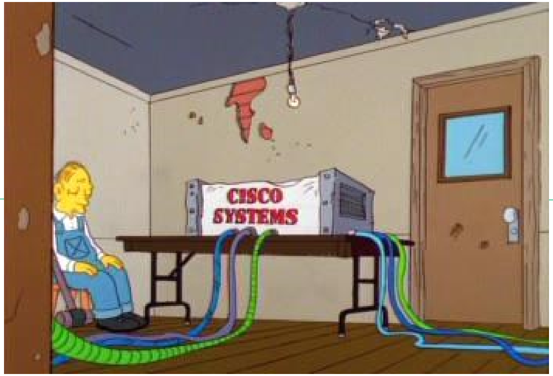
Securing IPv6 in the Cisco Space

Christopher Werny <cwerny@ernw.de>



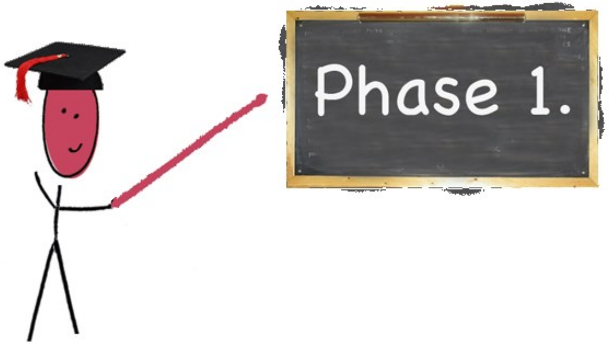
Agenda

- Cisco First-Hop Security Intro
- Secure Layer-2 configuration
- Secure Layer-3 configuration
- Routing Protocol Security configuration
- FHRP Protocol Security configuration
- Traffic Filter and Extension Header Filtering

Cisco First-Hop-Security

- Cisco name for various security features in IPv6
- Staged in three phases
- Every Phase will release/released more IPv6 security features to achieve feature parity with the IPv4 world

Phase I



- Available since Summer 2010
- Introduced RA Guard and Port based IPv6 ACLs
- In the beginning, only supported on datacenter switches
  - Since 15.0(2) supported on C2960S and C3560/3750-X

Phase II

- Available since end of 2011/ beginning of 2012 (depending on the plattform)
- Introduced DHCPv6 Guard and NDP Snooping
  - DHCP Snooping and Dynamic ARP Inspection in the IPv4 World
- As of march 2013, no support on access-layer switches available
  - Only on Cat 4500, Cat 4948 (E/F) and 7600 Routers

Phase 3

- Available since December 2012
- Introduced Destination-Guard
  - To mitigate Neighbor Cache Exhaustion attack
- Only available on the same switches as in Phase 2

General Principles on FH Command Interface[1]

Each FH feature provides a configuration mode to create and populate policies (+ one implicit “default” policy)

```
ipv6 nd raguard policy MYHOST
 device-role host
```

Each FH feature provides commands to attach policies to targets: box,vlan, port

```
vlan configuration 100
 ipv6 nd raguard attach-policy MYHOST
 ipv6 snooping
interface e0/0
 ipv6 nd raguard attach-policy MYROUTER
```

Packets are processed by the lowest-level matching policy for each feature

Packets received on e0/0 are processed by policy ra-guard “MYROUTER” AND policy snooping “default”

Packets received on any other port of vlan 100 are processed by policy ra-guard “MYHOST” AND policy snooping “default”

Cisco First Hop Security

Phase I

RA Guard – Host Mode

- Implements *isolation* principle similar to other L2 protection mechanisms already deployed in v4 world.
- RFC 6105
- Works quite well against some attacks.
  - But it seems currently no logging or port deactivation can be implemented. RA packets are just dropped.
- Can be easily circumvented

RA Guard – Host Mode

```
Router(config-if)#ipv6 nd ?
  raguard  RA_Guard Configuration Command
Router(config-if)#ipv6 nd raguard ?
   <cr>
Router(config-if)#switchport mode access
Router(config-if)#ipv6 nd raguard
Router(config-if)#exit
Router(config)#exit

Router# show version
Cisco IOS Software, s3223_rp Software (s3223_rp-
IPBASEK9-M), Version 12.2(33)SXI5, RELEASE SOFTWARE
(fc2)
```

