Cisco Live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now
Introduction to IPv6 Security: Threats and Mitigation

Eric Vyncke, Distinguished Engineer
@evyncke
BRKSEC-2003
Agenda

• Debunking IPv6 Myths
• Shared Issues by IPv4 and IPv6
• Specific Issues for IPv6
  • Extension headers, IPsec everywhere, tunnels, dual-stack
• Enforcing a Security Policy in IPv6
  • ACL, firewalls, IPS, Content security
  • Secure IPv6 transport over public network
• Summary
IPv6 Security Myths...
IPv6 Myths: Better, Faster, More Secure

Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

Source: Microsoft clip-art gallery
The Absence of Reconnaissance Myth

- Default subnets in IPv6 have $2^{64}$ addresses
- 10 Mpps = more than 50 000 years
Reconnaissance in IPv6
Scanning Methods Will Change

• If using EUI-64 addresses, just scan $2^{48}$
  • Or even $2^{24}$ if vendor OUI is known...

• Public servers will still need to be DNS reachable
  • More information collected by Google...

• Increased deployment/reliance on dynamic DNS
  • More information will be in DNS

• Using peer-to-peer clients gives IPv6 addresses of peers

• Harvest NTP client addresses by becoming a member of pool.ntp.org

• Administrators may adopt easy-to-remember addresses
  • ::1, ::80, ::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual-stack

• By compromising hosts in a network, an attacker can learn new addresses to scan
Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion (RFC 6583)

• Potential router CPU/memory attacks if aggressive scanning
  • Router will do Neighbor Discovery... And waste CPU and memory

• Local router DoS with NS/RS/…
Mitigating Remote Neighbor Cache Exhaustion

• Built-in rate limiter with options to tune it
  • Since 15.1(3)T: ipv6 nd cache interface-limit
  • Or IOS-XE 2.6: ipv6 nd resolution data limit
• Destination-guard is part of First Hop Security
• Priority given to refresh existing entries vs. discovering new ones

• Using a /64 on point-to-point links => a lot of addresses to scan!
  • Using /127 could help (RFC 6164)

• Internet edge/presence: a target of choice
  • Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only

• Using infrastructure ACL prevents this scanning
  • iACL: edge ACL denying packets addressed to your routers
  • Easy with IPv6 because new addressing scheme 😊

http://www.insinuator.net/2013/03/ipv6-neighbor-cache-exhaustion-attacks-risk-assessment-mitigation-strategies-part-1
The IPsec Myth: IPsec End-to-End will Save the World

• “IPv6 mandates the implementation of IPsec”

• Some organizations believe that IPsec should be used to secure all flows…

“Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.

If enacted globally, this would make it easier to catch cyber criminals, Prof W. said.”
The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 “IPsec SHOULD be supported by all IPv6 nodes”
- Some organizations still believe that IPsec should be used to secure all flows...
  - Need to trust endpoints and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - Network telemetry is blinded: NetFlow of little use
  - Network services hindered: what about QoS or AVC?

Recommendation: do not use IPsec end to end within an administrative domain.

Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4
Shared Issues
IPv6 Bogon and Anti-Spoofing Filtering

- Bogon filtering (data plane & BGP route-map):
  http://www.cymru.com/Bogons/ipv6.txt

- Anti-spoofing = uRPF
Remote Triggered Black Hole

- RFC 5635 RTBH is as easy in IPv6 as in IPv4
- uRPF is also your friend for black holing a source
- RFC 6666 has a specific discard prefix
  - 100::/64

Neighbor Discovery Issue#1 StateLess Address Auto Configuration

SLAAC Rogue Router Advertisement

- **Router Advertisements (RA)** contains:
  - Prefix to be used by hosts
  - Data-link layer address of the router
  - Miscellaneous options: MTU, DHCPv6 use, …

RA w/o Any Authentication
Gives Exactly Same Level
of Security as DHCPv4
(None)

1. **RS:**
   - Data = Query: please send RA

2. **RA:**
   - Data = options, prefix, lifetime, A+M+O flags

DoS
MITM
BRKSEC-2003 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Neighbor Discovery Issue#2
Neighbor Solicitation

Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange Packets on This Link

Security Mechanisms Built into Discovery Protocol = None
Last Come is Used
=> Very similar to ARP

Attack Tool from THC: Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...
ARP Spoofing is now NDP Spoofing: Mitigation

• **GOOD NEWS**: First-Hop-Security for IPv6 is available
  • First phase (Port ACL & RA Guard) available since Summer 2010
  • Second phase (NDP & DHCP snooping) available since Summer 2011
  • Third phase (Source Guard, Destination Guard) available since Summer 2013

