



IPv6 Security



Scott Hogg

GTRI - Director of Technology Solutions
Chair - Rocky Mountain IPv6 Task Force
CCIE #5133, CISSP #4610

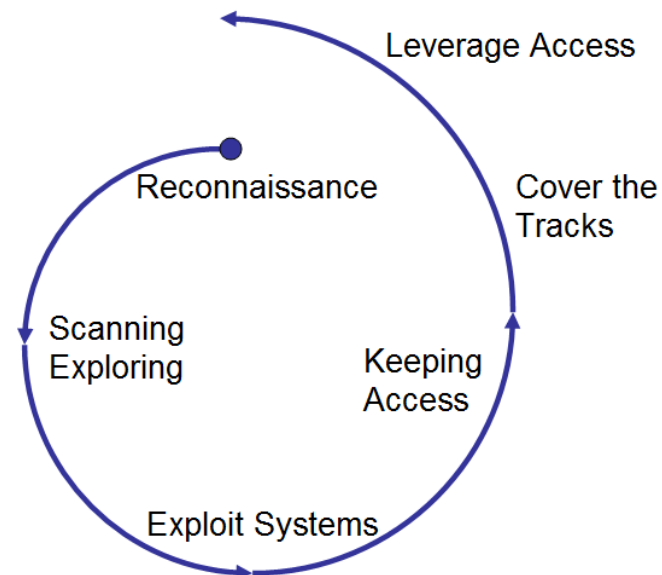
IPv6 Security



- Even if you haven't started using IPv6 yet, you probably have some IPv6 running on your networks already and didn't know it
- Do you use Linux, MacOS X, BSD, or MS Vista/Windows 7?
 - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
 - They may try to use IPv6 first and then fall-back to IPv4
 - Or they may create IPv6-in-IPv4 tunnels to Internet resources to reach IPv6 content
 - Some of these techniques take place regardless of user input or configuration
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist

IPv6 Security Threats

- There isn't much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular – IPv6 will gain the hacker's attention
- Many vendors (Cisco, Juniper, Microsoft, Sun, Open Source) have already published IPv6 bugs/vulnerabilities
- Attacks at the layers below and above the network layer are unaffected by the security of IPv6





Reconnaissance



- Enumeration, checking registries (whois), DNS (nslookup, dig, etc.), Google Hacking
- Ping sweeps, port scans, application vulnerability scans
- IPv6 makes the ping sweeps problematic
 - The address space is too large to scan
 - Brute-force scanning a /64 is not practical
 - “At a very conservative one probe per second, such a scan may take some 5 billion years to complete.” - RFC 5157 IPv6 Implications for Network Scanning
 - “And even at a scan rate of 1 million probes per second (more than 400 Mbps of traffic), it would take more than 28 years of constant scanning to find the first active host” - Sean Convery, Darrin Miller

Reconnaissance (Cont.)



- There are ways to speed up the discovery of hosts on a /64 prefix
 - Ping FF02::1 may give results
 - Node Information Queries (RFC 4620) – BSD
 - Scanning for specific EUI-64 addresses using specific OUIs
 - Scanning IPv4 and getting IPv6 info
 - Scanning 6to4, ISATAP, Teredo addresses
 - Attackers may find one host and leverage the neighbor cache
- Attackers will look in other places for IPv6 addresses
 - DHCPv6 logs, DNS servers, server logs, NMSs, Google

IPv6 Privacy Addressing



- Privacy of addresses is an issue with IPv6
 - EUI-64 addresses are derived from the host's MAC
 - That could be used to track user's activity and thus identity
- Temporary host portions of an IPv6 address intended to protect the identity of the end-user
 - MD5 hash of the EUI-64 concatenated with a random number that can change over time
 - Different implementations rotate the address at different frequencies – can be disabled
- Forensics and troubleshooting are difficult with privacy addresses
- Dynamic DNS and firewall state will also need to update
- Difficulty creating granular firewall policy when IP addresses change often

IPv6 Attack Tools

- **THC IPv6 Attack Toolkit**



- parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6

- **Scanners**

- Nmap, halfscan6, Scan6, CHScanner

- **Packet forgery**

- Scapy6, SendIP, Packit, Spak6

- **DoS Tools**

- 6tunneldos, 4to6ddos, Imps6-tools

ICMPv6



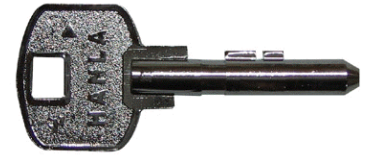
- More powerful than ICMPv4
- ICMPv6 uses IPv6 extension header # 58 (RFC 2463)

