_chapter09186a00801d65ed.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html)

**Also supported on IOS-XR**

# Cisco IOS IPv6 e-ACL and IPv6 HW FW

- **IPv6 extended ACL requires the capability for IPv6 hardware forwarding platforms to parse option headers**

**Cisco 12000 Engine 3 and Engine 5**

**Cisco 6500 and 7600 sup. 720**

- **The hardware may parse as deep as N bytes in hardware**

**Packets are punt into software path if headers are longer**

**This configuration is platform dependent**

- **Packets with hop-by-hop options are also generally punt to software**

# Cisco IOS Enhanced IPv6 e-ACL

- **Adds support for filtering field inside an IPv6 option header**

**Currently routing type only**

**Used to enable Mobile IPv6 (type=2) but filter source routing (type=0) traffic**

- **Initial implementation available on Cisco IOS® Software Release 12.4(2)T**

**Implementation has dependencies on hardware for IPv6 HW FW platforms**

# Cisco IOS Firewall IPv6 Support

- Introduced in Release 12.3(7)T – now Releases 12.4 and 12.4T

FTP inspection on Release 12.3(11)T

- Stateful inspection of IPv6 packets

IPv6 DoS attack mitigation

Fragmented packet inspection

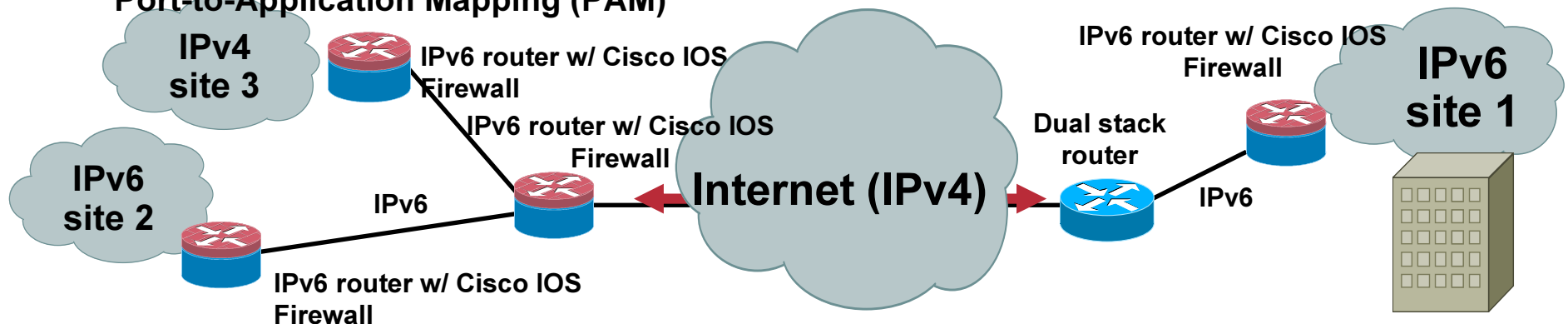
IPv6 DoS attack mitigation; mitigation mechanisms have been implemented in the same manner as the current IPv4 implementation, including SYN half-open connections

Tunneled packet inspection; tunneled IPv6 packets terminated at a Cisco IOS Firewall router can be inspected by the Cisco IOS Firewall for IPv6

Stateful packet inspection of TCP, UDP, ICMPv6, and FTP sessions

Interpretation or recognition of most IPv6 extension header information, including routing header, hop-by-hop options header, and fragment header.

Port-to-Application Mapping (PAM)





# Cisco IOS 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**

# Cisco IOS 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
```

# Cisco IOS 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 instead of by name)**

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

# Cisco IOS 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
```

# Cisco IOS 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 minutes), 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**

# Cisco IOS IPv6 ACL Reflexive (Cont.)

- **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**



# Cisco IOS IPv6 ACL CLI (2 Cont.)

- **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
```

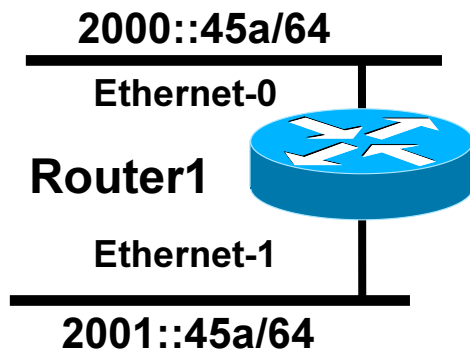
- **Restricting access to the router**

```
(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



**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
```

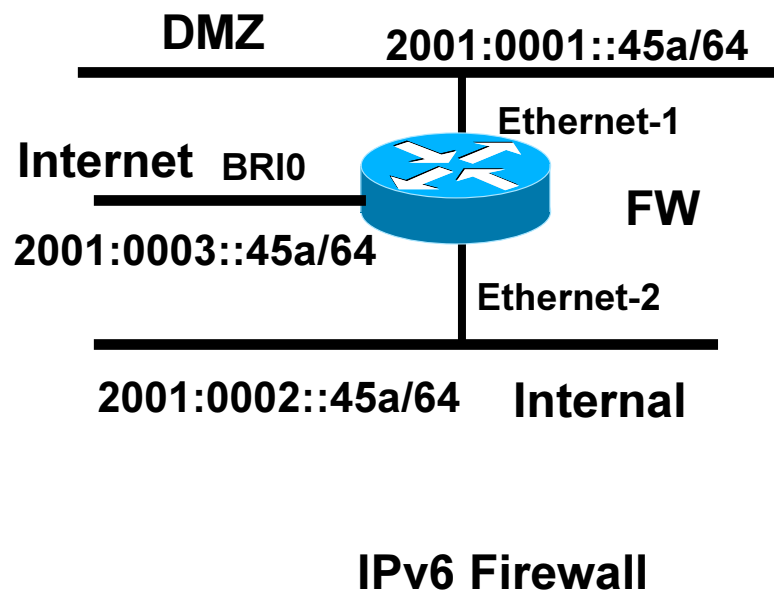
# Cisco IOS IPv6 ACL Display

```
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)



*FW#*

```
interface ethernet-1
  ipv6 address 2001:0001::45a/64
  ipv6 traffic-filter dmz-in6 in
interface ethernet-2
  ipv6 address 2001:0002::45a/64
  ipv6 traffic-filter internal-in6 in
  ipv6 traffic-filter internal-out6 out
interface BRI0
  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 Behavior

- **Common ACL name space**
  - ACL names cannot begin with a number
- **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**



# CISCO SYSTEMS



# Q and A



# Additional Information

- **Cisco.com IPv6**

[www.cisco.com/ipv6](http://www.cisco.com/ipv6)

- **Cisco IPv6 Solutions**

[www.cisco.com/en/US/tech/tk872/technologies\\_white\\_paper09186a00802219bc.shtml](http://www.cisco.com/en/US/tech/tk872/technologies_white_paper09186a00802219bc.shtml)

- **IPv6 Application Notes**

[www.cisco.com/en/US/products/ps6553/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html)