• *(kind of) GOOD NEWS*: Secure Neighbor Discovery
  • SeND = NDP + crypto
  • IOS 12.4(24)T
  • But not in Windows 7, 2008, 2012 and 8, Mac OS/X, iOS, Android

• Other **GOOD NEWS**:
  • Private VLAN works with IPv6
  • Port security works with IPv6
  • IEEE 801.X works with IPv6 (except downloadable ACL)
Mitigating Rogue RA: Host Isolation

- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in ‘AP Isolation Mode’
  - 1 VLAN per host (SP access network with Broadband Network Gateway)

- Link-local multicast (RA, DHCP request, etc.) sent only to the local official router: no harm
  - Side effect: breaks Duplicate Address Detection (DAD)
First Hop Security: RAguard since 2010 (RFC 6105)

• **Port ACL**
  blocks all ICMPv6 RA from hosts
  ```
  interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
  ```

• **RAguard lite** (12.2(33)SX14 & 12.2(54)SG )
  also dropping all RA received on this port
  ```
  interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
  ```

• **RAguard** (12.2(50)SY, 15.0(2)SE)
  ```
  ipv6 nd raguard policy HOST device-role host
  ipv6 nd raguard policy ROUTER device-role router
  ipv6 nd raguard attach-policy HOST vlan 100
  interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
  ```
ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMPv4</th>
<th>ICMPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Checks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Informational/Error Messaging</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fragmentation Needed Notification</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address Assignment</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Address Resolution</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Router Discovery</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Multicast Group Management</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mobile IPv6 Support</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

=> ICMP policy on firewalls needs to change
## Generic ICMPv4

**Border Firewall Policy**

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv4 Type</th>
<th>ICMPv4 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>8</td>
<td>0</td>
<td>Echo Request</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>0</td>
<td>Dst. Unreachable—Net Unreachable</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>4</td>
<td>Dst. Unreachable—Frag. Needed</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>11</td>
<td>0</td>
<td>Time Exceeded—TTL Exceeded</td>
</tr>
</tbody>
</table>
### Equivalent ICMPv6

**RFC 4890: Border Firewall Transit Policy**

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv6 Type</th>
<th>ICMPv6 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>128</td>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>129</td>
<td>0</td>
<td>Echo Request</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>1</td>
<td>0</td>
<td>Unreachable</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>2</td>
<td>0</td>
<td>Packet Too Big</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>0</td>
<td>Time Exceeded—HL Exceeded</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>4</td>
<td>0</td>
<td>Parameter Problem</td>
</tr>
</tbody>
</table>

Needed for Teredo traffic

---

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
# Potential Additional ICMPv6

## RFC 4890: Border Firewall Transit Policy

### Table of ICMPv6 Types and Codes

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv6 Type</th>
<th>ICMPv6 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>2</td>
<td>0</td>
<td>Packet too Big</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>4</td>
<td>0</td>
<td>Parameter Problem</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>130–132</td>
<td>0</td>
<td>Multicast Listener</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>135/136</td>
<td>0</td>
<td>Neighbor Solicitation and Advertisement</td>
</tr>
<tr>
<td>Deny</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*For locally generated by the device*
Remote NDP Floods...


- RFC 4890 is a little too open

- RFC 4861 (Neighbor Discovery)
  - Hop Limit MUST be 255
  - Source should be link-local, unspecified or global address belonging to the link and not "any"
Preventing IPv6 Routing Attacks

Protocol Authentication

• BGP, ISIS, EIGRP no change:
  • An MD5 authentication of the routing update

• OSPFv3 has changed and pulled MD5 authentication from the protocol and instead rely on transport mode IPsec (for authentication and confidentiality)
  • But see RFC 6506 7166 (but not widely implemented yet)

• IPv6 routing attack best practices
  • Use traditional authentication mechanisms on BGP and IS-IS
  • Use IPsec to secure protocols such as OSPFv3
IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4.

- **Application layer attacks**
  - The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent.

- **Rogue devices**
  - Rogue devices will be as easy to insert into an IPv6 network as in IPv4.

- **Man-in-the-Middle Attacks (MITM)**
  - Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4.

- **Flooding**
  - Flooding attacks are identical between IPv4 and IPv6.

