



Cisco Expo
2009

IPv6 Security Threats and Mitigations



Eric Vyncke, Distinguished Engineer, evyncke@cisco.com

Starts at 14:05

Stops at 14:50

About this WebEx session

1. VoIP usage
2. Recording will be used
3. Local panelists to help
4. Chat possibility
5. Q&A at the end
6. Survey after leaving the session

Session Objectives

1. IPv6 vs. to IPv4 from a threat and mitigation perspective
2. Advanced IPv6 security topics like transition options and dual stack environments
3. **Requirements: basic knowledge of the IPv6 and IPSec protocols as well as IPv4 security best practices**

For Reference Slides



**For Your
Reference**

1. There are more slides in the hand-outs than presented during the class
2. Those slides are mainly for reference and are indicated by the book icon on the top right corner (as on this slide)

Agenda

1. Shared Issues by IPv4 and IPv6
2. Specific Issues for IPv6
IPsec everywhere, dual-stack, tunnels and 6VPE
3. Enforcing a Security Policy in IPv6
ACL, Firewalls and Host IPS
4. Enterprise Secure Deployment
Secure IPv6 transport over public network

Shared Issues



Security Issues Shared by IPv4 and IPv6

Reconnaissance in IPv6

Subnet Size Difference

1. Default subnets in IPv6 have 264 addresses
10 Mpps = more than 50 000 years
2. NMAP doesn't even support ping sweeps on IPv6 networks

Reconnaissance in IPv6

Scanning Methods Are Likely to Change

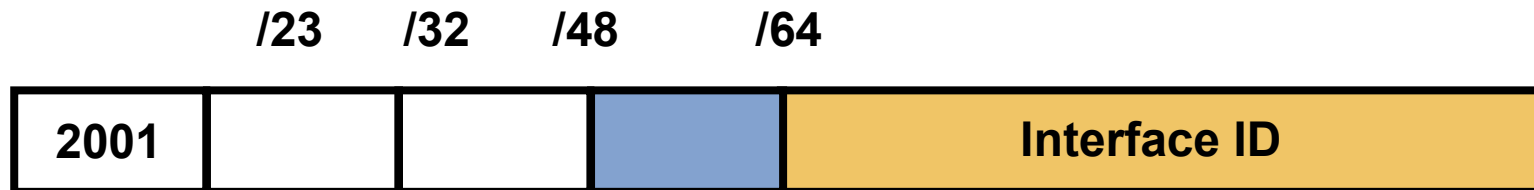
1. Public servers will still need to be DNS reachable
⇒ More information collected by Google...
2. Increased deployment/reliance on dynamic DNS
=> More information will be in DNS
3. Using peer-to-peer clients gives IPv6 addresses of peers
4. Administrators may adopt easy-to-remember addresses
(::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
5. By compromising hosts in a network, an attacker can learn new addresses to scan
6. Transition techniques (see further) derive IPv6 address from IPv4 address => can scan again

Viruses and Worms in IPv6

1. Viruses and email worms: IPv6 brings no change
2. Other worms:
 - IPv4: reliance on network scanning
 - IPv6: not so easy (**see reconnaissance**) => will use alternative techniques

1. Worm developers will adapt to IPv6
2. IPv4 best practices around worm detection and mitigation remain valid
3. Potential router CPU attacks if aggressive scanning
Router will do Neighbor Discovery...

IPv6 Privacy Extensions (RFC 3041)

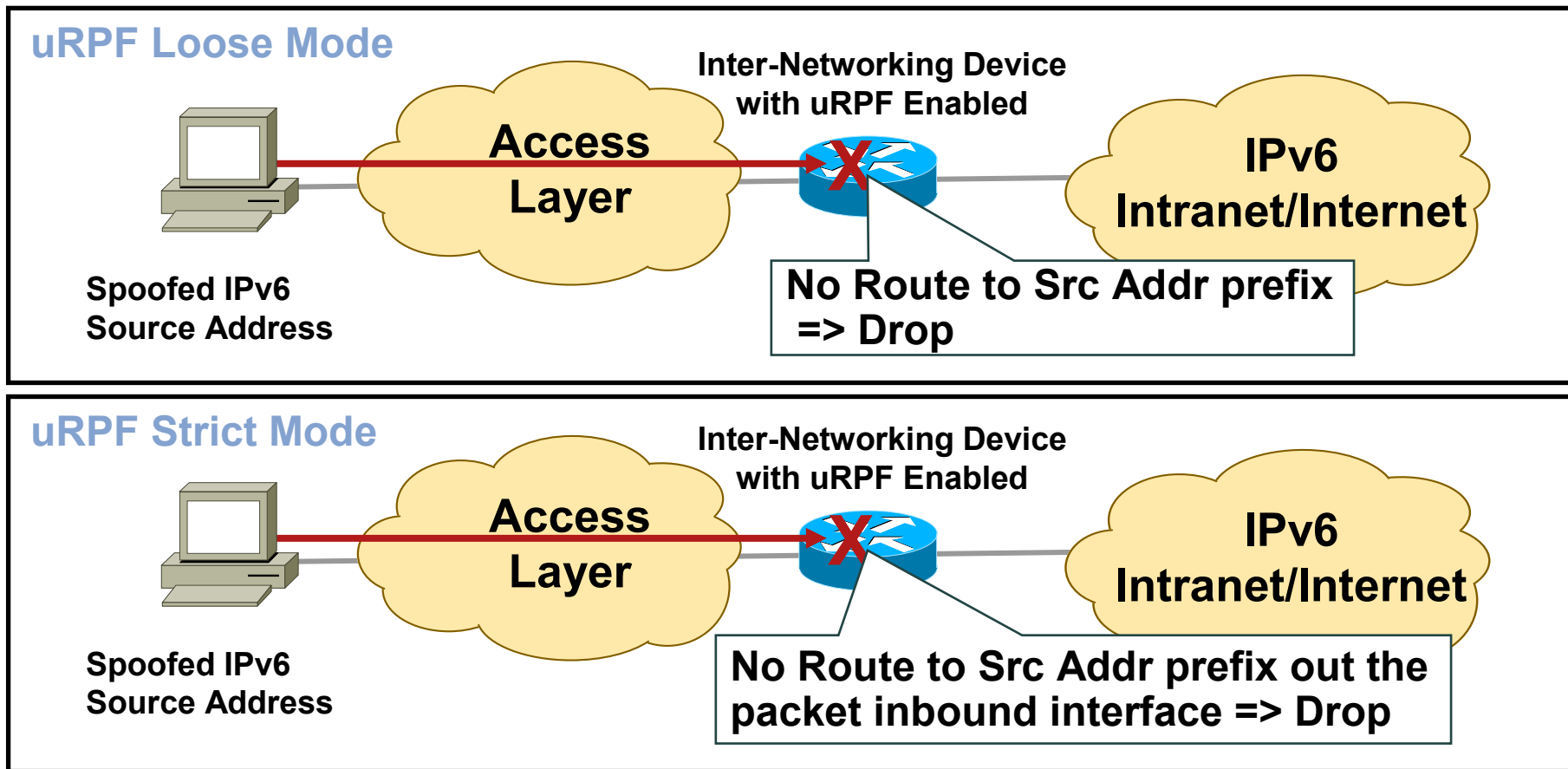


1. Temporary addresses for IPv6 host client application, e.g. web browser
 - Inhibit device/user tracking
 - Random 64 bit interface ID, then run Duplicate Address Detection before using it
 - Rate of change based on local policy

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

L3 Spoofing in IPv6

uRPF Remains the Primary Tool for Protecting Against L3 Spoofing



ICMPv4 vs. ICMPv6

1. Significant changes
2. More relied upon

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

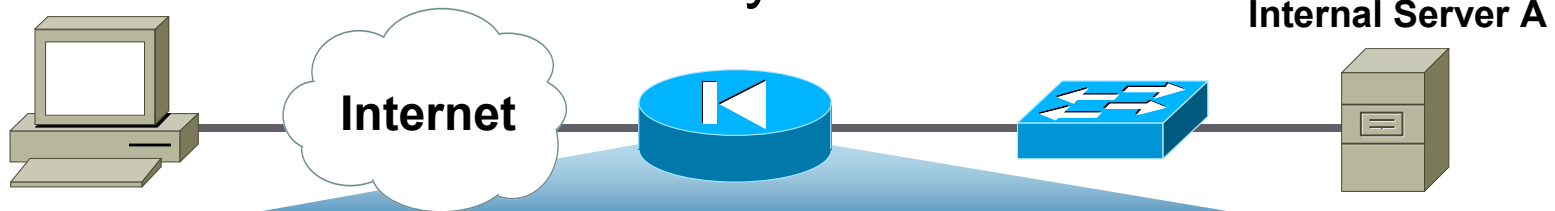
3. => ICMP policy on firewalls needs to change

Equivalent ICMPv6

Border Firewall Transit Policy*



For Your Reference



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded— TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

