



IP COMMUNICATIONS

Securing Cisco IP Telephony Networks

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

Securing Cisco IP Telephony Networks

Akhil Behl

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Securing Cisco IP Telephony Networks

Akhil Behl
Copyright © 2013 Cisco Systems, Inc.
Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing September 2012

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58714-295-6

ISBN-10: 1-58714-295-3

Warning and Disclaimer

This book is designed to provide information about securing Cisco IP Telephony networks. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S. please contact:
International Sales
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger	Business Operation Manager, Cisco Press: Anand Sundaram
Associate Publisher: Dave Dusthimer	Manager Global Certification: Erik Ullanderson
Executive Editor: Brett Bartow	Development Editor: Eleanor C. Bru
Managing Editor: Sandra Schroeder	Copy Editor: Apostrophe Editing Services
Project Editor: Seth Kerney	Technical Editors: Zeeshan Farees, Alvin Laguerta
Editorial Assistant: Vanessa Evans	Cover Designer: Gary Adair
Composition: Mark Shirar	Proofreader: Sheri Cain
Indexer: Larry Sweazy	



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCOVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigADrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author

Akhil Behl, CCIE No. 19564, is a Senior Network Consultant in Cisco Services, focusing on Cisco Collaboration and Security Architectures. He leads collaboration and security projects worldwide for Cisco Services and the Collaborative Professional Services (CPS) portfolio for the commercial segment. Prior to his current role, he spent ten years working in various roles at Linksys as a Technical Support Lead, as an Escalation Engineer at Cisco Technical Assistance Center (TAC), and as a Network Consulting Engineer in Cisco Advanced Services.

Akhil has a bachelor of technology degree in electronics and telecommunications from IP University, India, and a master's degree in business administration from Symbiosis Institute, India. He is a dual Cisco Certified Internetwork Expert (CCIE) in Voice and Security. He also holds many other industry certifications, such as Project Management Professional (PMP), Information Technology Infrastructure Library (ITIL) professional, VMware Certified Professional (VCP), and Microsoft Certified Professional (MCP). Over the course of his career, he has presented and contributed in various industry forums such as Interop, Enterprise Connect, Cloud Connect, Cloud Summit, Computer Society of India (CSI), Cisco Networkers, and Cisco SecCon. He also has several research papers published to his credit in various international journals.

About the Technical Reviewers

Alvin M. Laguerta, CCIE Voice # 13976, is a Senior Network Consulting Engineer for Cisco Advanced Services Unified Communications (UC) Practice at Cisco Systems. He is the Virtual Team technical lead focused on Unified Communications Security for Voice and Video technologies and helped many customers in planning, designing and deploying UC Security over the past 11 years. Alvin's experience extends into other networking technologies over the course of his 20+ years and holds various industry certifications. Alvin holds a Bachelor of Science in Electronics and Communications Engineering from the University of Santo Tomas, Philippines and MBA in IT Management from WGU, Utah.

Zeeshan Farees, CCIE # 20963, is a Technical Marketing Engineer for Unified Communications Security in the Collaboration and Communications Group at Cisco. Her focus is on security for Voice and Video technologies within the Cisco Unified Communications Solution. She has authored the security content of multiple design guides, including the Cisco Unified Communications Solution Reference Network Design (SRND) document. Prior to becoming a TME, Zeeshan was an Escalation Engineer for Voice related products at the Cisco Technical Assistance Center (TAC). Zeeshan holds a Bachelor of Science degree in Computer Science from the University of Illinois, Urbana-Champaign.

Dedication

This book is dedicated first to my family, my dear wife Kanika and my lovely son, Shivansh, for without their support, encouragement, and patience, it would not exist. Secondly, to my parents Vijay and Ravi Behl, who provided resources and direction when I was young, and inspiration and support as I got older. Lastly, to my brothers, Nikhil and Ankit, who have always been there when I needed them.

Acknowledgments

I would like to thank the following amazing people and teams for helping me create this book.

I would like to thank my wife Kanika. She sacrificed many days and weekends over the past year so that I could work on this book. Without her patience and support, this book would not have been possible.

The technical reviewers, Alvin Laguerta and Zeeshan Farees, for their invaluable feedback and providing exceptional technical coverage.

The Cisco Press team: Brett Bartow, the executive editor, for seeing the value and vision in the proposed title and providing me the opportunity to build this title. Eleanor Bru, development editor, and Christopher Cleveland, senior development editor, for their support and guidance to edit and polish my rough manuscript and develop it into a fine piece of technical literature. It is my sincere hope to work again with them in the near future. Lastly, everyone else in the Cisco Press production team for their support and commitment.

Contents at a Glance

	Introduction	xxiii
Part I	Introduction to Cisco IP Telephony Security	3
Chapter 1	What Is IP Telephony Security and Why Do You Need It?	3
Chapter 2	Cisco IP Telephony Security Building Blocks	19
Chapter 3	What Can You Secure and How Can You Secure It?	35
Chapter 4	Cisco IP Telephony Security Framework	59
Part II	Cisco IP Telephony Network Security	93
Chapter 5	Cisco IP Telephony Physical Security	95
Chapter 6	Cisco IP Telephony Layer 2 Security	105
Chapter 7	Cisco IP Telephony Layer 3 Security	135
Chapter 8	Perimeter Security with Cisco Adaptive Security Appliance	171
Part III	Cisco IP Telephony Application and Device Security	233
Chapter 9	Cisco Unified Communications Manager Security	235
Chapter 10	Cisco Unity and Cisco Unity Connection Security	309
Chapter 11	Cisco Unified Presence Security	339
Chapter 12	Cisco Voice Gateway Security	377
Chapter 13	Cisco Voice Gatekeeper and Cisco Unified Border Element Security	405
Chapter 14	Cisco Unified Communications Manager Express and Cisco Unity Express Security	421
Chapter 15	Cisco IP Telephony Endpoint Security	441
Part IV	Cisco IP Telephony Network Management Security	471
Chapter 16	Cisco IP Telephony: Network Management Security	473
Part V	Cisco IP Telephony Security Essentials	517
Appendix A	Cisco IP Telephony: Authentication and Encryption Essentials	519
Appendix B	Cisco IP Telephony: Firewalling and Intrusion Prevention	551
	Glossary	585

Contents

	Introduction	xxiii
Part I	Introduction to Cisco IP Telephony Security	3
Chapter 1	What Is IP Telephony Security and Why Do You Need It?	3
	Defining IP Telephony Security	4
	What Is IP Telephony?	4
	What Is IP Telephony Security?	4
	What Is the Rationale Behind Securing an IP Telephony Network?	6
	What Can You Do to Safeguard Your IP Telephony Network?	7
	IP Telephony Security Threats	8
	How Do Hackers Attack an IP Telephony Network?	8
	<i>Foot Printing</i>	9
	<i>Scanning</i>	9
	<i>Enumeration</i>	9
	<i>Exploit</i>	9
	<i>Covering Tracks</i>	10
	What Are IP Telephony Security Threats and Countermeasures?	10
	Threats	11
	Countermeasures	12
	An Insight to VoIP Security Tools	12
	IP Telephony Security/Penetration Tools	13
	<i>Sniffing Tools</i>	13
	<i>Scanning and Enumeration Tools</i>	14
	<i>Flooding/DoS Tools</i>	14
	<i>Signaling and Media-Manipulation Tools</i>	15
	Business Challenges and Cisco IP Telephony Security Responses	15
	Common Business Challenges Associated with IP Telephony Security	15
	Cisco IP Telephony Security Responses	16
	Summary	17
Chapter 2	Cisco IP Telephony Security Building Blocks	19
	Introduction to IP Telephony Security Methodology	19
	Understanding the IP Telephony Security Methodology	19
	Demystifying IP Telephony Security Methodology	21
	IP Telephony Security Architecture	22

- Exploring IP Telephony Security Methodology and Defining Security Architecture 24
 - IP Telephony Security Assessment and Security Policy Development 24
 - IP Telephony Network Security Implementation 26
 - Physical Security* 28
 - Layer 2 Security* 29
 - Layer 3 Security* 29
 - Perimeter Security* 30
 - IP Telephony Application Security Implementation 31
- Defining the IP Telephony Network Components That Should Be Secured 32
 - IP Telephony Network Elements That Should Be Secured 32
- Summary 34

Chapter 3 What Can You Secure and How Can You Secure It? 35

- Layered Security Approach for IP Telephony Security 35
 - IP Telephony Layered Security Approach 36
 - Case Study* 36
 - Enabling IP Telephony Security: Layer upon Layer 37
- Cisco IP Telephony Security Controls 40
 - Discovering IP Telephony Security Controls 40
 - Cisco IP Telephony Security Controls 41
 - Cisco IP Telephony Network Security Controls* 41
 - Cisco IP Telephony Device Security Controls* 43
 - Cisco IP Telephony Application Security Controls* 45
 - Cisco IP Telephony Endpoint Security Controls* 48
- Cisco IP Telephony Security Overview 50
 - Discovering End-to-End IP Telephony Security 50
 - Understanding Each IP Telephony Component and its Relative Security Control 52
 - XYZ Headquarters (Main Data Center)* 52
 - IP Telephony Data Center Security Insight* 54
 - IP Telephony Remote Data Center Security Insight* 54
 - IP Telephony Remote Site Security Insight* 56
 - Telecommuter Solution Security Insight* 56
- Summary 57

Chapter 4	Cisco IP Telephony Security Framework	59
	Cisco IP Telephony Security Life Cycle	60
	Enabling IP Telephony Security	61
	<i>Security and Risk Assessment</i>	61
	<i>IP Telephony Security Policy Development and Enforcement</i>	62
	<i>Planning and Designing</i>	63
	<i>IP Telephony Network and Application Security Deployment</i>	63
	<i>Operate and Manage</i>	64
	<i>Monitor</i>	64
	Developing an IP Telephony Security Policy	64
	Building an IP Telephony Security Policy/Strategy In line with Your Corporate Security Policy	64
	Risk Assessment	65
	Components of IP Telephony Security Policy	69
	<i>IP Telephony Security Policy/Strategy</i>	70
	<i>Core IP Telephony Security Policies</i>	72
	Physical Security of IP Telephony Equipment	74
	Physical Security Policy	75
	Local-Area Network Security Policy	76
	Wide-Area Network and Perimeter Security Policy	77
	IP Telephony Server Security Policy	78
	Voice Application Security Policy	79
	Endpoint Security Policy	79
	Conclusion	80
	Evaluating Cost of Security—Cost Versus Risk	80
	Cost of Implementing IP Telephony Security	81
	Cost of a Security Breach	81
	How to Balance Between Cost and Risk	82
	Determining the Level of Security for Your IP Telephony Network	84
	Case Study	84
	<i>The Riddles Are Over</i>	86
	Putting Together All the Pieces	87
	IP Telephony Security Framework	87
	Summary	92

Part II	Cisco IP Telephony Network Security	93
Chapter 5	Cisco IP Telephony Physical Security	95
	IP Telephony Physical Security	95
	What Is IP Telephony Physical Security All About?	96
	Physical Security Issues	97
	Restricting Access to IP Telephony Facility	97
	<i>Securing the IP Telephony Data Center Perimeter</i>	98
	<i>IP Telephony Data Center Internal Security</i>	99
	Personnel Training	100
	Disaster Recovery and Survivability	100
	Locking Down IP Telephony Equipment	101
	Environmental Factors	102
	Summary	103
Chapter 6	Cisco IP Telephony Layer 2 Security	105
	Layer 2 Security Overview	105
	Cisco IP Telephony Layer 2 Topology Overview	106
	Why Bother with Layer 2 Security?	107
	IP Telephony Layer 2 Security Issues and Mitigation	108
	VLAN Hopping Attack and Mitigation	109
	<i>Attack Details</i>	109
	<i>Mitigation</i>	111
	Spanning Tree Protocol (STP) Manipulation	112
	<i>Attack Details</i>	112
	<i>Mitigation</i>	112
	DHCP Spoofing	113
	<i>Attack Details</i>	113
	<i>Mitigation</i>	114
	ARP Spoofing	114
	<i>Attack Details</i>	115
	<i>Mitigation</i>	116
	MAC Address Spoofing Attack	116
	<i>Attack Details</i>	116
	<i>Mitigation</i>	117
	IP Spoofing Attack	119
	<i>Attack Details</i>	119
	<i>Mitigation</i>	120

	CAM Table Overflow and DHCP Starvation Attack	120
	<i>Attack Details</i>	121
	<i>Mitigation</i>	122
	Dealing with Rogue Endpoints: 802.1x	123
	What Is 802.1x and How Does it Work?	123
	EAP Authentication Methods	125
	802.1x for IP Telephony	126
	Layer 2 Security: Best Practices	131
	Summary	133
Chapter 7	Cisco IP Telephony Layer 3 Security	135
	Layer 3 Security Fundamentals: Securing Cisco IOS Routers	136
	Cisco IOS Platform Security	136
	Restricting Management Access	137
	Securing the Console Port	138
	Securing the Auxiliary Port	139
	Securing the VTY Ports	139
	Securing the HTTP Interface	140
	Disabling Unnecessary IOS Services	142
	Small Services	142
	Finger Service	143
	BootP	143
	Cisco Discovery Protocol (CDP)	143
	Proxy ARP	145
	Directed Broadcast	146
	Source Routing	147
	Classless Routing	148
	Configuration Autoloading	148
	Securing TFTP	149
	Securing Routing Protocols	150
	Routing Information Protocol v2 (RIPv2)	151
	Enhanced Interior Gateway Routing Protocol (EIGRP)	152
	Open Shortest Path First (OSPF)	152
	Border Gateway Protocol (BGP)	153
	Securing Hot Standby Routing Protocol (HSRP)	153
	Safeguarding Against ICMP Attacks	154
	ICMP Unreachables	154
	ICMP Mask Reply	154

- ICMP Redirects 154
 - Constraining ICMP 155
- Securing User Passwords 156
- Controlling User Access and Privilege Levels 157
 - Enabling Local Authentication and Authorization 157
 - Enabling External Server-based Authentication, Authorization, and Accounting (AAA) 158
 - Configuring Cisco TACACS+ Based Authentication* 158
 - Configuring Cisco TACACS+ Based Authorization* 159
 - Configuring Cisco TACACS+ Based Accounting* 159
- Antispoofing Measures 160
 - RFC 2827 Filtering 161
 - Unicast Reverse Packet Forwarding (uRPF) 162
- Router Banner Messages 163
- Securing Network Time Protocol (NTP) 164
- Blocking Commonly Exploited Ports 165
- Extending Enterprise Security Policy to Your Cisco Router 165
 - Password Minimum Length 165
 - Authentication Failure Rate 166
 - Block Logins 166
 - Disable Password Recovery 166
- Layer 3 Traffic Protection—Encryption 168
- Layer 3 Security—Best Practices 168
- Summary 169

Chapter 8 Perimeter Security with Cisco Adaptive Security Appliance 171

- IP Telephony Data Center’s Integral Element: Cisco Adaptive Security Appliance 172
 - An Introduction to Cisco ASA Firewall 172
 - Cisco ASA Firewall and OSI layers* 174
 - Cisco ASA Basics 175
 - Cisco ASA: Stateful Firewall* 175
 - Cisco ASA Firewall: Interfaces* 175
 - Cisco ASA Firewall: Security Levels* 177
 - Cisco ASA: Firewall Modes* 179
 - Cisco ASA: Network Address Translation* 180
 - Cisco ASA: UTM Appliance* 180
 - Cisco ASA: IP Telephony Firewall* 181

Securing IP Telephony Data Center with Cisco ASA	182
Case Study: Perimeter Security with Cisco ASA	184
<i>Cisco ASA QoS Support</i>	186
<i>Firewall Transiting for Endpoints</i>	186
<i>Cisco ASA Firewall (ACL Port Usage)</i>	188
Introduction to Cisco ASA Proxy Features	201
Cisco ASA TLS Proxy	203
Cisco ASA Phone Proxy	212
Cisco VPN Phone	222
Cisco VPN Phone Prerequisites	223
Implementing VPN Phone	224
Remote Worker and Telecommuter Voice Security	227
Summary	231
Part III	Cisco IP Telephony Application and Device Security 233
Chapter 9	Cisco Unified Communications Manager Security 235
Cisco Unified Communications Manager (CUCM) Platform Security	236
CUCM Linux Platform Security	237
Certificate-Based Secure Signaling and Media: Certificate Authority Proxy Function	238
Enabling CUCM Cluster Security: Mixed-Mode	240
Security by Default (SBD)	249
TFTP Download Authentication	249
TFTP Configuration File Encryption	250
Trust Verification Service (Remote Certificate and Signature Verification)	251
Using External Certificate Authority (CA) with CAPF	253
Using External Certificate Authority (CA) with Cisco Tomcat	256
Enabling Secure LDAP (LDAPS)	258
Enabling Secure LDAP Connection Between CUCM and Microsoft Active Directory	259
Securing IP Phone Conversation	261
Securing Cisco IP Phones	262
Identifying Encrypted and Authenticated Phone Calls	264
Securing Third-Party SIP Phones	264
Configuring Third-Party SIP Phone	267
Secure Tone	267

