# IPv6 Security

Eric Vyncke
Distinguished Engineer
Cisco System, CTO/Consulting Engineering

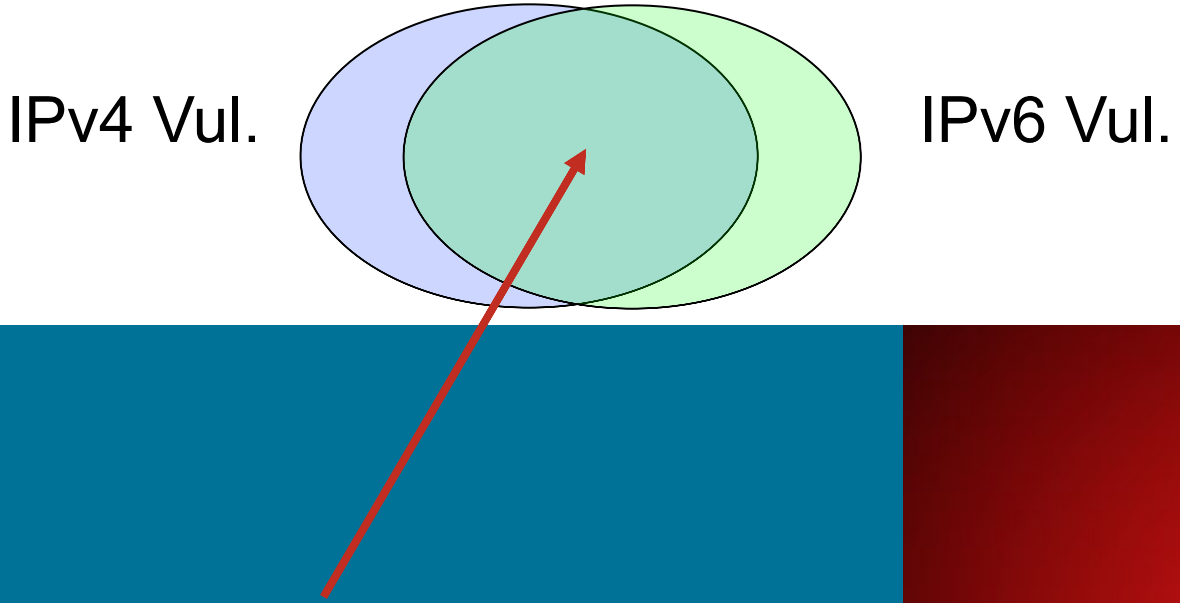
# Agenda

- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6

  IPsec everywhere, dual-stack, tunnels and 6VPE
- Enforcing a Security Policy in IPv6

  ACL, Firewalls and IPS
- Enterprise Secure Deployment

  Secure IPv6 transport over public network



IPv4 Vul.

IPv6 Vul.

# Shared Issues

Security Issues Shared by IPv4 and IPv6

# Reconnaissance in IPv6
## Scanning Methods Are Likely to Change

- ***Default subnets in IPv6 have $2^{64}$ addresses***

  ***10 Mpps = more than 50 000 years***

- 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

- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan

# Viruses and Worms in IPv6

- Viruses and email, IM worms: IPv6 brings no change
- Other worms:

  IPv4: reliance on network scanning

  IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

# IPv6 Bogon Filtering Anti-Spoofing

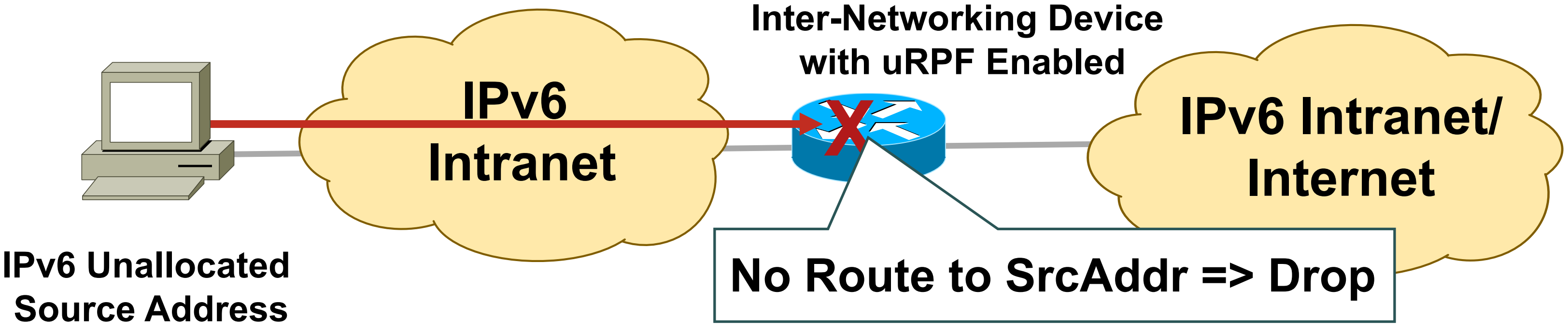
- In IPv4, easier to block bogons than to permit non-bogons
- In IPv6, in the beginning when a small amount of top-level aggregation identifiers (TLAs) has been allocated

  Easier to permit non-bogons

  Now, more complex: http://www.cymru.com/Bogons/ipv6.txt

- Now IPv6 is in a similar situation as IPv4

  => Same technique = uRPF


Inter-Networking Device with uRPF Enabled
IPv6 Intranet
IPv6 Intranet/ Internet
IPv6 Unallocated Source Address
No Route to SrcAddr => Drop

# ICMPv4 vs. ICMPv6

- Significant changes
- 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 |

- => ICMP policy on firewalls needs to change

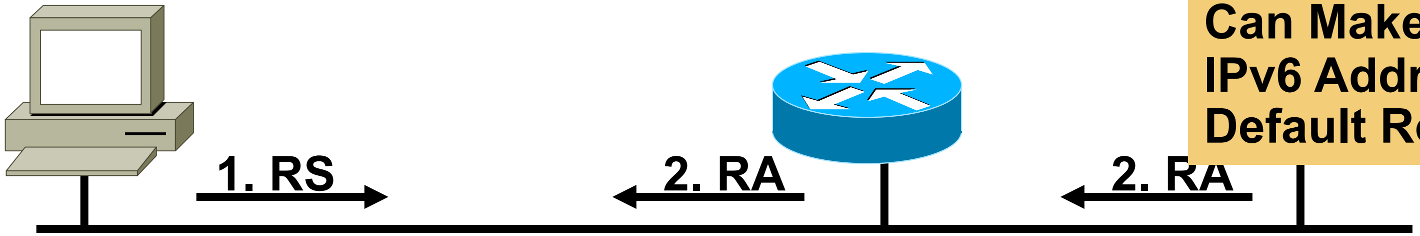
# Neighbor Discovery Issue#1 Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

**RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)**

**Attack Tool: fake_router6**

**Can Make Any IPv6 Address the Default Router**



1. RS:

   Src = ::