Type	Description
1	Destination Unreachable
2	Packet to Big
3	Time exceeded
4	Parameter problem
128	Echo Request
129	Echo Reply
130	Multicast Listener Query – sent to ff02::1 (all nodes)
131	Multicast Listener Report
132	Multicast Listener Done – sent to ff02::2 (all routers)
133	Router Solicitation (RS) – sent to ff01::2 (all routers)
134	Router Advertisement (RA) – sent to ff01::1 (all nodes)
135	Neighbor Solicitation (NS) – sent to ff02:0:0:0:0:1:ff00::/104
136	Neighbor Advertisement (NA)
137	Redirect message

Annotations:

- Teal line: PING (points to type 128)
- Grey line: MLD (points to type 130)
- Blue line: Prefix Advertisement (points to type 134)
- Red line: ARP Replacement (points to type 135)
- Green line: Router Redirection (points to type 137)

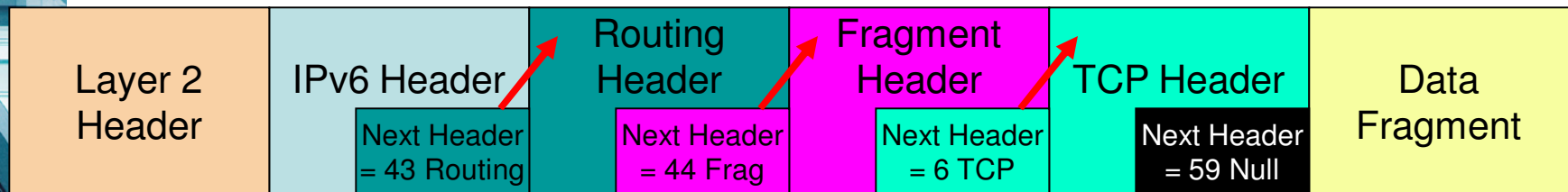
LAN Threats



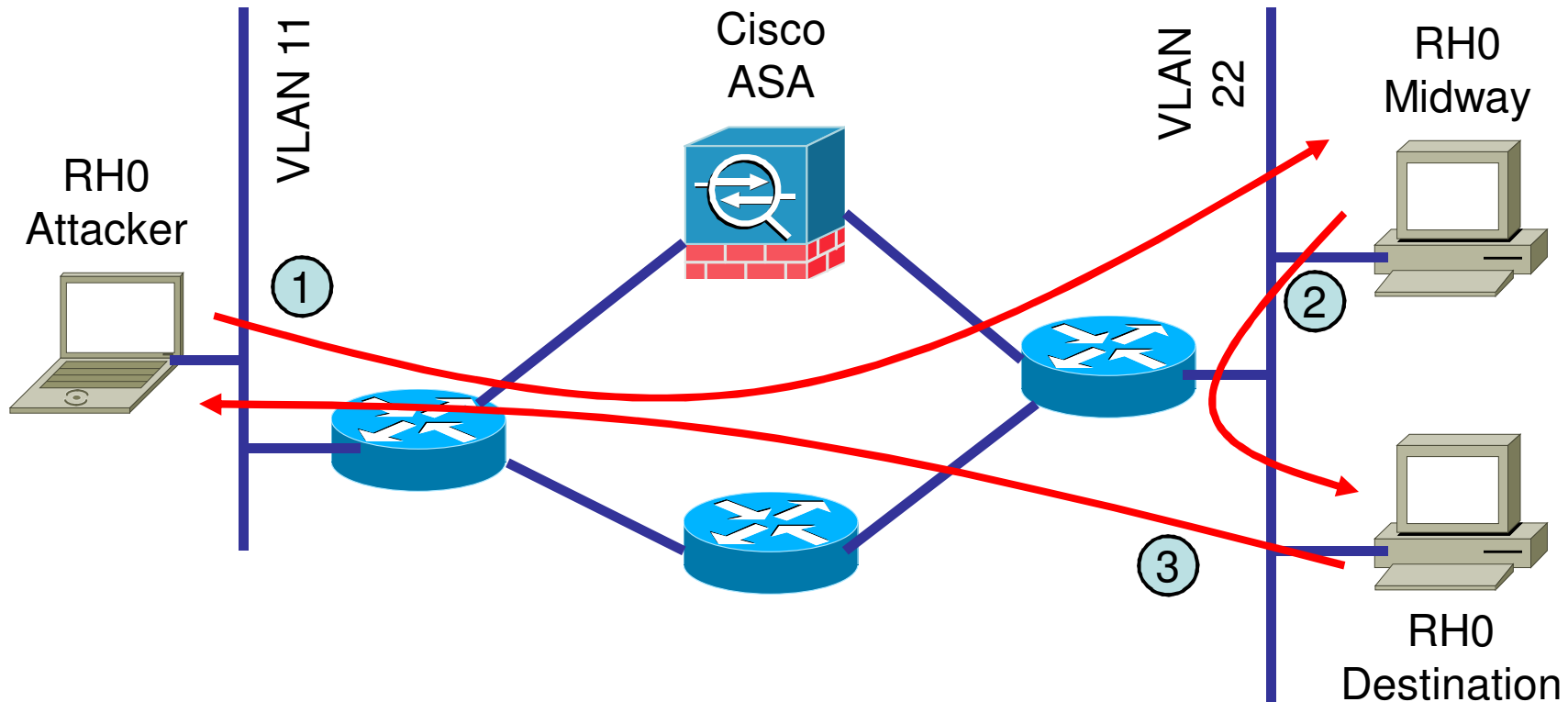
- IPv6 uses ICMPv6 for many LAN operations
 - Stateless auto-configuration
 - Neighbor Discovery Protocol (NDP)
 - IPv6 equivalent of IPv4 ARP
- Spoofed RAs can renumber hosts or launch a MITM attack
- Forged NA/NS messages to confuse NDP
- Redirects – same as ICMPv4 redirects
- Forcing nodes to believe all addresses are on-link
- DHCPv6 spoofing, resource consumption

