IP COMMUNICATIONS

Securing Cisco IP Telephony Networks

The real-world guide to securing Cisco-based IP telephony applications, devices, and networks

ciscopress.com

Akhil Behl, CCIE® No. 19564

Securing Cisco IP Telephony Networks

Akhil Behl

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Securing Cisco IP Telephony Networks

Table of Contents

Contents
Introduction
Part I: Introduction to Cisco IP Telephony Security
Chapter 1 What Is IP Telephony Security and Why Do You Need It?
Defining IP Telephony Security
IP Telephony Security Threats
An Insight to VoIP Security Tools
Business Challenges and Cisco IP Telephony Security Responses
Summary
Chapter 2 Cisco IP Telephony Security Building Blocks
Introduction to IP Telephony Security Methodology
IP Telephony Security Architecture
Exploring IP Telephony Security Methodology and Defining Security Architecture
Defining the IP Telephony Network Components That Should Be Secured
Summary
Chapter 3 What Can You Secure and How Can You Secure It?
Layered Security Approach for IP Telephony Security
Cisco IP Telephony Security Controls
Cisco IP Telephony Security Overview
Summary
Chapter 4 Cisco IP Telephony Security Framework
Cisco IP Telephony Security Life Cycle
Developing an IP Telephony Security Policy
Evaluating Cost of SecurityCost Versus Risk

Table of Contents

Determining the Level of Security for Your IP Telephony Network
Putting Together All the Pieces
Summary
Part II: Cisco IP Telephony Network Security
Chapter 5 Cisco IP Telephony Physical Security
IP Telephony Physical Security
Physical Security Issues
Locking Down IP Telephony Equipment
Environmental Factors
Summary
Chapter 6 Cisco IP Telephony Layer 2 Security
Layer 2 Security Overview
IP Telephony Layer 2 Security Issues and Mitigation
Dealing with Rogue Endpoints: 802.1x
Layer 2 Security: Best Practices
Summary
Chapter 7 Cisco IP Telephony Layer 3 Security
Layer 3 Security Fundamentals: Securing Cisco IOS Routers
Cisco IOS Platform Security
Restricting Management Access
Disabling Unnecessary IOS Services
Securing Routing Protocols
Securing Hot Standby Routing Protocol (HSRP)
Safeguarding Against ICMP Attacks
Securing User Passwords
Controlling User Access and Privilege Levels
Antispoofing Measures
Router Banner Messages
Securing Network Time Protocol (NTP)
Blocking Commonly Exploited Ports

Table of Contents

Extending Enterprise Security Policy to Your Cisco Router

Layer 3 Traffic ProtectionEncryption

Layer 3 SecurityBest Practices

Summary

Chapter 8 Perimeter Security with Cisco Adaptive Security Appliance

IP Telephony Data Centers Integral Element: Cisco Adaptive Security Appliance

Securing IP Telephony Data Center with Cisco ASA

Cisco ASA TLS Proxy

Cisco ASA Phone Proxy

Cisco VPN Phone

Remote Worker and Telecommuter Voice Security

Summary

Part III: Cisco IP Telephony Application and Device Security

Chapter 9 Cisco Unified Communications Manager Security

Cisco Unified Communications Manager (CUCM) Platform Security

Certificate-Based Secure Signaling and Media: Certificate Authority Proxy Function

Security by Default (SBD)

Using External Certificate Authority (CA) with CAPF

Using External Certificate Authority (CA) with Cisco Tomcat

Enabling Secure LDAP (LDAPS)

Securing IP Phone Conversation

Secure Tone

CUCM Trunk Security

Trusted Relay Point (TRP)

Preventing Toll Fraud

Securing CTI/JTAPI Connections

Restricting Administrative Access (User Roles and Groups)

Fighting Spam Over Internet Telephony (SPIT)

CUCM Security Audit (Logs)

Table of Contents

Single Sign-On (SSO)

Summary

Chapter 10 Cisco Unity and Cisco Unity Connection Security

Cisco Unity/Unity Connection Platform Security

Securing Cisco Unity/Unity Connection Web Services

Preventing Toll Fraud

Secure Voicemail Ports

Secure LDAP (LDAPS) for Cisco Unity Connection

Securing Cisco Unity/Unity Connection Accounts and Passwords

Cisco Unity/Unity Connection Class of Service

Cisco Unity/Unity Connection Secure Messaging

Cisco Unity/Unity Connection Security Audit (Logs)

Cisco Unity Connection Single Sign-On (SSO)

Summary

Chapter 11 Cisco Unified Presence Security

Securing Cisco Unified Presence Server Platform

Securing CUPS Integration with CUCM

Securing CUPS Integration with LDAP (LDAPS)

Securing Presence Federation (SIP and XMPP)

Cisco Unified Personal Communicator Security

Summary

Chapter 12 Cisco Voice Gateway Security

Cisco Voice Gateway Platform Security

Preventing Toll Fraud on Cisco Voice Gateways

Securing Conference Resources

Securing Voice Conversations on Cisco Voice Gateways

Securing Survivable Remote Site Telephony (SRST)

Monitoring Cisco Voice Gateways

Summary

Chapter 13 Cisco Voice Gatekeeper and Cisco Unified Border

Table of Contents

Element Security

Physical and Logical Security of Cisco Gatekeeper and Cisco Unified Border Element

Gatekeeper SecurityWhat Is It All About?

Securing Cisco Gatekeeper

Cisco Unified Border Element Security

Summary

Chapter 14 Cisco Unified Communications Manager Express and Cisco Unity Express Security

Cisco Unified Communications Manager Express Platform Security

Preventing Toll Fraud on Cisco Unified Communications Manager Express

Cisco Unified CME: AAA Command Accounting and Auditing

Cisco IOS Firewall for Cisco Unified CME

Cisco Unified CME: Securing GUI Access

Cisco Unified CME: Strict ephone Registration

Cisco Unified CME: Disable ephone Auto-Registration

Cisco Unified CME: Call Logging (CDR)

Cisco Unified CME: Securing Voice Traffic (TLS and SRTP)

Securing Cisco Unity Express Platform

Enabling AAA for Cisco Unity Express

Preventing Toll Fraud on Cisco Unity Express

Cisco Unity Express: Secure GUI Access

Summary

Chapter 15 Cisco IP Telephony Endpoint Security

Why Is Endpoint Security Important?

Cisco Unified IP Phone Security

Cisco Unified Wireless IP Phone Security

Securing Cisco IP Communicator

Summary

Part IV: Cisco IP Telephony Network Management Security

Table of Contents

Chapter 16 Cisco IP Telephony: Network Management Security

Secure IP Telephony Network Management Design

Securing Network Management Protocols

Secure Network Monitoring with SNMPv3

Syslog

Secure Shell (SSH)

HTTP/HTTPS

Securing VNC Management Access

Securing Microsoft Remote Desktop Protocol

TFTP/SFTP/SCP

Managing Security Events

Summary

Part V: Cisco IP Telephony Security Essentials

Appendix A: Cisco IP Telephony: Authentication and Encryption Essentials

Appendix B: Cisco IP Telephony: Firewalling and Intrusion Prevention

Glossary

A

B

C

D

E

F

G

H

I

L

Pearson

Table of Contents

M
N
O
P
Q
R
S
T
U
V
W
X
Z
Index