   Dst = All-Routers multicast Address

   ICMP Type = 133

   Data = Query: please send RA

2. RA:

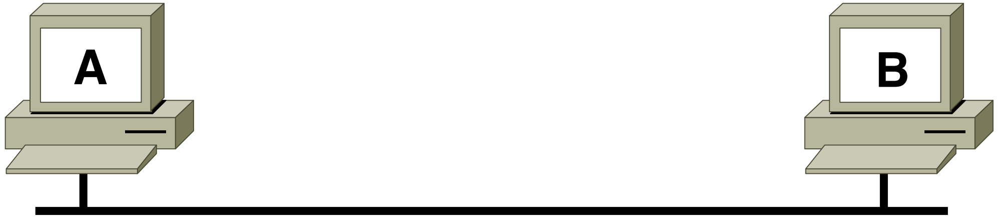
   Src = Router Link-local Address

   Dst = All-nodes multicast address

   ICMP Type = 134

   Data= options, prefix, lifetime, autoconfig flag

# 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**

**=> Very similar to ARP**

**Attack Tool:**
**Parasite6**
**Answer to all NS, Claiming to Be All Systems in the LAN...**

# ARP Spoofing is now NDP Spoofing: Mitigation

- **BAD NEWS**: nothing like dynamic ARP inspection for IPv6
  - Will require new hardware on some platforms
  - First phase of First Hop Security available since Summer 2010
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7
  - Crypto means slower...
- 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

# 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 is supposed to rely on transport mode IPSec
- RIPng, PIM also rely on IPSec
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPSec to secure protocols such as OSPFv3 and RIPng

# 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

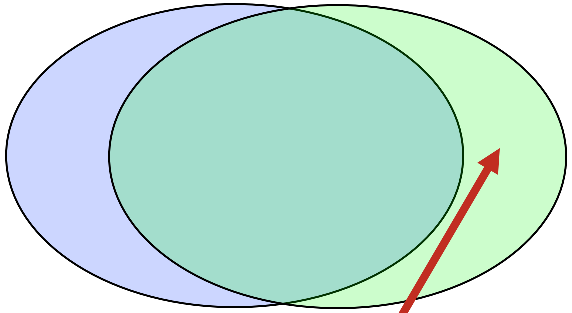
  Flooding attacks are identical between IPv4 and IPv6

# By the Way: It Is Real ☹
# IPv6 Hacking Tools

## Let the Games Begin

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap

- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6
- Complete tool
  - http://www.thc.org/thc-ipv6/



IPv4 Vul.

IPv6 Vul.

# Specific IPv6 Issues

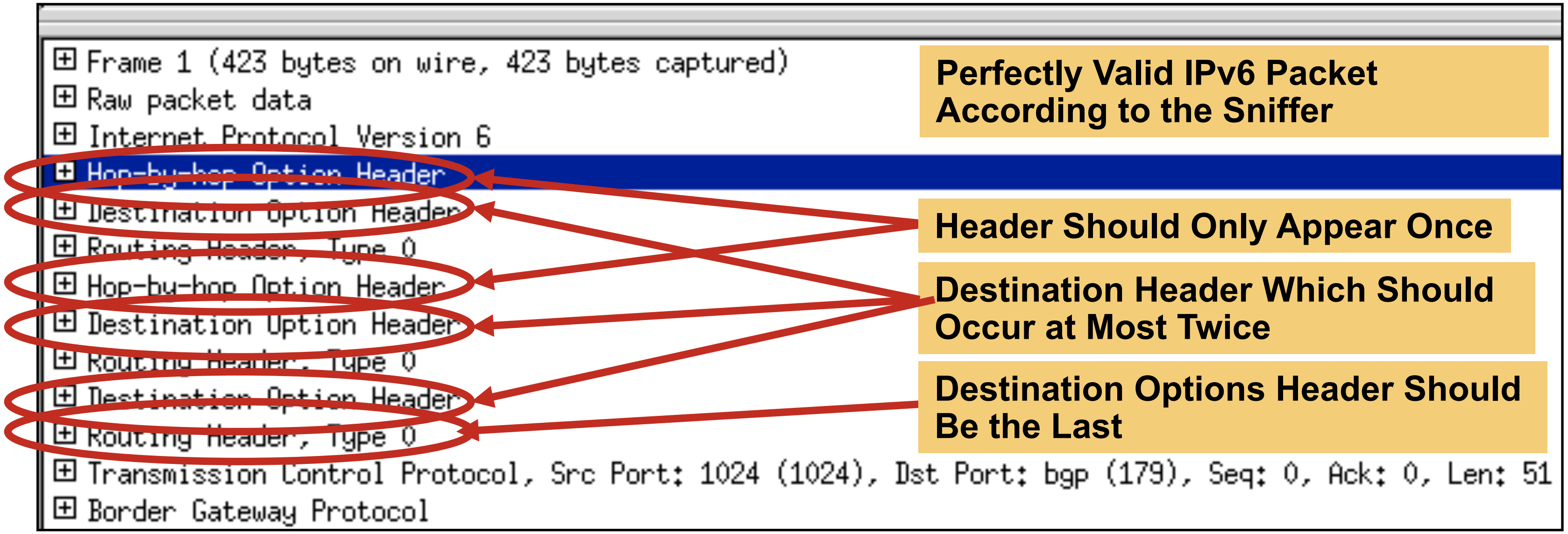
Issues Applicable only to IPv6

# 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?



```
⊞ Frame 1 (423 bytes on wire, 423 bytes captured)
⊞ Raw packet data
⊞ Internet Protocol Version 6
⊞ 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), Dst Port: bgp (179), Seq: 0, Ack: 0, Len: 51
⊞ Border Gateway Protocol
```