Extension Headers (EHs)

- Extension Headers
 - Each header should not appear more than once with the exception of the Destination Options header
 - Hop-by-Hop extension header should only appear once.
 - Hop-by-Hop extension header should be the first header in the list because it is examined by every node along the path.
 - Destination Options header should appear at most twice (before a Routing header and before the upper-layer header).
 - Destination Options header should be the last header in the list if it is used at all.
- Header Manipulation – Crafted Packets
- Large chains of extension headers
 - Separate payload into second fragment
 - Consume resources - DoS
- Invalid Extension Headers – DoS



Routing Header 0 Attack



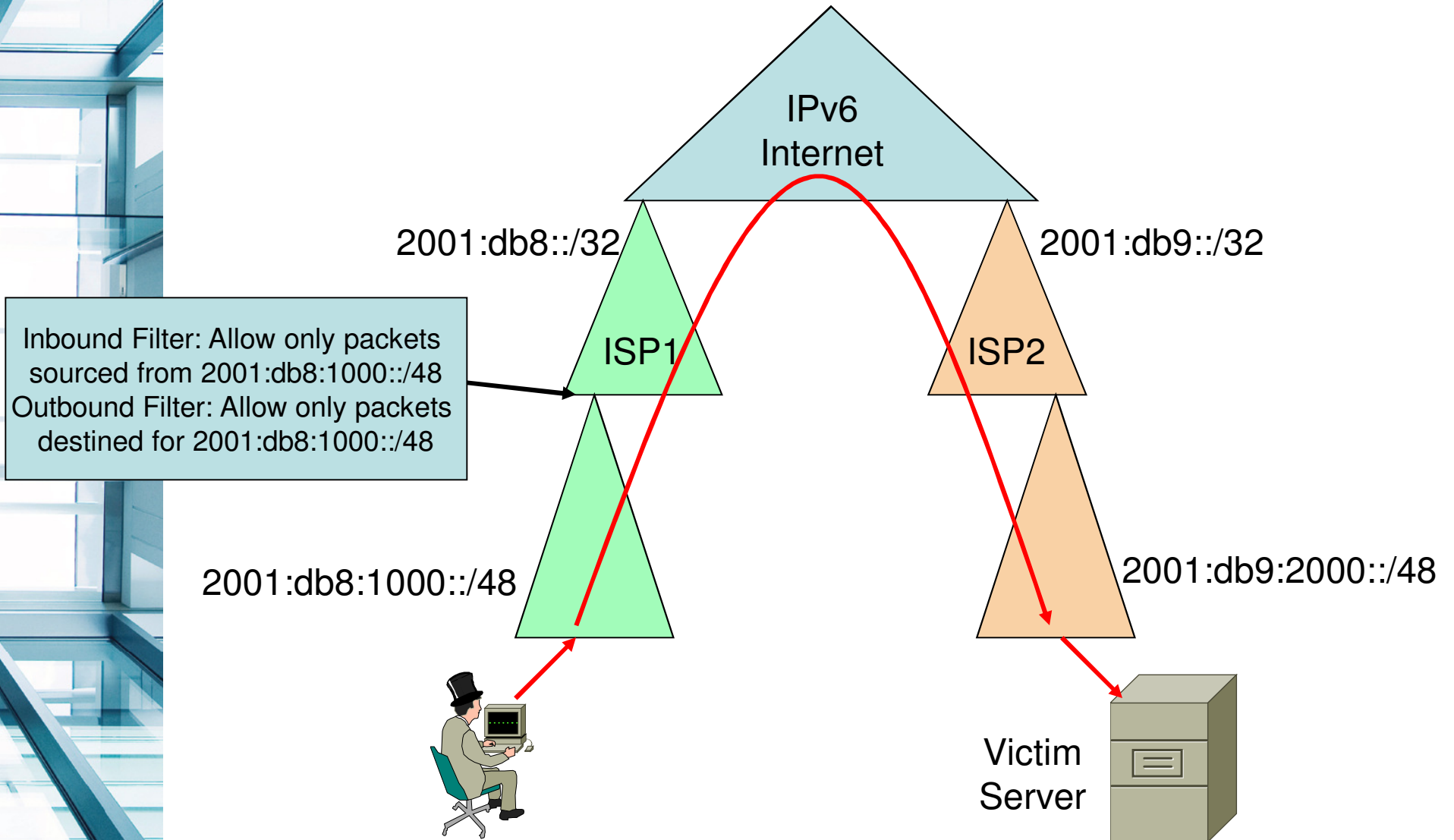
- Routers can be configured to block RH0
- Firewalls, Windows, Linux and MacOS all block RH0 by default