CUCM Trunk Security	271
ICT and H.225 (Gatekeeper Controlled) Secure Trunks	271
SIP Trunk Security	273
Inter Cluster Trunk Security	275
SME Trunk Security	275
Trusted Relay Point (TRP)	277
Preventing Toll Fraud	279
Partitions and Calling Search Spaces	280
Time of Day Routing	280
Block Off-Net to Off-Net Transfers	281
Conference Restrictions	281
Calling Rights for Billing and Tracking	281
Route Filters for Controlled Access	282
Access Restriction for Protocols from User VRF	282
Social Engineering	282
Securing CTI/JTAPI Connections	283
JTAPI Client Config	285
Restricting Administrative Access (User Roles and Groups)	286
Fighting Spam Over Internet Telephony (SPIT)	288
CUCM Security Audit (Logs)	290
Application Log	291
Database Log	291
Operating System Log	291
Remote Support Accounting Log	292
<i>Enabling Audit Logs</i>	292
<i>Collecting and Analyzing CUCM Audit Logs</i>	294
Analyzing Application Audit Logs	294
Single Sign-On (SSO)	295
SSO Overview	296
System Requirements for SSO	296
Configuring OpenAM SSO Server	297
Configuring Windows Desktop SSO Authentication Module Instance	300
Configure J2EE Agent Profile on OpenSSO Server	301
Configuring SSO on CUCM	303
Configuring Client Machine Browsers for SSO	306
<i>Internet Explorer</i>	306
<i>Mozilla Firefox</i>	306
Summary	307

Chapter 10 Cisco Unity and Cisco Unity Connection Security 309

- Cisco Unity/Unity Connection Platform Security 310
 - Cisco Unity Windows Platform Security 311
 - OS Upgrade and Patches* 311
 - Cisco Security Agent (CSA)* 311
 - Antivirus* 312
 - Server Hardening* 312
 - Cisco Unity Connection Linux Platform Security 313
- Securing Cisco Unity/Unity Connection Web Services 313
 - Securing Cisco Unity Web Services (SA, PCA, and Status Monitor) 313
 - Securing Cisco Unity Connection Web Services (Web Administration, PCA, and IMAP) 317
- Preventing Toll Fraud 317
- Secure Voicemail Ports 318
 - Cisco Unity: Secure Voicemail Ports with CUCM (SCCP) 319
 - Cisco Unity: Authenticated Voicemail Ports with CUCM (SIP) 321
 - Cisco Unity Connection: Secure Voicemail Ports with CUCM (SCCP) 323
 - Cisco Unity Connection: Secure Voicemail Ports with CUCM (SIP) 324
- Secure LDAP (LDAPS) for Cisco Unity Connection 327
- Securing Cisco Unity/Unity Connection Accounts and Passwords 327
 - Cisco Unity Account Policies 327
 - Cisco Unity Authentication 329
 - Cisco Unity Connection Account Polices 330
- Cisco Unity/Unity Connection Class of Service 331
 - Cisco Unity Class of Service (and Roles) 331
 - Cisco Unity Connection Class of Service (and Roles) 331
- Cisco Unity/Unity Connection Secure Messaging 332
 - Cisco Unity Secure Messaging 332
 - Cisco Unity Connection Secure Messaging 334
- Cisco Unity/Unity Connection Security Audit (Logs) 335
 - Cisco Unity Security Audit 335
 - Cisco Unity Connection Security Audit 337
- Cisco Unity Connection Single Sign-On (SSO) 338
- Summary 338

Chapter 11 Cisco Unified Presence Security 339

Securing Cisco Unified Presence Server Platform	339
Application and OS Upgrades	340
Cisco Security Agent (CSA)	340
Server Hardening	340
Securing CUPS Integration with CUCM	341
Securing CUPS Integration with LDAP (LDAPS)	345
Securing Presence Federation (SIP and XMPP)	345
CUPS SIP Federation Security	347
<i>Intra-Enterprise/Organization Presence SIP Federation</i>	347
<i>Inter-Enterprise/Organization Presence SIP Federation</i>	354
CUPS XMPP Federation Security	364
Cisco Unified Personal Communicator Security	368
Securing CUPC LDAP Connectivity	368
Securing CUPC Connectivity with Cisco Unified Presence	370
Securing CUPC Connectivity with CUCM	371
Securing CUPC Connectivity with Voicemail (Cisco Unity/Unity Connection)	372
Summary	375

Chapter 12 Cisco Voice Gateway Security 377

Cisco Voice Gateway Platform Security	377
Preventing Toll Fraud on Cisco Voice Gateways	378
Call Source Authentication	378
Voice Gateway Toll Fraud Prevention by Default	379
Class of Restriction (COR)	380
Call Transfer and Forwarding	383
Securing Conference Resources	384
Securing Voice Conversations on Cisco Voice Gateways	390
Configuring MGCP Support for SRTP	391
Configuring H.323 Gateway to Support SRTP	394
Configuring SIP Gateway to Support SRTP	396
Securing Survivable Remote Site Telephony (SRST)	399
Monitoring Cisco Voice Gateways	402
Summary	403

Chapter 13 Cisco Voice Gatekeeper and Cisco Unified Border Element Security 405

Physical and Logical Security of Cisco Gatekeeper and Cisco Unified Border Element	405
Gatekeeper Security—What Is It All About?	406
Securing Cisco Gatekeeper	406
Restricted Subnet Registration	407
Gatekeeper Accounting	407
Gatekeeper Security Option	410
Gatekeeper Intra-Domain Security	410
Gatekeeper Inter-Domain Security	411
Gatekeeper HSRP Security	413
Cisco Unified Border Element Security	414
Filtering Traffic with Access Control List	416
Signaling and Media Encryption	416
Hostname Validation	417
Firewalling CUBE	417
CUBE Inherited SIP Security Features	418
Summary	420

Chapter 14 Cisco Unified Communications Manager Express and Cisco Unity Express Security 421

Cisco Unified Communications Manager Express Platform Security	422
Preventing Toll Fraud on Cisco Unified Communications Manager Express	422
After-Hours Calling Restrictions	422
Call Transfer Restriction	423
Call Forward Restriction	424
Class of Restriction	425
Cisco Unified CME: AAA Command Accounting and Auditing	425
Cisco IOS Firewall for Cisco Unified CME	426
Cisco Unified CME: Securing GUI Access	426
Cisco Unified CME: Strict ephone Registration	427
Cisco Unified CME: Disable ephone Auto-Registration	428
Cisco Unified CME: Call Logging (CDR)	428
Cisco Unified CME: Securing Voice Traffic (TLS and SRTP)	429
Securing Cisco Unity Express Platform	435
Enabling AAA for Cisco Unity Express	437

Preventing Toll Fraud on Cisco Unity Express	438
Cisco Unity Express: Secure GUI Access	440
Summary	440

**Chapter 15 Cisco IP Telephony
Endpoint Security 441**

Why Is Endpoint Security Important?	442
Cisco Unified IP Phone Security	443
Wired IP Phone: Hardening	443
<i>Speakerphone</i>	444
<i>PC Port</i>	445
<i>Settings Access</i>	445
<i>Gratuitous Address Resolution Protocol ARP (GARP)</i>	445
<i>PC Voice VLAN Access</i>	445
<i>Video Capabilities</i>	446
<i>Web Access</i>	446
<i>Span to PC Port</i>	446
<i>Logging Display</i>	447
<i>Peer Firmware Sharing</i>	447
<i>Link Layer Discovery Protocol: Media Endpoint Discover (LLDP-MED)</i>	
<i>Switch Port</i>	447
<i>Link Layer Discovery Protocol (LLDP) PC Port</i>	447
Configuring Unified IP Phone Hardening	447
Wired IP Phone: Secure Network Admission	448
Wired IP Phone: Voice Conversation Security	448
Wired IP Phone: Secure TFTP Communication	449
Cisco Unified Wireless IP Phone Security	449
Cisco Wireless LAN Controller (WLC) Security	450
Cisco Wireless Unified IP Phone Security	454
Hardening Cisco Wireless IP Phones	454
<i>Profile</i>	455
<i>Admin Password</i>	455
<i>FIPS Mode</i>	456
Securing a Cisco Wireless IP Phone	456
Securing Cisco Wireless Endpoint Conversation	456
Securing Cisco Wireless Endpoint Network Admission	457
<i>Using Third-Party Certificates for EAP-TLS</i>	457
Wireless IP Phone: Secure TFTP Communication	463

Securing Cisco IP Communicator	463
Hardening the Cisco IP Communicator	464
Encryption (Media and Signaling)	465
Enable Extension Mobility for CIPC	466
Lock Down MAC Address and Device Name Settings	467
Network Access Control (NAC)-Based Secured Network Access	469
VLAN Traversal for CIPC Voice Streams	469
Summary	470




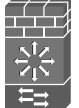










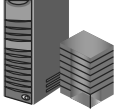


















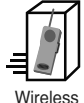


















Part IV Cisco IP Telephony Network Management Security 471

Chapter 16 Cisco IP Telephony: Network Management Security 473

Secure IP Telephony Network Management Design	473
In-Band Network Management	474
<i>Securing In-Band Management Deployment</i>	475
Out-of-Band (OOB) Network Management	475
<i>Securing OOB Management Deployment</i>	476
Hybrid Network Management Design	477
<i>Securing a Hybrid Network Management Deployment</i>	477
Securing Network Management Protocols	478
Secure Network Monitoring with SNMPv3	479
Cisco IP Telephony Applications with SNMPv3 Support	480
SNMP for Cisco IOS Routers and Switches	483
SNMP Deployment Best Practices	485
Syslog	485
Secure Syslog for IP Telephony Applications	486
Configuring Syslog in Cisco Network Devices (Cisco IOS Devices and Cisco ASA)	488
<i>Cisco IOS Devices Syslog</i>	488
<i>Cisco ASA Firewall Syslog</i>	489
Syslog Deployment Best Practices	490
Secure Shell (SSH)	491
Configuring SSH on IOS Devices	492
Enabling SSH Access on Cisco ASA	494
SSH Deployment Best Practices	495
HTTP/HTTPS	495
Enabling Cisco CP for Cisco IOS Routers	496
Enabling Cisco ASA ASDM	498
HTTPS Deployment Best Practices	500

Securing VNC Management Access	500
VNC Deployment Best Practices	501
Securing Microsoft Remote Desktop Protocol	501
Configuring IP Telephony Server for Accepting Secure RDP Connections	502
Configuring RDP Client for Initiating Secure RDP Session	504
RDP Deployment Best Practices	506
TFTP/SFTP/SCP	507
TFTP/SFTP/SCP Deployment Best Practices	508
Managing Security Events	508
The Problem	508
The Solution	509
Cisco Prime Unified Operations Manager (CUOM)	512
Cisco Prime Unified Service Monitor (CUSM)	513
Cisco Unified Service Statistics Manager (CUSSM)	514
Cisco Prime Unified Provisioning Manager (CUPM)	515
Summary	515
Part V	Cisco IP Telephony Security Essentials 517
Appendix A	Cisco IP Telephony: Authentication and Encryption Essentials 519
Appendix B	Cisco IP Telephony: Firewalling and Intrusion Prevention 551
Glossary	585

Icons Used

 Voice-Enabled Switch	 Core Switch (Secure)	 Core Switch	 Data Center Switch with Firewall Module	 Access Layer Switch	 Voice-Enabled Access Router	 IDS / IPS
 Cisco ASA 5500 Series Firewall	 Router with Firewall	 Distribution Layer Switch	 Data Center Switch	 DHCP Server	 AAA Server	 Mail Server
 XMPP Enterprise Server	 Web Server	 LDAP Server	 Microsoft OCS	 Cisco Unified Communications Manager	 Cisco Unity Connection	 Cisco Unified Presence Server
 Cisco Unified Communications Manager Express	 Cisco Unity Express	 Cisco Unity	 TFTP Server	 Cisco Unified Border Element	 CAPF Server	 Cisco Unified Personal Communicator
 Cisco Unified IP Phone	 Cisco Conference Phone	 Cisco IP Communicator	 Voice-Enabled Router	 Voice Gateway / Gatekeeper	 Wireless IP Phone	 PC
 Attacker / Hacker	 Wireless Access Point	 Cisco Wireless LAN Controller	 Lightweight Access Point	 WAN / Internet	 PSTN	 MPLS WAN
 IT Service Provider	 Management Endpoint	 Voice Service Provider Soft Switch	 End User	 Certificate Authority	 Headquarters (Main Data Center)	 Remote / Backup Data Center
 Branch Office / Remote Site	 Telecommuter	 Advance Telecommuter (Remote Worker)				

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ({{ }}) indicate a required choice within an optional element.

Introduction

Over the past several years, I have seen security becoming a key component in network design. With more organizations using IP Telephony as a business instrument today, security is more important than ever. Keeping pace with the rapid security technology evolution and the growing complexity of threats is a challenge, even in the best of times. Understanding and deploying IP Telephony network security is a key factor to determine whether your business, which relies on the same, will succeed.

The past couple of years have witnessed a dramatic increase in the threats to IP Telephony network security in corporate, financial, healthcare, education, and government institutions. The invent of IP Telephony has fundamentally changed the way organizations conduct business and communicate. Reliance on access to collaboration and communication resources has never been greater, which, in turn, makes the impact of IP Telephony network downtime increasingly devastating.

The costs that businesses have incurred over the past few years because of security vulnerabilities are staggering. In addition to the direct costs to your business if you suffer a network security compromise, you can also put other businesses or Internet users at risk because the compromise you suffered can be leveraged to attack against other network devices.

The purpose of this book is to explain an End-to-End IP Telephony Security approach and architecture and to show how each piece of the puzzle fits together. This book is focused on providing you with an in-depth understanding of the Cisco IP Telephony Security principles, features, protocols, and implementation best practices. Most topics start with the basics to help keep the discussion complete. This helps you read the book more easily and comprehend the topics.

The book provides an introduction to the key tools and techniques essential for securing a Cisco IP Telephony network of any size. This book answers the need for an easy-to-understand manual for IP Telephony engineers, managers, and architects seeking the knowledge to make important business and technical decisions. Unlike books that revolve around generic VoIP security concepts, this book is focused on Cisco IP Telephony Security. It addresses the important task of enabling you to implement and maintain a secure, stable, and robust Cisco IP Telephony network. This book provides the answers you need by showing you how to use a layered security approach to secure your Cisco IP Telephony network. This book will be an indispensable resource for anyone who needs to understand, build, and maintain Secure Cisco IP Telephony networks.

Objectives of This Book

The most important and obvious objective of this book is to explain not only the rationale behind securing your Cisco IP Telephony network, but also the best ways to do so to achieve a secure, robust, and resilient IP Telephony network. This book is focused on providing you with an in-depth understanding of the various IP Telephony network security principles, features, protocols, and implementations in today's networks. The goals of this book are as follows:

- Provide a complete discussion at a basic to an advanced level for all topics involved in the implementation of IP Telephony Security in today's networks.
- Provide detailed and in-depth discussion and insight into the workings of the protocols behind Cisco IP Telephony Security implementations.
- Detailed step-by-step walkthroughs of various Cisco IP Telephony application and underlying network gear configuration to achieve the ultimate goal of a secure network, which can evade and restrain attacks from within and outside your organization.
- Discuss security principles and leading practices that form the basis of successful Cisco IP Telephony Security implementations.
- Provide an insight into the operational needs and requirements to set up and maintain a Secure Cisco IP Telephony network.

Who Should Read This Book?

The answer to this question is uncomplicated: Everyone. Anyone who is interested in Cisco IP Telephony and network security should become familiar with the information included in this book. That includes audience from IP Telephony engineers and security engineers to architects to administrators to management and executives. The principles and leading practices covered in this book apply to almost every organization and every business vertical. This book covers not only numerous technical topics and scenarios, but also covers a wide range of operational best practices. This book is a valuable asset to anyone who is tasked with securing IP Telephony networks. In addition to technology perspective, this book provides an all-around business impact perspective of securing what is an asset and the lifeline of the modern-day organizations: IP-based communications. To get the most value from this book, you should have a basic knowledge of IP Telephony, networking, and security.

How This Book Is Organized

This book is both a reference and a guide. It begins by describing the quintessence of IP Telephony Security and by examining the threats that thwart today's IP Telephony networks. As technologies are dramatically changing the way we work and collaborate, there are associated risks and threats that you must think about. This book follows a

logical path that begins by giving you a quick introduction to the reasons why you must secure your Cisco IP Telephony network followed by IP Telephony network security mechanisms, and continues by showing you what you need to do to have your Cisco IP Telephony network secured, end-to-end.