Port-based ACLs

```
4948E(config)#ipv6 access-list IPv6
4948E(config-ipv6-acl)#deny ipv6 any any undetermined-
transport
4948E(config-ipv6-acl)#deny icmp any any router-
advertisement
4948E(config-ipv6-acl)#permit ipv6 any any
4948E(config)#interface g1/19
4948E(config-if)#ipv6 traffic-filter IPv6 in
```

Block Forwarding of RAs on Infrastructure Level

- RA Guard or ACLs
  - _Or_!
- RA Guard currently (Mar 2013) not a bullet-proof solution.
  - -DF switch in THC's `fakerouter6` does the trick.
    - See also http://www.insinuator.net/2011/05/yet-another-update-on-ipv6-security-some-notes-from-the-ipv6-kongress-in-frankfurt/
- ACLs might be operationally expensive.
  - Probably port based ACLs not part of your current ops model, right?
  - HW support needed
    - http://docwiki.cisco.com/wiki/Cisco_IOS_IPv6_Feature_Mapping#IPv6_Features
  - Still, currently best protection approach that's available
    - See also http://www.insinuator.net/2012/03/the-story-continues-another-ipv6-update/
- RA Guard will (hopefully) evolve
  - Some IETF drafts out there to address evasion problem
    - http://tools.ietf.org/html/draft-ietf-v6ops-ra-guard-implementation-07

Evaluation of RFC 6104 Controls

Control	Sec Benefit	Operational Feasibility
Manual configuration	4	1
RA Snooping (RA Guard)	4	4
Using ACLs	5	3
SEcure Neighbor Discovery (SEND)	5	1
Router Preference	2	5
Relying on Layer 2 Admission Control	5	2
Host-Based Packet Filters	3	1
Using an “Intelligent” Deprecation Tool	2	1
Using Layer 2 Partitioning	4	3

Cisco First Hop Security

Phase II

DHCPv6 Guard

- Similar functionality to DHCP Snooping in the IPv4 world
  - But more sophisticated
- Blocks reply and advertisement messages that originates from “malicious” DHCP servers and relay agents
- Provides finer level of granularity than DHCP Snooping.
- Messages can be filtered based on the address of the DHCP server or relay agent, and/or by the prefixes and address range in the reply message.

DHCPv6 Guard

```
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128

ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 trusted-port <optional>

interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add vlan 10

vlan 10
ipv6 dhcp guard attach-policy pol1

show ipv6 dhcp guard policy pol1
```

Cisco IPv6 Snooping

- IPv6 Snooping is the basis for several FHS security mechanisms
  - Including ND Inspection and address glean

- When configured on a target (VLAN, Interface etc.), it redirects NDP and DHCP traffic to the switch integrated security module

IPv6 ND Inspection

- Learns and secures bindings for addresses in layer 2 neighbor tables.
- Builds a trusted binding table database based on the IPv6 Snooping feature
- IPv6 ND messages that do not have valid bindings are dropped.
- A message is considered valid if the MAC-to-IPv6 address is verifiable

IPv6 ND Configuration

```
Device(config)#ipv6 snooping policy policy1

Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1

Device(config)# ipv6 nd inspection policy policy1

Device(config-nd-inspection)# drop-unsecure
Device(config-nd-inspection)# device monitor
```

Cisco First Hop Security

Phase III

IPv6 Destination Guard

Overview

- Blocks and filters traffic from an unknown source and filters IPv6 traffic based on the destination address.
- Uses „first-hop security binding table“
  - populates all active destinations into it and blocks data traffic when the destination is not identified.

IPv6 Destination Guard

Requirements

- Implemented in Cisco 7600, Cisco Catalyst 4500/4900, 3560-X/3750-X and 2960S
- Requires 15.3S, 15.2S, 15.1SG or 15.0(2)SE

IPv6 Destination Guard

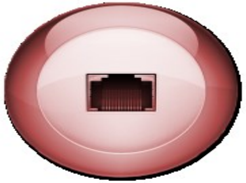
Example Configuration

```
Router(config)# vlan configuration 300
Router(config-vlan-config)# ipv6 destination-guard attach-policy destination
% Warning - 'ipv6 snooping' should be configured before destination-guard


Router(config-vlan-config)# ipv6 snooping attach-policy ND
Router(config)# vlan configuration 300
Router(config-vlan-config)# ipv6 destination-guard attach-policy destination
Router(config-vlan-config)#

Router# show ipv6 destination-guard policy destination
Destination guard policy Destination:
  enforcement always
        Target: vlan 300
```

Layer 3 configuration

Suppress Emission of RAs on Infrastructure Level

Comes in different flavors (full suppress vs. clearing A-flag)
Will just prevent “benign” host processing, but not prevent attacks against hosts from their (potentially compromised) neighbors.