Perfectly Valid IPv6 Packet According to the Sniffer

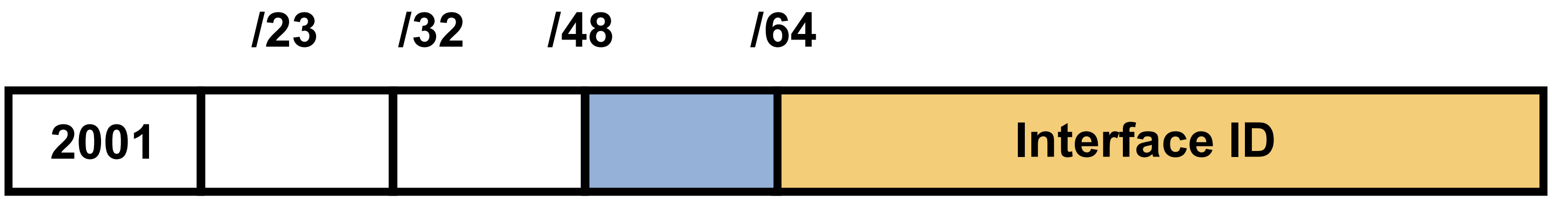
Header Should Only Appear Once

Destination Header Which Should Occur at Most Twice

Destination Options Header Should Be the Last

See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

# IPv6 Privacy Extensions (RFC 3041)



- 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)**

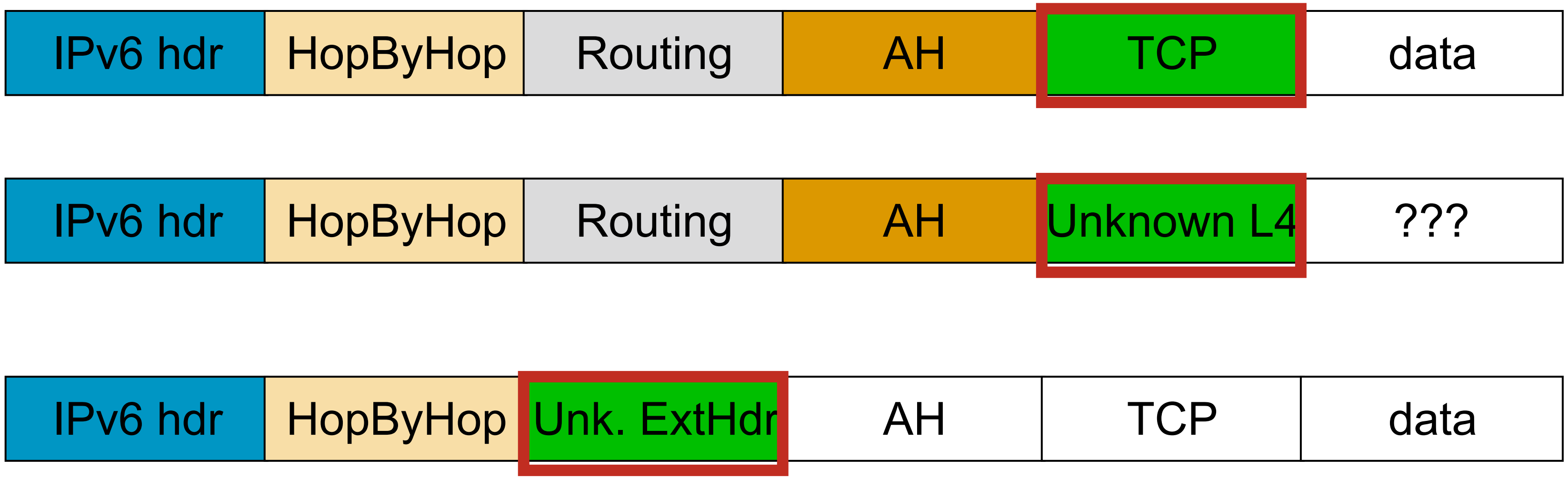
# Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6

  Skip all known extension header

  Until either known layer 4 header found => **SUCCESS**

  Or unknown extension header/layer 4 header found... => **FAILURE**



IPv6 hdr | HopByHop | Routing | AH | TCP | data

IPv6 hdr | HopByHop | Routing | AH | Unknown L4 | ???

IPv6 hdr | HopByHop | Unk. ExtHdr | AH | TCP | data

# The IPsec Myth:
# IPsec End-to-End will Save the World

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...

    Interesting **scalability** issue ($n^2$ issue with IPsec)

    Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall

        IOS 12.4(20)T can parse the AH

    Network **telemetry is blinded**: NetFlow of little use

    Network **services hindered**: what about QoS?

**Recommendation:** do not use IPsec end to end within an administrative domain.
**Suggestion:** Reserve IPsec for residential or hostile environment or high profile targets.

# 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

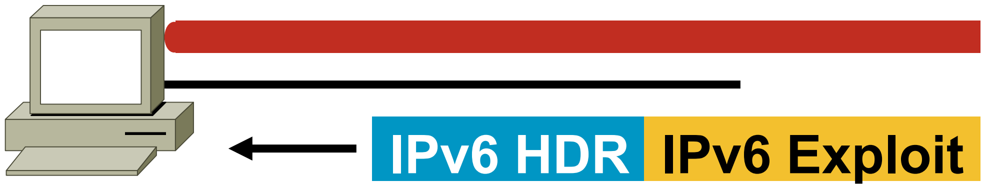
  **Fate sharing**: as secure as the least secure stack...

- 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**

**Dual Stack Client**



**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 (Vista, 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

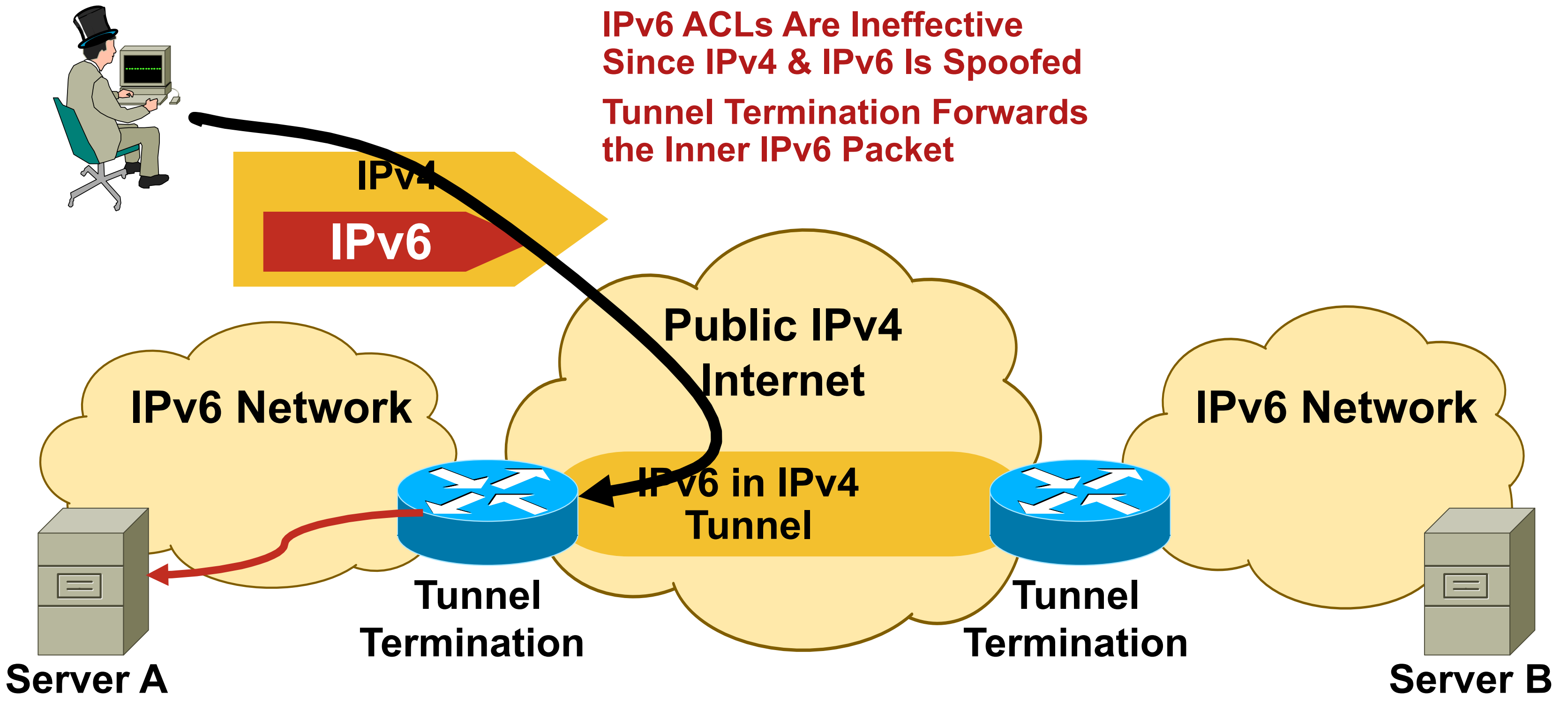
# IPv6 Tunneling Summary

- RFC 1933/2893 configured and automatic tunnels
- RFC 2401 IPSec tunnel
- RFC 2473 IPv6 generic packet tunnel
- RFC 2529 6over4 tunnel
- RFC 3056 6to4 tunnel
- RFC 5214 ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- RFC 4380 Teredo tunnels
- RFC 5569 6RD