You learn about the challenges and threats that today's organizations and businesses face as they struggle to fully embrace the value that Cisco IP Telephony has to offer, without sacrificing enterprise security.

This book contains sixteen chapters and two appendixes that cover the core areas of Cisco IP Telephony Security, from basic concepts to advance configurations to leading practices. An overview of each chapter follows.

Part I: Introduction to Cisco IP Telephony Security

- **Chapter 1, “What Is IP Telephony Security and Why Do You Need It?”:** This chapter covers an introduction to IP Telephony as a technology and provides an insight to rationale as to why you should be concerned about the security of your IP-based communications. In addition, it gives an overview of the threats that pester the sanctity of your Cisco IP Telephony network. Moreover, it gives an overview of the attack vectors and follows footsteps of an attacker/hacker to give you an insight to how they go about attacking an IP Telephony network. Finally, this chapter concludes with introduction to IP Telephony Security and penetration tools and addresses questions relevant to business challenges associated with adoption and secure operation of IP Telephony.
- **Chapter 2, “Cisco IP Telephony Security Building Blocks”:** This chapter starts with an introduction to Cisco IP Telephony Security methodology and delves into demystifying the otherwise perceived complex IP Telephony Security methodology. The chapter covers concepts pertinent to layered security, from the physical layer up to the application layer. In addition, Cisco IP Telephony network components that should be secured to attain a robust and secure Cisco IP Telephony network are explored.
- **Chapter 3, “What Can You Secure and How Can You Secure It?”:** In this chapter you learn the layered security approach (Defense-in-Depth strategy), which is instrumental to secure your Cisco IP Telephony network. This chapter details the various components that form the basis of a Cisco IP Telephony network and walks you through their relevant security controls. The chapter presents a case study in which you are introduced to Cisco IP Telephony Security in context to an organization, which has geographically diversified IP Telephony deployment at a main data center, and at a remote (backup) data center, a remote site, and must also support telecommuters.
- **Chapter 4, “Cisco IP Telephony Security Framework”:** This is one of the most important chapters of this book. It covers many important topics such as Cisco IP Telephony Security life cycle, risk assessment, IP Telephony Security strategy, cost of security, and so on. The intent is to help you create a well-defined IP Telephony Security Framework, which acts as a blueprint for planning, deploy-

ment, and management of your secured Cisco IP Telephony network. This chapter starts with insight to specifics of Cisco IP Telephony Security life cycle and then guides you through the risk assessment and IP Telephony Security strategy (policy) development. Topics such as the cost of security (the cost of deploying security versus assuming the risk of security breach) and determining the level of security for your Cisco IP Telephony network are covered in this chapter. A case study fortifies the concept on level of security required and helps you decide what should and shouldn't be considered while planning and deploying security for your IP Telephony network. This chapter concludes with the IP Telephony Security Framework demystified and defined.

Part II: Cisco IP Telephony Network Security

- **Chapter 5, “Cisco IP Telephony Physical Security”:** This chapter covers the topic of physical security as it pertains to Cisco IP Telephony to help you better prepare your network infrastructure, security policies, procedures, and organization as a whole against physical security threats from within and outside of your organization. You will learn numerous tips on how to increase the security of your Cisco IP Telephony network infrastructure and how to better secure critical network assets from human or environmental induced threats.
- **Chapter 6, “Cisco IP Telephony Layer 2 Security”:** This chapter starts with an introduction to OSI Layer 2 security issues as they pertain to Cisco IP Telephony. This chapter explores various threats to Cisco IP Telephony Layer 2 network infrastructure and their mitigation techniques. This is complemented by an introduction of 802.1x technology, followed by a detailed walk-through, which enables you to keep out those rogue endpoints from being admitted into your IP Telephony network. In addition, this chapter provides leading practice recommendations for Layer 2 security.
- **Chapter 7, “Cisco IP Telephony Layer 3 Security”:** This chapter starts with an overview of the OSI Layer 3 security fundamentals. It explains the various kinds of threats that you'll face in securing your Cisco IP Telephony network (Layer 3) infrastructure and the solutions that you can use to deal with these threats. The chapter categorizes security threats and lists some common and not so common security threats you'll face, and an in-depth approach to how you can mitigate them. Cisco router control plane, management plane, and data plane security specifics are discussed in great detail as they pertain to IP Telephony networks. The chapter concludes with leading practice recommendations that you can leverage to secure your IP Telephony network.
- **Chapter 8, “Perimeter Security with Cisco Adaptive Security Appliance”:** This chapter introduces Cisco Adaptive Security Appliance (ASA) as an IP Telephony Firewall and shows you how to implement your organization's security policy, leveraging the features that the Cisco ASA offers. The chapter builds on Cisco ASA Firewall's functionality as a data center perimeter firewall followed by an introduction and detailed configuration of IP Telephony-centric features such as TLS Proxy, Phone Proxy, VPN Phone, and Telecommuter VPN features. All these

features are detailed and their relevant configuration examples are presented in an easy-to-follow manner. This chapter lays the groundwork for the firewall technologies that Cisco offers to protect the perimeter of your IP Telephony network.

Part III: Cisco IP Telephony Application and Device Security

- **Chapter 9, “Cisco Unified Communications Manager Security”:** The cost-savings and features introduced with Voice over IP (VoIP) solutions can be significant. However, these benefits can be heavily impacted if you do not have the appropriate security mechanisms in place to control the heart and soul of your Cisco IP Telephony network, the call control, which makes this chapter an indispensable companion to the security of your IP Telephony network. This chapter covers detailed steps to secure a multitude of technologies pertaining to the Cisco UCM and its integration with applications and endpoints, for example, secure phone conversations, secure trunks to ITSP and gateways, thwart toll fraud, secure CTI/JTAPI connections, and fighting SPIT. In addition, this chapter addresses the requirements to enable auditing on your Cisco UCM and to integrate it with a Single-Sign On solution for your organization.
- **Chapter 10, “Cisco Unity and Unity Connection Security”:** This chapter covers both Cisco Unity and Cisco Unity Connection voice messaging solution security, from an application and from a platform perspective. In this chapter you learn how to secure Cisco Unity/Unity Connection voice messaging platforms to curb toll fraud, eavesdropping, Man-In-The-Middle, and account hijacking attacks. In addition, you are introduced to secure integration of Cisco Unity/Unity Connection with Cisco Unified Communications Manager, Cisco Unified IP Phones, Cisco Unified Personal Communicator, and other applications. This chapter details how you can reinforce end user-to-administrator rights at granular level and how to enable audit for the voicemail system.
- **Chapter 11, “Cisco Unified Presence Security”:** This chapter starts with a discussion around the security of Cisco Unified Presence solution. It then delves deep into the Secure Presence Federation – Intra-domain and Inter-domain for Cisco Unified Presence servers and the Microsoft OCS Server respectively, where detailed examples help you comprehend secure federation fundamentals as well as associated advance topics. The chapter concludes with a deep dive into the Cisco Unified Personal Communicator Security, which ensures that you have all the ammunition you need from a knowledge standpoint to protect the softphone client.
- **Chapter 12, “Cisco Voice Gateway Security”:** This chapter starts with an introduction to Cisco IOS Voice Gateway platform security. It then walks you through one of the most drastic issues, toll fraud – its intricacies and remediation. This chapter provides guidance and detailed examples to implement secure conferencing and securing voice media and signaling streams pertinent to protocols and applications on Voice Gateways for SIP to H.323 to MGCP to SRST. In addition, you will learn about strategies and methodologies for monitoring your Cisco Voice Gateways.

- **Chapter 13, “Cisco Voice Gatekeeper and Cisco Unified Border Element Security”:** This chapter builds on Cisco IP-IP Gateway Security, which becomes of paramount importance when you liaise with third-party and IT Service Provider (ITSP) networks. It covers Cisco Voice Gatekeeper and Cisco Unified Border Element security. It presents easy-to-comprehend concepts and examples to ensure that you are well equipped to restrain threats originating from your partner organizations and ITSP network.
- **Chapter 14, “Cisco Unified Communications Manager Express and Cisco Unity Express Security”:** This chapter provides a comprehensive coverage of security of Cisco Unified Communications Manager Express call-control solution and Cisco Unity Express voice-messaging solution. Detailed configuration examples help you build on a plan and execute the plan to secure the express communication solution from Cisco. You will comprehend solutions to security issues such as toll fraud, user authentication/authorization, insecure configuration and management access, rogue endpoint admission, and so on.
- **Chapter 15, “Cisco IP Telephony Endpoint Security”:** This chapter covers the security of Cisco Unified IP Phones, Cisco Wireless IP Phones, and Cisco IP Communicator. The chapter starts with a discussion about the importance of endpoint security and walks you through various attack vectors pertinent to Cisco Unified IP Phones and softphones. You will learn about securing Cisco Unified IP Phones (wired and wireless) by hardening the endpoints as well as securing the network connectivity. In addition, you will comprehend voice media and signaling security as it pertains to wired and wireless Cisco Unified IP Phones. You will find comprehensive coverage of wireless Cisco Unified IP Phones as well as underlying wireless infrastructure security. The chapter concludes with addressing security concerns around Cisco IP Communicator as a softphone from an administrative and system perspective.

Part IV: Cisco IP Telephony Network Management Security

- **Chapter 16, “Cisco IP Telephony: Network Management Security”:** This chapter focuses on securing IP Telephony network and application management aspect. The chapter starts with an insight to various network management options such as In-Band, Out-Of-Band, and Hybrid management setups. Then it covers the wide spectrum of management protocols for Cisco IP Telephony network and applications, for example Telnet, SSH, VNC, RDP, SNMP, Syslog, ASDM, Cisco Configuration Professional, and so on, and the particulars about how you can ensure the security of these management protocols in a sustainable and efficient manner. Detailed practical examples help you plan for and execute secure management setup for your IP Telephony network. The last part of the chapter briefly discusses the Security Event Management System (SEMS) that you can envision and deploy for attack event correlation and central logging leading to event aggregation.

Part V: Cisco IP Telephony Security Essentials

- **Appendix A, “Cisco IP Telephony: Authentication and Encryption Essentials”:**
This appendix covers the basics of Cisco IP Telephony Security. It covers basic to advance concepts such as authentication, encryption, Public Key Infrastructure (PKI), certificates, and everything else that as a technology component helps you secure your Cisco IP Telephony network. This appendix is a great primer for people who are new to the world of Cisco IP Telephony and network security, and a refresher for veterans.
- **Appendix B, “Cisco IP Telephony: Firewalling and Intrusion Prevention”:**
This appendix leads you into a deep insight of the Cisco Firewall and Intrusion Prevention and Detection technology as it pertains to Cisco IP Telephony network and application security. This appendix helps you be cognizant of the Cisco ASAs advance firewall features as well as Cisco IOS Firewall benefits and features for small organizations. Detailed configuration examples combined with real-life experiences help you achieve optimum security without sacrificing performance or features. Moreover, leading practice recommendations on deployment of Intrusion Prevention Solutions (network and host) pave the way for you to make tactical decisions to secure your Cisco IP Telephony network.

This page intentionally left blank

Cisco IP Telephony Security Framework

The threats, the remediation, IP Telephony Security methodology and much more has been discussed in previous chapters. However, the objective has always been to amalgamate IP Telephony and conventional data services onto a shared network infrastructure, without compromising the security of either service. The intention has been to apply protective mechanisms against all types of attacks that must be applied in a holistic manner throughout the enterprise network. The two main principles of an IP Telephony Security Framework are the simplification of design and configuration, and the limitation of exposure.

It is time to start putting together your IP Telephony network security strategy together. With the basics of what makes your secure IP Telephony network out of the ordinary, it is time to move on and choose the best style of security network to suit your needs. In many ways, this can be a subjective process because you might prefer one type of network security rather than another regardless of objective criteria. There's nothing wrong with taking that approach as long as you're armed with the facts, and that's what this chapter is all about.

This chapter covers the following topics:

- Cisco IP Telephony Security life cycle
- Develop an IP Telephony Security policy
- Evaluate cost versus risk
- Determine the level of security required for your IP Telephony network
- Develop Cisco IP Telephony Security Framework

Cisco IP Telephony Security Life Cycle

Cisco understands and values the importance of network security and continuously drives toward building robust, scalable, and secure products, and networks. It is vital that security is induced in design wherever possible (rather than implemented post-deployment of the network). The process of developing and securing your IP Telephony network should follow what is popularly known as a *security wheel*. After developing an IP Telephony Security policy, you can secure your IP Telephony network. (An IP Telephony Security policy acts as a guide for implementing various security measures without which the IP Telephony network security will neither be complete nor based on the ethics and principles of your organization.)

The security wheel, as shown in Figure 4-1, projects the verity that IP Telephony network security is a continuous process built around your corporate security policy.

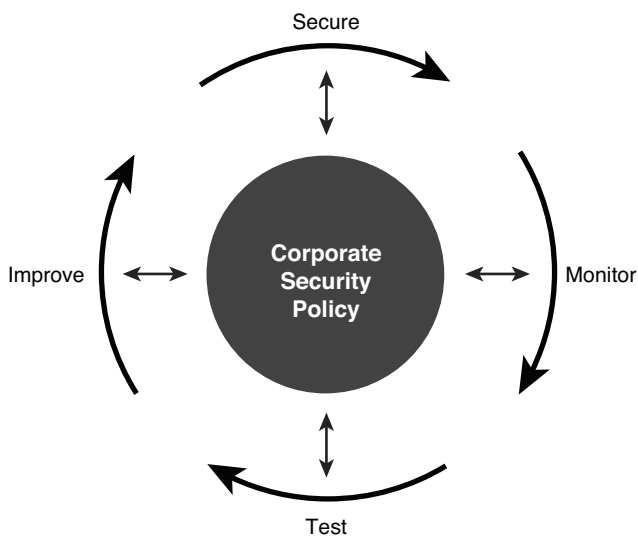


Figure 4-1 *Cisco Security Wheel*

After the IP Telephony network is secured, it should be monitored for any deviations from normal behavior, for example, abnormal usage of services, network and application level attacks, illicit scans, and log analysis to ensure that it stays secure.

After the monitoring phase comes the testing phase. Testing can be done by an organization, or it can be outsourced to a third-party, such as the Cisco Advanced Services. Network and IP Telephony administrators and engineers should use the information from the monitoring and testing phase to make improvements to the security implementation. They should also adjust the IP Telephony Security policy as new vulnerabilities and risks are identified.

For more details on the security services offered by Cisco Advance Services and other security groups within Cisco, visit http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

Enabling IP Telephony Security

Implementing and enabling IP Telephony Security is neither a single step nor a one-time process. It is a constant and continually improving cycle, which must be reiterated time and again as and when new threats evolve or new requirements need to be addressed.

Figure 4-2 illustrates the IP Telephony Security cycle and its various phases.

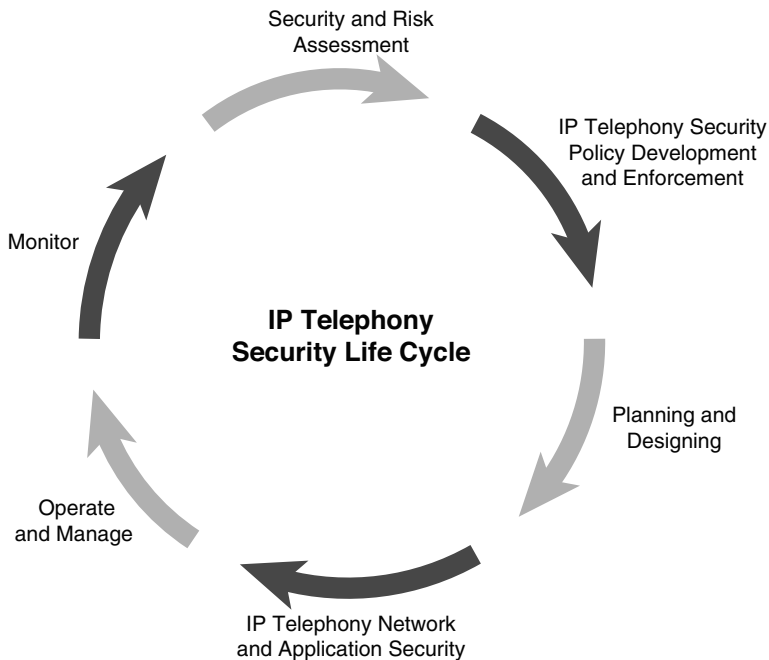


Figure 4-2 *IP Telephony Security Life Cycle*

At the core, this cycle is based on the Cisco security wheel; however, it is more detailed and explicit toward the IP Telephony network security process.

