Cisco IOS
IPv6 Access Control Lists

János Mohácsi
NIIF/HUNGARNET

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
- Minimum Cisco IOS releases
  - Cisco IOS 12.2(2)T or 12.3(1)M
  - Cisco IOS 12.0(21)ST1 and Cisco 12.0(22)S on Cisco 12000 series only
  - Cisco 12.2(14)S

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.
- Minimum Cisco IOS releases
  - Cisco IOS 12.2(13)T or 12.3(1)M
  - Cisco 12.0(23)S on Cisco 12000 series only, 12.0(25)S adds hardware assisted ACL on Engine 3
  - Cisco 12.2(14)S

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
- Extended ACL can apply even if option headers are in a packet

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
  - Be careful, when you add “deny ipv6 any any log” at the end

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 rather than 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.
- Evaluate
  - Apply the packet against a reflexive 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]

End

- Further information:
  - http://www.cisco.com/go/ipv6