- Full suppression
  - Cisco:
    ```
    L3_device(config-if)#ipv6 nd ra suppress [all]
    ```
  - On some devices/OSs RAs might still be triggered by some host on local link sending router solicitation (RS) packets.
    - E.g. in Cisco land different behavior between 12.4 and 15.x releases. See also CSCth90147.
  - Default route will have to be configured statically on hosts then, too.
    - Might have influence on first hop redundancy approach.
      Probably not relevant for these types of networks though.
  - Must be kept in mind for future activities in $SEGMENT.
    - People (other admins…) might expect it (RAs) “just to be there”.
    - We don’t like the suppress_RAs approach anyway. Deviation from default…

Tuning the Neighbor Cache Size

- `ipv6 nd cache interface-limit`
  - See also http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-i3.html#GUID-FC37F82B-5AAC-4298-BB6C-851FB7A06D88
  - This one provides some logging, too. Might come in handy for attack detection.
    - `Mar 10 15:11:51.719: %IPV6_ND-4-INTFLIMIT: Attempt to exceed interface limit on GigabitEthernet0/1 for 2001:DB8:0:900D::2:329A` (So use it in any case!)
- on IOS-XE 2.6: `ipv6 nd resolution data limit`.

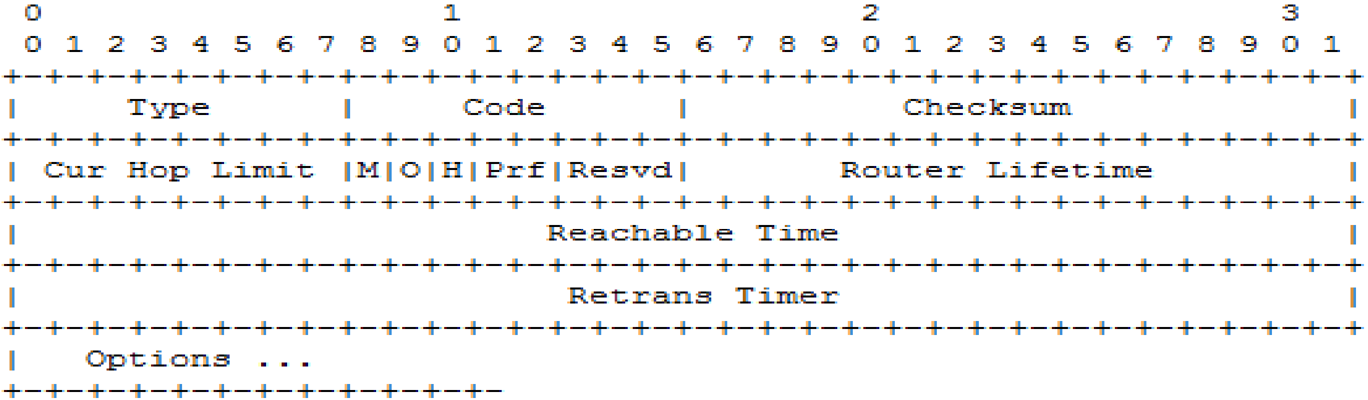
Unicast Reverse Path Forwarding for IPv6

- Supported for IPv6 since 12.2(13)T / 12.2(28)SB
  - Before using it in an production environment, check if it is done in software on your platform (e.g. Cat 6500 with SUP720).

```
interface GigabitEthernet 5/0/0
  ipv6 verify unicast reverse-path
```