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

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

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



IPv6 ACLs Are Ineffective Since IPv4 & IPv6 Is Spoofed

Tunnel Termination Forwards the Inner IPv6 Packet

# TEREDO?

- Teredo navalis

  A shipworm drilling holes
  in boat hulls

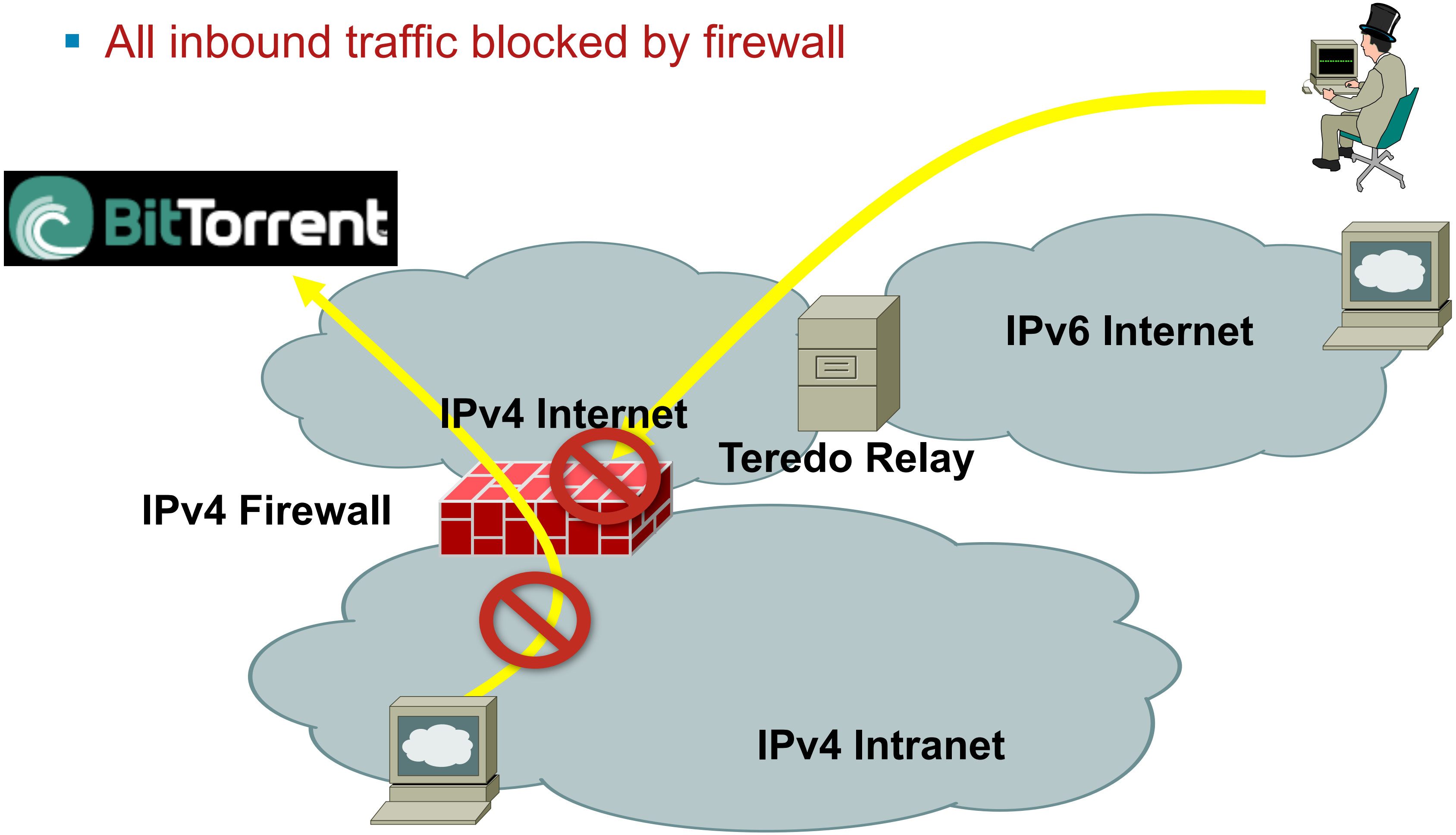
- Teredo Microsoftis

  IPv6 in IPv4 punching holes
  in NAT devices

Source: United States Geological Survey

# Teredo Tunnels (1/3)
## Without Teredo: Controls Are in Place

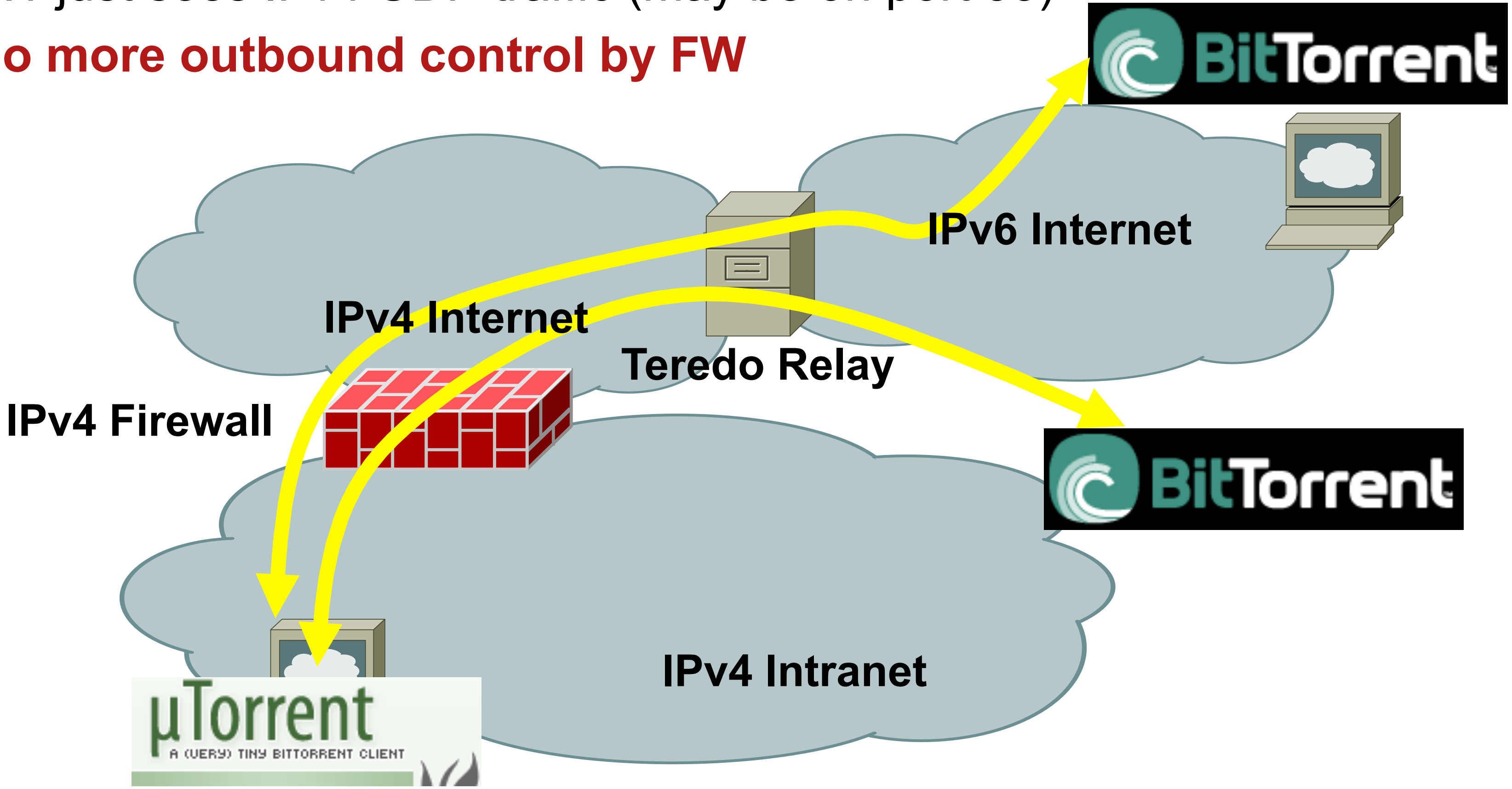
- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall



# Teredo Tunnels (2/3)
## No More Outbound Control

Teredo threats—IPv6 over UDP (port 3544)

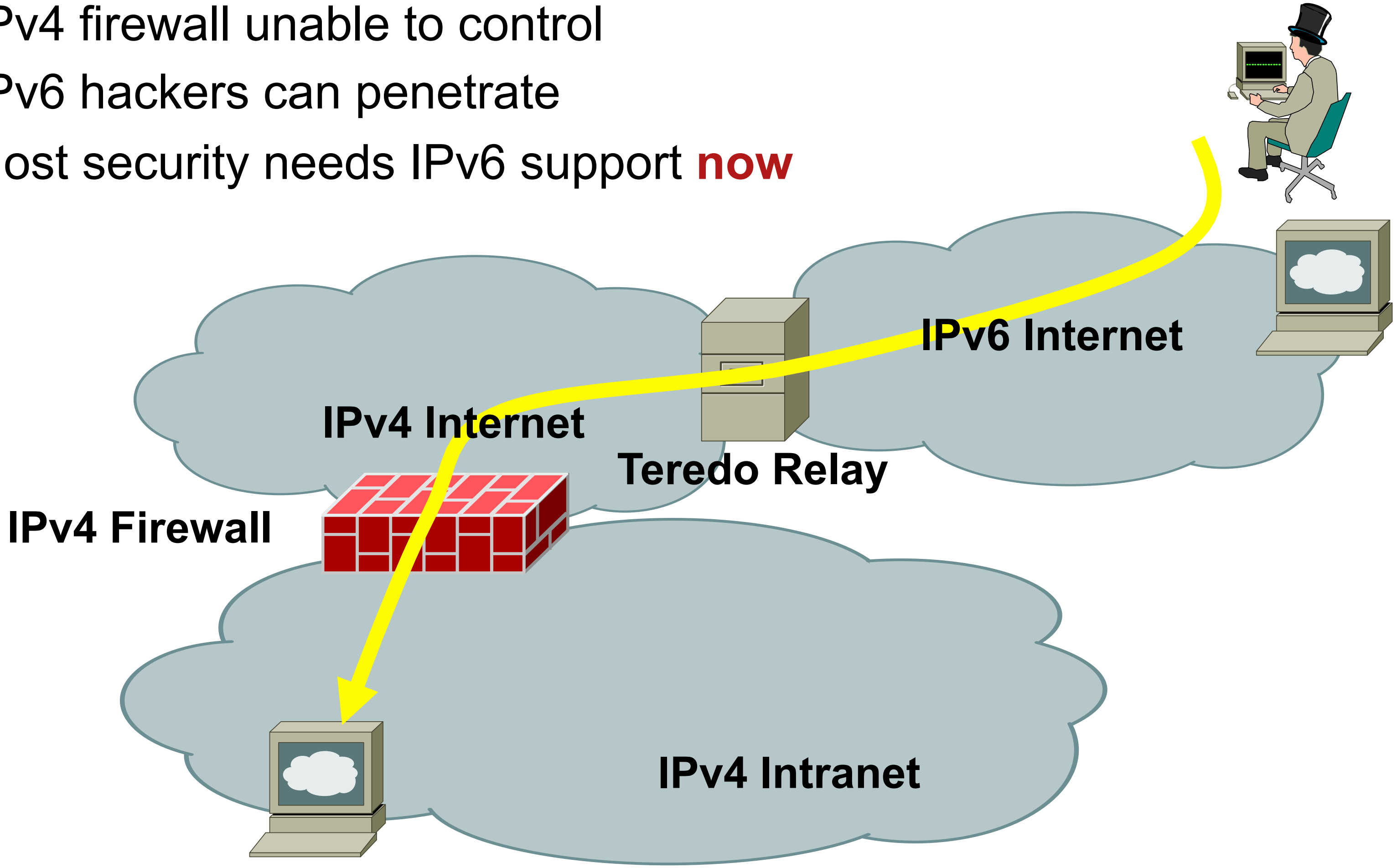
- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**



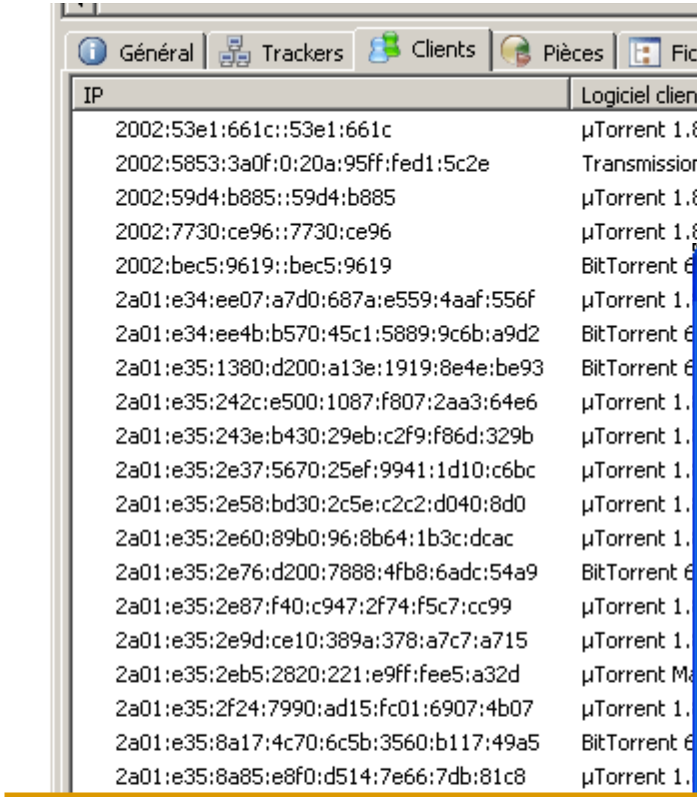
# Teredo Tunnels (3/3)
## No More Outbound Control