IPv6 Rate Limiting



- HbH option packets like “Router Alert” packets are processed by each network device along the forwarding path
 - Resource consumption attack potential
- ASR, ISR, CRS, 7600 can rate-limit IPv6 packets
- Attackers send packets that initiate ICMPv6 unreachable – resource consumption
 - Disable ICMPv6 unreachable messages on interfaces, null 0, and loopback 0
 - **no ipv6 unreachables**

Hierarchy and Traceback



Layer-3/4 Spoofing



- Spoofing of IPv6 packets is easy (Scapy6)
- IPv6 BOGON (Martians) Filtering
 - Filter traffic from unallocated space and filter router advertisements of bogus prefixes
 - Permit Legitimate Global Unicast Addresses
- Hierarchical addressing and ingress/egress filtering
- Use Inbound Infrastructure ACLs (iACLs) that deny packets sent to infrastructure IPv6 addresses
- Use IPv6 Receive ACL (rACLs) on Cisco devices
- Unicast-RPF Checks (BCP38/RFC 2827)

Transition Mechanism Threats

- Dual Stack - Preferred
 - You are only as strong as the weakest of the two stacks.
 - Running dual stack will give you at least twice the number of vulnerabilities
- Manual Tunnels - Preferred
 - Filter tunnel source/destination and use IPsec
 - If spoofing, return traffic is not sent to attacker
- Dynamic Tunnels
 - 6to4 Relay routers are “open relays”
 - ISATAP – potential MITM attacks
 - Attackers can spoof source/dest IPv4/v6 addresses
- Protocol Translation – Not recommended
- Deny packets for transition techniques not in use
 - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
 - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling



IPv6 Firewalls



- Don't just use your IPv4 firewall for IPv6 rules
- Don't just blindly allow IPsec or IPv4 Protocol 41 through the firewall
- Separate firewall policy for IPv6
- Look for vendors that support Extension Headers, Fragmentation, PMTUD, and granular filtering of ICMPv6 and multicast
- Some hosts may have multiple IPv6 addresses so this could make firewall troubleshooting tricky
- Layer-2/Transparent firewalls are more difficult to implement with IPv6 because of the required ICMPv6 ND/NS/NUD/RA/RS messages



IPv6-Capable Firewalls

- Many vendors already have IPv6 capabilities
 - Cisco Router ACLs, Reflexive ACLs, IOS-based Firewall, PIX, ASA
 - CheckPoint, Juniper, Fortinet, others
 - iptables, ip6fw, ipf, pf, pfSense, m0n0wall
 - Windows XP SP2, Vista IPv6 Internet Connection Firewall
- IPv6 firewalls may not have all the same full features as IPv4 firewalls
 - UTM/DPI/IPS/content filtering features may only work for IPv4
 - Vendors are working toward feature parity