*RFC 4890

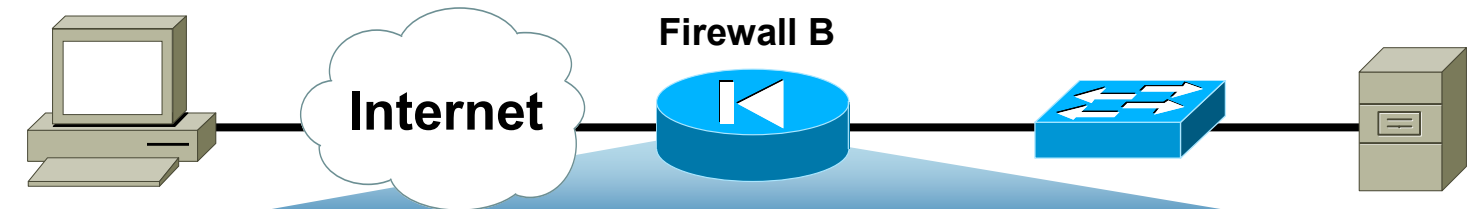
Potential Additional ICMPv6

Border Firewall Receive Policy*



For Your Reference

Internal Server A

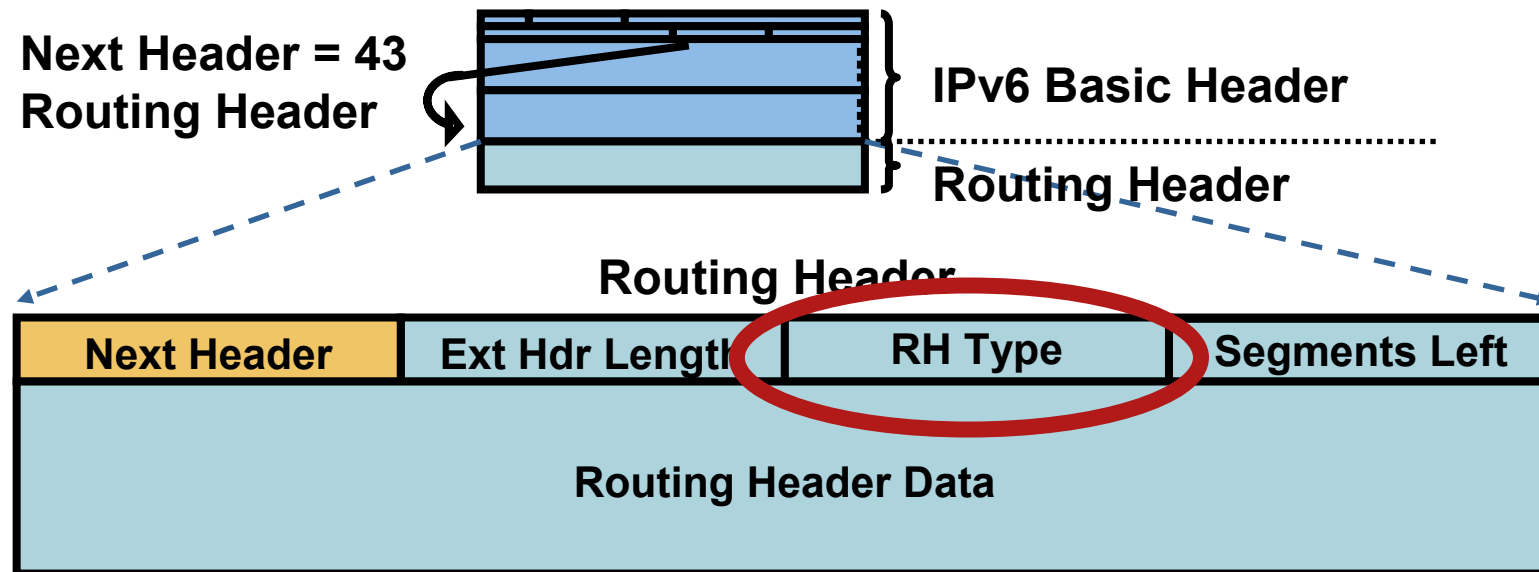


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	0	Parameter Problem

*RFC 4890

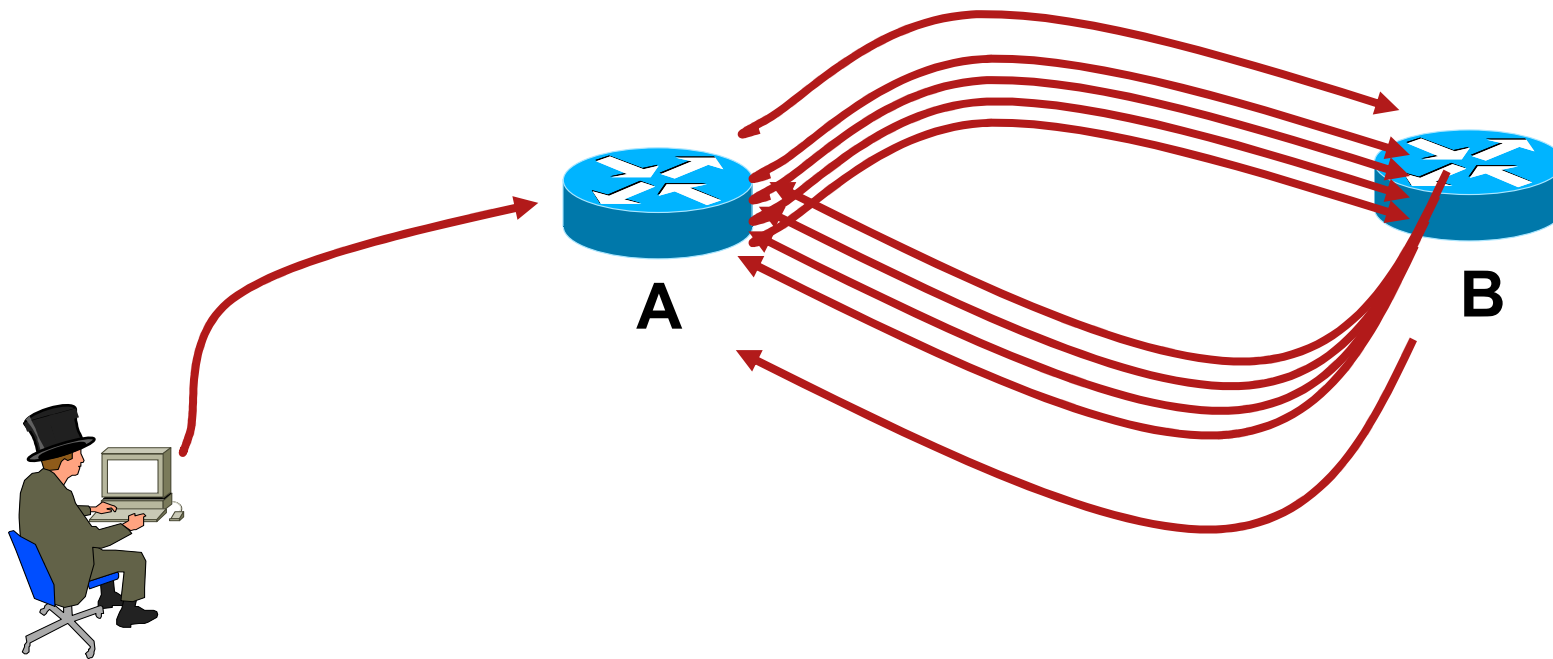
IPv6 Routing Header

1. An extension header
2. Processed by the listed intermediate routers
3. Two types
 - Type 0: similar to IPv4 source routing (multiple intermediate routers)
 - Type 2: used for mobile IPv6



Type 0 Routing Header Issue #2: Amplification Attack

1. What if attacker sends a packet with RH containing
A -> B -> A -> B -> A -> B -> A -> B -> A
2. Packet will loop multiple time on the link R1-R2
3. An amplification attack!



Preventing Routing Header Attacks

1. Apply same policy for IPv6 as for Ipv4:
Block Routing Header type 0
2. Prevent processing at the intermediate nodes
`no ipv6 source-route`
Windows, Linux, MacOS: default setting
3. At the edge
With an ACL blocking routing header
4. RFC 5095 (Dec 2007) RH0 is deprecated
Default IOS will change in 12.5T

ARP Spoofing is now NDP Spoofing: Threats

1. ARP is replaced by Neighbor Discovery Protocol
 - Nothing authenticated
 - Static entries overwritten by dynamic ones
2. Stateless Address Autoconfiguration
 - rogue RA (malicious or not)
 - All nodes badly configured
 - DoS
 - Traffic interception (Man In the Middle Attack)
3. Attack tools exist (from THC – The Hacker Choice)
 - Parasit6
 - Fakerouter6
 - ...



