



**SECURITY**

# IPv6 Security

Information assurance for the next-generation  
Internet Protocol



# IPv6 Security

**Scott Hogg, CCIE No. 5133**  
**Eric Vyncke**

**Cisco Press**

Cisco Press  
800 East 96th Street  
Indianapolis, IN 46240 USA

# IPv6 Security

## Table of Contents

### Contents

### Introduction

### Chapter 1 Introduction to IPv6 Security

Reintroduction to IPv6

IPv6 Update

IPv6 Vulnerabilities

Hacker Experience

IPv6 Security Mitigation Techniques

Summary

Recommended Readings and Resources

### Chapter 2 IPv6 Protocol Security Vulnerabilities

The IPv6 Protocol Header

ICMPv6

Multicast Security

Extension Header Threats

Extension Header Overview

Extension Header Vulnerabilities

Hop-by-Hop Options Header and Destination Options Header

Routing Headers

Fragmentation Header

Unknown Option Headers

Upper-Layer Headers

Reconnaissance on IPv6 Networks

# **Table of Contents**

- Scanning and Assessing the Target
- Speeding Up the Scanning Process
- Protecting Against Reconnaissance Attacks

## **Layer 3 and Layer 4 Spoofing**

- Summary

- References

## **Chapter 3 IPv6 Internet Security**

### **Large-Scale Internet Threats**

- Packet Flooding
- Internet Worms
- Distributed Denial of Service and Botnets

### **Ingress/Egress Filtering**

- Filtering IPv6 Traffic
- Filtering on Allocated Addresses
- Bogon Filtering
- Bogon Filtering Challenges and Automation

### **Securing BGP Sessions**

- Explicitly Configured BGP Peers
- Using BGP Session Shared Secrets
- Leveraging an IPsec Tunnel
- Using Loopback Addresses on BGP Peers
- Controlling the Time-to-Live (TTL) on BGP Packets
- Filtering on the Peering Interface
- Using Link-Local Peering
- Preventing Long AS Paths
- Limiting the Number of Prefixes Received
- Preventing BGP Updates Containing Private AS Numbers
- Maximizing BGP Peer Availability
- Logging BGP Neighbor Activity

# **Table of Contents**

Securing IGP

Extreme Measures for Securing Communications Between BGP Peers

## **IPv6 over MPLS Security**

Using Static IPv6 over IPv4 Tunnels Between PE Routers

Using 6PE

Using 6VPE to Create IPv6-Aware VRFs

## **Customer Premises Equipment**

### **Prefix Delegation Threats**

SLAAC

DHCPv6

## **Multihoming Issues**

### **Summary**

### **References**

## **Chapter 4 IPv6 Perimeter Security**

### **IPv6 Firewalls**

Filtering IPv6 Unallocated Addresses

Additional Filtering Considerations

Firewalls and NAT

### **Cisco IOS Router ACLs**

Implicit IPv6 ACL Rules

Internet ACL Example

IPv6 Reflexive ACLs

### **Cisco IOS Firewall**

Configuring IOS Firewall

IOS Firewall Example

IOS Firewall Port-to-Application Mapping for IPv6

### **Cisco PIX/ASA/FWSM Firewalls**

Configuring Firewall Interfaces

# **Table of Contents**

- Management Access
- Configuring Routes
- Security Policy Configuration
- Object Group Policy Configuration
- Fragmentation Protection
- Checking Traffic Statistics
- Neighbor Discovery Protocol Protections

Summary

References

## **Chapter 5 Local Network Security**

Why Layer 2 Is Important

ICMPv6 Layer 2 Vulnerabilities for IPv6

- Stateless Address Autoconfiguration Issues
- Neighbor Discovery Issues
- Duplicate Address Detection Issues
- Redirect Issues

ICMPv6 Protocol Protection

- Secure Neighbor Discovery
- Implementing CGA Addresses in Cisco IOS
- Understanding the Challenges with SEND

Network Detection of ICMPv6 Attacks

- Detecting Rogue RA Messages
- Detecting NDP Attacks

Network Mitigation Against ICMPv6 Attacks

- Rafixd
- Reducing the Target Scope
- IETF Work
- Extending IPv4 Switch Security to IPv6