IPv6 Intrusion Prevention

- Few signatures exist for IPv6 packets
- IPSs should send out notifications when non-conforming IPv6 packets are observed
- Faulty parameters, bad extension headers, source address is a multicast address
- IPv6-Capable IPSs
 - Cisco 4200 IDS appliances, AIP (v7.X)
 - Sourcefire 3D IPS, Snort 2.8 Beta and 3.0 Alpha
 - Check Point IPS-1 (NFR Sentivist)
 - Juniper/NetScreen ScreenOS
 - IBM/ISS Proventia/RealSecure
 - Command Information Assure6
 - SandVine PTS 8210, PTS 14000, PTS 24000
 - Ipoque Protocol and Application Classification Engine (PACE) library for OpenDPI
 - Enterasys IPS



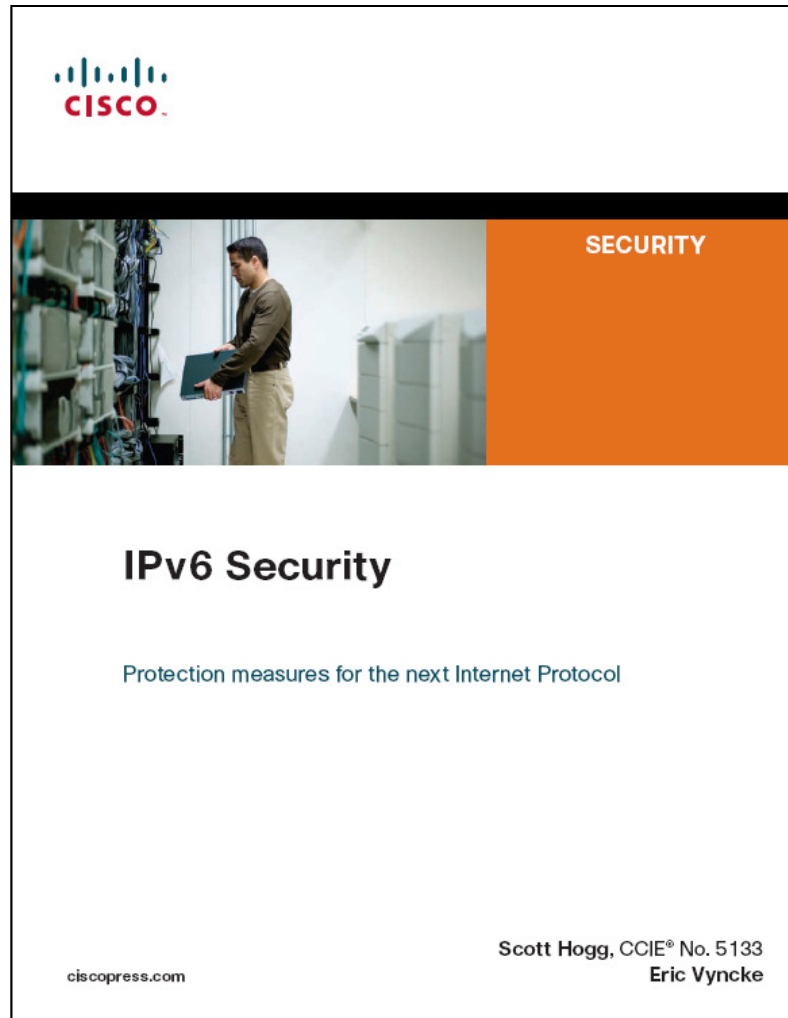
IPv6 Security Summary



- IPv6 is no more or less secure than IPv4
 - Lack of IPv6 knowledge and experience is a serious issue
- Learn about IPv6 and strive to achieve equal protections for IPv6 as with IPv4
- Ask your vendors about IPv6-capable products
- Use a NAC/802.1X solution and Ethernet port security while you wait for SEND
- Perform RFC2827-like IPv6 perimeter and Unicast Reverse Path Forwarding (Unicast RPF) checks throughout the network
- Use manual tunnels instead of dynamic tunnels and filter on tunnel endpoints
- Leverage IPsec for everything possible (No NAT)
- Deny packets for transition techniques not in use



IPv6 Security Book



shogg@gtri.com

303-949-4865

10/12/2010

© 2010 Global Technology Resources, Inc. All Rights Reserved.

20