Good news: IPv4 IPS signatures can be re-used.
Specific IPv6 Issues
IPv6 Privacy Extensions (RFC 4941)  
AKA Temporary Addresses

• Temporary addresses for IPv6 host client application, e.g. web browser
  • Inhibit device/user tracking
  • Random 64 bit interface ID, then run Duplicate Address Detection before using it
  • Rate of change based on local policy
• Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)
Disabling Privacy Extension

• Alternatively disabling stateless auto-configuration and force DHCPv6
  • Send Router Advertisements with
  • all prefixes with A-bit set to 0 (disable SLAAC)
  • M-bit set to 1 to force stateful DHCPv6

```bash
interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag

• Use DHCP to a specific pool + ingress ACL allowing only this pool
```
Extension Headers

- Extension Headers Are Daisy Chained
- Upper Layer Headers, must be last, following extension headers
IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?
  - Mitigation: a firewall such as ASA which can filter on headers

Perfectly Valid IPv6 Packet According to the Sniffer

- Hop-by-hop Option Header
- Destination Option Header
- Routing Header, type 0
- Hop-by-hop Option Header
- Destination Option Header
- Routing Header, type 0
- Destination Option Header
- Routing Header, type 0
- Transmission Control Protocol, Src Port: 1024 (1024), Destination Port: 77
- Border Gateway Protocol

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => MATCH
  - Or unknown extension header/layer 4 header found... => NO MATCH
Fragment Header: IPv6

- In IPv6 fragmentation is done **only** by the end system
  - Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Most OS implement it in 2012
- Attackers can still fragment in intermediate system on purpose ==> a great obfuscation tool

![IPv6 Fragment Header Diagram]
Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large that it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment

IPv6 hdr | HopByHop | Routing | Fragment1 | Destination
---|---|---|---|---
IPv6 hdr | HopByHop | Routing | Fragment2 | TCP | Data

Layer 4 header is in 2nd fragment
Parsing the Extension Header Chain Fragments and Stateless Filters

- Layer 4 information could be in 2\textsuperscript{nd} fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented
- RFC 3128 is not applicable to IPv6 but
  - RFC 6980 ‘nodes MUST silently ignore NDP ... if packets include a fragmentation header’ ;-
  - RFC 7112 ‘A host that receives a First Fragment that does not satisfy ... SHOULD discard the packet’ ;-

```
IPv6 hdr   HopByHop   Routing   Fragment1   Destination ...
```
```
IPv6 hdr   HopByHop   Routing   Fragment2   ... Destination   TCP   Data
```

Layer 4 header is in 2\textsuperscript{nd} fragment, Stateless filters have no clue where to find it!
IPv6 Fragmentation & IOS ACL

Fragment Keyword

• This makes matching against the first fragment non-deterministic:
  • layer 4 header might not be there but in a later fragment
    ⇒ Need for stateful inspection

• fragment keyword matches
  • Non-initial fragments (same as IPv4)

• undetermined-transport keyword does not match
  • If non-initial fragment
  • Or if TCP/UDP/SCTP and ports are in the fragment
  • Or if ICMP and type and code are in the fragment
  • Everything else matches (including OSPFv3, RSVP, GRE, ESP, EIGRP, PIM …)
  • Only for deny ACE

RFC 7112 router MAY drop those packets ;(-)
Is there NAT for IPv6? - “I need it for security”

- Network Prefix Translation, RFC 6296,
  - 1:1 stateless prefix translation allowing all inbound/outbound packets.
  - Main use case: multi-homing

- Else, IETF has not specified any N:1 stateful translation (aka overload NAT or NAPT) for IPv6

- Do not confuse stateful firewall and NAPT* even if they are often co-located

- Nowadays, NAPT (for IPv4) does not help security
  - Host OS are way more resilient than in 2000
  - Hosts are mobile and cannot always be behind your ‘controlled NAPT’
  - Malware are not injected from ‘outside’ but are fetched from the ‘inside’ by visiting weird sites or installing any trojanized application

NAPT = Network Address and Port Translation
PCI DSS 3.0 Compliance and IPv6

• Payment Card Industry Data Security Standard (latest revision November 2013):
  • **Requirement 1.3.8** Do not disclose private IP addresses and routing information to unauthorized parties.
  • Note: Methods to obscure IP addressing may include, but are not limited to: Network Address Translation (NAT)
    ...
  • the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.

