IPv6 Security Best Practices

Eric Vyncke
evyncke@cisco.com
Distinguished System Engineer

Agenda

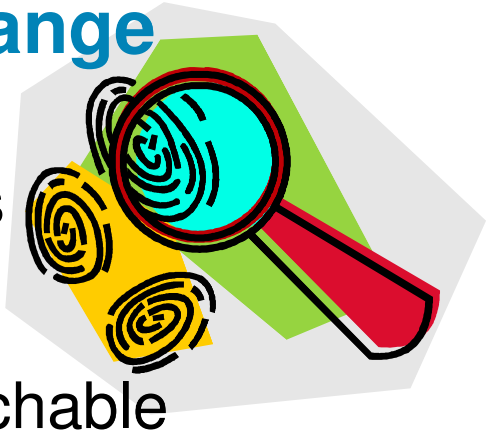
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - IPsec everywhere, dual-stack, tunnels
- Cisco IPv6 Security Solutions
  - ACL and Firewalls
  - Secure IPv6 transport over public network

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
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)

- *See also draft-ietf-v6ops-scanning-implications-03.txt*

Viruses and Worms in IPv6

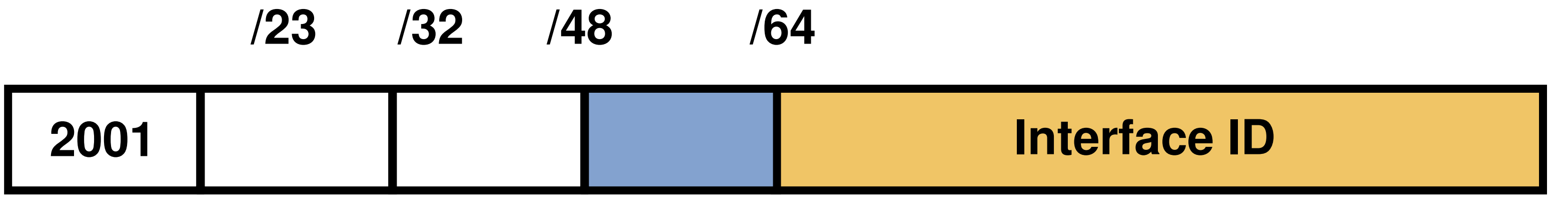
- Viruses and email worms: IPv6 brings no change
- Other worms:

  IPv4: reliance on network scanning

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

Worm developers will adapt to IPv6

IPv6 Privacy Extensions (RFC 3041)