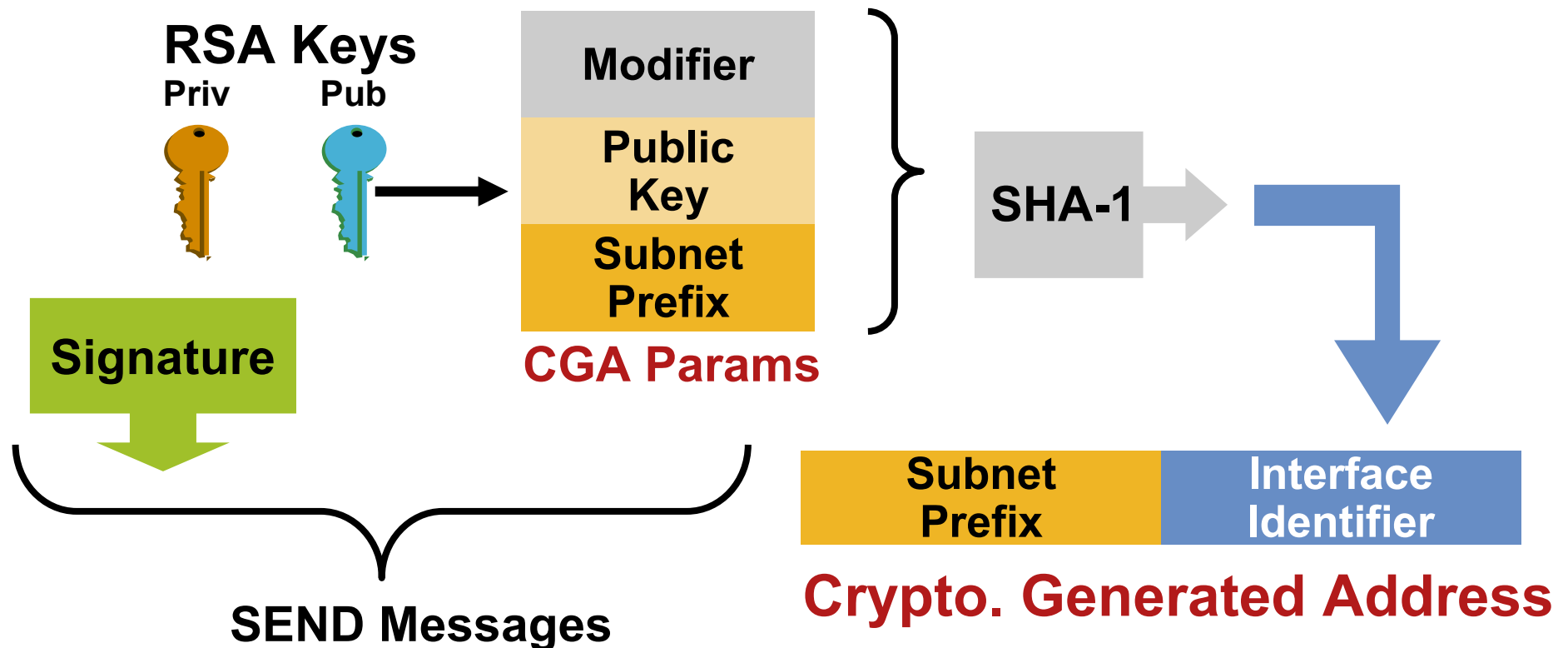
The Hacker's Choice

ARP Spoofing is now NDP Spoofing: Mitigation

- 1. BAD NEWS:** nothing like dynamic ARP inspection for IPv6
Will require new hardware on some platform (7600 should be OK)
Not before end of 2009...
- 2. GOOD NEWS:** Secure Neighbor Discovery
SEND = NDP + crypto
is coming in IOS
But not in Windows Vista, wait for next Windows version...
Crypto means slower...
- 3. Other GOOD NEWS:**
Private VLAN works with IPv6
Port security works with IPv6
801.x works with IPv6
For FTTH & other broadband, DHCP-PD means not need to NDP-proxy

Cryptographically Generated Addresses CGA RFC 3972 (Simplified)

1. Each devices has a RSA key pair (no need for cert)
2. Ultra light check for validity
3. Prevent spoofing a valid CGA address



Secure Neighbor Discovery: Caveats

1. Private/public key pair on all devices for CGA

2. Overhead introduced

Routers have to do many public/private key calculation
(some may be done in advance of use)

=> Potential DoS target

Routers need to keep more state

3. Available:

Unix (DoCoMo)

Cisco IOS 12.4(24)T

4. Microsoft:

no support in Vista, in Windows 2008 (and probably not Windows7)

IPv6 Attacks with Strong IPv4 Similarities

1. Sniffing

Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

2. Application layer attacks

Even with IPsec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPsec will do nothing to prevent

3. Rogue devices

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

4. Man-in-the-Middle Attacks (MITM)

Without IPsec, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

5. Flooding

Flooding attacks are identical between IPv4 and IPv6

IPv6 Stack Vulnerabilities

1. IPv6 stacks are new and could be buggy
2. Some examples

CVE-2008-2476	Oct 2008	FreeBSD OpenBSD NetBSD and others	Lack of validation of NDP messages
CVE-2008-2136	May 2008	Linux	DoS caused by memory leak in IPv6 tunnels
CVE-2008-1153	Mar 2008	IOS	Cisco IOS dual-stack router IPv6 DoS
CVE-2007-4689	Nov 2007	Apple Mac OS X	Packet processing double-free memory corruption
CVE-2007-3038	Aug 2007	Microsoft	Microsoft Windows Vista Teredo interface firewall bypass

By the Way: It Is Real ☹️

IPv6 Hacking Tools

1. Sniffers/packet capture

Snort

TCPdump

Sun Solaris snoop

COLD

Wireshark

Analyzer

Windump

WinPcap



The Hacker's Choice

1. Scanners

IPv6 security scanner

Halfscan6

Nmap

Strobe

Netcat

2. DoS Tools

6tunneldos

4to6ddos

Imps6-tools

3. Packet forgers

Scapy6

SendIP

Packit

Spak6

4. Complete tool

<http://www.thc.org/thc-ipv6/>

Specific IPv6 Issues



Issues Applicable only to IPv6

IPv4 to IPv6 Transition Challenges

1. 16+ methods, possibly in combination
2. Dual stack
 - Consider security for both protocols
 - Cross v4/v6 abuse
 - Resiliency (shared resources)
3. Tunnels
 - Bypass firewalls (protocol 41 or UDP)
 - Can cause asymmetric traffic (hence breaking stateful firewalls)

Dual Stack Host Considerations

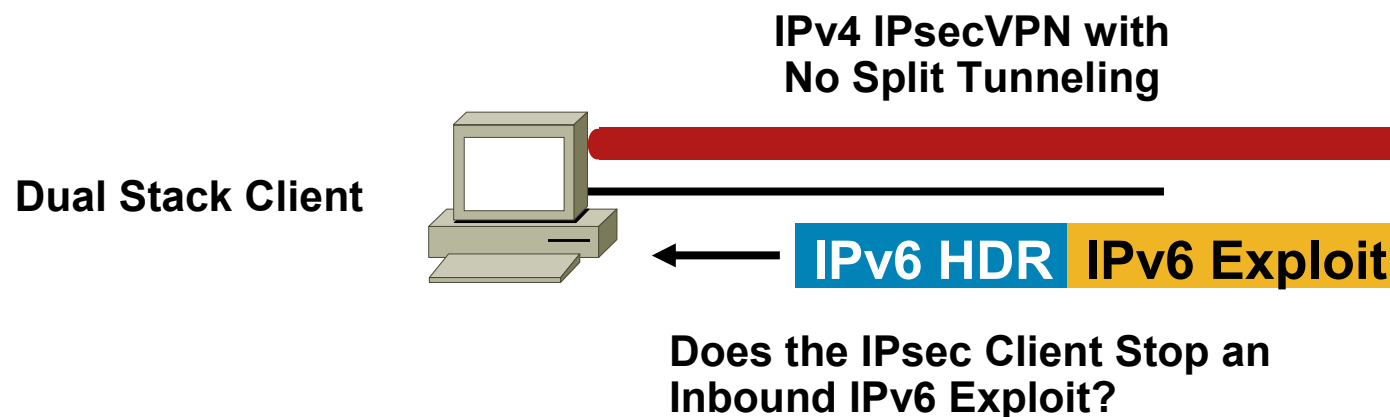
1. Host security on a dual-stack device

Applications can be subject to attack on both IPv6 and IPv4

Fate sharing: as secure as the least secure stack...

2. Host security controls should block and inspect traffic from both IP versions

Host intrusion prevention, personal firewalls, VPN clients, etc.



Dual Stack with Enabled IPv6 by Default

1. Your host:
 - IPv4 is protected by your favorite personal firewall...
 - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
2. Your network:
 - Does not run IPv6
3. Your assumption:
 - I'm safe
4. Reality
 - You are **not** safe
 - Attacker sends Router Advertisements
 - Your host configures silently to IPv6
 - You are now under IPv6 attack
5. => **Probably time to think about IPv6 in your network**

Enabling IPv6 on a Remote Host (in this Case Mac OS/X)

2) Hacker: I'm the Router

1) Dual-Stack MacOS:
any IPv6 Router?