Security and Risk Assessment

The process begins at security and risk assessment; during this stage any new or existing vulnerabilities and security loopholes are discovered. During this phase, a rigorous process consisting of multiple objectives is carried out. These include however not limited to the following:

- Evaluating and identifying the principle assets
- Identifying any existing security concerns

- Exploring any possible new threats or attack vectors
- Evaluating the cost of security

The security assessment of the enterprise IP Telephony network infrastructure helps support key business processes. The IP Telephony Security assessment should cover the following elements of your IP Telephony environment:

- Network devices (routers and switches) vulnerabilities
- Network and security services (firewall, routing protocols, and anti-spoofing services)
- Network access layer, where endpoints connect to the network, and the distribution and core layers of the internal network
- IP Telephony services, endpoints, and applications, such as Presence, IP Phones, Call Control, gateways, and so on

The objective of security assessment is to identify potential weaknesses in your IP Telephony network, which may lead to toll fraud, denial-of-service (DoS), eavesdropping on voice calls, and unauthorized access to voice mail systems within your IP Telephony environment. The result is a report on the network security posture, including recommendations for network infrastructure and IP Telephony application security improvements.

Note: The assessment report should ideally include a priority list of suggestions on how to decrease risks, adapted to the environment and special needs of an organization.

Risk assessment helps identify the vital assets of your IP Telephony network and evaluate the potential cost of security. The topic of risk assessment is covered in detail in the section “Risk assessment.” The completion of the risk assessment phase triggers the next phase, in which IP Telephony Security policy (strategy) is developed.

IP Telephony Security Policy Development and Enforcement

The process of development and enforcement of IP Telephony Security policy is based on corporate security policy and objectives. An IP Telephony Security policy is much like a network security policy. However, the major difference is that the IP Telephony Security policy is explicitly developed for IP Telephony network covering the network, applications, and services relevant to IP Telephony infrastructure and services. You must recognize that the development of an IP Telephony Security policy is not a lone effort by the IP Telephony team. Instead, it should be done in collaboration with the network and security teams to ensure that all aspects and view points are covered as they pertain to IP Telephony Security.

Note: Do not be surprised if your organization does not have any existing IP Telephony Security policy because most organizations tend to apply or extend the network security policy to their IP Telephony network. It is however vital to have a specific IP Telephony Security policy to tackle the issues that a network security policy just cannot address.

Planning and Designing

The subsequent phase is the planning and designing phase, in which you plan and design the blueprint for deployment of your IP Telephony network. As a best practice, it is in this phase that you should integrate security with the design being developed instead of deploying security after your IP Telephony network has been deployed. The design should be such that the IP Telephony network and the services based on it are scalable, robust, supple, and most obviously, secure. The planning for deployment should include security as the integral component and should be done in such a manner that a layered security approach is adopted instead of concentrating security at one point, for example, at enterprise perimeter.

Note: If an IP Telephony network is a green field deployment, it is optimum to incorporate security in design. If the IP Telephony network is already set up, then following assessment and policy phases, you can skip to the application and network security phase.

IP Telephony Network and Application Security Deployment

This is the phase where maximum action can be expected. It goes right from deploying and enabling security on IP Telephony applications (Call Manager and Unity Connection) on servers to IP Telephony network (access layer switches, routers) to IP Telephony endpoints. As mentioned earlier, if security is planned into the design, it becomes much easier to implement in coherence with the underlying functional network. In other words, implementing security for IP Telephony network becomes seamless.

IP Telephony network security can be organized into the following categories:

- Hardware and device security (endpoints and servers)
- Network security (Layers 2 and 3 and upper layers)
- Application security (Call Control, voice messaging, presence, and so on)
- Management and monitoring (SSH and logging)

Operate and Manage

In this penultimate phase, you leverage the services offered by your IP Telephony network. It is time to reap the benefits of your hard work! Your IP Telephony network is fully operational, and you could bring it into production. However, it is also time to ensure that things go the way they were planned and that there are minimal hiccups from the intended operational and management perspective. Ensure that proper administrative and other privileges are assigned to the intended authorized staff. Furthermore, ensure that only the legitimate users can leverage the IP Telephony services without any loss of service or disruption in the IP Telephony environment. This phase almost amalgamates with the last phase, that is, monitor the IP Telephony network.

Monitor

At this point, your IP Telephony network should be under ideal conditions fully functional, and to ensure that it remains that way, you must consistently keep an eye on the health of your IP Telephony network. IP Telephony monitoring tools, techniques, security, and best practices are discussed in Chapter 16, “Cisco IP Telephony: Network Management Security.” Monitoring and responding to potential threats is a manifold process and requires monitoring and reporting any ‘deviations’. Now, let’s consider the scope of word deviation in perspective of IP Telephony network management and monitoring. Deviation could be described on one hand as the anomaly induced by improper or unjustified use of the services provided by your IP Telephony network. On the other hand it can be described as the threats that have matured and cause the loss of integrity, confidentiality, and availability of your IP Telephony network. Thus, it becomes paramount to have proper monitoring mechanisms in place and have these deviations reported as soon as they are discovered so that they can be dealt with either via an automatic defense system (for example, Firewall, Network IPS, or Host IPS) or manually.

Developing an IP Telephony Security Policy

This section covers the intricacies behind building an IP Telephony Security policy because without one you cannot enforce IP communications’ pertinent security effectively.

Building an IP Telephony Security Policy/Strategy In line with Your Corporate Security Policy

An IP Telephony network security policy (the words policy and strategy will be used interchangeably) defines a construct to protect the assets connected to a network that supports IP Telephony, based on a risk assessment analysis. It defines the access limitations and rules for accessing various assets connected to an IP Telephony network. It is the source of information for users and administrators as they set up, use, and audit the network.

It is imperative that the IP Telephony network security policy is general and broad in scope. This implies that it should provide a high-level view of the corporate ideology based on which security-related decisions should be made. However, it should not go into the details of how the policy should be implemented. The rationale is that the details can change overnight, but the general principles of what these details must achieve should remain the same. An IP Telephony Security policy needs to balance between ease of use and ease of implementation, network performance, and the security aspects in defining the rules and regulations.

Building an IP Telephony Security policy is not a one-time process. It requires adjusting policy as per new requirements, objectives, threats, or challenges. Also, IP Telephony Security policy is not an isolated or a single team effort. It requires participation and support from all segments: the IP Telephony team, network team, security team, and most importantly, management (executive sponsor). The security policy needs to be supported by management and other respective engineering teams within an organization; otherwise, it is difficult to have user buy-in.

Note: A security policy is not a static document and must be updated on a regular basis depending on the need to address new security challenges or to meet organizational objectives. For example, if an organization supports remote working (telecommuters), it is not feasible to chalk off remote access. Furthermore, a security policy is intended to harden the system with rules however not to deteriorate any process or production potential.

The first step toward developing an effective IP Telephony Security policy is to assess the risk associated with the network assets to be protected. Risk assessment in quintessence is a method to outline why the resources in your IP Telephony network should be protected. The next section investigates risk assessment and the fundamentals of the risk assessment process for an IP Telephony network.

Risk Assessment

Let us go over this intriguing topic to understand what goes behind performing a risk assessment exercise and why it might just save you from a certain catastrophe.

Note: As pointed out earlier in Chapter 2, “Cisco IP Telephony Security Building Blocks,” the IP Telephony Security assessment includes the plans for areas that have scope for improvement. Risk assessment is partially covered in almost every security assessment.

At a high level, the risk management process helps you attain the following goals:

- **It helps achieve the organization’s objectives (vision and goals):** By highlighting the assets that are important or central to an organization’s functions. This helps protect those vital assets.

- **It ensures the network and infrastructure availability for rightful users:** By helping categorizing network assets in terms of their importance for the network to be up and running, thereby helping with the scale of economy.
- **It assists in maintaining a strong security posture:** To deter attacks against an organization's vital assets by deploying appropriate security controls against identified and potential threats.
- **It ensures compliance with organization's rules, regulations, standards, and policies:** By helping to understand the various components of the network that could be exploited and misused, thereby building policies, rules, and regulations around their use or access mechanisms.

Figure 4-3 gives an insight to the various benefits perceived by carrying out the risk management process.



Figure 4-3 *Risk Management: Areas Addressed*

A typical IP Telephony risk assessment activity may well be outlined via the following steps:

- Step 1.** Identify sensitive information and critical systems.
- Step 2.** Estimate the value of IP Telephony system (information and components).
- Step 3.** Identify potential threats and vulnerabilities to your IP Telephony network (covered in security assessment).
- Step 4.** Estimate the likelihood of a potential attack or penetration being realized.
- Step 5.** Identify countermeasures against perceived threats and vulnerabilities (covered in security assessment).
- Step 6.** Estimate the cost of implementing countermeasures versus not implementing them.

Step 7. Select suitable countermeasures for implementation (covered in security assessment).

Before taking a deep dive to understand the different processes that work within a risk assessment exercise, you must realize an important fact. Not all risks are present and applicable in all different types of IP telephony implementations; every IP Telephony network is unique and has its own set of strengths and weaknesses. However, it is important to create an overall IP Telephony Security policy or strategy in which all assets, potential risks, existing issues, and mitigation methods are listed. Although, it is advisable to perform a risk assessment on existing IP telephony implementation(s), it is equally important to perform an initial risk assessment, including a review of the impact on the data network for new implementations.

Step 1. Identify Sensitive IP Telephony Information and Critical Systems

Organizations should pinpoint the various systems that form the baseline for IP Telephony, from internal servers to external network components, to understand where their critical information may potentially be stored, processed, managed, or viewed. As a disseminated system, IP Telephony network has many individual components that must be protected. Any attack vector realized at any point of time can render the system unusable for legit users. This includes and is not limited to the following:

- Endpoints and servers targeted for DoS/DDoS or MITM attacks
- Changes in routing protocols, leading to failed or hijacked calls
- Change in the IP Telephony application or device configuration

Step 2. Estimate the Value of IP Telephony System (Information and Components)

After identifying the critical information and systems, organizations can then estimate the value of data loss based on where sensitive information is sent, depending on who sends it, and how often it happens. For example, an organization may find that the majority of data loss risks are associated with employees inside the organization who unconsciously put information at risk in the course of their day-to-day activities at work, for example, placing CDR data on a USB drive in preparation to work at home. Also, an estimate of loss of revenue because of a loss of communication or unavailability of the IP Telephony system should be evaluated.

Step 3. Identify Potential Threats and Vulnerabilities to Your IP Telephony Network

Identifying the threats to your IP Telephony network and understanding the vulnerabilities (gaps) is the key to secure your network. Threats can be various, such as the following:

- Inside attacks from malicious users
- Outside attacks from hackers and phreakers

- Viruses, Trojan horses, and worms
- DoS or DDoS
- Man-in-the-middle attacks
- Hardware or software failures
- Loss of critical systems

Vulnerability can range from a simple software defect to a sophisticated implementation for application and network security. A gap could be introduced because of a defect that may allow an attacker to implant a back door or because there was no host protection applied, as the system was supposed to be insulated.

Step 4. Estimate the Likelihood of a Potential Attack/Penetration Being Realized

To assess the probability of an attack from malicious individuals who are either inside or outside the organization and network, application security or penetration tests could be carried out. No matter if these tests are conducted by security professionals inside the organization or outside (for example, third-party security consultants), the end result should be to identify the specific attack vectors that may be used by malicious users or outsiders to gain access to critical information and, in turn, identify and validate potential vulnerabilities that could lead to data loss.

Step 5. Identify Countermeasures Against Perceived Threats and Vulnerabilities

At the termination of an information security revelation or a penetration assessment, an organization should develop an alleviation plan based on their risk tolerance. This plan should detail the findings of the information exposure risks and explain the estimated business impact in case a vulnerability is exploited or an attack is established. The report must also address an assessment of the security measures currently in place.

Most importantly, organizations must also formulate a prioritized action plan for remediation together with a list of recommendations to enhance security and reduce risk.

Step 6. Estimate Cost of Implementing Countermeasures Versus Not Implementing Them

Always remember that security is a balance between risk and cost. To achieve a balance, there must be a plan well in advance and resources to put the plan in action. Too less or too much security can be a serious disadvantage to your IP Telephony network because it will either pave a way for the attackers to invade your network or may cost much more than you expected it to (in terms of financial and performance cost). For example, elevated operational costs because of fraudulent usage of the system by unauthorized users and high-usage bills can ensue.

Note: Since the equation of cost versus risk is a delicate one, you need to comprehend it and understand what you can do within your budget to apply the best possible yet effective security. This topic is covered in detail in the section, “IP Telephony Security Cost Versus Risk.”

No two networks and their security needs could possibly be similar, and the same applies to IP Telephony network as well. Thus, to cover this topic, that is the level of security required, there’s a dedicated section that explains the level of security required for your IP Telephony network to enable you to make the right decisions for your network.

Step 7. Select Suitable Countermeasures for Implementation

The last part of the risk assessment process is the contingency plan. The contingency plan usually consists of what to do if the systems do not work as expected, or in other words, they backfire. For example, if there is a natural or unnatural disaster, what should be done to contain the damage to a minimum. Fortified with the data collected during risk assessment and the final outcome, an organization should have a precise understanding of where its exposures are and how it can leverage this information to take a risk-based, prioritized approach to create a secure IP Telephony environment.

Note: It is important that you classify the data resident on the various servers, end user workstations, and so on. Classification can be done in terms of the type of data “Company Confidential,” “Company Public,” or sensitive client data.

It is important to understand that although risk assessment requires high-level participation and decision making, it’s actually a team effort. The process of risk assessment should be initiated and fronted by the top management in an organization. However, feedback from all levels is required, and everyone right from inventory maintenance to network administration to IP Telephony (telecom) team to CTO should be involved as stakeholders during risk assessment.

Identifying risk and conducting risk assessment are vital components of any successful and comprehensive security strategy. This significantly helps to underline what is valuable and at risk. It helps to ensure that the security planned and applied is effective and is aligned with the organization’s objectives.

Components of IP Telephony Security Policy

There are standards around which a security policy should be built and implemented. These standards are guided by RFC 2196, which lists the elements of a security policy. Although RFC 2196 provides a generic security policy outline, an IP Telephony Security policy should follow these guidelines and be built on the lines of either an existing corporate security policy or developed from scratch.

As described in RFC 2196, “The Site Security Handbook:”

A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.

IP Telephony Security Policy/Strategy

Following is an example of an IP Telephony Security policy built to protect not only the underlying network, but also the IP Telephony servers, applications, endpoints, and related assets.

Note: We are going to consider an example of a fictitious organization XYZ, trying to formulate its IP Telephony Security policy or strategy.

An IP Telephony Security policy statement follows:

It shall be the responsibility of the IP Telephony/IT Department to provide adequate protection and confidentiality of all IP Telephony-specific corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of IP Telephony data, network access, and programs to all authorized members of staff and to ensure the integrity of all data and configuration controls.

The security policy for IP Telephony must address the following areas:

- Acceptable use of organizational IP Telephony equipment (for example, hard phones, soft phones, WLAN phones, voicemail, and conferencing). The acceptable use includes calling plan restrictions (for example, calls to 900 numbers or international calls). These restrictions are also translated to configuration parameters on the respective IP Telephony components (for example, IP-PBX or SIP proxy). Acceptable use of IP Telephony equipment pertains also to contractors, vendors, and other third parties who interact with the organization.
- Protection of IP Telephony services, including the following:
 - Service access (for example, password-protected conferencing sessions and voice mailbox access controls)
 - Signaling and media encryption for interactions in which sensitive information is handled (for example, calls or videoconferencing in which customer or patient health information or financial information is communicated)
- Media retention based on the minimum duration that media should be kept based on regulatory or other industry, state, or federal requirements. The types of media include, but are not limited to, CDRs (call detail records), voicemail, call or videoconferencing recordings, instant messages, or backup.

- Signaling or media interception to satisfy law enforcement requirements (for example, CALEA). Although the requirement for lawful intercept pertains to carrier networks, it is helpful to provide such capability in an enterprise network to support the investigation of unforeseen incidents or circumstances.
- A vulnerability management process should be in place to categorize and prioritize the impact of vulnerabilities that may affect the organization's IP Telephony infrastructure and service.