- Temporary addresses for IPv6 host client application

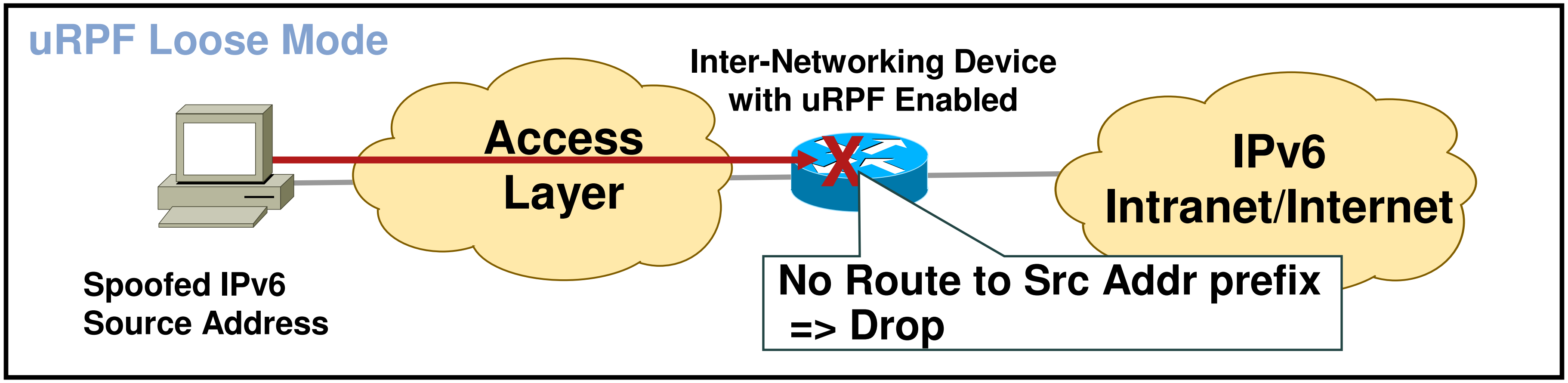
  Inhibit device/user tracking

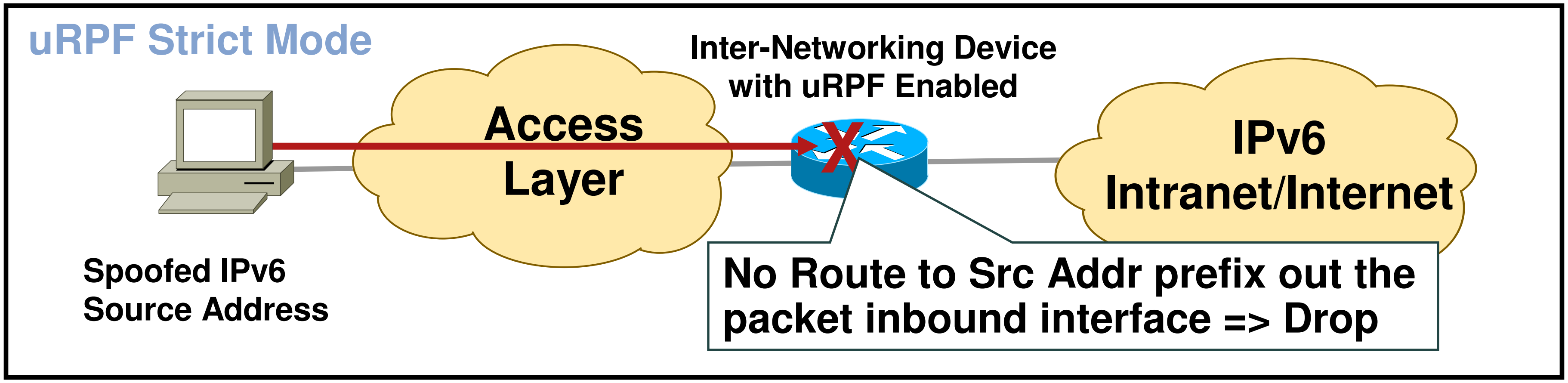
  Random 64 bit interface ID

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


uRPF Loose Mode
Inter-Networking Device with uRPF Enabled
Access Layer
IPv6 Intranet/Internet
Spoofed IPv6 Source Address
No Route to Src Addr prefix => Drop


uRPF Strict Mode
Inter-Networking Device with uRPF Enabled
Access Layer
IPv6 Intranet/Internet
Spoofed IPv6 Source Address
No Route to Src Addr prefix out the packet inbound interface => Drop

ICMPv4 vs. ICMPv6

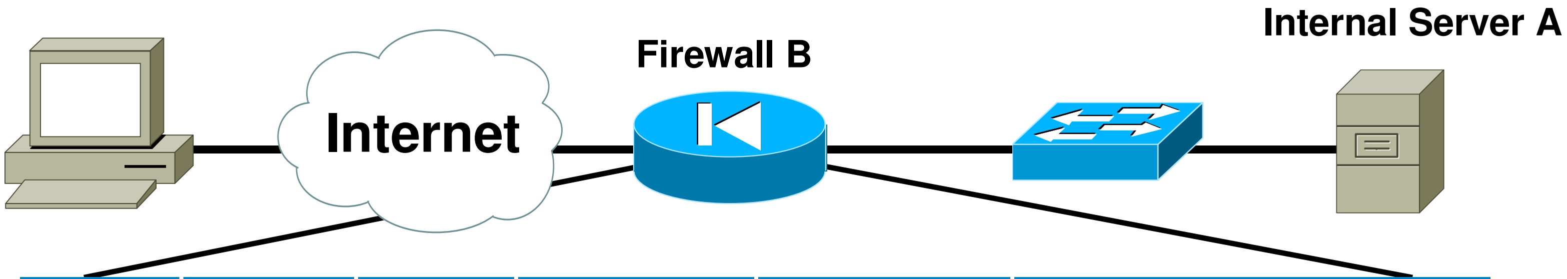
- Significant changes
- More relied upon

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
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change
- See RFC 4890

Potential Additional ICMPv6
Border Firewall Policy

For Your Reference



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A, B	4	1, 2	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement

Routing Header Attacks

- **CanSecWest Vancouver 2007:**

  Fun with IPv6 routing headers – P. Biondi & A. Ebalard

  Good old Ipv4 tricks (rebound to bypass firewall + amplification)

- Solution:

  Apply same policy for IPv6 as for Ipv4: Block Routing Header type 0

- At the intermediate nodes

```
    no ipv6 source-route
```

Neighbor Discovery

Security Mechanisms Built into Discovery Protocol = None

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

Attack Tool:
Parasite6

Secure Neighbor Discovery (SEND) RFC 3971

- Use cryptography to secure the IPv6 <-> MAC
- Can also be used to secure stateless autoconfiguration
- IOS availability in 2008
- Some impact on performance (RSA signatures)

Still requires *port security* to secure MAC <-> port

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

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

- 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

- Flooding

  Flooding attacks are identical between IPv4 and IPv6

IPv6 Stacks Vulnerabilities

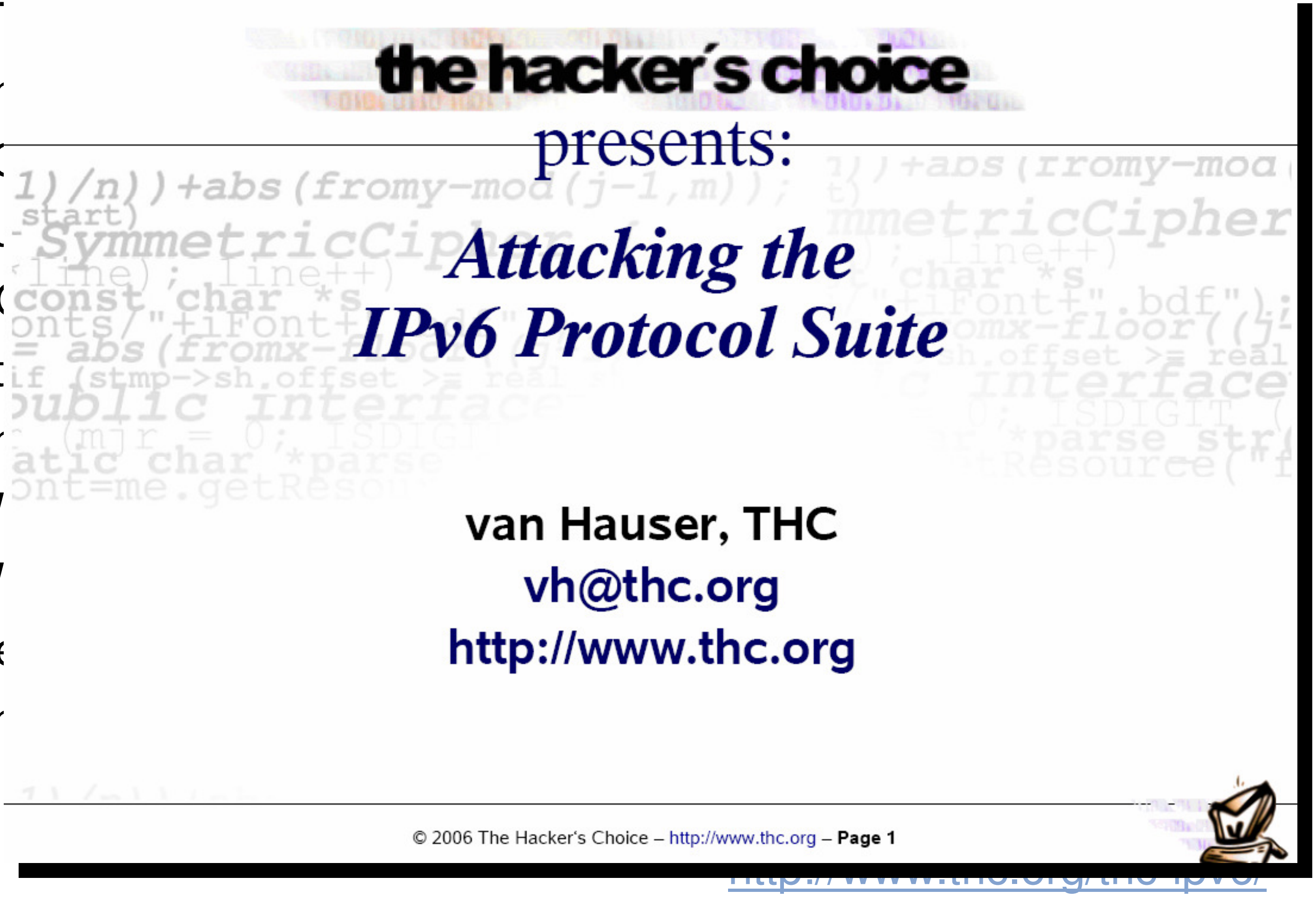
- IPv6 stack are new and could be buggy
- IPv6 enabled application can have bugs
- Some examples
  - Python getaddreinfo() remote IPv6 buffer overflow
  - Apache remote IPv6 buffer overflow
  - Postfix IPv6 unauthorized mail relay vulnerability
  - Linux kernel IPv6 DoS
  - OpenBSD remote code execution in IPv6 stack (March 07)