	Destination	Protocol	Info
3	ff02::1:ff00:22	ICMPv6	Neighbor solicitation
4	ff02::1:ff00:22	ICMPv6	Neighbor solicitation
5	ff02::1	ICMPv6	Router advertisement
6	ff02::1	ICMPv6	Router advertisement
7	ff02::2	ICMPv6	Router solicitation
8	ff02::1	ICMPv6	Router advertisement
9	ff02::1:ff38:c874	ICMPv6	Neighbor solicitation
10	ff02::2:52a6:75e2	ICMPv6	Multicast listener report
11	ff02::2:52a6:75e2	ICMPv6	Multicast listener report
12	ff02::2	ICMPv6	Multicast listener done
13	ff02::1	ICMPv6	Router advertisement
14	ff02::1	ICMPv6	Router advertisement
15	ff02::1:ff38:c874	ICMPv6	Neighbor solicitation

Frame 9 (78 bytes on wire, 78 bytes captured)	
Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst: IPv6-Neighbor-Discovery_ff02::1:ff38:c874	
Internet Protocol Version 6	
Internet Control Message Protocol v6	
Type:	135 (Neighbor solicitation)
Code:	0
Checksum:	0x48da [correct]
Target:	2001:db8:dead:0:20d:93ff:fe38:c874

4) The Full IPv6 Address of the MacOS

3) Newly Enabled IPv6 MacOS does DAD

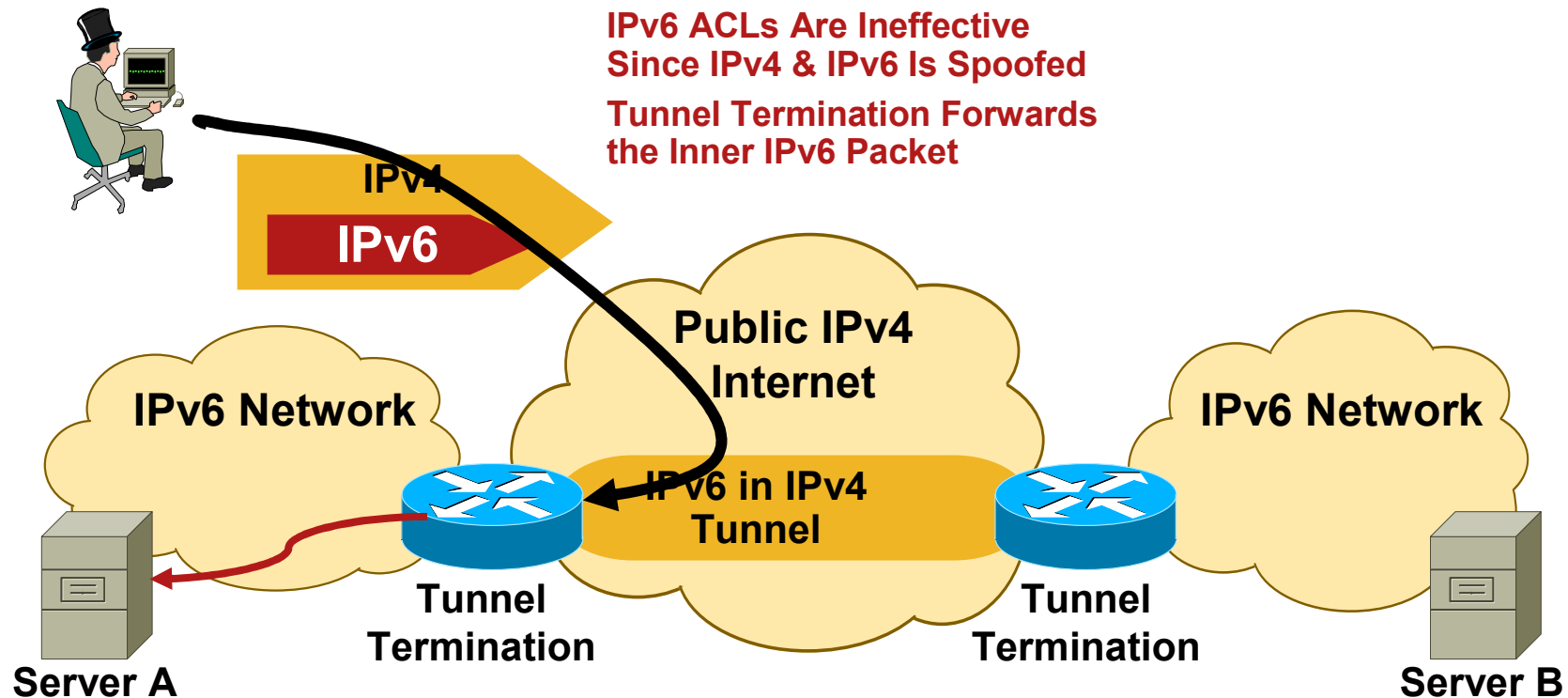
IPv6 Tunneling Summary

1. RFC 1933/2893 configured and automatic tunnels
2. RFC 2401 IPsec tunnel
3. RFC 2473 IPv6 generic packet tunnel
4. RFC 2529 6over4 tunnel
5. RFC 3056 6to4 tunnel
6. RFC 5214 ISATAP tunnel
7. MobileIPv6 (uses RFC2473)
8. RFC 4380 Teredo tunnels

1. Only allow authorized endpoints to establish tunnels
2. Static tunnels are deemed as “more secure,” but less scalable
3. Automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks
4. These tools have the **same risk** as IPv4, just new avenues of exploitation
5. Automatic IPv6 over IPv4 tunnels could be secured by IPv4 IPsec

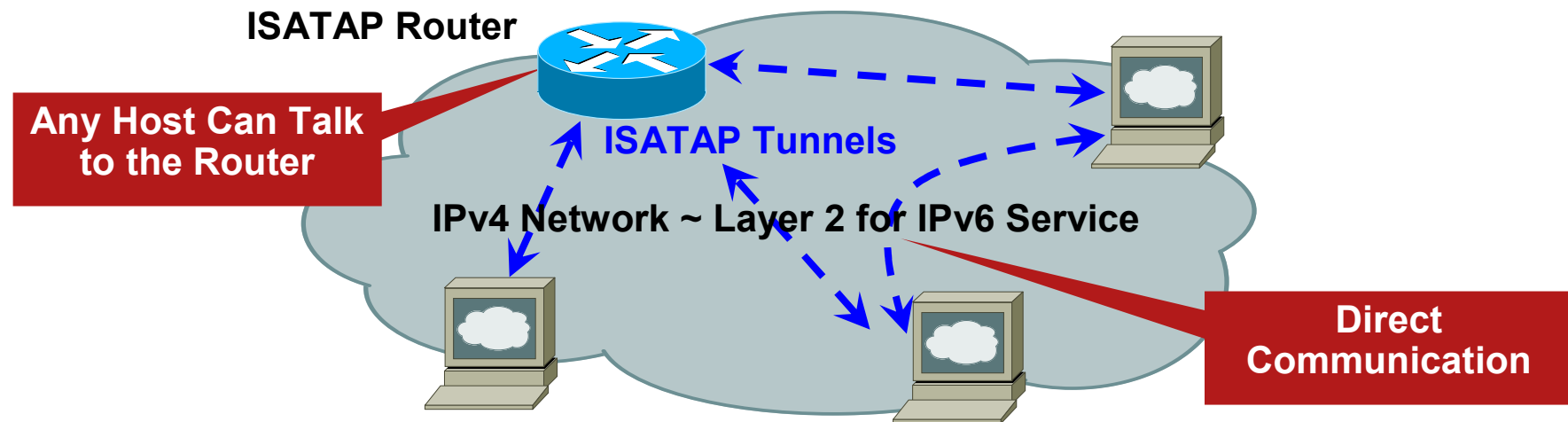
L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

1. Most IPv4/IPv6 transition mechanisms have no authentication built in
2. => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses

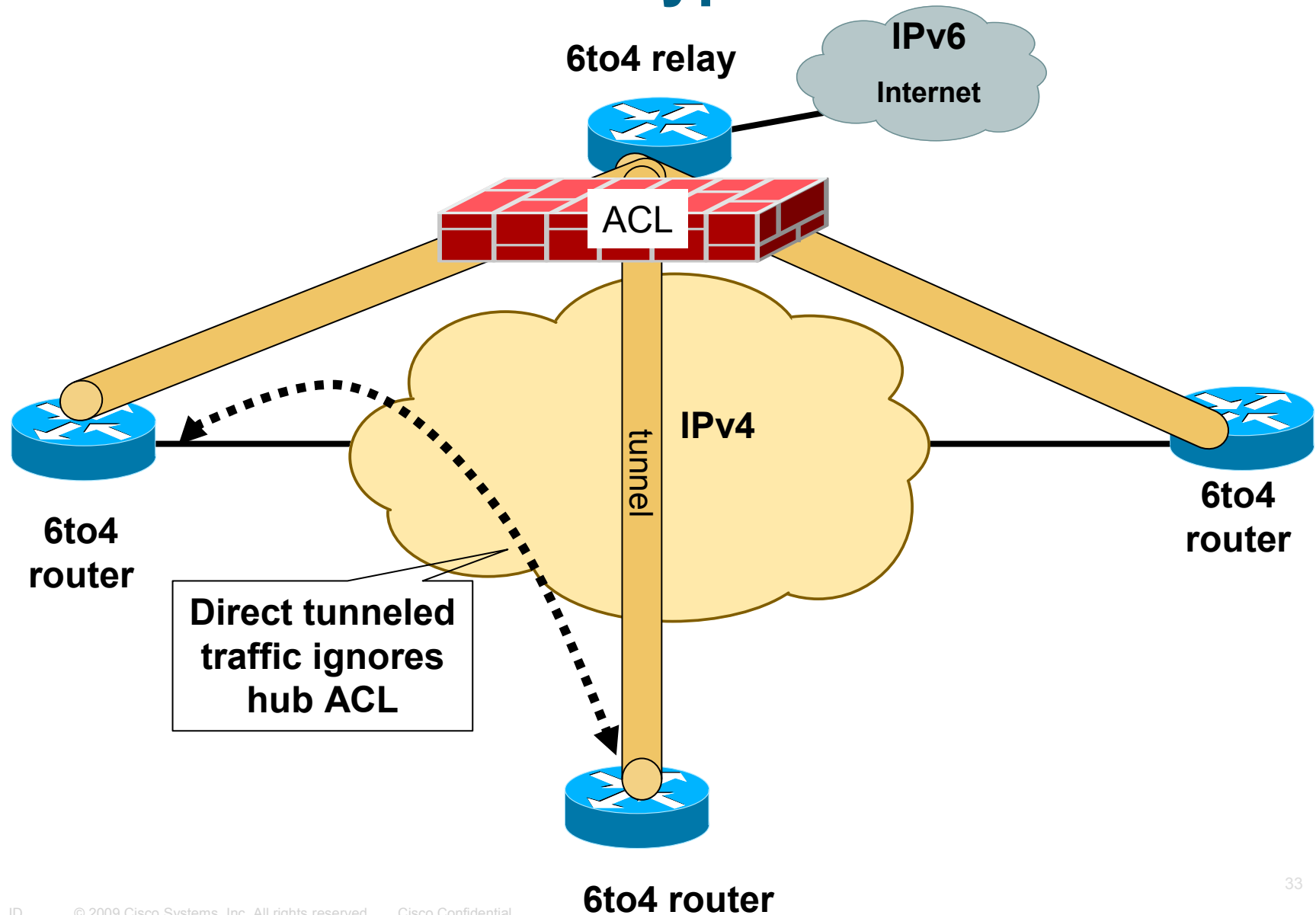


Transition Threats—ISATAP

1. Unauthorized tunnels—firewall bypass (protocol 41)
2. IPv4 infrastructure looks like a Layer 2 network to ALL ISATAP hosts in the enterprise
This has implications on network segmentation and network discovery
3. No authentication in ISATAP—rogue routers are possible
Windows default to *isatap.example.com*
4. Ipv6 addresses can be guessed based on IPv4 prefix



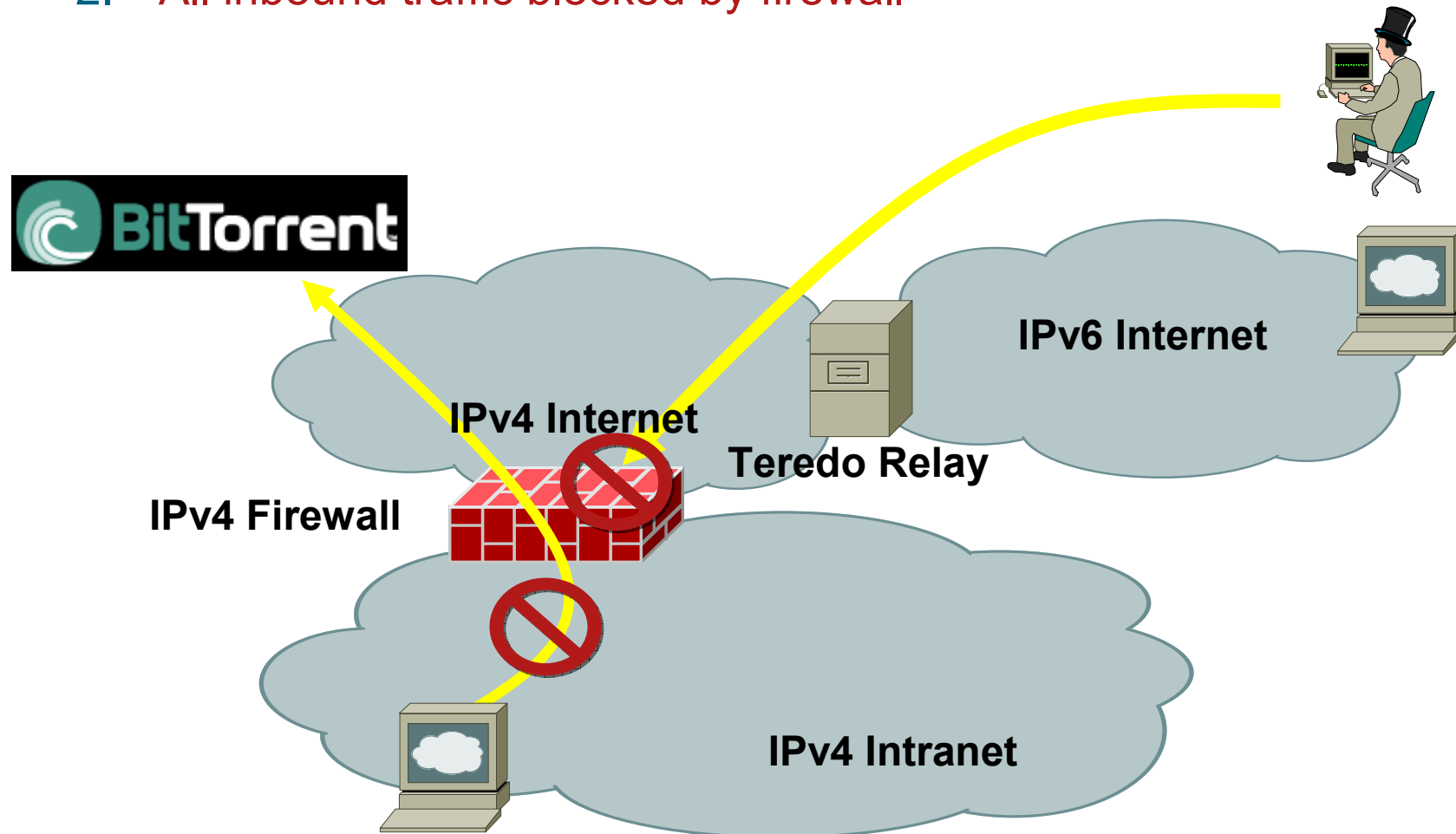
6to4/ISATAP Tunnels Bypass ACL



Teredo Tunnels (1/3)