Once Teredo Configured

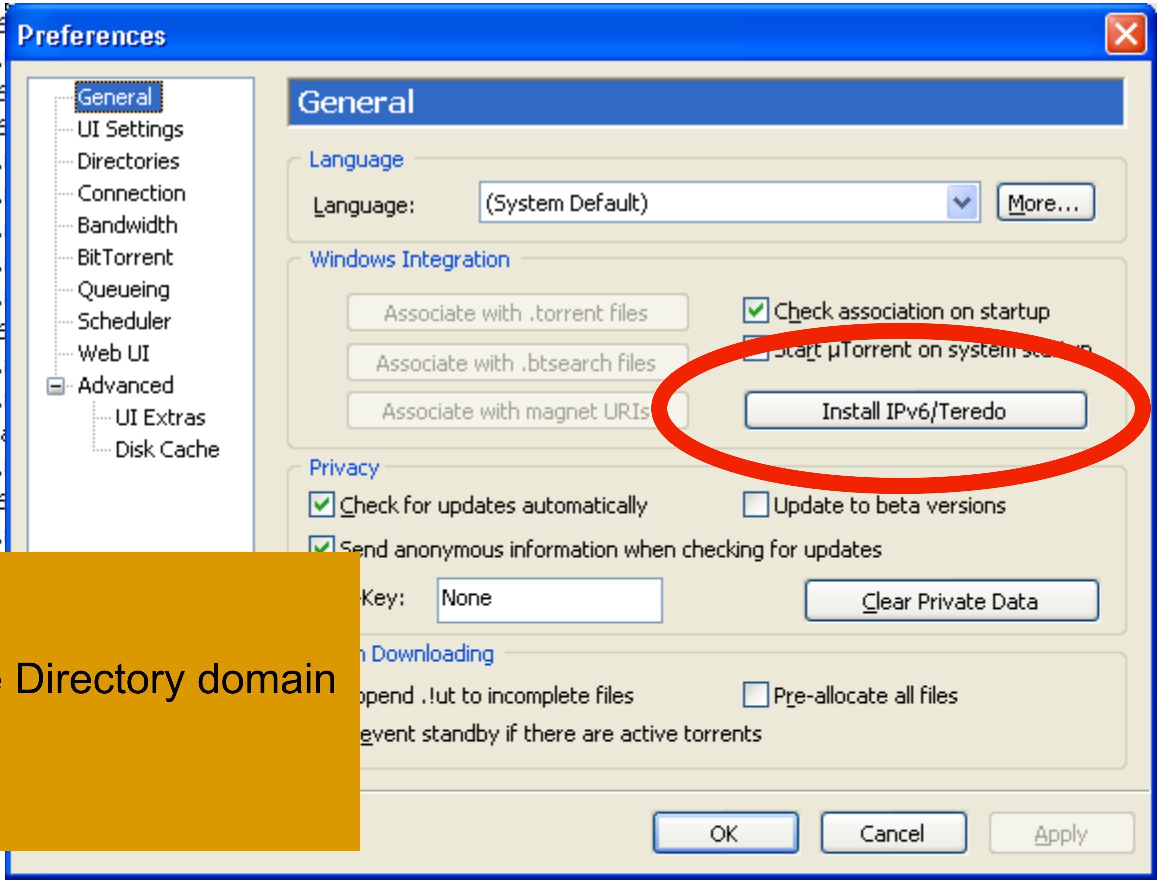
- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support **now**



# Is it real?
# May be uTorrrent 1.8 (released Aug 08)



| IP | Logiciel client |
|---|---|
| 2002:53e1:661c::53e1:661c | µTorrent 1.8.2 |
| 2002:5853:3a0f:0:20a:95ff:fed1:5c2e | Transmission 1.51 |
| 2002:59d4:b885::59d4:b885 | µTorrent 1.8.2 |
| 2002:7730:ce96::7730:ce96 | µTorrent 1.8.2 |
| 2002:bec5:9619::bec5:9619 | BitTorrent 6 |
| 2a01:e34:ee07:a7d0:687a:e559:4aaf:556f | µTorrent 1. |
| 2a01:e34:ee4b:b570:45c1:5889:9c6b:a9d2 | BitTorrent 6 |
| 2a01:e35:1380:d200:a13e:1919:8e4e:be93 | BitTorrent 6 |
| 2a01:e35:242c:e500:1087:f807:2aa3:64e6 | µTorrent 1. |
| 2a01:e35:243e:b430:29eb:c2f9:f86d:329b | µTorrent 1. |
| 2a01:e35:2e37:5670:25ef:9941:1d10:c6bc | µTorrent 1. |
| 2a01:e35:2e58:bd30:2c5e:c2c2:d040:8d0 | µTorrent 1. |
| 2a01:e35:2e60:89b0:96:8b64:1b3c:dcac | µTorrent 1. |
| 2a01:e35:2e76:d200:7888:4fb8:6adc:54a9 | BitTorrent 6 |
| 2a01:e35:2e87:f40:c947:2f74:f5c7:cc99 | µTorrent 1. |
| 2a01:e35:2e9d:ce10:389a:378:a7c7:a715 | µTorrent 1. |
| 2a01:e35:2eb5:2820:221:e9ff:fee5:a32d | µTorrent Ma |
| 2a01:e35:2f24:7990:ad15:fc01:6907:4b07 | µTorrent 1. |
| 2a01:e35:8a17:4c70:6c5b:3560:b117:49a5 | BitTorrent 6 |
| 2a01:e35:8a85:e8f0:d514:7e66:7db:81c8 | µTorrent 1. |



General

Language

Language: (System Default) More...

Windows Integration

Associate with .torrent files
Associate with .btsearch files
Associate with magnet URIs

☑ Check association on startup

☐ Start µTorrent on system startup

Privacy

☑ Check for updates automatically ☐ Update to beta versions

☑ Send anonymous information when checking for updates

Key: None

Downloading

ppend .!ut to incomplete files ☐ Pre-allocate all files

event standby if there are active torrents

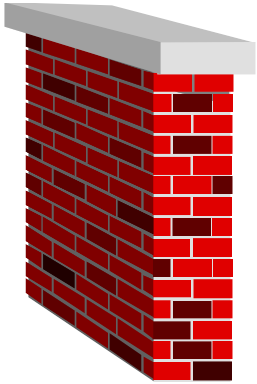
Note: on Windows Teredo is:

- -Disabled when firewall is disabled
- -Disabled when PC is part of Active Directory domain
- -Else enabled

-User can override this protection

# Enforcing a Security Policy

# IOS IPv6 Extended ACL



- Can match on

  Upper layers: TCP, UDP, SCTP port numbers

  TCP flags SYN, ACK, FIN, PUSH, URG, RST

  ICMPv6 code and type

  Traffic class (only six bits/8) = DSCP

  Flow label (0-0xFFFFF)

- IPv6 extension header

  `routing` matches any RH, `routing-type` matches specific RH

  `mobility` matches any MH, `mobility-type` matches specific MH

  `dest-option` matches any, `dest-option-type` matches specific destination options

  `auth` matches AH

  Can skip AH (but not ESP) since IOS 12.4(20)T

- `fragments` keyword matches

  Non-initial fragments (same as IPv4)

  And the first fragment if the L4 protocol cannot be determined

- `undetermined-transport` keyword matches (only for deny)

  Any packet whose L4 protocol cannot be determined: fragmented or unknown extension header