• ➔ how to comply with PCI DSS
  • Application proxies or SOCKS
  • Strict data plane filtering with ACL
  • Strict routing plane filtering with BGP route-maps

• Cisco IPv6 design for PCI with IPv6
IPv4 to IPv6 Transition Challenges

• 16+ methods, possibly in combination

• Dual stack
  • Consider security for both protocols
  • Cross v4/v6 abuse
  • Resiliency (shared resources)

• Tunnels
  • Bypass firewalls (protocol 41 or UDP)
  • Can cause asymmetric traffic (hence breaking stateful firewalls)
Dual Stack Host Considerations

• Host security on a dual-stack device
  • Applications can be subject to attack on both IPv6 and IPv4
  • Fate sharing: as secure as the least secure stack...

• Host security controls should block and inspect traffic from both IP versions
  • Host intrusion prevention, personal firewalls, VPN clients, etc.

IPv4 IPsecVPN with No Split Tunneling

IPsec VPN Client on dual-stack host

IPv6 HDR IPv6 Exploit

Does the IPsec Client Stop an Inbound IPv6 Exploit?
Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Windows7 & 8.x, Linux, Mac OS/X, ...)

- Your network:
  - Does not run IPv6

- Your assumption:
  - I’m safe

- Reality
  - You are **not** safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack

=> Probably time to think about IPv6 in your network
Vulnerability Scanning in a Dual-Stack World

- Finding all hosts:
  - Address enumeration does not work for IPv6
  - Need to rely on DNS or NDP caches or NetFlow

- Vulnerability scanning
  - IPv4 global address, IPv6 global address(es) (if any), IPv6 link-local address
  - Some services are single stack only (currently mostly IPv4 but who knows...)
  - Personal firewall rules could be different between IPv4/IPv6

- **IPv6 vulnerability scanning MUST be done for IPv4 & IPv6 even in an IPv4-only network**
  - IPv6 link-local addresses are active by default
Can We Block Rogue Tunnels?

- Rogue tunnels by naïve users:
  - Sure, block IP protocol 41 and UDP/3544, UDP/3074
  - In Windows:

```
netsh interface 6to4 set state state=disabled undoonstop=disabled
netsh interface isatap set state state=disabled
netsh interface teredo set state type=disabled
```

- Really rogue tunnels (covert channels)
  - No easy way...
  - Teredo will run over a different UDP port of course
  - Network devices can be your friend (more to come)

- **Deploying native IPv6 (including IPv6 firewalls and IPS) is probably a better alternative**

- Or disable IPv6 on Windows through registry
  - HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents
  - But Microsoft does not test any Windows application with IPv6 disabled
Can We Block / **Detect** Rogue Tunnels?

- Using AVC with NBAR2 with ISR G2 Routers
- Using NETFLOW with IPv6 on Routers & Switches
- Using NGIPS
- Using NGFW
Enforcing a Security Policy
IOS IPv6 Extended ACL

- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers, ICMPv6 code and type
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - Traffic class (only six bits/8) = DSCP, Flow label (0-0xFFFFF)

- IPv6 extension headers
  - `routing` matches any RH, `routing-type` matches specific RH
  - `mobility` matches any MH, `mobility-type` matches specific MH
  - `dest-option` matches any destination options
  - `auth` matches AH
  - `hbh` matches hop-by-hop (since 15.2(3)T)

- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)

- `undetermined-transport` keyword does not match
  - TCP/UDP/SCTP and ports are in the fragment
  - ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, …)
  - Only for deny ACE

*Check your platform & release as your mileage can vary…*
IPv6 ACL Implicit Rules
RFC 4890

• Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

```plaintext
... permit icmp any any nd-na
permit icmp any any nd-ns
```

• This is different on IOS XE (i.e. ASR1k) : no default permit of ND / NA Packets
IPv6 ACL Implicit Rules – Cont.
Adding a deny-log

- The beginner’s mistake is to add a deny log at the end of IPv6 ACL

```plaintext
! Now log all denied packets
deny ipv6 any any log
! Heu . . . I forget about these implicit lines
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

Solution, explicitly add the implicit ACE

```plaintext
! Now log all denied packets
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```
IPv6 ACL to Protect VTY

```plaintext
ipv6 access-list VTY
    permit ipv6 2001:db8:0:1::/64 any
line vty 0 4
    ipv6 access-class VTY in
```

**MUST BE DONE** before `ipv6 enable` on any interface!

- Beware there is no equivalent for HTTP => use ACL
- The ‘management-interface’ command of ‘control-plane host’ is IPv4 only => use ACL
- In IOS-XR, the command is ‘access-class VTY ingress’, the IPv4 and IPv6 ACL must have the same name
Non-Congruent Security Policies 😞