# **Table of Contents**

Privacy Extension Addresses for the Better and the Worse

DHCPv6 Threats and Mitigation

Threats Against DHCPv6

Mitigating DHCPv6 Attacks

Point-to-Point Link

Endpoint Security

Summary

References

## **Chapter 6 Hardening IPv6 Network Devices**

Threats Against Network Devices

Cisco IOS Versions

Disabling Unnecessary Network Services

Interface Hardening

Limiting Router Access

Physical Access Security

Securing Console Access

Securing Passwords

VTY Port Access Controls

AAA for Routers

HTTP Access

IPv6 Device Management

Loopback and Null Interfaces

Management Interfaces

Securing SNMP Communications

Threats Against Interior Routing Protocol

RIPng Security

EIGRPv6 Security

IS-IS Security

# **Table of Contents**

OSPF Version 3 Security

First-Hop Redundancy Protocol Security

Neighbor Unreachability Detection

HSRPv6

GLBPv6

Controlling Resources

Infrastructure ACLs

Receive ACLs

Control Plane Policing

QoS Threats

Summary

References

## **Chapter 7 Server and Host Security**

IPv6 Host Security

Host Processing of ICMPv6

Services Listening on Ports

Checking the Neighbor Cache

Detecting Unwanted Tunnels

IPv6 Forwarding

Address Selection Issues

Host Firewalls

Microsoft Windows Firewall

Linux Firewalls

BSD Firewalls

Sun Solaris

Securing Hosts with Cisco Security Agent 6.0

Summary

References



# **Table of Contents**

## **Chapter 8 IPsec and SSL Virtual Private Networks**

### **IP Security with IPv6**

IPsec Extension Headers

IPsec Modes of Operation

Internet Key Exchange (IKE)

IPsec with Network Address Translation

IPv6 and IPsec

### **Host-to-Host IPsec**

### **Site-to-Site IPsec Configuration**

IPv6 IPsec over IPv4 Example

IPv6 IPsec Example

Dynamic Multipoint VPN

### **Remote Access with IPsec**

### **SSL VPNs**

### **Summary**

### **References**

## **Chapter 9 Security for IPv6 Mobility**

### **Mobile IPv6 Operation**

### **MIPv6 Messages**

Indirect Mode

Home Agent Address Determination

Direct Mode

### **Threats Linked to MIPv6**

Protecting the Mobile Device Software

Rogue Home Agent

Mobile Media Security

Man-in-the-Middle Threats

Connection Interception

# **Table of Contents**

Spoofing MN-to-CN Bindings

DoS Attacks

Using IPsec with MIPv6

Filtering for MIPv6

Filters at the CN

Filters at the MN/Foreign Link

Filters at the HA

Other IPv6 Mobility Protocols

Additional IETF Mobile IPv6 Protocols

Network Mobility (NEMO)

IEEE 802.16e

Mobile Ad-hoc Networks

Summary

References

## **Chapter 10 Securing the Transition Mechanisms**

Understanding IPv4-to-IPv6 Transition Techniques

Dual-Stack

Tunnels

Protocol Translation

Implementing Dual-Stack Security

Exploiting Dual-Stack Environment

Protecting Dual-Stack Hosts

Hacking the Tunnels

Securing Static Tunnels

Securing Dynamic Tunnels

Securing 6VPE

Attacking NAT-PT

IPv6 Latent Threats Against IPv4 Networks

# **Table of Contents**

Summary

References

## **Chapter 11 Security Monitoring**

Managing and Monitoring IPv6 Networks

Router Interface Performance

Device Performance Monitoring

Router Syslog Messages

Benefits of Accurate Time

Managing IPv6 Tunnels

Using Forensics

Using Intrusion Detection and Prevention Systems

Cisco IPS Version 6.1

Testing the IPS Signatures

Managing Security Information with CS-MARS

Managing the Security Configuration

Summary

References

## **Chapter 12 IPv6 Security Conclusions**

Comparing IPv4 and IPv6 Security

Similarities Between IPv4 and IPv6

Differences Between IPv4 and IPv6

Changing Security Perimeter

Creating an IPv6 Security Policy

Network Perimeter

Extension Headers

LAN Threats

Host and Device Hardening

Transition Mechanisms

# **Table of Contents**

IPsec

Security Management

On the Horizon

Consolidated List of Recommendations

Summary

References

Index