By the Way: It Is Real ☹
IPv6 Hacking Tools

Let the Games Begin

- Snif
  - Sr
  - TC
  - Su
  - Cc
  - Et
  - Ar
  - W
  - W
  - Ne
  - Sr

- Scanners



the hacker's choice

presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC

vh@thc.org

http://www.thc.org

© 2006 The Hacker's Choice – http://www.thc.org – **Page 1**

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

Specific IPv6 Issues

Issues Applicable only to IPv6

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

  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.
Residential use is probably recommended

Dual Stack Host Considerations

- Host security on a dual-stack device

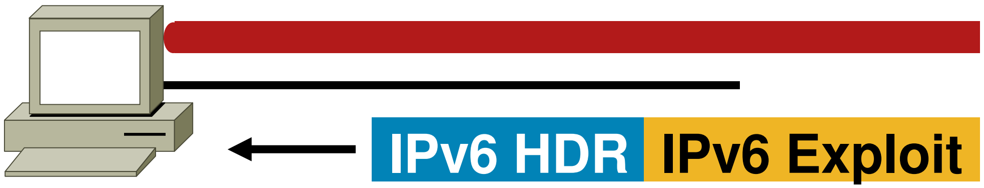
  Applications can be subject to attack on both IPv6 and IPv4

- 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



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, MacOS, ...)
- 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 configure IPv6 on 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
- ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- Teredo tunnels

- Multiple solutions...
- No authentication but for IPsec

Issues with Tunnels

- Explicitly configured tunnels

  E.g. ISATAP protocol 41

  Under network administrator control

  No authentication => threat limited to traffic injection

- Implicitly configured tunnels

  E.g. Teredo on Windows Vista UDP/3544

  Preconfigured

  No control by network administrator

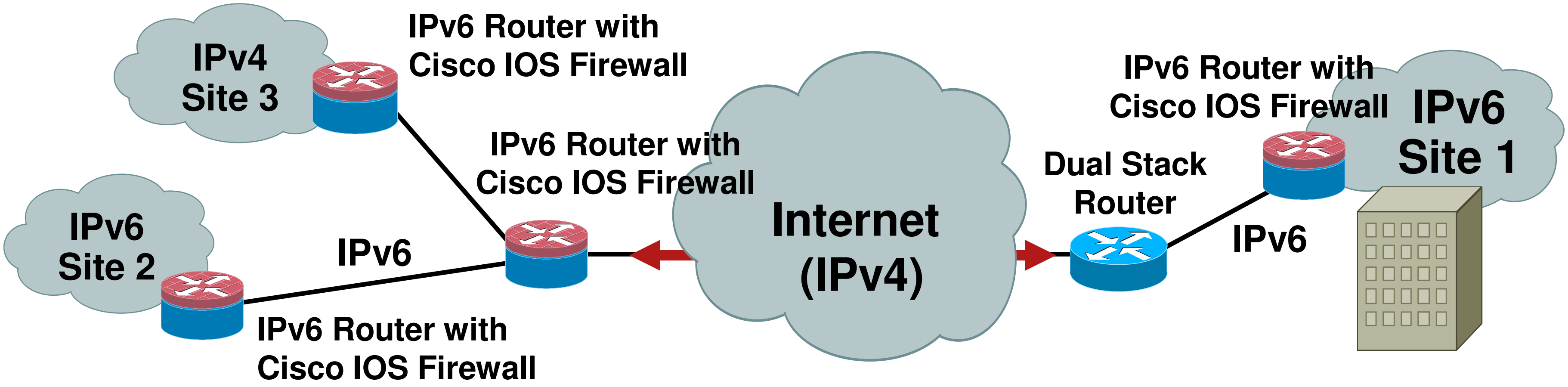
  Can bypass corporate firewall...