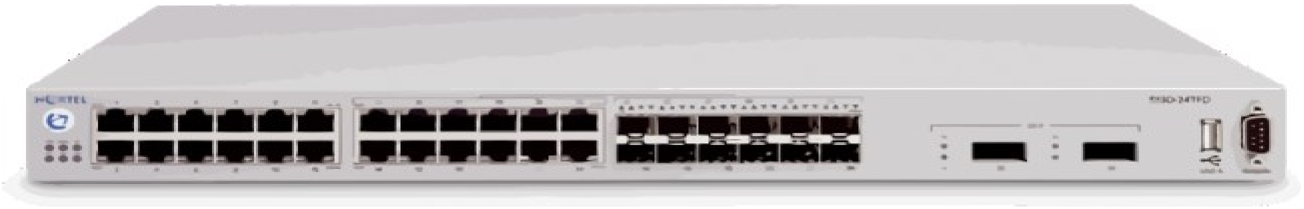
Default Router Preference

- In RFC 4191 an additional flag was introduced within RA messages to indicate the preference of a default router in case more than one are present on the local link.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|H|Prf|Resvd|       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-
```

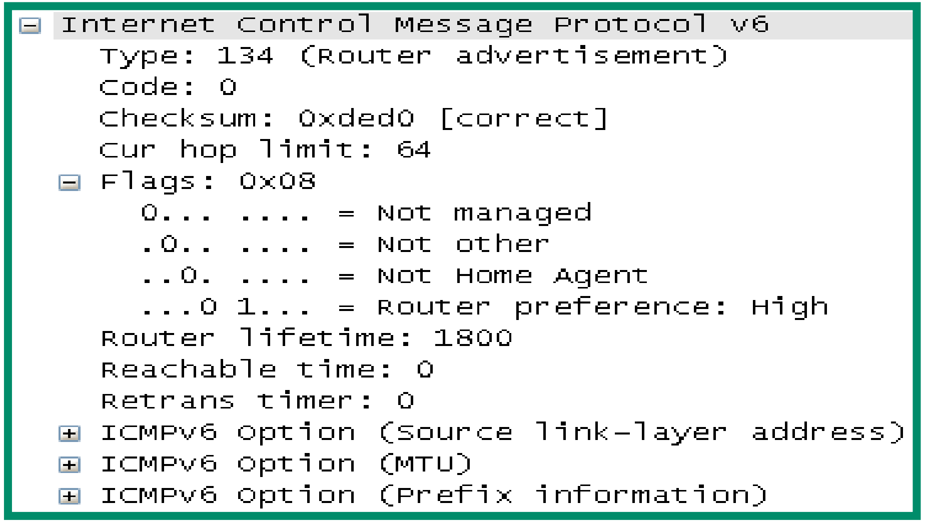
Router Preference Values



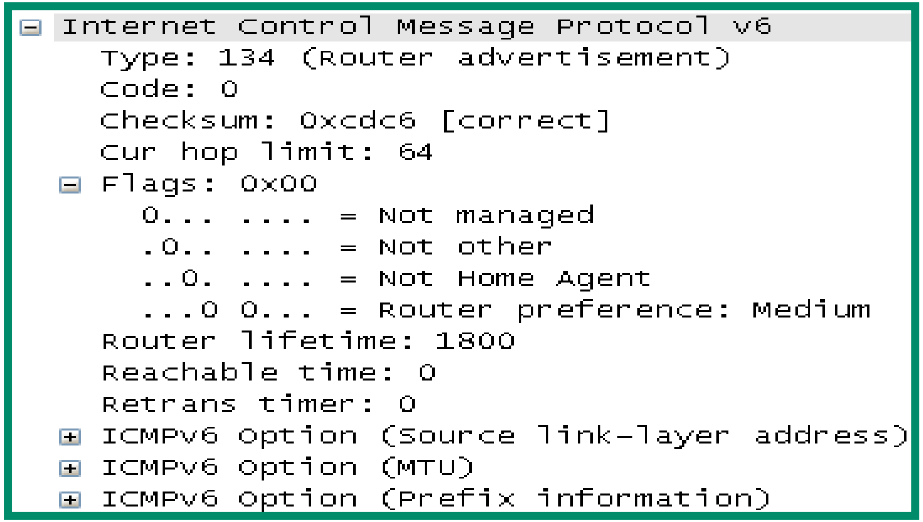
- The *preference* values are encoded as a two-bit signed integer with the following values:
  - 01 High
  - 00 Medium (default)
  - 11 Low
  - 10 Reserved

RA Messages

- When the *preference* is set, the RA messages look like:



```
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xded0 [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x08
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 1... = Router preference: High
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 0
  ⊞ ICMPv6 Option (Source link-layer address)
  ⊞ ICMPv6 Option (MTU)
  ⊞ ICMPv6 Option (Prefix information)
```



```
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xcdc6 [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x00
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 0
  ⊞ ICMPv6 Option (Source link-layer address)
  ⊞ ICMPv6 Option (MTU)
  ⊞ ICMPv6 Option (Prefix information)
```

Configuration (Cisco)

- The configuration of the preference is done with the following command:

```
–   Router(config)# interface f0/1
–   Router(config-if)# ipv6 nd router-preference {high | medium | low}
```

- If the command is not configured, the default value of medium will be used in the RA messages.

- Command available since IOS Version 12.4(2)T

Miscellaneous

- Miscellaneous stuff already known from IPv4, but still applicable in the IPv6 World:

-
  ```
  (config-int)#no ipv6 redirects
  (config-int)#no ipv6 mask-reply
  ```

-
  ```
  (config)#no ipv6 source-route
  ```

Routing Protocol Security

Routing Protocol Security

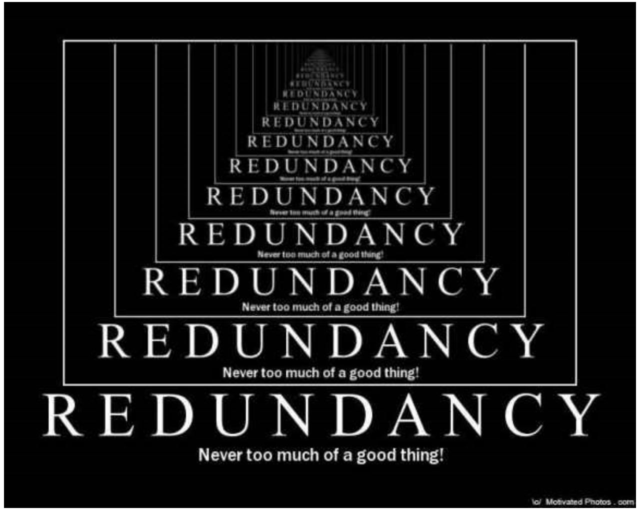
- BGP, ISIS, EIGRP no change required
  - MD5 authentication of the routing peers
- OSPFv3 has changed and pulled the authentication from the protocol and instead rely on transport mode Ipsec
  - But see draft-ospf-auth-trailer-ospfv3

Best Current Practices

- Interface Ethernet0/0
  - ipv6 ospf 1 area 0
  - ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890 ABCDEF
- Interface Ethernet0/0
  - ipv6 authentication mode eigrp 100 md5
  - ipv6 authentication key-chain eigrp 100 MYCHAIN
- Key chein MYCHAIN
  - Key 1
  - Key-string 1234567890abcdef

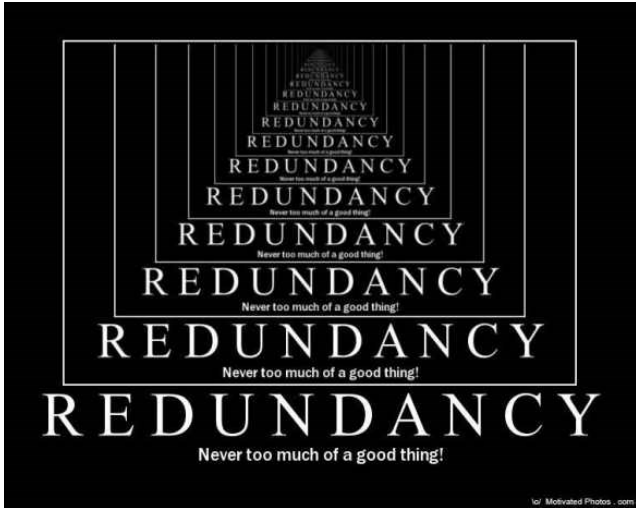
IPv6 FHRP Protocols

FHRP



- Not much changed in the FHRP Space
- Same mechanisms in the IPv4 world are used in IPv6 for securing FHRP protocols
  - Which boils down to MD5 authentication

HSRPv2



- HSRP IPv6 group has a virtual mac address
  - Derived from the HSRP-group
- Virtual IPv6 link-local address
  - Derived from the virtual-mac
- Uses UDP Port 2029

HSRPv2 Configuration

- interface FastEthernet0/0
- no ip address
- ipv6 address 2020:AB8:2001::1010/64 ipv6 enable standby version 2
- standby 1 ipv6 autoconfig
- standby 1 ipv6 2001:DB8::2/64
- standby 1 ipv6 2001:DB8::3/64
- standby 1 ipv6 2001:DB8::4/64
- standby 1 authentication md5 key-string troopers

GLBP Configuration