- Test done in 2016 on 25K routers
- SSH is more open in IPv6 (9%) than IPv4 (4%)
- Telnet is more open in IPv6 (6%) than in IPv4 (3%)

https://www.ietf.org/proceedings/95/slides/slides-95-maprg-0.pdf (Mark Allman)
Control Plane Policing for IPv6
Protecting the Router CPU

• Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
• Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
  class ICMP6_CLASS
    police 8000
  class OSPF_CLASS
    police 200000
  class class-default
    police 8000
!
control-plane cef-exception
service-policy input COPPr
```
ASA Firewall IPv6 Support

• Since version 7.0 (April 2005)
• IPv6 header security checks (length & order)
• Management access via IPv6: Telnet, SSH, HTTPS, ASDM
• Routed & transparent mode, fail-over
• v6 App inspection includes: DNS, FTP, HTTP, ICMP, SIP, SMTP, and IPSec pass-through
• IPv6 support for site-to-site VPN tunnels was added in 8.3 (IKEv1 in ASA 8.3.1, and IKEv2 in ASA 8.4.1)
• Selective permit/deny of extension headers (added in ASA 8.4.2)
• OSPFv3, DHCPv6 relay, stateful NAT64/46/66, mixed mode objects (ASA 9.0)
ASA 8.4.2+ : IPv6 Extension Header Filtering
ASA 9.0: Single Rule Table & Mixed Mode Objects

![ASA Configuration](image-url)
Cisco Threat Defense: Stealth Watch

- NetFlow supports IPv6 fields & counters
- Detection & Analysis of IPv6 Traffic to find
  - unknown IPv6 Routers
  - unknown IPv6 Hosts
  - tunneled traffic
  - malware on Dual Stack Hosts
FIREpower NG IPS and IPv6

- FIREsight passive network discovery correlates Events & Host IP
- Very easy to find out the sender / destination in Dual Stacked environments!
Web Security Appliance and IPv6

- Client can be IPv4, IPv6 or Dual-Stacked
- Explicit and transparent mode (WCCP) are supported
- Easy Access for Clients in IPv4 networks to IPv6 Websites
Summary of Cisco IPv6 Security Products

- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 over IPv4 (ASA 8.0) over IPv6 (ASA 9.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)

- ASA-SM
  - Leverage ASA code base, same features ;-) 16 Gbps of IPv6 throughput

- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)

- IPS
  - Since 6.2 (released 2008)

- Email Security Appliance (ESA) support since 7.6.1 (May 2012)

- Web Security Appliance (WSA) with explicit and transparent proxy

- Cisco Cloud Web Security (ScanSafe) & OpenDNS work in progress (need IPv6 connectivity for all towers...)

- FIREpower NGIPS provides Decoder for IPv4 & IPv6 Packets
Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

<table>
<thead>
<tr>
<th>Public Network</th>
<th>Site 2 Site</th>
<th>Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>6in4/GRE Tunnels Protected by IPsec</td>
<td>ISATAP Protected by RA IPsec</td>
</tr>
<tr>
<td></td>
<td>DMVPN 12.4(20)T</td>
<td>SSL VPN Client AnyConnect</td>
</tr>
<tr>
<td></td>
<td>FlexVPN</td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>IPsec VTI 12.4(6)T</td>
<td>SSL VPN Client AnyConnect 3.1 &amp; ASA 9.0</td>
</tr>
<tr>
<td></td>
<td>DMVPN 15.2(1)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FlexVPN</td>
<td></td>
</tr>
</tbody>
</table>
Secure Site to Site IPv4/IPv6 Traffic over IPv4/IPv6 with DMVPN & FlexVPN

• IPv6 packets over DMVPN IPv4/IPv6 tunnels
  • In IOS release 12.4(20)T (2008)
  • In IOS-XE release 3.5 (2011)
  • IPv6 and/or IPv4 data packets over same GRE tunnel

• Complete set of NHRP commands
  • network-id, holdtime, authentication, map, etc.

• NHRP registers two addresses
  • Link-local for routing protocol (Automatic or Manual)
  • Global for packet forwarding

• FlexVPN (= DMVPN phase 4) integrates site-2-site and remote access in a single unified CLI and supports dual-stack or IPv6-only
DMVPN for IPv6 Configuration

Hub