Summary of Main IP Telephony Security Policies:

- Confidentiality of all data is to be maintained through discretionary and mandatory access controls.
- No Internet and other external service access is allowed to or from IP Telephony data center.
- Calling restrictions access will be implemented globally on all call-control clusters.
- Only authorized IP Telephony and IT staff are allowed to enter the data center. (The only exception is third-party and vendor employees escorted by IP Telephony and the IT team).
- Voice communication will be secured by using encryption techniques and by Layer 2 or Layer 3 mechanisms where possible and required.
- Voice equipment will be placed behind firewalls restricting access to users. A dedicated management VLAN will be used to manage IP Telephony devices.
- Antivirus and HIPS products will be installed and enabled wherever applicable.
- OS and administrator passwords must consist of a mixture of at least eight alphanumeric characters must be changed every 30 days, and must be unique.
- IP Telephony configurations may be changed only by IP Telephony and the IT staff.
- To prevent the loss of availability of IP Telephony resources, measures must be taken to back up data, applications, and configurations of IP Telephony equipment.
- A business continuity plan will be developed and tested on a regular basis.
- Technology purchasing guidelines must be well laid out and defined to ensure that only a vendor that passes certain criteria is to be considered for the IP Telephony solution.
- The authentication, accountability, and access (AAA) policy should clearly define the level of access, authorization for different work levels, and monitoring requirements for the access to IP Telephony system.
- Availability Statement.
- Information Technology Systems and Network Maintenance Policy.
- Supporting information.

Policy General Guidelines and Statements

Following are organization XYZ's IP Telephony Security policy general statements and guidelines.

IP Telephony Technology Purchasing Guidelines:

- All IP Telephony and network-related equipment must be purchased keeping in mind XYZ's requirements for confidentiality, integrity, and availability (CIA).
- It is essential for the equipment to incorporate mechanisms for secure and confidential administration.

Availability Statement:

- The network is available to bona fide users at all times of the day except for outages that occur for various reasons. When a trade-off must be made between confidentiality and network availability, confidentiality is always given priority.

Supporting Information:

- All information regarding XYZ IP Telephony operations must be kept confidential and must never be divulged to sources outside the company. All publicity-related matters should be handled through the Corporate Press Relations office.
- Any later conflicts and issues about the security policy must be resolved with the intervention of the chief security officer, who bears the ultimate responsibility for the security policy.

Policy Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

Core IP Telephony Security Policies

Accountability Policy:

- All users (end users and administrators) of the network are accountable for their actions that may result in network security concerns.
- It is the responsibility of every user to be familiar with the guidelines for the services offered through the XYZ network. Also, every user is responsible to report to the system administrator about any suspected inappropriate use of IP Telephony endpoints or malicious activity on the network.
- All users are accountable for use of their phone and in the manner it is used.

Authentication Policy:

- All information assets on the IP Telephony network require authentication before someone is given access to them. Access attempts are logged for auditing.

- Remote-access users need to go through two layers of authentication to authenticate themselves to the access servers connecting them to the network and then to gain access to individual resources on the network.
- Authentication is carried out using security servers on the network. Steps must be taken to safeguard the security servers against attacks and intrusions from the outside or inside network.
- Authentication should be carried out using one-time passwords. Authentication must be accompanied by authorization and accounting on the security servers. Authorization should be used to restrict user access to resources that are intended for users based on their belonging to a certain group. Accounting should be used to further track authorized user activities. This is a basic safeguard that must be supplemented along with intrusion detection systems.

Acceptable Usage Policy:

- XYZ's IP Telephony network is available for use by employees any time of the day or night for the sole purpose to address business-related conversations.
- Using telephony, voicemail, and all IP Telephony resources for any function that is non business-related or for personal use is prohibited.

Access Policy:

- Data center access will be strictly restricted. Access will be allowed by assuming that all access is denied unless specifically required. Access to IP Telephony data center will be given to only the following:
 - IP Telephony administrators
 - IP Telephony network administrators
 - IP Telephony management team
 - Authorized vendors or third-party employees
- The IP Telephony resources must be accessed while an authorized IT or IP Telephony staff employee is located on the local network or from one of the remote sites or by one of the authorized telecommuters (only through company-approved procedures for remote-access users). Access from any other location is prohibited.
- Access to network resources will be on an as-needed basis. Information assets are protected by giving access to specific groups and denying access to all others. Increasing access privileges for a given asset requires approval from the management.
- All remote users must get management approval before they can use the resources to remotely access the corporate network. Users from the remote sites and telecommuters are treated the same as local users who use network resources. Similar access restrictions are placed on these users for accessing the various network resources.

- Remote-access users must comply with corporate guidelines to make sure that their PCs are safe to connect to the corporate network.
- It is the responsibility of the employees using remote access to ensure that their remote-access equipment is not used by unauthorized individuals to gain access to the resources on the corporate network.

IP Telephony Network Maintenance Policy:

- All IP Telephony and related network equipment is to be managed only by the full-time and authorized employees of XYZ Inc. who have the privileges to do so. Giving an individual permission to work on any network equipment for administrative purposes requires management approval.
- Remote access to administer the networking equipment is allowed, but it requires that the access be done using encryption and that authentication for login access takes place against the security servers. All management sessions, internal and external, must be encrypted.

Violations and Security Incident Reporting and Handling Policy:

- Documented processes must be set up to identify when intrusions and network attacks take place. These processes of detection must include manual reporting and automatic reporting tools.
- The following processes need to be set up for incident reporting and handling:
 - As soon as it has been confirmed that a breach has taken place or an attack is taking place, a process must be invoked to inform all the necessary network administrators of the problem and what their role is in tackling the situation.
 - A process needs to be set up to identify all the information that will be recorded to track the attack and for possible prosecution.
 - A process must be in place to contain the incident that has occurred or that is occurring. The process must be written keeping in mind that confidentiality and integrity is a bigger concern for XYZ than availability.
- A process must be in place to follow up on attacks that have occurred to make sure that all the vulnerabilities exposed through the attack are corrected and that similar attacks can be avoided in the future.

Physical Security of IP Telephony Equipment

Physical Security of IP Telephony equipment must comply with the guidelines as detailed:

- **Data center equipment:** All IP Telephony equipment, which includes IP Telephony servers, appliances, routers, switches, firewalls, and any IP Telephony related data center equipment.

- **High-risk situations:** This refers to any IP Telephony data center area that is accessible:
 - At the ground floor level
 - At the first floor level, but accessible from the adjoining roof
 - At any level via external fire escapes or other features providing access
 - Rooms in remote, concealed, or hidden areas
- **Lockdown devices:** The IP Telephony equipment will be locked down by placing it in dedicated racks placed in the secured data center.

Physical Security Policy

The following section summarizes the required physical security features for an IP Telephony data center or remote sites hosting IP Telephony equipment.

- IP Telephony servers, routers, and switches locked down to rack.
- Racking of equipment away from windows.
- High-risk situations should be addressed by window locks, shutters, and bars.
- Blinds should be deployed for observable windows.
- Intruder alarm installed by an approved company.
- Install movement detectors where applicable and possible.
- Door specification for entry/exit to/from data center.
- Visual or audio alarm confirmation.
- Strict badge access to data center.
- Access to only authorized Network Operation Center (NOC) and IP Telephony or IT team personnel.
- Break glass alarm sensors.
- Anti masking intruder alarm sensors in the data center and access routes.
- Alarm shunt lock on door.
- Superior protection of alarm signal transmission.
- Security marking.
 - All IP Telephony and related hardware should be prominently security marked by branding or etching with the name of the establishment and area postcode. Advisory signs informing that all property has been security marked should be prominently displayed externally. The following are considered inferior methods of security marking: text composed solely of initials or abbreviations, marking by paint or ultra violet ink (indelible or otherwise), or adhesive labels that do not include an etching facility.

Local-Area Network Security Policy

This section details the essential LAN security mechanisms that should be implemented to safeguard IP-based communications.

- LAN equipment
 - IP Telephony LAN equipment, hubs, bridges, repeaters, routers, and switches will be kept in secure hub rooms.
 - Hub rooms will be kept locked at all times.
 - Access to hub rooms will be restricted to IT and IP Telephony staff only.
 - Other staff and contractors requiring access to hub rooms will notify the IT department in advance so that the necessary supervision can be arranged.
 - All unused ports on switches must be in administrative shut down mode.
 - Trunk ports will allow only specific VLANs to traverse the switch trunks.
 - All VTP domains should be password protected, and VTP should be pruned.
 - Essential port security should be enabled allowing only three MAC addresses on the access port.
 - DAI and DHCP snooping should be implemented.
 - Appropriate provisions for preventing CAM table overflow, IP, and MAC spoofing attacks should be implemented.
- Workstations
 - Users must logout of their workstations when they leave their workstation for any length of time. A password protected screen saver will be implemented on all user workstations (helps prevent CIPC, sniffer-based attacks).
 - All unused workstations must be switched off outside working hours.
- LAN wiring
 - All network wiring will be fully documented.
 - All unused network points will be deactivated when not in use.
 - All network cables will be periodically scanned and readings recorded for future reference.
 - Users must not place or store any item on top of network cabling.
 - Redundant cabling schemes will be used where possible.
- Monitoring software
 - The use of LAN analyzer and packet sniffing software is restricted to the IT department.

- LAN analyzers and packet sniffers will be securely locked up when not in use.
- Intrusion detection systems will be implemented to detect unauthorized access to the network.
- Servers and other related equipment
 - All IP Telephony switches and routers will be kept securely under lock and key in the hub room. All IP Telephony servers will be kept in a secure data center.
 - Access to the system console and server disk, tape, and network share drives will be restricted to the authorized IT/IP Telephony staff only.
- Electrical security
 - All IP Telephony servers will be fitted with UPS, which also condition the power supply.
 - In the event of a mains power failure, the UPSs will have sufficient power to keep the network and servers running until the generator takes over.
 - All UPSs will be tested periodically.
- Inventory management
 - The IT/IP Telephony department will keep a full inventory of all servers, network gear, computer equipment and software in use throughout the organization.
- Audit
 - IP Telephony and underlying hardware and software audits will be carried out periodically. These audits will be used to track unauthorized changes to hardware and software configurations and to trace the source of change.

Wide-Area Network and Perimeter Security Policy

This section details the WAN and network perimeter security guidelines:

- IP Telephony equipment will be based off XYZ HQ and Remote data center, protected by firewalls.
- Remote users' alias telecommuters will be required to connect over IPSec or SSL VPN connections to the corporate VPN server for any IP Telephony services to be availed.
- Wireless LANs will make use of the most secure encryption and authentication facilities available (for example, WPA and WPA2).
- Users will not install their own wireless equipment, switches, and phones under any circumstances.
- Unnecessary protocols and services will be disabled on routers.
- The preferred method of connection to outside organizations is by a secure VPN connection, using IPSec or SSL connections.

- Permanent connections to the Internet will be via a firewall to regulate network traffic.
- Permanent connections to other external networks for offsite processing and so on will be via a firewall to regulate network traffic.
- Where firewalls are used, a dual-homed firewall (a device with more than one TCP and IP address) will be the preferred solution.
- Firewall redundancy in Active/Standby mode is preferred.
- Network equipment will be configured to close inactive sessions.

IP Telephony Server Security Policy

This section details security policy as it applies to Windows and Linux IP Telephony servers:

- The operating system will be kept up to date and patched on a regular basis.
- Servers will be checked daily for viruses (applicable to Windows servers only).
- Servers will be locked in a data center.
- Where appropriate the server console feature (HP ILO or IBM RSA) will be activated.
- Remote management passwords will be different from the application and OS administrator passwords.
- Users possessing administrator rights will be limited to trained members of the IT/IP Telephony staff only.
- Use of the Administrator accounts will be kept to a minimum. MLA/Roles will be enabled.
- Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
- Users' access to IP Telephony applications will be limited by the access control features (ACL).
- Intrusion detection and lockout will be enabled.
- The system auditing facilities will be enabled.
- All accounts will be assigned a password of a minimum of eight characters, alphanumeric.
- Administrators will change the server passwords every 180 days. (180 days is an example here; the number of days for changing passwords for servers may differ for different organizations and business verticals.)
- Unique passwords will be used for OS administrator and the web application administrator.

- FTP or SFTP facilities will be restricted to authorized staff only.
- SSH facilities will be restricted to authorized users.

Voice Application Security Policy

This section details the specifics of IP Telephony application level security:

- Call accounting will be used to monitor access and abnormal call patterns.
- Internal and external call forwarding privileges will be separated to prevent inbound calls being forwarded to an outside line.
- The operator will endeavor to ensure that an outside call is not transferred to an outside line.
- Use will be made of multilevel passwords and access authentication where available on IP Telephony applications.
- Voicemail accounts will use a password with a minimum length of six digits.
- The voicemail password should never match the last six digits of the phone number.
- Caller to a voice mail account will be locked out after three failed attempts at password validation.
- Dialing paid numbers will be prevented.
- Telephone bills will be checked carefully to identify any misuse of the telephone system.
- A conference call will be dropped when the initiator leaves.
- The phones of all executive level employees and managers and above must be encrypted.
- Use of encrypted conferences is preferred.
- CFA CSS can forward only calls to internal VoIP numbers.
- Auto registration of phones is not permitted; manual registration should be used.

Endpoint Security Policy

This section details the specifics of endpoint security (applies to wired and wireless IP Phones and soft phones):

- Web access to IP Phones will be disabled. (If web access is enabled, it should be either restricted by ACLs or should leverage HTTPS URLs.)
- Video capabilities where not needed should be disabled.
- Settings button access should be restricted or disabled.

- PC Voice VLAN access should be always disabled.
- PC port should be disabled on lobby, elevator, and rest room phones.
- GARP should be disabled on all IP Phones.

Conclusion

As apparent in various sections of the sample security policy, each asset in the IP Telephony network needs to be protected right from the perimeter to endpoints. It is essential that your IP Telephony Security policy covers all components as, leaving anything unguarded can possibly open up flood gates to attacks.

After you formulate your IP Telephony Security policy, it is time to look into some common questions that would mushroom in any IP Telephony or network security administrator's mind. Two of the most burning questions are as follows:

- What is the cost of implementing security in my Cisco IP Telephony network?
- What is the right level of security for my Cisco IP Telephony network?

In the following sections, you will be introduced to the facts that can help you decide both the level of security and the cost to implement (versus not implementing) security for your Cisco IP Telephony network.

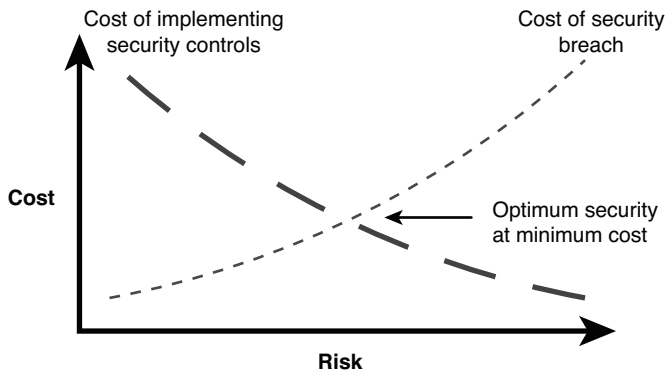
Evaluating Cost of Security—Cost Versus Risk

The best way to put forth cost versus risk in implementing IP Telephony Security is a single phrase, "There's no such thing as a free lunch."

There's a cost for everything whether it is setting up your IP Telephony network or securing it. In the context of cost, consider the following:

- What do you think is the cost to secure your IP Telephony network?
- What should you do to minimize the cost and to maximize the security? In other words, not to put at risk what is the lifeline of your organization, the communications network, yet decrease the cost of securing this asset.

It is sometimes complicated to calculate the ROI for security implemented for your IP Telephony network. However, the damage sourced by the absence of efficient security controls is far greater than the cost to implement them. Figure 4-4 depicts the analytic details of the cost of security.



Analysis of cost vs. risk
Cost of implementing security vs. cost of security breach

Figure 4-4 *Cost vs. Risk Evaluation*

Note: Cost is in context of two major factors: monetary and human resource. In other words, how much it costs to deploy a security control or process and how many man-hours does that exercise demands.

Two factors contribute to the overall cost of security for an IP Telephony system:

- Cost of IP Telephony Security
- Cost of IP Telephony Security breach

Cost of Implementing IP Telephony Security

The first factor is the cumulative cost of all system security components. For example, the costs to set up Certificate Authentication Proxy Function (CAPF) with a third-party certificate to encrypt media and signaling, administer user accounts and passwords, and to set up and operate routine data backup and recovery procedures. In the long run, if planned properly this cost pays off quite well.

Cost of a Security Breach

The second cost factor arises from the expected cost (damages) resulted by IP Telephony Security breaches. For example, the organization's reputation damage, cost of recovering damaged IP Telephony information, and cost of losing data to a competition. This is the cost that would be incurred if the IP Telephony system was compromised and sensitive and critical data about call records, recordings, and customer's data were destroyed or exposed to the wrong people.

Thus, it is expected that any organization using IP Telephony would invest rationally in security controls for its IP Telephony system (as long as you invest your money judiciously), and as a result the cost of the expenditure for damages from security breaches should go down.

As described in RFC 2196, “The Site Security Handbook:”

One old truism in security is that the cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you. Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures.

How to Balance Between Cost and Risk

With the preceding discussion about cost of security in context, let’s look at the cost versus risk evaluation and understand how this can affect your decision to implement security controls in your IP Telephony network. Figure 4-5 depicts the verity that “Security is a balance between cost and risk.”