  ... And drill a hole in the firewall...

Cisco IPv6 Security Solutions

Cisco IOS IPv6 ACL
Cisco IOS Firewall IPv6 Support

- Standard/Extended IPv6 ACL
- IOS firewall since March 2004/12.3(7)T
- Stateful protocol inspection of IPv6: fragmented packets, TCP, UDP, ICMP and FTP traffic
- IPv4/v6 coexistence, no need for new hardware, just software
- Recognizes IPv6 extension header information such as routing header, hop-by-hop options header, fragment header, etc.



ASA and PIX Firewall IPv6 Support

- Since ASA 7.0 (April 05)
- IPv4/IPv6 coexistence
- Application awareness

  HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- Management access via IPv6

  Telnet, SSH, HTTPS
- Caveat: no fail-over support

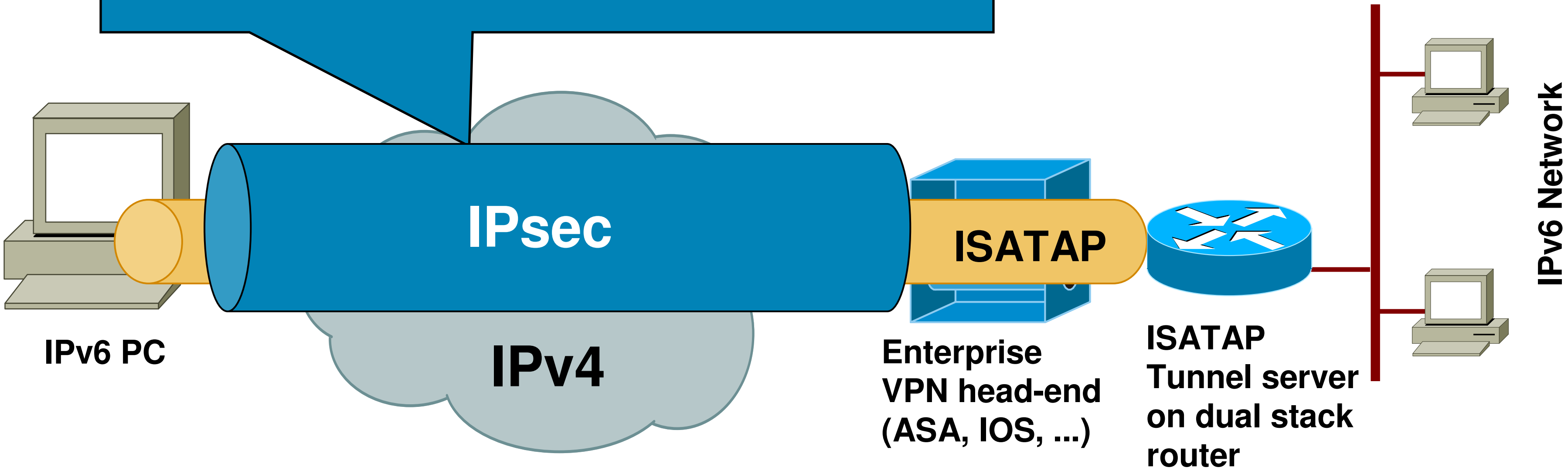
Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection

Public Network	Site 2 Site	Remote Access
IPv4	▪6in4/GRE tunnels protected by IPsec	▪ISATAP protected by IPsec ▪SSL VPN Client AnyConnect 2.0
IPv6	▪IPsec VTI 12.4(6)T	N/A

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

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


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

Conclusion

Key Take Away

- So, nothing really new in IPv6

  Lack of operation experience may hinder security for a while

- Security enforcement is possible

  Control your IPv6 traffic as you do for IPv4

- Leverage IPsec and SSL to secure IPv6 when possible
- Beware of the IPv6 latent threat: your network may **ALREADY** be vulnerable to IPv6 attacks