```
interface FastEthernet0/0
no ip address
ipv6 enable
ipv6 address 2020:AB8:2001::1010/64
glbp 10 ipv6 FE80::1
glbp 10 timers 5 18
glbp 10 load-balancing host-dependent
glbp 10 priority 254
Glbp 10 authentication md5 key-string troopers
```

Traffic Filter and Extension Header Filtering

Basic Bogon Filter List 1/2

Packets to Block	Addresses
Deny unspecified address	::
Deny loopback address	::1
Deny IPv4-compatible addresses	::/96
Deny IPv4-mapped addresses (obsolete)	::ffff:0.0.0.0/96
Deny automatically tunneled packets using compatible addresses (deprecated RFC 4291)	::0.0.0.0/96
Deny other compatible addresses	::224.0.0.0/100 ::127:0.0.0/104 ::0.0.0.0/104 ::255.0.0.0/104

Basic Bogon Filter List 2/2

Packets to Block	Addresses
Deny false 6to4 packets	2002:e000::/20 2002:7f00::/24 2002:0000::/24 2002:ff00::/24 2002:0a00::/24 2002:ac10::/28 2002:c0a8::/32
Deny link-local addresses	fe80::/10
Deny site-local addresses (deprecated)	fec0::/10
Deny unique-local packets	Fc00::/7
Deny multicast packets (only as a source address)	Ff00::/8
Deny documentation address	2001:db8::/32
Deny 6Bone addresses (deprecated)	3ffe::/16

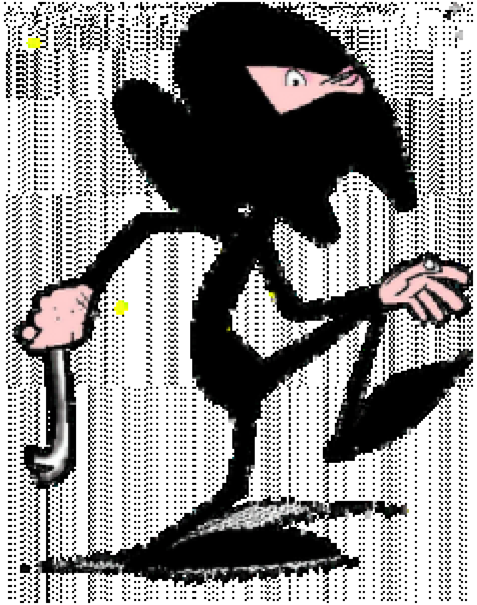
IPv6 ACL@ERNW

Up to Discussion:

```
deny ipv6 host ::1 any log
remark ===Deny IPv4-compatible===
deny ipv6 ::/96 any log
remark ===Deny IPv4-mapped===
deny ipv6 0:0:0:FFFF::/96 any log
remark ===Deny Site-Local===
deny ipv6 FEC0::/10 any log
remark ===Deny ULA===
deny ipv6 FC00::/7 any log
remark ===Deny Documentation===
deny ipv6 2001:DB8::/32 any log
remark Deny ===6Bone===
deny ipv6 3FFE::/16 any log
remark ===Permit T-COM Address===
permit icmp host 2003:60:4010::1 any log
remark ===Deny own address space inbound===
deny ipv6 2003:60:4010::/48 any log
remark ===Permit icmp===
permit icmp any any log
```

- remark ===Allow DNS===
- permit udp any eq domain 2003:60:4010::/48 log
- remark ===TCP Established===
- permit tcp any any established
- remark ===Deny Rest===
- sequence 270 remark ===mx1.ernw.net===
- permit tcp any host 2003:60:4010:10A0::11 eq smtp
- permit tcp any host 2003:60:4010:10A0::11 eq 22
- remark ===www + troopers===
- permit tcp any host 2003:60:4010:1090::11 eq www
- permit tcp any host 2003:60:4010:1090::11 eq 443
- permit tcp any host 2003:60:4010:1090::12 eq www
- permit tcp any host 2003:60:4010:1090::12 eq 443
- permit tcp any host 2003:60:4010:1090::13 eq www
- remark ===Insinuator===
- permit tcp any host 2003:60:4010:11B0::11 eq www

Full Bogon List



- Full Bogon List can be found here:
  - https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

Extension Header

- The ASA supports Extension Header Filtering since 8.2(2)
- Modular Policy Framework used in conjunction with service-policy on an interface

Extension Header

- The ASA to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet:

- •Hop-by-Hop Options
- •Routing (Type 0)
- •Fragment
- •Destination Options
- •Authentication
- •Encapsulating Security Payload

Configuration Parameters

- Class-map ipv6-ext-hdr

  match header count gt. 2

- policy-map type inspect ipv6
  - Class ipv6-ext-hdr
  - action drop
- Service policy ipv6 in interface outside

References

- [1] IPv6 First Hop Security: Eric Vyncke