Increasing Cost, Decreasing Risk

Low Default Security, No Additional Cost	Medium Moderate Security, Nominal Cost	High Highly Secure, Cost Increase
Separate Voice and Data VLANs	IP Telephony-aware Network Firewalls	TLS/Phone Proxy
Port Security	Develop IP Telephony security policy	Third-party certificate (e.g., CAPF)
Layer 2, Layer 3 ACLs	Wireless infrastructure security	Telecommuter solution
Server hardening	Host Intrusion Prevention System	802.1X
Class of Restriction (Toll Fraud)	Encrypted TFTP transfer	Network IPS
Antivirus	TLS/SRTP - Phones, Applications	Security Event Management
Scavenger QOS	IPSec/SRTP to Gateways, Trunks	
Signed Firmware		
Phone Security Settings		

IP Telephony Security: A Balance Between Risk And Cost

Figure 4-5 *Security Is a Balance Between Cost and Risk*

As you can discern, the cost of implementing a security control and process increases from left to right. The security implemented in an IP Telephony network can be broadly categorized in three categories: low, medium and high.

Let's explore what each one of these cover and the trade-off to invest heavily versus not investing in IP Telephony Security:

- **Low (or default level of) security:** As it is evident, a low-level of security costs nothing to minimum. This level of security is provided at a default level by IP Telephony applications and network elements. As a matter of fact, it is just about enabling it on an IP Telephony application or an underlying network component. Although this level of security might be right for networks considered to be low profile or networks where intrusion and breaches would not interest hackers, it is also an open invitation for attacks.
- **Medium (or moderate level of) security:** This level requires a moderate level of investment (not only in terms of cost however, also in terms of increasing complexity). At this level, the investment into security (fiscal and manpower) is higher than the default security level; however, it provides a much better security level to organizations (for example, SMBs to enterprises) where security breaches into IP communication network are almost imminent. The investment, both manpower and cost, pays in the long terms as, the assets are protected, and the chances of damage as a result of malicious attacks from inside or outside are minimized.
- **High (or maximum level of) security:** This is the most secure level that an IP Telephony network can be elevated to and may require a lot of planning and investment. The result is an IP Telephony solution that is secure, end-to-end. This kind of deployment is recommended for highly secure environments; however, it can be opted for by organizations where cost and manpower are next to security concerns. At the maximum security level, the monetary cost also goes up to ensure that the performance does not take a dip because of encryption overhead. To counter the same, more equipment might be required (for example, an increase in CUCM cluster size or the use of dedicated hardware encryption modules in IOS gateways instead of software encryption).

With this discussion in view, you can start thinking about the cost of implementing versus not implementing security in your IP Telephony network and make a conscious decision on how you will go about securing your IP Telephony network.

To address the second question about the level of security, let us go through the next section of evaluating the level of security required for your IP Telephony network before you can comprehend the cost versus risk equivalence with complexity versus security level. The same matrix would be leveraged to describe the level of security, complexity, and manpower or man-hours required to implement various levels of security for different IP Telephony networks.

Determining the Level of Security for Your IP Telephony Network

Let's start with a fundamental fact: Not all five fingers of a hand are equal. The same applies to IP networks, organizations, and people. No two people or two organizations are precisely identical. And the same applies to IP Telephony networks as well; no networks are ever exactly the same.

With that said, more likely than not, you must be thinking about your own IP Telephony network and how dissimilar it is to another IP Telephony network you've had a chance to work with (or designed). The question here is, "How can you compare the security applied in that other IP Telephony network to your network?" And consider if the level of security applied was perhaps too much for your network, or maybe it was lesser than what you would like to have employed in your network.

To help you with these questions, let's take an example of different organizations and their expectations from their IP Telephony network. Let's go through a series of brief case studies to help you understand which level of security may be right for your organization.

Note: The levels of security and their constituents are illustrative. These levels and their constituents may be different or represented differently by your organization. Refer to Figure 4-5 to see a broad perspective of the various security levels that can be adapted to your network and requirements, respectively.

Case Study

The following organizations are considering securing their Cisco IP Telephony network:

- A university
- Sport store with multiple branches
- Financial institution
- Government agency

All these institutions want to leverage Cisco's world-class IP Telephony solution for addressing their telecommunications requirement. They are all very excited to experience IP Telephony and IP-based collaboration solutions. However, they are also concerned about the security of their communication channels, stored call records, rogue devices, unauthorized access, and other practical issues that plague the integrity and confidentiality of their IP Telephony network. They are all striving to secure their IP Telephony network. Let's analyze the level of security each one of them should logically and practically implement. The following examples are based on assumptions relevant to IP Telephony network security that different organizations or business verticals might plan for.

Before beginning, we will use the same matrix we used in the section, “How to Balance Between Cost and Risk,” for reference. However, now the discussion is no longer about the cost of security or risk. Instead, it revolves around the level of security and the associated complexity, as shown in Figure 4-6.

Increasing Complexity, Security Level, Manpower

Low Default Security, Provides Minimum Protection	Medium Moderate Security, Provides Reasonable Protection	High Highly Secure, Provides Maximum Protection
Separate Voice and Data VLANs	IP Telephony-aware Firewalls	TLS/Phone Proxy
Port Security	Develop IP Telephony Security policy	Third-party certificate (e.g., CAPF)
Layer 2, Layer 3 ACLs	Wireless infrastructure security	Telecommuter solution
Server hardening	Host Intrusion Prevention System	802.1X
Class of Restriction (Toll Fraud)	Encrypted TFTP transfer	Network IPS
Antivirus	TLS/SRTP - Phones, Applications	Security Event Management
Scavenger QOS	IPSec/SRTP to Gateways, Trunks	
Signed Firmware		
Phone Security Settings		

IP Telephony Security: Level of Security

Figure 4-6 *IP Telephony Security Levels*

Note: Security levels on the right (refer to Figure 4-6) include the features from the left, that is, moving from left to right, it is imperative that the right (successor) security level has all features from its left counterpart (predecessor).

University: At the university, because of openness and availability of resources, it is essential to prevent unauthorized access to IP Telephony facility. Moreover, any rogue devices should be barred from registering to the CUCM cluster. Also, the university IT staff would like to have the wireless communication encrypted because many students will be using Cisco Unified Presence Client (CUPC) or Cisco IP Communicator soft phones installed on their laptops. No remote access via VPN is allowed. Maintaining the IP Telephony network and cost are some of the challenges for the university’s IP Telephony department.

Given the details, what do you think is the right level of security for the university's IP Telephony network? Could it be low, medium, or high? Give it a thought and write down your answer.

Sport Store: The sport store organization has multiple branches and hosts a decentralized IP Telephony network with clustering over WAN and SRST support at remote sites. The employees are allowed to access the network remotely enabling them to work from home. Thus, VPN is also part of the solution. Thanks to stiff competition, the organization wants to protect its communication streams from any possible tapping or service outage. Also, the organization intends to safeguard its IP Telephony network resources from any intrusion attempt. The security must be within a set budget and implemented in a predefined timeline.

Can you guess what level of security this organization is aspiring for, by referring to Figure 4-6?

Financial institution: A popular and successful financial institution plans to secure its Cisco IP Telephony deployment. Although it does not want to let go of any native security feature, it does not want to increase the complexity level too much. One important aspect is that as per the security policy of the organization, no endpoints can register unless they have been authenticated by the AAA server on its premises. Also, no auto-registration of the endpoints is allowed. The IP Telephony staff of the organization maintains a separate IP Telephony Security policy that it must follow meticulously. Cost is not an issue and neither is manpower.

Equipped with this information, what do you think is the level of security this financial institution is planning for?

Government agency: A government agency is considering implementing its new IP Telephony network. It chose Cisco as its vendor. It wants to have it secured end-to-end with no exception. The level of security must meet guidelines set by its telecom and network security department security policy. Also, it has a contingency plan to address any security issues that may show up during normal operations. Cost, manpower, and time have virtually no frills.

With this information, can you think of the right security level to satisfy the government agency's need for end-to-end security (based on security levels depicted in Figure 4-6)?

The Riddles Are Over

It is time to put all these riddles to an end and explore the options these institutions should "ideally" opt for.

University: Because the security needed is minimal and basic, a low or default level of security should suffice for the university IP Telephony network. This can enable it to secure its IP Telephony network with minimal additional cost and manpower. (The only exception is the addition of wireless security that overlaps with a medium or moderate security level.)

Sport store: The store is aspiring for a non-default level of security because the requirement was to encrypt the communication (media and signaling) streams and to evade any DoS attacks (use of a firewall to prevent malicious attack attempts). Thus, a medium or moderate level of security will be an ideal fit for it.

Financial organization: The financial organization does not want a complex solution yet one that provides maximum protection. This calls for a medium or moderate security level with the exception that it requires that the endpoints use its AAA server (for 802.1x). This overlaps with the high or maximum security level.

Government agency: A government agency, as you might have guessed, is a maximum protection facility. Also, keeping in view the end-to-end security requirements along with a contingency plan (security event management), only the highest level of IP Telephony Security can satisfy its requirements.

As you can probably figure out, it is not always that the need for security is addressed by a static set of security controls defined within a security level. Sometimes, these may overflow or overlap to the next level as some of the security requirements cannot be satisfied by the current level. However, at the same time it is important to note that, the cost, time to plan or deploy, and man-hours also increase.

Putting Together All the Pieces

It is finally time to put together all the pieces to outline a security framework for your Cisco IP Telephony network:

- Security strategy
- Risk assessment
- Security controls
- Identified threats, attacks and vulnerabilities, and mitigations
- Organization objectives

The driving force is that an IP Telephony Security Framework should help in the enrichment of IP Telephony services, enabling the users to feel confident in the privacy and integrity of their communication. In other words, a security framework should enhance and not form an obstruction to the IP-based communications.

IP Telephony Security Framework

The main ideologies that drive an IP Telephony Security Framework are as following:

- Supports simplification of design and configuration for security for IP Telephony network
- Ascertain confidentiality, integrity, and availability of IP Telephony network
- Provides defense in opposition to internal and external threats and diverse attacks

- Provides for scalable IP Telephony architecture by integrating multiple layers for security
- Based on corporate security policies and strategy
- Should function in a mixed environment of secured and unsecured IP Telephony components

To describe the security framework for your IP Telephony network, a useful approach would be to divide the tangible IP Telephony solution into logical domains and to pin down threats and vulnerabilities within each domain. The logical domains in which an IP Telephony solution can be broken down into following categories:

- IP Telephony Call Control servers (CUCM)
- IP Telephony media servers (Unity and Unity Connection)
- IP Telephony application servers (Attendant console and UCCX)
- IP Telephony billing, user data servers (CDR and LDAP)
- IP Telephony end-user devices (IP Phone, soft phone, and CUPC)
- IP Telephony operational and management access
- Peripheral servers (voice gateways)
- Communication transit in internal networks (Intranet or Extranet)
- Communication transit in a public network (Internet)

Note: Each domain must be fortified and equipped with authentication, encryption, authorization, accounting, and security mechanisms.

Figure 4-7 outlines the logical domains pertinent to an IP Telephony Security Framework.

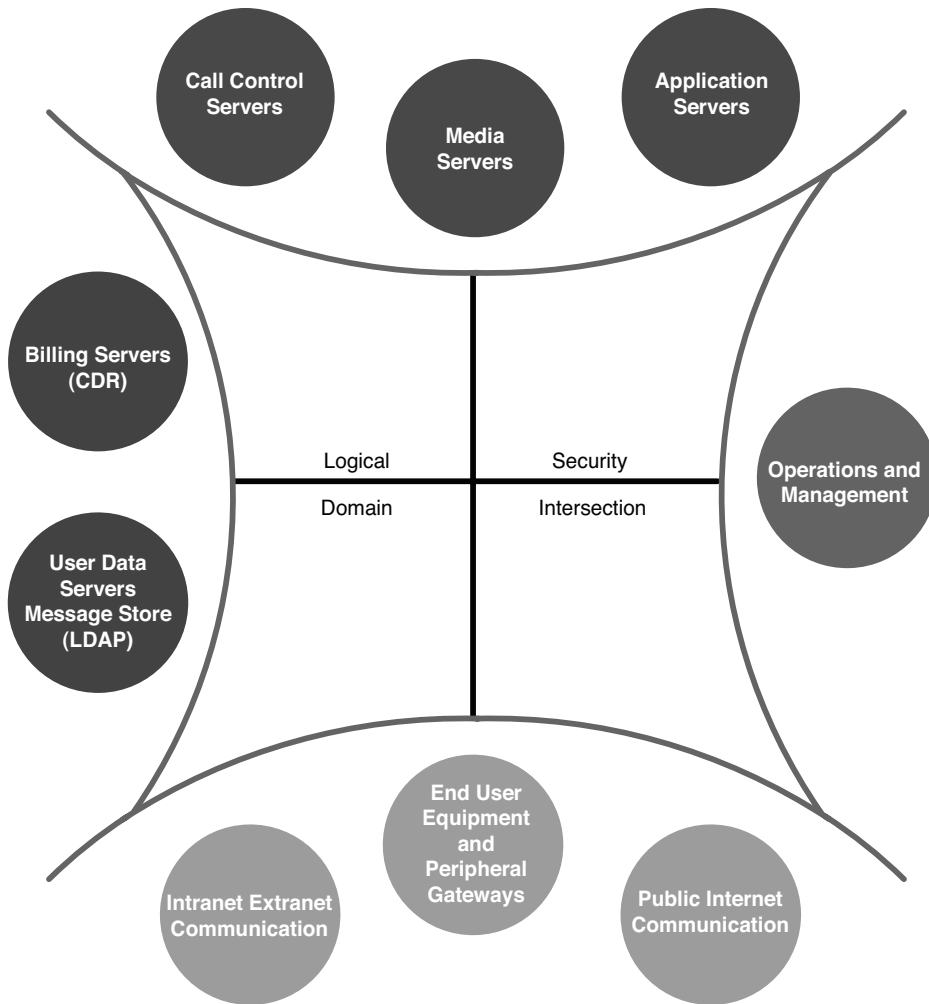


Figure 4-7 *IP Telephony Security Framework: Logical Security Domains*

In essence, at a high level, the IP Telephony Security Framework can be envisioned as a blend of the following elements:

- Technology involved
- Management support
- Regulatory aspects
- Organization processes
- Training requirements

It is around these elements that a security framework revolves. Let's comprehend what each element contributes to the IP Telephony Security Framework:

- **Technology involved:** The most critical element for maintaining confidentiality, integrity, and availability of IP Telephony services. Technology goes from evading passive intrusion attempts to sophisticated attack mitigation techniques (as discussed in Chapter 1, "What Is IP Telephony Security and Why Do You Need It?"). It is the core of an IP Telephony network and plays the most significant role in defining the security controls and processes to be followed. The technology aspect involves (but is not limited to) the following:
 - Attack mitigation
 - Pre- and Post-deployment risk, vulnerability, and security assessment
 - Define standards for encryption, key management, and authentication within the organization
- **Management support:** As a well-known fact, no (IP Telephony) project will commence devoid of apt funding and support by higher management. The decision makers, stakeholders, and executives should be supportive to have a secure and robust IP Telephony network in place. In other words, they should be better informed about the cost of security breaches and the ROI so they not only support the financial cause, but also support from a leadership and involvement perspective. (Remember risk assessment and security strategy requires participation from stakeholders.)
- **Regulatory aspects:** The U.S. Communications Assistance for Law Enforcement Act (CALEA) may require access at various security levels. A service provider is obliged to provide the necessary session keys to law enforcement personnel. Despite that private companies may be exempt, a 2007 U.S. government regulation, CALEA, requires public VoIP carriers to comply with federal wiretapping standards. There are other regulatory acts that come into action pertinent to VoIP systems, for example, the Fighting Internet and Wireless Spam (FISA) Act and USA Patriotic (also known as Patriot) Act. Moreover, some organizations (for example, financial institutions) are required to meet global certifications. See the following URL for more information on how Cisco products cater to these requirements:

http://www.cisco.com/web/strategy/government/sec_cert.html
- **Organization processes:** The organization processes have a strong influence on the security framework because they drive the organization's objective to which the security framework should be aligned with. Furthermore, a security strategy must be aligned with organization's mission and vision, objectives, and goals. IP Telephony Security requires continuous vigilance and should be integrated into existing processes rather than viewed as a one-time task. In essence, the processes elements include the following:
 - Security strategy
 - Organization objectives and goals

- **Training requirements:** The Cisco IP Telephony system provides users with an extensive range of security features. These features are however useless if users of IP Telephony do not understand how to use them. Thus, it is important that end users are involved early in the implementation phase and IP Telephony administrators are involved during planning phase. Furthermore, cross-training should also be provided by the organization to the IT and telecom staff who may not have worked together prior to an IP Telephony implementation. Because IP Telephony systems are more complex than traditional telephone systems and use the underlying network, getting IT, telecom, and network teams aligned and training collectively is crucial to build and maintain a secure IP Telephony system.