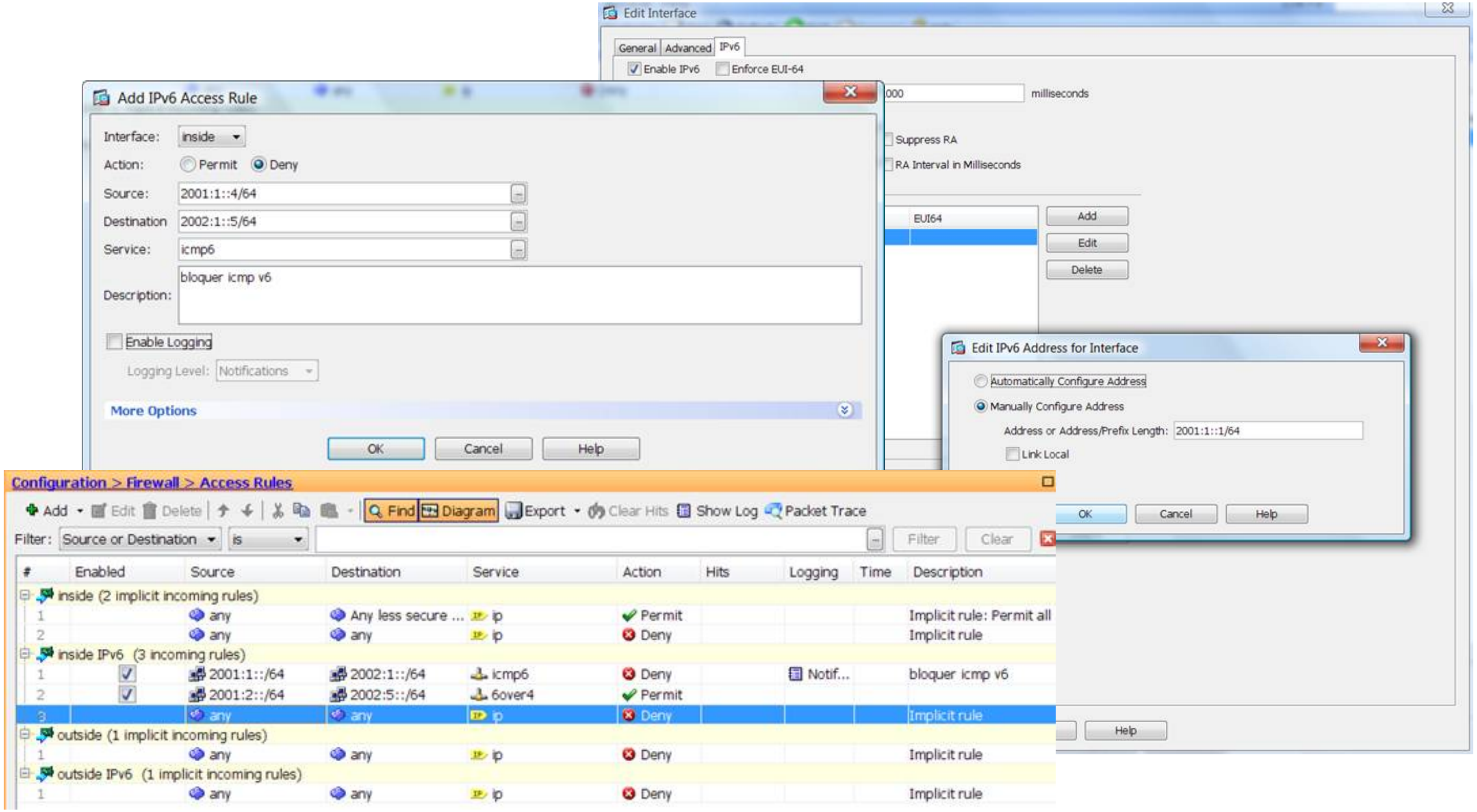
# Example: Rogue RA & DHCP Port ACL

```
ipv6 access-list ACCESS_PORT
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit any any

Interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```

*Note: PACL replaces RACL for the interface (or is merged with RACL)*
*In August 2010, Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4*

# ASA Firewall IPv6 Support



Add IPv6 Access Rule

Interface: inside

Action: ○ Permit ● Deny

Source: 2001:1::4/64

Destination 2002:1::5/64

Service: icmp6

Description: bloquer icmp v6

□ Enable Logging

Logging Level: Notifications

More Options

Edit Interface

☑ Enable IPv6 □ Enforce EUI-64

000 milliseconds

□ Suppress RA

□ RA Interval in Milliseconds

EUI64

Edit IPv6 Address for Interface

○ Automatically Configure Address

● Manually Configure Address

Address or Address/Prefix Length: 2001:1::1/64

□ Link Local

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 |

# IPS 6.2 adds IPv6 Support

- IPS supports IPv6 since IPS 6.2 (November 2008)
- Engines
  - Specific to IPv6
  - Common to IPv4 and IPv6
  - TCP reset works over IPv4
- *IPS Manager Express* can view IPv6 events
- *IPS Device Manager* can configure IPv6
- All management plane is over IPv4 only
  - Not critical for most customers

# 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 (ASA 8.0)
  - Stateful-Failover (ASA 8.2.2)
  - No header extension parsing
- FWSM
  - IPv6 in software... 80 Mbps … Not an option (put an IPv6-only ASA in parallel)
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
- Cisco Security Agent (EOS)
  - Since version 6.0.1 for IPv6 network protection