Without Teredo: Controls Are in Place

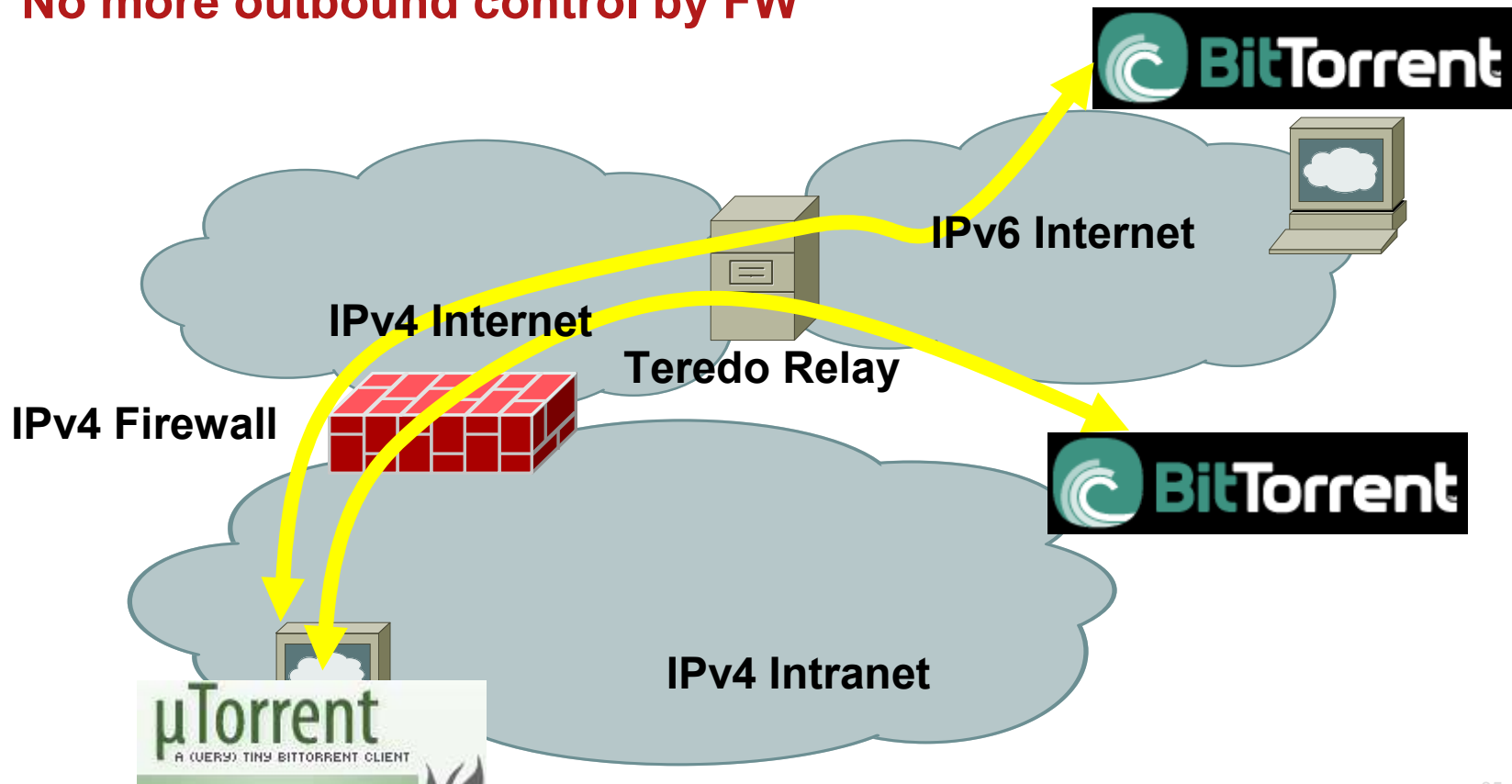
1. All outbound traffic inspected: e.g., P2P is blocked
2. All inbound traffic blocked by firewall



Teredo Tunnels (2/3)

No More Outbound Control

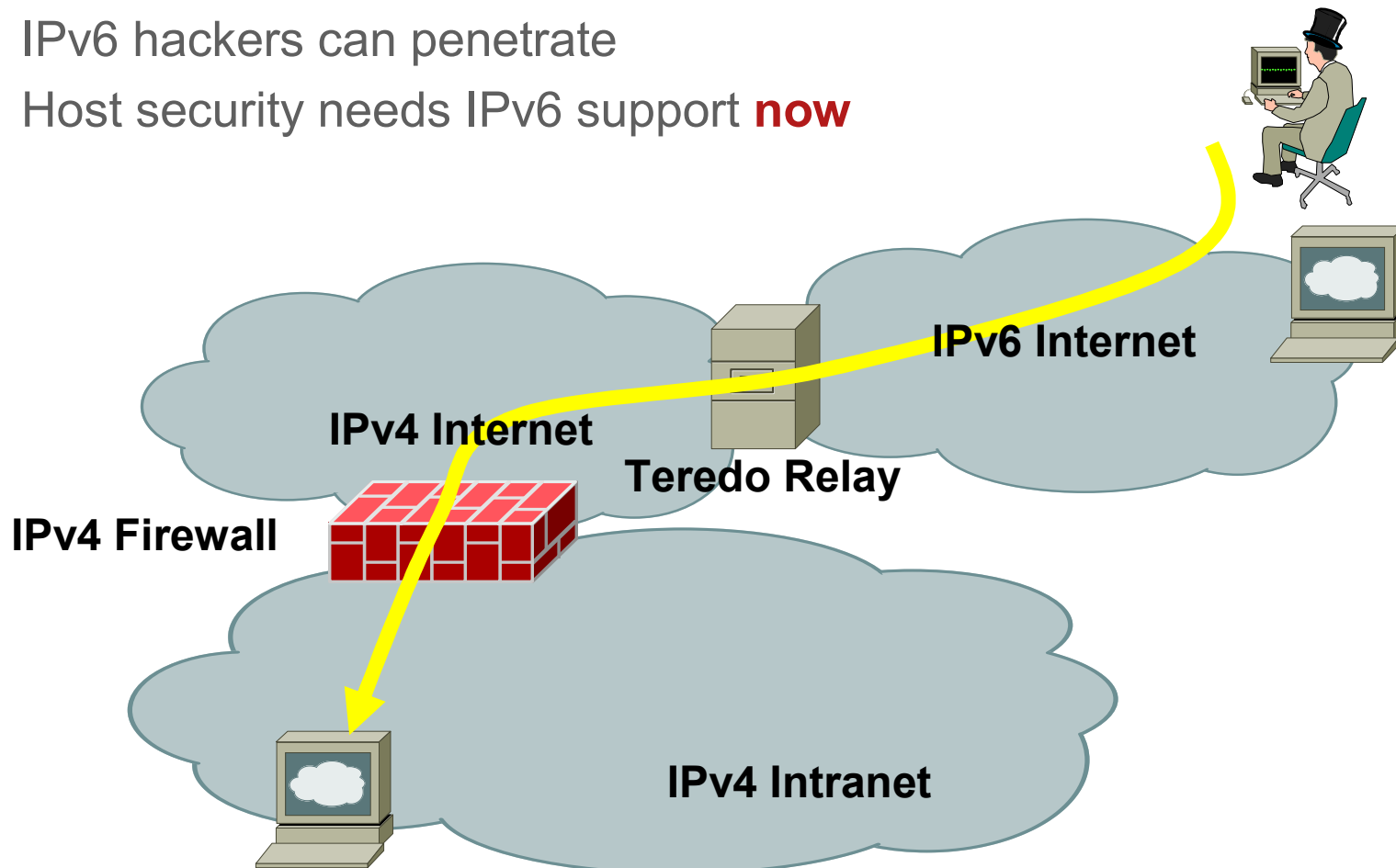
1. Internal users wants to get P2P over IPv6
2. Configure the Teredo tunnel (already enabled by default!)
3. FW just sees IPv4 UDP traffic (may be on port 53)
4. **No more outbound control by FW**



Teredo Tunnels (3/3)

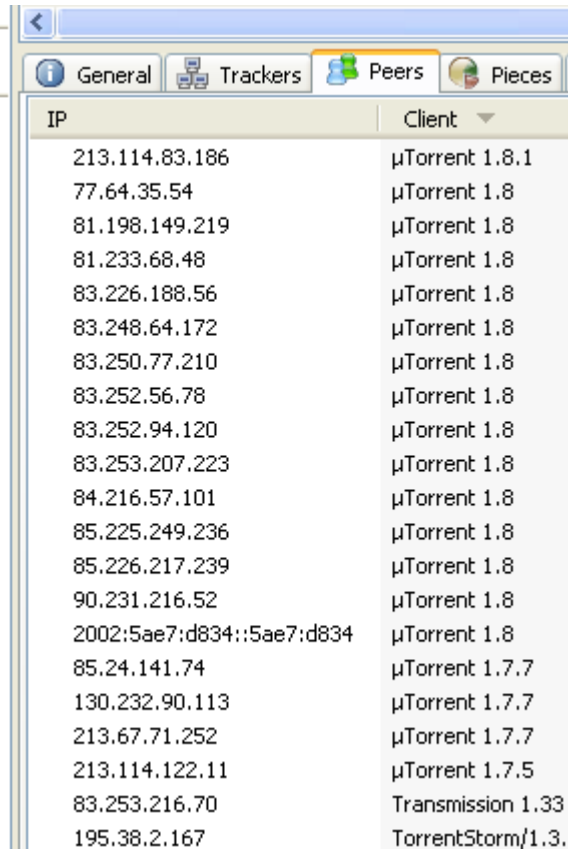
No More Outbound Control

1. **Inbound** connections are allowed
2. IPv4 firewall unable to control
3. IPv6 hackers can penetrate
4. Host security needs IPv6 support **now**