Therefore, it is the accumulation of all the elements discussed (in Chapters 1 through 4), that derive the security framework for an IP Telephony network, as illustrated in Figure 4-8.

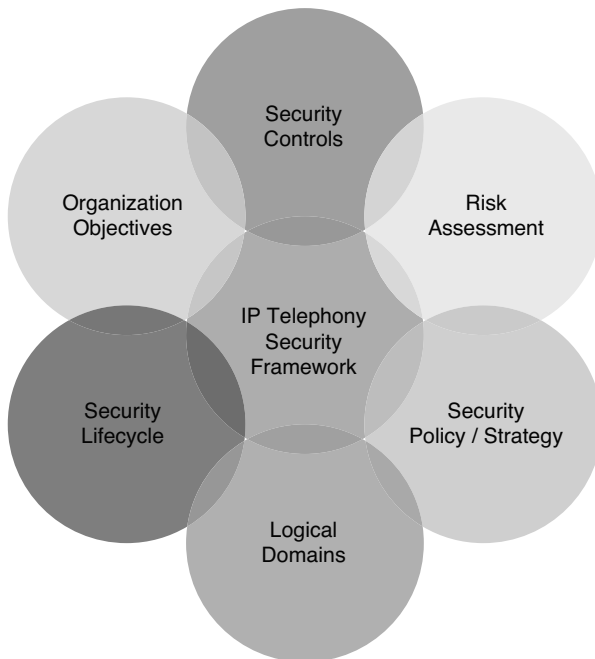


Figure 4-8 *IP Telephony Security Framework*

The IP Telephony Security Framework (refer to Figure 4-8) should serve as the baseline to protect your IP Telephony network and its services. The implementation of this framework is detailed in the subsequent chapters via security construct in design, configuration, and implementation.

Summary

While forming a security framework for your Cisco IP Telephony network, it is vital to have a handle on the various components that form the security framework. The Cisco security life cycle must be followed meticulously to implement the four phases and fit them to your IP Telephony network. This should be followed by the planning and designing of security into your IP Telephony network. Then is the rigorous exercise of risk assessment, countermeasures, and a contingency plan for every recognized asset for your IP Telephony system and underlying network equipment the organization or business owns or operates. IP Telephony Security policy is an imperative component of your IP Telephony Security Framework, without which you simply cannot position proper security controls even if you have them penned down.

A security policy is not a fixed document because it needs to be updated on a regular basis to counter any new security challenge or to address a new requirement. When designing a secure IP Telephony network, some goals (for example, objectives an organization; intent to ensure IP Telephony system availability, confidentiality, and integrity; readiness for lawful interception; alignment with overall organization security objectives; and so on) need to be taken into consideration. This chapter also discussed how much it costs when threats are realized and the IP Telephony system is out of service, that is, the cost of security. Also, you can work out the right level of security for your IP Telephony network based on the covered case studies presented in this chapter.

Part II, “Cisco IP Telephony Network Security”, shows you how to protect your IP Telephony network by securing Layer 1 (physical layer), Layer 2 (switching infrastructure), Layer 3 (routing infrastructure), and network perimeter. You will learn about the importance of network security pertinent to IP Telephony, and the ways in which you can secure your IP Telephony network against internal and external threats.

Index

A

- AAA (Authentication, Accountability, and Access), 71, 157
 - Cisco Gatekeeper, 407-409
 - CUCME, 425
 - CUE, 437
 - enabling, 158-160
 - logins, 138
 - voice gateways, monitoring, 403
 - WLAN configuration, 452
- Acceptable Usage Policy, 73
- acceptable use, 70
- accept-lifetime command, 151
- access, 28. *See also* Access Policy;
logins; security
 - administration restrictions, 286-288
 - Anyconnect VPN configuration, 224
 - authorization, 98
 - badges, 75, 99
 - CDA, 39
 - Cisco Unity servers, 312
 - consoles, 138-139
 - CUE, 435
 - data center authorization, 71
 - GUIs, 426-427, 440
 - hard-coded access modes, 111
 - hub rooms, 76
 - layers, 106. *See also* Layer 2
 - line VTYS using ACLs, limitations, 140
 - management
 - Layer 3 restrictions, 137-142*
 - restrictions, 132*
 - NAC, 469
 - PSTNs, 318
 - restrictions, 71, 99
 - physical security, 97-100*
 - protocols from user VRF, 282*
 - services, 70
 - settings, 445
 - SSH on ASAs, enabling, 494
 - switches, 38, 132
 - TFTP servers, 216
 - types of, 137
 - users, Layer 3 security, 157-160
 - VLANs, 445, 447
 - VNC, 500-501

- WAP, 449
- Web, 446
- access control lists. *See* ACLs
- access control servers. *See* ACSs
- Access Policy, 73-74
- Accountability Policy, 72
- accounting. *See also* AAA
 - Cisco Gatekeeper, 407-409
 - remote support accounting logs, 292-294
 - TACACS+ configuration, 159-160
- accounts
 - Cisco Unity, 327-330
 - Cisco Unity Connection, 330
 - temporary lockouts, 438
- acknowledgments, DHCP, 114
- ACLs (access control lists), 565
 - anti-spoofing, 161
 - ASA firewall interfaces, 178
 - Call Source Authentication, 378
 - CUBE, 415
 - defining, 567
 - ICMP redirects, disabling, 155
 - MAC address spoofing, 116
 - ports
 - blocking*, 165
 - usage (Cisco ASA firewalls)*, 188
 - RFC 2827 filtering, 161
 - traffic, filtering, 416
 - uRPF, 162
 - voice gateways, monitoring, 403
- ACSs (access control servers), 461
- Active Directory. *See* AD
- Active/Standby failover, 552
- AD (Active Directory), 259-261, 369
- Adaptive Security Appliances. *See* ASAs
- adding
 - destination IP addresses, 379
 - hashes, 520
 - non-default call-restriction rules, 318
 - OCS static routers (with TLS), 350
 - sensors, 577
 - SIP Trunk Security profiles, 322
 - TFTP hosts, 319
 - third-party SIP Phone profiles, 265
 - user groups/roles, 288
- addresses
 - IP, 379. *See also* IP
 - MAC, 467-468 *See* MAC addresses
 - NAT, 179, 180
 - table switches, 117
- Address Resolution Protocol. *See* ARP
- administration. *See also* management
 - access restrictions, 286-288
 - Cisco Unity Connection, 317
 - passwords, 71, 237
 - security controls, 40
 - wireless IP Phones, 455
- administrator logins, troubleshooting, 336
- admission, networks, 448
- Admission Request. *See* ARQ
- Advanced Encryption Standard. *See* AES
- AES (Advanced Encryption Standard), 522
- after-hours calling restrictions, 422
- agents
 - Cisco Security Agent, 237
 - J2EE Agent Profile configuration, 301-302
 - NAC, 469

- AIC (Application Inspection Control), 559**
- alarms, 40, 75, 99**
 - break glass sensors, 99
 - Cisco Unity, 311
 - intruder, 98
 - shunt locks, 99
- alerts, IPS, 579**
- algorithms**
 - asymmetric encryption, 522
 - DES, 522
- alternative routing, 99**
- AMIS (Audio Messaging Interchange Specification), 318**
- analysis**
 - application audit logs, 294-295
 - CUCM audit logs, 294
 - information, 26
 - LANs, 76
 - traffic, 14
- anti-spoofing measures, 160-162**
- antivirus programs, 40**
 - CIPC, 469
 - Cisco Unity, 312
 - policies, 71
- Anyconnect VPN access configuration, 224**
- appliances**
 - ASAs. *See* ASAs
 - UTM, 36
- Application Inspection Control. *See* AIC**
- applications, 4, 35**
 - AIC functions, 559
 - analysis, 294-295
 - antivirus. *See* antivirus programs
 - audit logs, 291
 - CBAC firewalls, 566
 - CSM, 511
 - CTIManager, 283
 - CTL Client, 529-533
 - CUCM, 287
 - CUPS, 191, 340
 - deployment, 63
 - implementation, 23
 - layered security design, 37
 - NIPS, 571
 - PKI, 523-525
 - protocol inspection, 175
 - RealVNC, 500
 - security controls, 44
 - SNMPv3 support, 480-483
 - SSH support, 492
 - SSO, 295
 - Syslog, 486
 - TurboVNC, 501
 - UltraVNC, 501
- applying COR, 380**
- APR (ARP Poisoning Routing), 13**
- architecture**
 - CUPS, 341
 - security, 22-24
- ARP (Address Resolution Protocol), 10**
 - Proxy ARP, disabling, 145
 - spoofing, 114-116
- ARQ (Admission Request), 406, 407**
- ASAs (Adaptive Security Appliances), 551**
 - ASDM, 498-499
 - certificates, uploading, 224
 - Cisco VPN Phone, 222-227

- data centers, 182-203
 - proxy servers*, 201-203
 - zones*, 183
- failover, 552-554
- firewalls, 54, 181-182, 426, 551-564.
 - See also* firewalls
 - interfaces*, 174-177
 - security levels*, 177-178
- interface configuration, 178
- IPSec configuration, 395
- NAT, 180, 354
- overview of, 172-182
- perimeter security, 171, 184-201
- Phone proxy, 212-222
- remote workers, 227-231
- RSA keypairs, 356
- self-signed certificates, 356
- SSH, enabling access on, 494
- stateful firewalls, 174
- Syslog, 488-490
- TLS proxy, 203-212
- UTM, 180
- ASDM (Adaptive Security Device Manager), 498-499**
- assessment**
 - architecture, 23
 - policy development, 65-69
 - risk, 61-62
 - security, 24-26
 - tools, 13
- assets, 61, 65**
- assignments**
 - COR lists to voice dial peers, 382
 - CTI security, 284
 - DMZs, 178
 - line passwords, 138
 - partitions, 280
 - roles/permissions, 287
- asymmetric encryption algorithms, 522**
- asymmetric keys, 525**
- Asynchronous Line.** *See* TTY
- attacks.** *See also* security; threats; vulnerabilities
 - AIC functions, 559
 - anti-spoofing measures, 160-162
 - ARP spoofing, 114-116
 - brute-force, 312
 - CAM table overflow, 120-122
 - CIPC, 464
 - Cisco Unity, 311
 - CUPS, server hardening, 340
 - data manipulation, 524
 - DDoS, 10
 - DHCP spoofing, 113-114
 - dictionary-based, 312
 - DoS, 10, 11, 29, 62
 - endpoints, 442
 - examples of public, 7
 - flooding, 10
 - GARP packets, 445
 - hacker techniques, 8-10
 - hopping (VLANs), 109-111
 - ICMP, 154-156
 - integrity, 30
 - Layer 2 security, 29
 - likelihood of, estimations, 68
 - mitigation, 90
 - MITM, 7, 11, 30, 540. *See also* MITM
 - monitoring, 581
 - route poisoning, 30
 - security. *See* security
 - server hardening, 237
 - Smurf, 146
 - SPIT, 288

- starvation, 120-122
- tracking, 62
- Violations and Security Incident Reporting and Handling Policy, 74
- audio alarms, 98, 99**
- Audio Messaging Interchange Specification.** *See* AMIS
- audits**
 - applications, 291
 - Cisco Unity/Unity Connection, 335-337
 - CUCM security, 290-295
 - databases, 291
 - enabling, 292
 - LANs, 77
 - OSs (operating systems), 291-292
 - trails, 567
- authentication, 31, 519, 520**
 - BGP, enabling, 153
 - calls, 544
 - Call Source Authentication, 378-379
 - Cisco Unity, 329
 - CUCM, 321-322
 - default, 249
 - deployment, 240
 - devices, 541
 - Digest Authentication, 265
 - EAP, 125
 - failure rates, 166
 - FAST, 457
 - HSRP, 153
 - in-band network management, 475
 - IP Phones, 264
 - local, 157-158
 - MD5, 150
 - MDA, 127
 - messages, 536, 541
 - NTP, 164
 - OSPF, 152-153
 - overview of, 520-522, 537-542
 - plain text, 150
 - RDP, 502
 - rogue endpoints, 125
 - routing protocols, 150
 - servers, TLS proxy, 205
 - SIP, 322
 - SNMPv3, 479
 - SSH retries, 493
 - TACACS+ (Cisco), 158-160
 - TFTP
 - downloading, 249-250*
 - mitigation, 149*
 - tokenless, 410
 - trustpoints, 431
 - Unified IP Phone, 540
 - users, enabling IOS router HTTP servers, 142
 - voice call signaling, 541-542
 - Windows Desktop SSO Authentication Module, 300
- Authentication, Accountability, and Access.** *See* AAA
- Authentication Policy, 72-73**
- authenticators, 124**
- Auth-Fail VLANs, 126**
- authorization, 20, 520.** *See also* AAA
 - access, 98
 - Cisco TACACS+, 130
 - data centers, 71
 - enabling, 157-158
 - hosts, CUPS, 351
 - manipulation, 11
 - SIP Phones, 267
 - TACACS+ configuration, 159

autoloading, disabling configuration,
148-149

automatic grant of certificates,
disabling, 386

auto-registration, disabling, 428

AUX (Auxiliary Port), 137, 139

availability, 66

ASAs, 172-173

conversations, 20

HA, 552

losses, 71

statements, 71, 72

B

backdoor programs, 10

backups, 52, 101, 102

badges

access, 75

identification, 98

RFID-based access, 99

bandwidth, SRTP, 548

banners, routers, 163-164

best practices

HTTPS, 500

Layer 2 security, 131-133

Layer 3 security, 168-169

RDP, 506

SCP, 508

server hardening, 312

SFTP, 508

SNMP, 485

SSH, 495

Syslog, 490

TFTP, 508

VNC, 501

BGP (Border Gateway Protocol), 153

billing, 281

blinds, physical security, 98

blocking

logins, 166

ports, 165

Block OffNet to OffNet Transfers,
281

blog postings, 9

BootP servers, disabling, 143

Border Gateway Protocol. *See* BGP

BPDU (Bridge Protocol Data Units),
112

breaches, cost of, 81-82

break glass alarm sensors, 99

Bridge Protocol Data Units. *See*
BPDU

bridging

Conference Bridges, 389

VLANs, 215

broadcasts, disabling directed, 146

browsers. *See* interfaces

brute-force attacks, 312

building blocks of security, 19

business continuity, 7

business value, 7

C

CA (Certificate Authority), 276

conferencing, 385

CUPS, 347

enrollment, 386

external

with CAPF, 253-256

with Tomcat, 256-258

OCS server configuration, 347

RDP, 502

- Root certificates, importing, 358
- servers
 - enabling*, 430
 - trustpoints*, 358
- signed certificates
 - importing*, 360
 - installations*, 315
- wireless IP Phones, 457
- Cain & Abel, 13
- CALEA (U.S. Communications Assistance for Law Enforcement Act), 90
- Call Control, 4, 35
 - access switches, 38
 - ACL configuration, 378
 - CUCM. *See* CUCM
 - CUCME. *See* CUCME
 - layered security design, 37
 - remote data centers, 56
 - secure signaling, 535
- Call Detail Records. *See* CDRs
- call-forward max-length command, 424
- CallManager, fallback configuration, 401
- CallManager.pem certificates, 342, 388
- Call Progress icon, 264
- calls
 - after-hours calling restrictions, 422
 - authentication, 544
 - Call Source Authentication, 378-379
 - encryption, 544
 - forwarding, 280, 383-384
 - hijacking, 10, 11
 - IP Phones to/from IOS Voice Gateway, 383
 - logging (CUCME), 428
 - pattern tracking, 10
 - redirection, 10
 - restrictions, 71, 424-425
 - SRTP, 544, 546-547
 - transfers, 383-384, 423-424
 - voice signaling, 541-542
- Call Search Space. *See* CSS
- CAM (Content Addressable Memory), 120
- cameras, 28, 98
- CAM table overflow attacks, 120-122
- capabilities, video (CUVA), 446
- CAPF (Certificate Authority Proxy Function), 81, 238-249
 - end user profiles, 284
 - IP Phones, 263
 - servers, defining, 433
 - wireless IP Phones, 456
- card readers, 28
- case studies
 - layered security approaches, 36-37
 - levels of security, 84-87
 - perimeter security with Cisco ASA, 184-201
- Catalyst 3550 switches, 106
- categorizing assets
- CBAC (Context-Based Access Control), 564
 - CUCME firewalls, 426
 - IOS firewalls, 565-568
- CCKM (Cisco Centralized Key Management), 451
- CCTV cameras, 102. *See also* cameras
- CCX (Cisco Compatible Extensions), 451
- CDA (Core Distribution Access), 39
- CDP (Cisco Discovery Protocol), 107, 143-145