- IPS
  - Since 6.2 (released 2008)
- Email Security Appliance (ESA) under beta testing early 2010
- Web Security Appliance (WSA) not before 2011

# Enterprise Deployment: Secure IPv6 Connectivity

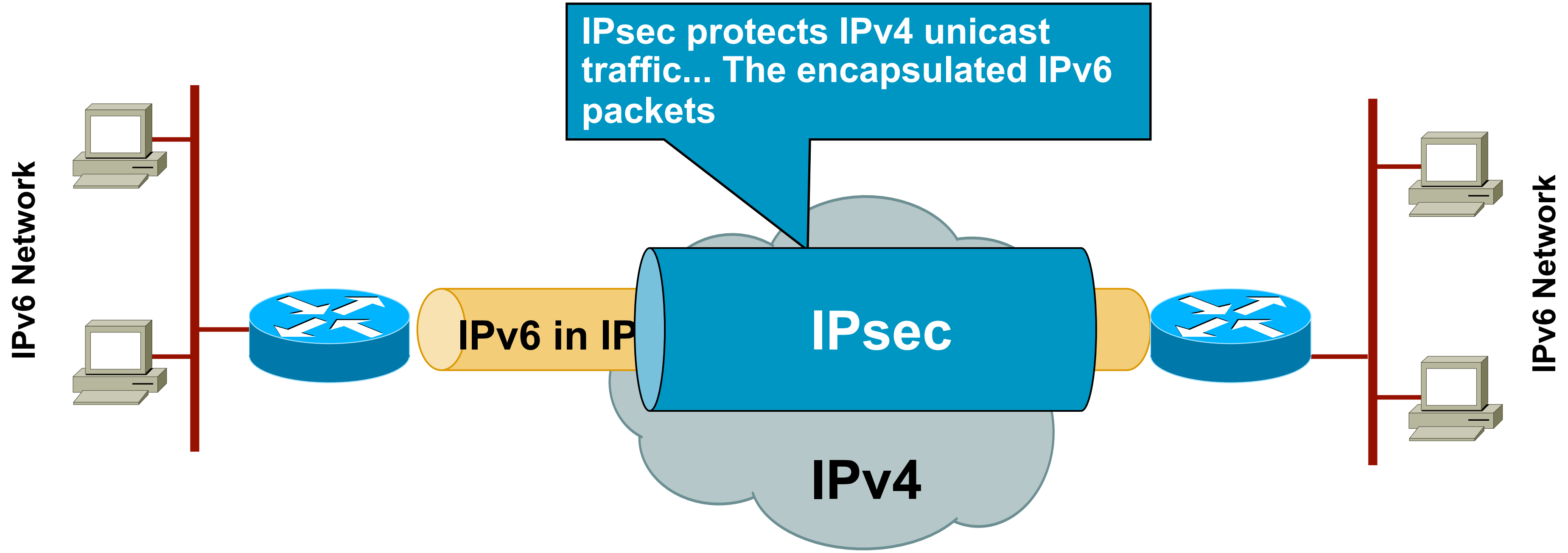
How to Secure IPv6 over the WAN

# Secure IPv6 over IPv4/6 Public Internet

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

| Public Network | Site 2 Site | Remote Access |
|---|---|---|
| IPv4 | ▪6in4/GRE Tunnels Protected by IPsec<br>▪DMVPN 12.4(20)T | ▪ ISATAP Protected by RA IPsec<br>▪ SSL VPN Client AnyConnect |
| IPv6 | IPsec VTI 12.4(6)T | N/A |

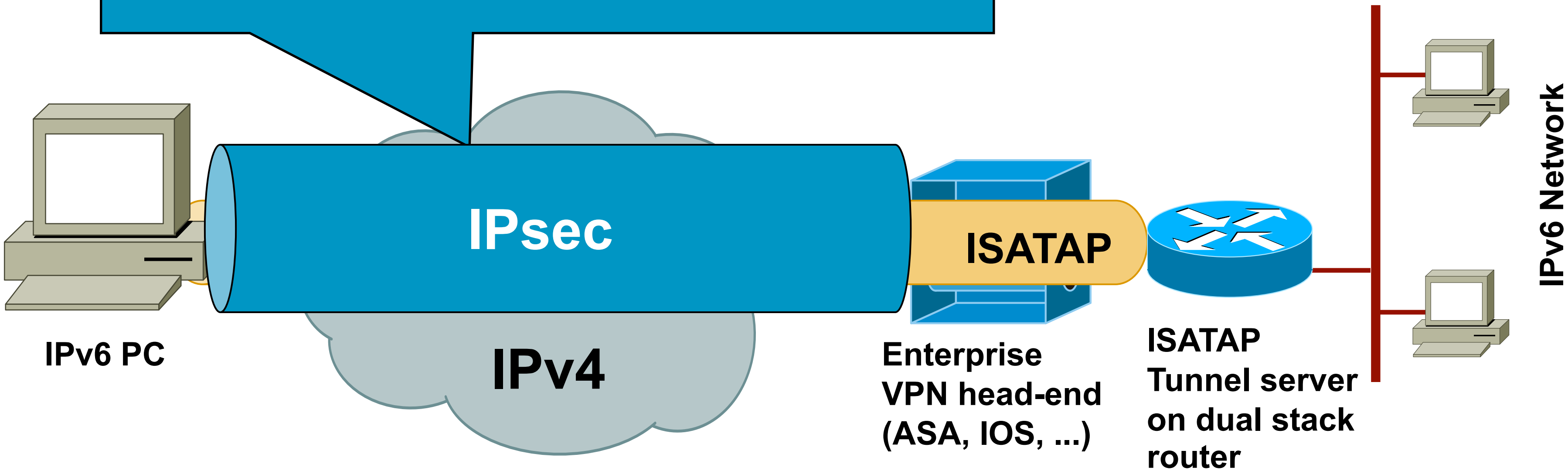
# Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec


IPsec protects IPv4 unicast traffic... The encapsulated IPv6 packets
IPv6 Network
IPv6 in IP
IPsec
IPv4
IPv6 Network

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

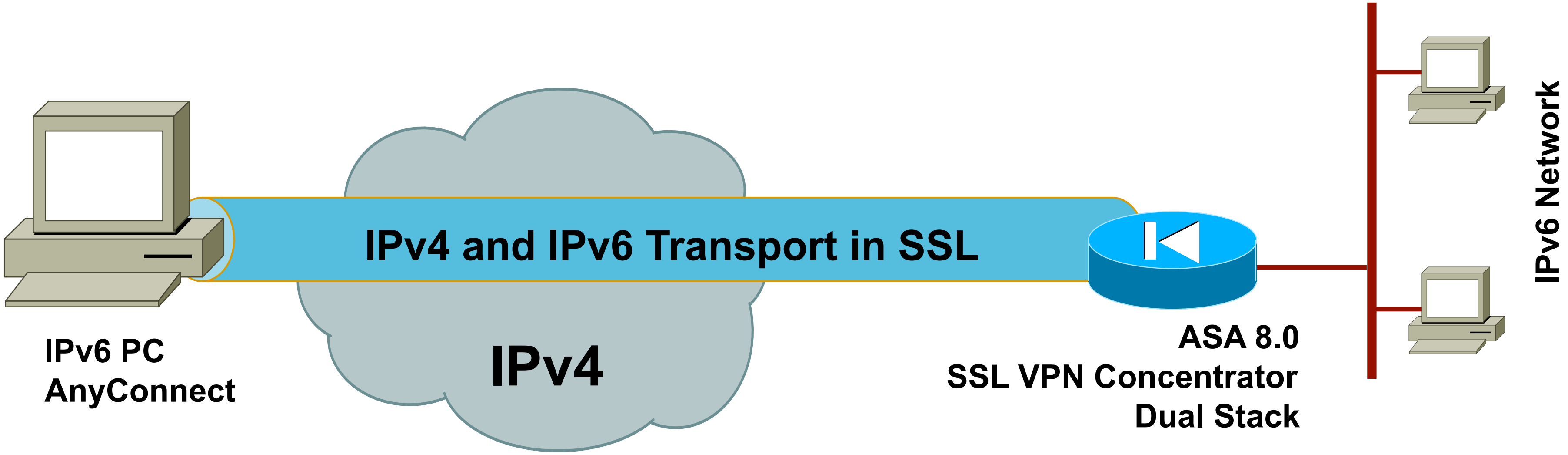
# Secure RA IPv6 Traffic over IPv4 Public Network: ISATAP in IPSec

IPsec protects IPv4 unicast traffic... The encapsulated IPv6 packets


IPsec
ISATAP
IPv6 PC
IPv4
Enterprise VPN head-end (ASA, IOS, ...)
ISATAP Tunnel server on dual stack router
IPv6 Network

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

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



# Wrap-Up

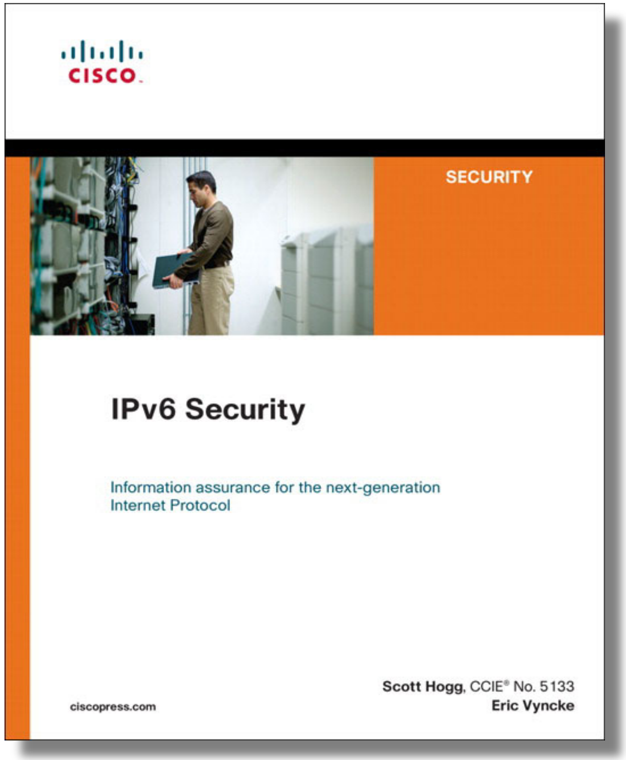
# Key Take Away

- So, nothing really new in 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

# Recommended Reading



SECURITY

IPv6 Security

Information assurance for the next-generation Internet Protocol

ciscopress.com

Scott Hogg, CCIE® No. 5133
Eric Vyncke

Source: Cisco Press