```
interface Tunnel0
  ipv6 address 2001:db8:100::1/64
  ipv6 eigrp 1
  no ipv6 split-horizon eigrp 1
  no ipv6 next-hop-self eigrp 1
  ipv6 nhrp map multicast dynamic
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  tunnel source Serial2/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof

interface Ethernet0/0
  ipv6 address 2001:db8:0::1/64
  ipv6 eigrp 1

interface Serial2/0
  ip address 172.17.0.1 255.255.255.252

ipv6 router eigrp 1
no shutdown
```

Spoke

```
interface Tunnel0
  ipv6 address 2001:db8:100::11/64
  ipv6 eigrp 1
  ipv6 nhrp map multicast 172.17.0.1
  ipv6 nhrp map 2001:db8:100::1/128 172.17.0.1
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  ipv6 nhrp nhs 2001:db8:100::1
  tunnel source Serial1/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof

interface Ethernet0/0
  ipv6 address 2001:db8:1::1/64
  ipv6 eigrp 1

interface Serial1/0
  ip address 172.16.1.1 255.255.255.252

ipv6 router eigrp 1
no shutdown
```

All combinations of IPv4 and IPv6 are allowed
FlexVPN Site-to-site: e.g. IPv6 over IPv4

- IPv4/IPv6 FlexVPN over IPv4 or IPv6 are allowed (IPv6 over IPv4 shown)

```bash
interface Tunnel0
 ipv6 address fe80::1 link-local
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.2.1
 tunnel protection ipsec profile default

interface FastEthernet0/1
 ipv6 address 2001:db8:cafe::1/64
 ipv6 ospf 1 area 0

interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
```

```bash
interface Tunnel0
 ipv6 address fe80::2 link-local
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface FastEthernet0/1
 ipv6 address 2001:db8:beef::1/64
 ipv6 ospf 1 area 0

interface FastEthernet0/0
 ip address 172.16.2.1 255.255.255.0
```
Secure RA IPv* over IPv* Public Network: AnyConnect SSL VPN Client 3.1 & ASA 9.0

- AnyConnect supports native IPv4/6 connectivity
- Connecting via IPv4/6 Internet to ASA
- SSL Tunneling IPv6 in IPv6, IPv4 in IPv4, IPv6 in IPv4, IPv4 in IPv6
- IPv6 in IPv6 for IKEv2 coming in ASA 9.2
- No support for DHCPv6 yet
- AnyConnect Mobile does not support IPv6 transport
Summary
Key Take Away

• So, **nothing really new in IPv6**
  • Reconnaissance: address enumeration replaced by DNS enumeration
  • Spoofing & bogons: uRPF is our IP-agnostic friend
  • NDP spoofing: RA guard and FHS Features
  • ICMPv6 firewalls need to change policy to allow NDP
  • Extension headers: firewall & ACL can process them
  • NGIPS / NGFW can detect & filter applications over IPv6

• Lack of operation experience may hinder security for a while: **Training is required**

• Security enforcement is possible
  • Control your IPv6 traffic as you do for IPv4

• Leverage IPsec to secure IPv6 when suitable

• **Experiment with IPv6 here at Cisco Live! Or at home ;-)**
Is IPv6 in My Network?

• Easy to check!

• Look inside NetFlow records
  • Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  • IPv4 address: 192.88.99.1 (6to4 anycast server)
  • UDP 3544, the public part of Teredo, yet another tunnel
  • ICMPv6 Packets, especially RA

• Check your IPS System for discovery of ICMPv6 Traffic

• Look into DNS server log for resolution of ISATAP & Microsoft Teredo servers

• Beware of the IPv6 latent threat:

  Your IPv4-only network may be vulnerable to IPv6 attacks NOW!
Recommended Reading

IPv6 Security

Information assurance for the next-generation Internet Protocol

OPSEC
Internet-Draft
Intended status: Informational
Expires: September 22, 2016

Operational Security Considerations for IPv6 Networks
draft-ietf-opsec-v6-08

K. Chittimaneni
Dropbox Inc.
M. Kaeo
Double Shot Security
E. Vyncke
Cisco
March 21, 2016
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your IPv6 Education

• Demos in the Cisco campus: SRv6, 6CN (DevNet Zone)
• Walk-in Self-Paced Labs: LABCRS-1000, LTRRST-2016
• Lunch & Learn: Tuesday, Wednesday
• Meet the Engineer 1:1 meetings
• Related sessions: BRKRST-2667, BRKRST-2616, BRKSEC-2003, BRKSEC-3033, BRKSEC-3771, BRKRST-3304, BRKRST-2044, BRKRST-2312, BRKRST-3045, BRKSEC-3003, BRKRST-2022, BRKSPG-2300, BRKSEC-3200
• World of Solutions: ask about IPv6 support ;-)
Thank you