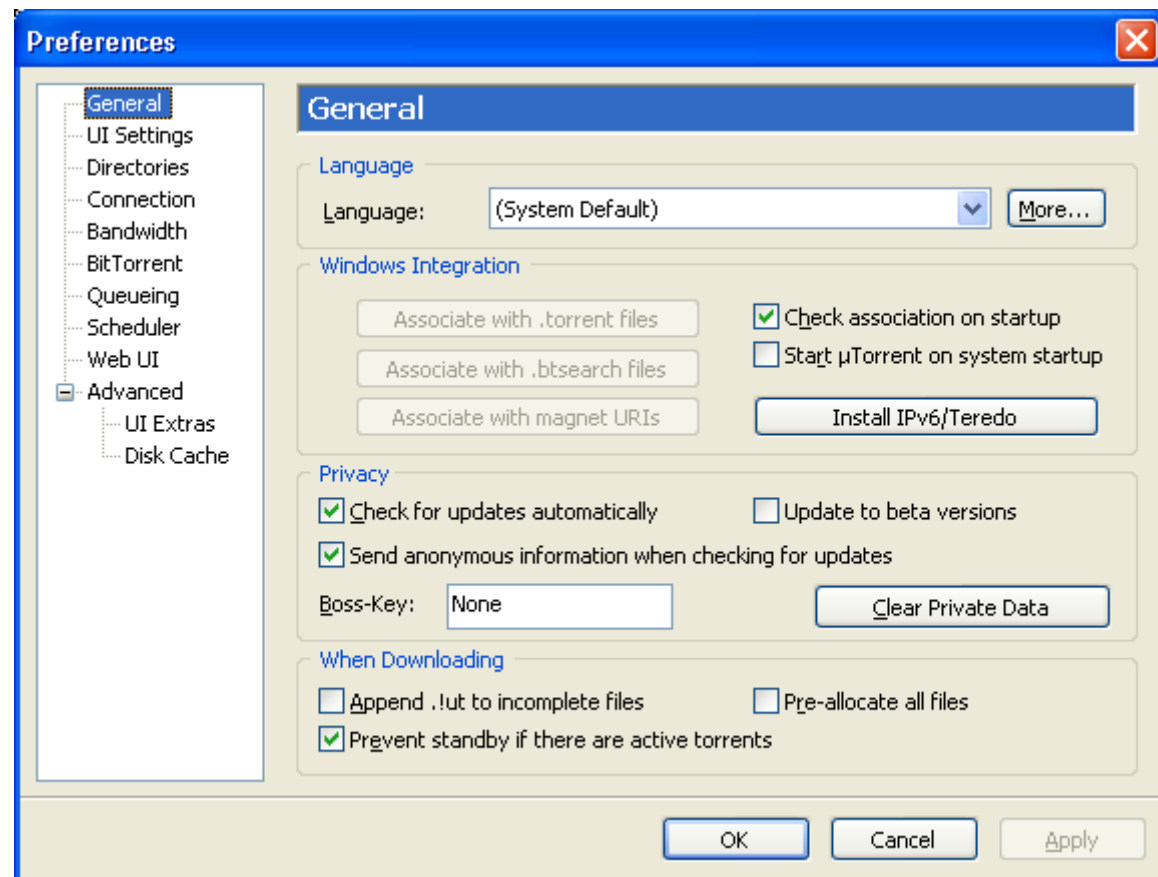
Is it real?

May be uTorrent 1.8 (released Aug 08)



IP	Client
213.114.83.186	µTorrent 1.8.1
77.64.35.54	µTorrent 1.8
81.198.149.219	µTorrent 1.8
81.233.68.48	µTorrent 1.8
83.226.188.56	µTorrent 1.8
83.248.64.172	µTorrent 1.8
83.250.77.210	µTorrent 1.8
83.252.56.78	µTorrent 1.8
83.252.94.120	µTorrent 1.8
83.253.207.223	µTorrent 1.8
84.216.57.101	µTorrent 1.8
85.225.249.236	µTorrent 1.8
85.226.217.239	µTorrent 1.8
90.231.216.52	µTorrent 1.8
2002:5ae7:d834::5ae7:d834	µTorrent 1.8
85.24.141.74	µTorrent 1.7.7
130.232.90.113	µTorrent 1.7.7
213.67.71.252	µTorrent 1.7.7
213.114.122.11	µTorrent 1.7.5
83.253.216.70	Transmission 1.33
195.38.2.167	TorrentStorm/1.3.

Test August 08, 1 IPv6 (6to4) out of 35...
Via PEX = peer exchange (not via a IPv6 tracker)



Can We Block Rogue Tunnels?

1. Rogue tunnels by naïve users:

Sure, block IP protocol 41 and UDP/3544

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
```

2. 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)

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

4. **Or disable IPv6 on Windows through GPO or CSA 6.0**

Enforcing a Security Policy



Cisco IOS IPv6 ACL

A Trivial Example

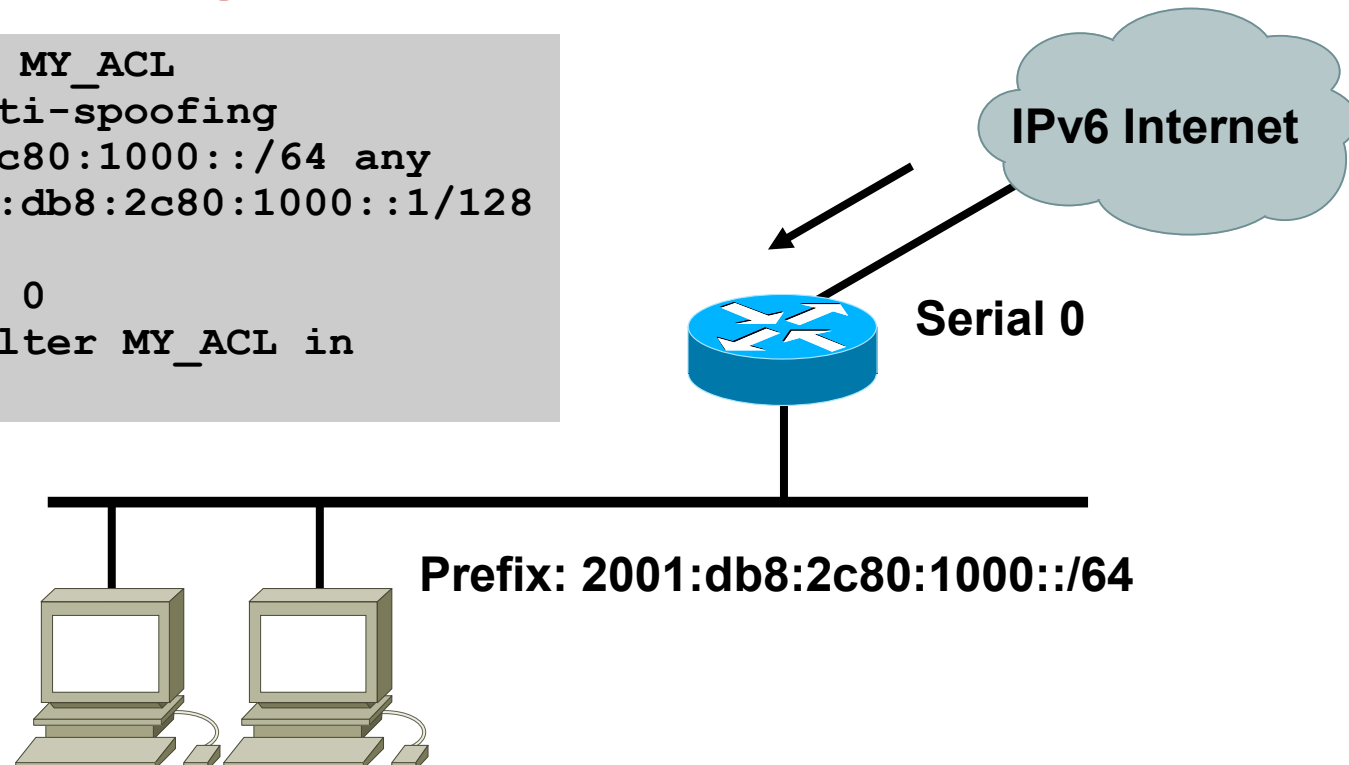
Filtering inbound traffic to one specific destination address

☑ 2001:db8:2c80:1000::1

⊘ others

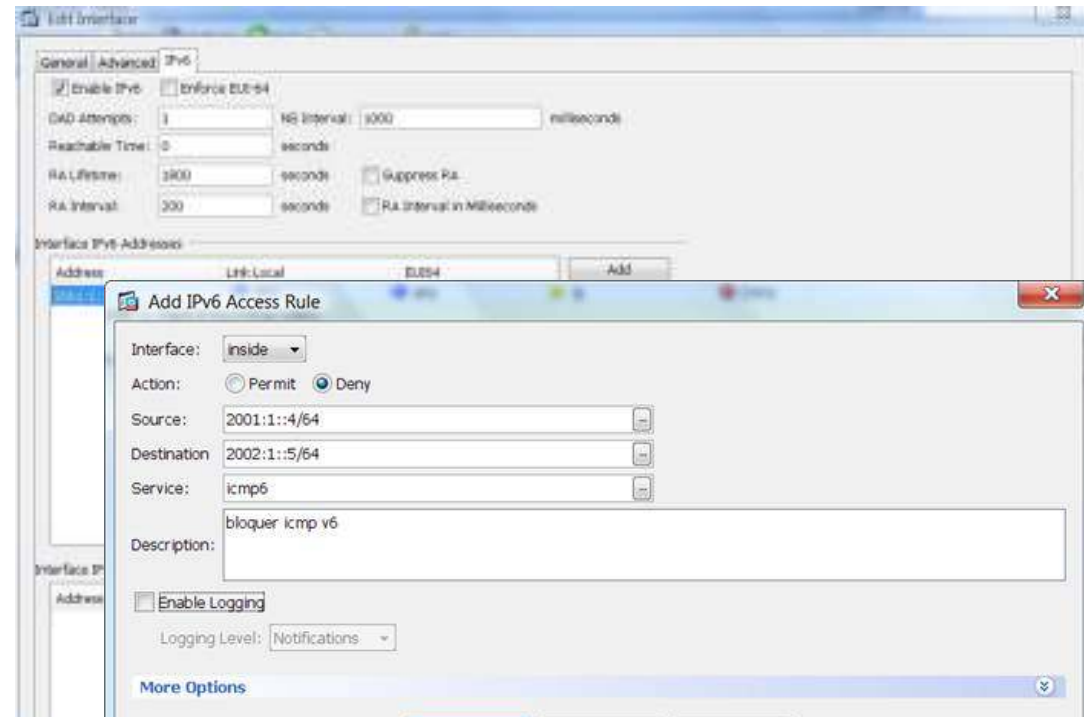
```
ipv6 access-list MY_ACL
  remark basic anti-spoofing
  deny 2001:db8:2c80:1000::/64 any
  permit any 2001:db8:2c80:1000::1/128

interface Serial 0
  ipv6 traffic-filter MY_ACL in
```



ASA Firewall IPv6 Support

1. Since version 7.0 (April 2005)
2. Dual-stack, IPv6 only, IPv4 only
3. Extended IP ACL with stateful inspection
4. Application awareness
HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
5. uRPF and v6 Frag (disabled)
6. IPv6 header security
7. Management access IPv6
Telnet, SSH, HTTPS
8. Caveat: no fail-over



Configuration > Firewall > Access Rules

Filter: Source or Destination is

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
inside (2 implicit incoming rules)									
1		any	Any less secure ...	ip	Permit				Implicit rule: Permit all
2		any	any	ip	Deny				Implicit rule
inside IPv6 (3 incoming rules)									
1	✓	2001:1::/64	2002:1::/64	icmp6	Deny		Notif...		bloquer icmp v6
2	✓	2001:2::/64	2002:5::/64	6over4	Permit				
3		any	any	ip	Deny				Implicit rule
outside (1 implicit incoming rules)									
1		any	any	ip	Deny				Implicit rule
outside IPv6 (1 implicit incoming rules)									
1		any	any	ip	Deny				Implicit rule

Other Security Products

1. ASA Firewall

Since version 7.0

Flexibility: Dual stack, IPv6 only, IPv4 only

SSL VPN for IPv6 (ASA 8.0)

No header extension parsing, no stateful-failover (coming)

2. FWSM

IPv6 in software...

3. Cisco Security Agent

Since version 6.0 for IPv6 network protection

4. IPS

Since 6.2 (November 2008)

Enterprise Deployment: Secure IPv6 Connectivity



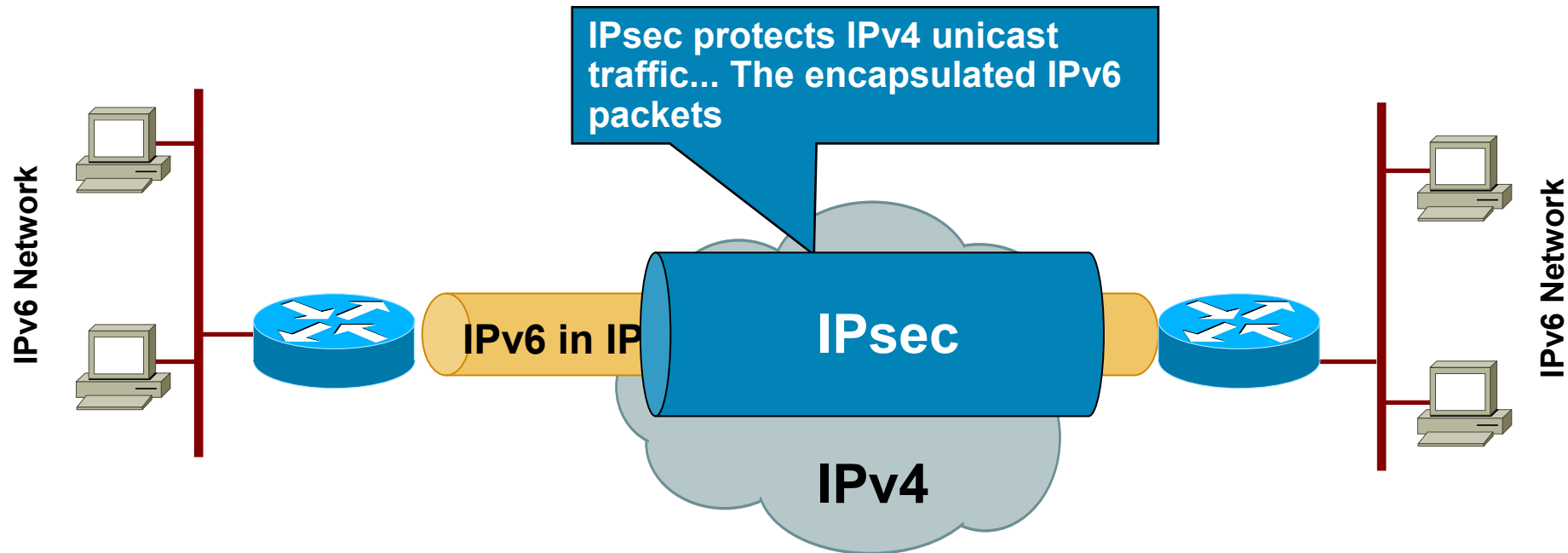
How to Secure IPv6 over the WAN

Secure IPv6 over IPv4/6 Public Internet

1. No traffic sniffing
2. No traffic injection
3. No service theft

Public Network	Site 2 Site	Remote Access
IPv4	1.6in4/GRE Tunnels Protected by IPsec 2.DMVPN 12.4(20)T	1.ISATAP Protected by RA IPsec 2.SSL VPN Client AnyConnect
IPv6	IPsec VTI 12.4(6)T	N/A

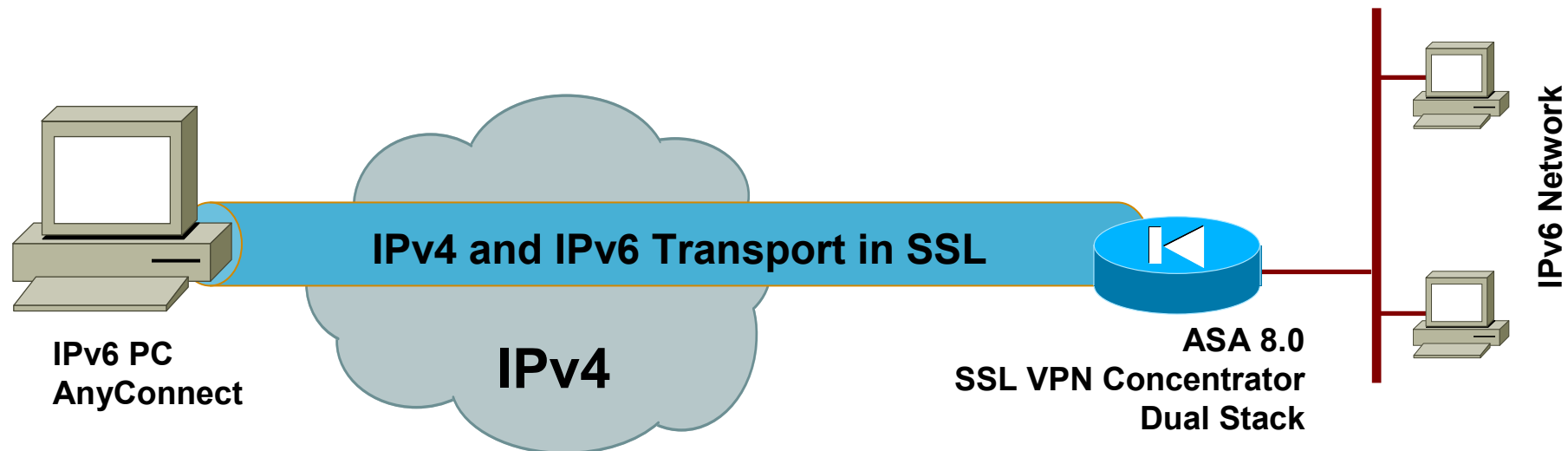
Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec



GRE tunnel can be used to transport both IPv4 and IPv6 in the same tunnel

See reference slides for more details

Secure RA IPv6 Traffic over IPv4 Public Network: AnyConnect SSL VPN Client



IPsec with NAT-T can traverse NAT
ISATAP encapsulates IPv6 into IPv4

Conclusion



Key Take Away

1. So, nothing really new in IPv6
 - Lack of operation experience may hinder security for a while
2. Security enforcement is possible
 - Control your IPv6 traffic as you do for IPv4
3. Leverage IPsec to secure IPv6 when suitable
4. Beware of the IPv6 latent threat: ***your network may be vulnerable to IPv6 attacks***

Q and A