- CDRs (Call Detail Records), 281, 289, 428
- CEF (Cisco Express Forwarding), 162
- Certificate Authentication Proxy Function. *See* CAPF
- Certificate Authority. *See* CA
- Certificate Export Wizard, 259
- certificates
 - ASAs, uploading, 224
 - automatic grant of, disabling, 386
 - CA. *See* CA
 - CallManager.pem, 342, 388
 - Cisco Unity, 320
 - CUCM, 204
 - enrollment*, 401
 - exchange*, 396
 - servers*, 525
 - CUPS, 342, 357
 - errors, 505
 - eTokens, 243
 - exporting, 387
 - front-end server, 349
 - IIS, 349
 - importing, 387
 - LSC, 126, 465, 525
 - management, 347
 - MIC, 525
 - PKI
 - external CA signed*, 526
 - LSC*, 528
 - MIC*, 527
 - self-signed*, 526
 - Root, 255, 257
 - Cisco Unity*, 320
 - importing*, 358
 - self-signed, 356
 - sources, 534
 - third-party, 457
 - Tomcat, 370
 - Unified IP Phone, 533
 - X.509, 259
 - X.509 v3, 533-534
- Certificate Signing Requests. *See* CSRs
- Certificate Trust List. *See* CTL
- challenge-response-based authentication, 125
- challenges, security, 15-16
- Chargen service, 142
- Chief Technology Officer. *See* CTO
- CIA (confidentiality, integrity, and availability), 72
- CIPC (Cisco IP Communicator), 463-469
 - EM, 466
 - encryption, 465-466
 - hardening, 464-465
 - MAC addresses, 467-468
 - NAC, 469
 - VLAN traversal, 469
- Cisco Adaptive Security Device Manager. *See* ASDM
- Cisco Advance Services, 61
- Cisco Catalyst Switches, configuration, 574
- Cisco Centralized Key Management. *See* CCKM
- Cisco Compatible Extensions. *See* CCX
- Cisco Configuration Professional. *See* Cisco CP
- Cisco CP (Cisco Configuration Professional), 141
- Cisco Discovery Protocol. *See* CDP
- Cisco Express Forwarding. *See* CEF

- Cisco Express Unity. *See* CUE
- Cisco Gatekeeper
 - physical/logical security, 405-406
 - security, 406-414
 - accounting*, 407-409
 - HSRP*, 413
 - inter-domain*, 411-413
 - intra-domain*, 410-411
 - options*, 410
 - restricted subnet registration*, 407
- Cisco IOS
 - Firewalls (CUCME), 426
 - platform security, 136-137
 - routers
 - remote management*, 140
 - security*, 136
 - unnecessary services, disabling, 142-149
- Cisco IP Communicator. *See* CIPC
- Cisco IPS 4200 series appliances
 - deployment, 572-574
 - events, monitoring, 581
 - interfaces, 576
 - promiscuous mode, 575-578
 - signatures, 578-582
 - virtual sensors, configuration, 577
- Cisco Notification Service, 137
- Cisco Presence Foundation, 345-368
- Cisco Security Agent (HIPS), 237
- Cisco Security Alert. *See* CSA
- Cisco Security Manager. *See* CSM
- Cisco TACACS+, 129. *See also* TACACS+
- Cisco Trust List Client. *See* CTL Client
- Cisco Unified Border Element. *See* CUBE
- Cisco Unified Communication Manager. *See* CUCM
- Cisco Unified Communication Manager Express. *See* CUCME
- Cisco Unified Contact Center Express, 37
- Cisco Unified IP Phones
 - wired, 46
 - wireless, 46-50
- Cisco Unified Operations Manager. *See* CUOM
- Cisco Unified Personal Communicator, 37
- Cisco Unified Presence Client. *See* CUPC
- Cisco Unified Presence Server. *See* CUPS
- Cisco Unified Provisioning Manager. *See* CUPM
- Cisco Unified Service Monitor. *See* CUSM
- Cisco Unified Service Statistics Manager. *See* CUSSM
- Cisco Unified Unity Express, 37
- Cisco Unified Video Advantage. *See* CUVA
- Cisco Unity
 - accounts, 327-330
 - audit (logs), 335-337
 - authentication, 329
 - controls, 47-46
 - CoS, 331
 - CUCM, 321-322
 - platforms, 310-313
 - port usage, end-user station, 194
 - SCCP, 319-321
 - secure messaging, 332-335
 - security, 309

- toll fraud prevention, 317-318
- voicemail port security, 318-327
- Voice Messaging, 37
- Web services, 313-317
- Windows platform security, 311-313
- Cisco Unity Connection**
 - account policies, 330
 - audits, 337
 - Linux platform security, 313
 - SCCP, 323-324
 - SIP, 324-327
 - SLDAP, 327
 - SSO, 338
 - Web services, 317
- Cisco Unity Telephony Integration Management.** *See* UTIM
- Cisco Unity/Unity Connection.**
See Cisco Unity; Cisco Unity Connection
- Cisco VPN Phones, 222-227**
- Cisco Wireless Security Suite.**
See CWSS
- civil unrest protection, 102**
- classification**
 - components, 53
 - controls, 40
 - traffic, 557
- classless routing, disabling, 148**
- class maps**
 - configuration, 361
 - defining, 570
- Class of Restriction.** *See* COR
- Class of Service.** *See* CoS
- clients**
 - Cisco Gatekeeper, 408
 - CTL Client, 432, 529-533
 - CUPC, 85
 - JTAPI Client, 285-286
 - MOC, 347
 - RDP, 501, 504-506
 - softphones, 466
 - TLS, 535-536
- Client Service Framework.** *See* CSF
- Closed User Group.** *See* CUG
- clusters**
 - CUCM, 207, 319, 525. *See also* CUCM
 - ICTs, 271-273
 - intra ports, 188
 - mixed-mode, 217
 - nodes, rebooting, 255
 - non-secure to cluster conversions, 240
 - restrictions, 71
 - security mode, 247
 - WANs, 554-557
- codecs, complexity, 395**
- coherence, layers, 39**
- collapsed cores, 39**
- commands**
 - accept-lifetime, 151
 - call-forward max-length, 424
 - enable secret, 156
 - failover active, 552
 - ip scp server enable, 508
 - ip source-address, 427
 - log audit status, 292
 - no cdp run, 144
 - no failover active, 552
 - same-security-traffic permit interface, 178
 - SELinux, 582
 - send-lifetime, 151
 - service password-encryption, 156
 - show, 119
 - show cdp neighbors detail, 144*
 - show version command, 137*

- ssh scopy enable, 508
- transfer max-length, 423
- transfer-pattern, 423
- verification (CUCME), 434
- communications, 4**
- complexity, codecs, 395**
- components**
 - Cisco Gatekeeper, 406
 - interactions, 4
 - layers, 27
 - physical security, 378
 - policy development, 69-74
 - security, 32-33
 - security controls, 52-57
 - value estimations, 67
- Compressed RTP. *See* CRTP**
- Computer Telephony Integration.**
See CTI
- Computer Telephony Interface Quick Buffer Encoding. *See* CTIQBE**
- conditions, trust, 30**
- conferencing, 38**
 - acceptable use, 70
 - profiles, 389
 - restrictions, 281
 - voice gateways, 384-390
- confidentiality, 20, 522, 536**
 - integrity, and availability. *See* CIA
 - policy summaries, 71
 - RTP payloads, 544
- configuration**
 - 801.1x, 126-131
 - AAA, 437
 - ACLs, Call Source Authentication, 378
 - after-hours calling restrictions, 422
 - Anyconnect VPN access, 224
 - ARP spoofing, 116
 - ASAs
 - IPSec*, 395
 - NAT*, 354
 - ASDM, 498-499
 - authentication, 539
 - autoloading, disabling, 148-149
 - banners, 163
 - CallManager, fallback, 401
 - Cisco Catalyst Switches, 574
 - Cisco Gatekeeper
 - AAA*, 407-409
 - inter-domain security*, 411-413
 - security*, 413
 - Cisco IPS 4200 series appliances, 577
 - Cisco TACACS+, 129
 - Cisco Unity
 - account policies*, 327-328
 - secure messaging*, 332-335
 - class-maps, 361
 - codecs, complexity, 395
 - COR, 380-383
 - CTL Client, 432
 - CUCM, 236
 - audit log parameters*, 292
 - LDAPS*, 259-261
 - mixed mode*, 240-249
 - SBD*, 249-253
 - trustpoint certificates*, 400
 - CUPS
 - CA*, 347
 - LDAP*, 369
 - trustpoints*, 357
 - device encryption, 543
 - DHCP snooping, 114
 - domain names, 493

- DSPFarm, 395
- EDI, 369
- ephones, 433
- errors, troubleshooting, 270
- Federation Routing Parameters, 352
- files, TFTP encryption, 250
- global-policies, 361
- H.323 gateways, 394-396
- hard-coded access modes, 111
- HSRP, 153
- HTTPS (CUE), 440
- interfaces, 176, 178
- IP Phones, 443-448, 543
- IPSec tunnels, 272
- IPTRouter, 164
- J2EE Agent Profiles, 301-302
- JTAPI Client, 285-286
- MAC address spoofing, 117-119
- modifying, 71
- NTP authentication, 164
- OCS servers, 347, 361
- OpenAM SSO servers, 297-299
- passwords
 - modifying*, 438
 - wireless IP Phones*, 455
- policies, 570
- policy maps, 570
- ports, 110
- profiles, SCCP, 389
- promiscuous mode, 572
- RDP
 - clients*, 504-506
 - servers*, 502-504
- root guards, 113
- routers
 - CA, 385
 - erasing*, 29
 - SCP, 508
 - SIP trunk security, 273
 - SRST, 383, 399
 - SRTP, 396-398
 - SSH on IOS devices, 492-494
 - SSO, 306-307
 - subnets, restricted registration, 407
 - switches, ports, 128
 - Syslog, 488-490
 - TACACS+
 - accounting*, 159-160
 - authentication*, 158
 - authorization*, 159
 - third-party SIP Phone security, 264-267
 - TLS Proxy, 360
 - Unified IP Phone authentication, 540
 - uRPF, 162
 - violation rules, 118
 - Windows Desktop SSO Authentication Module, 300
 - WLANs, 450
- connections**
 - assessments, 62
 - Cisco Unity Connection security, 309
 - CTIManager security, 283
 - CUPC
 - CUCM*, 371-372
 - CUPS*, 370-371
 - LDAP*, 368-369
 - voicemail*, 372-374
 - data centers, 37
 - drops, 559
 - ITSP, 52
 - switches, port configurations, 110
- connectivity schemes, 52**

- consoles
 - CSM, 512
 - port security, 138-139
- constraining ICMP, 155-156
- Content Addressable Memory.
 - See* CAM
- Context-Based Access Control.
 - See* CBAC
- contexts
 - sharing, 179
 - TLS, 344
- continuity, 7, 71
- controls, security, 26, 40-50
 - components, 52-57
 - implementation, 41-50
 - overview of, 40
- convergence, 5
- conversations
 - availability, 20
 - confidentiality, 20
 - dumps, 14
 - integrity, 20
 - reconstructions, 13
 - security, 7. *See also* security
 - sniffing, 109
 - voice
 - gateways*, 390-398
 - IP Phones*, 448
 - wireless IP Phones endpoints, 456
- conversions, non-secure clusters to secure clusters, 240
- COR (Class of Restriction), 380-383
 - SRST configuration, 383
 - toll fraud prevention, 425
- Core Distribution Access. *See* CDA
- cores, networks, 38
- core security policies, 72-74
 - Acceptable Usage Policy, 73
 - Access Policy, 73-74
 - Accountability Policy, 72
 - Authentication Policy, 72-73
 - Endpoint Security Policy, 79-80
 - IP Telephony Network Maintenance Policy, 74
 - LAN Security Policy, 76-77
 - physical security of equipment, 74-75
 - Server Security Policy, 78-79
 - Voice Application Security Policy, 79
 - WAN and Perimeter Security Policy, 77-78
- corrections, controls, 40
- CoS (Class of Service), 331
- costs, 4, 62
 - of breaches, 81-82
 - of countermeasures, 68-69
 - of implementation, 81
 - of security, 80-83
- countermeasures, 26
 - costs, 68-69
 - implementation, 69
 - security threats, 10-11, 12
 - threats, 68
- covering tracks, 10
- CP (Cisco Configuration Professional), 496-498
- credentials, 10
 - SIP, 322
 - SRST configuration, 399
 - SSO, 295
 - wireless IP Phones, 458
- critical systems

- identification, 67
- losses as potential threats, 68
- critical VLANs, 126
- CRTP (Compressed RTP), 548
- cryptography
 - authentication, 520-522
 - EAP authentication methods, 125
 - encryption, 522-523
 - overview of, 519-523
 - RSA keys, 493
- CSA (Cisco Security Alert), 582
 - Cisco Unity, 311
 - CUPS, 340
 - default policies, 237
- CSF (Client Service Framework), 371
- CSM (Cisco Security Manager), 511
- CSRs (Certificate Signing Requests), 359, 459
- CSS (Call Search Space), 280, 380, 381
- CTI (Computer Telephony Integration), 283-286
- CTIManager security, 283
- CTIQBE (Computer Telephony Interface Quick Buffer Encoding), 175, 283
- CTL (Certificate Trust List), 204, 239
 - ASA Phone proxy, 214
 - files, 246
 - services, 241
- CTL Client (Cisco Trust List Client), 529-533
 - certificate lists, 243
 - configuration, 432
 - downloading, 241
 - eTokens, 244
 - installations, 241
 - wizards, 246
- CTO (Chief Technology Officer), 135
- CTY (Line Console), 137
- CUBE (Cisco Unified Border Element), 44, 405, 414-419
 - physical/logical security, 405-406
 - security controls, 54
- CUCM (Cisco Unified Communication Manager), 37, 46, 235-236
 - administrative access restrictions, 286-288
 - ASA trust, 205-206
 - CAPF, 238-249
 - certificates, 204
 - enrollment*, 401
 - exchanges*, 396
 - trustpoint configuration*, 400
 - CIPC, 466
 - Cisco Unity, 321-322
 - clusters, 525
 - conferencing, 385
 - COR, 380-383
 - CUPC connectivity, 371-372
 - CUPS integration, 341-345
 - data centers, 54
 - end-user stations to port usage, 192
 - enrollment, 388
 - external CAs
 - CAPF*, 253-256
 - with Tomcat*, 256-258
 - HTTP/HTTPS, 496
 - integration, 319
 - LDAPS, 258-261, 259-261
 - Linux platform security, 237-238
 - mixed mode, 240-249
 - performance (TLS), 548

- platform security, 236-238
- ports, endpoints, 188-190
- RSA key pairs, 217
- SBD, 249-253
- Secure Tone, 267-270
- security
 - audit (logs)*, 290-295
 - controls*, 43-44
 - CTI/JTAPI*, 283-286
 - IP Phones*, 261-267
 - modes*, 239
 - SPIT*, 288-290
 - SSO*, 295-307
 - TRP*, 277-279
 - trunks*, 271-276
- S RTP
 - call flow*, 547
 - session keys*, 536
- telecommuters, 228
- toll fraud prevention, 279-282
- voicemail port security, 324-327
- VPN group configuration, 225
- wired IP Phones, 443
- CUCME (Cisco Unified CME), 399**
 - AAA, 425
 - auto-registration, disabling, 428
 - call logging, 428
 - Cisco IOS Firewalls, 426
 - GUI access, 426-427
 - logins, 436
 - platforms, 422
 - strict ephone registration, 427
 - toll fraud prevention, 422-425
 - verification commands, 434
 - voice traffic security, 429-434
- CUCM OS CLI command, 247**
- CUE (Cisco Express Unity), 429**
 - AAA, 437
 - GUI access security, 440
 - platforms, 435-437
 - remote data centers, 56
 - security controls, 44
 - toll fraud prevention, 438-439
- CUG (Closed User Group), 464**
- culture of security, 6**
- CUOM (Cisco Unified Operations Manager), 512-513**
- CUPC (Cisco Unified Presence Client), 85**
 - connectivity
 - CUCM*, 371-372
 - CUPS*, 370-371
 - voicemail*, 372-374
 - security, 368-374
- CUPM (Cisco Unified Provisioning Manager), 515**
- CUPS (Cisco Unified Presence Server), 48, 339**
 - applications, 191
 - certificates, importing, 357
 - Cisco Presence Foundation, 345-368
 - CUPC connectivity, 370-371
 - host authorization, 351
 - HTTP/HTTPS, 496
 - integration, 341-345
 - LDAP, 345, 369
 - OCS Federation, 354
 - platforms, 339-341
 - Presence, 54
 - static routes, 350
 - trustpoint configuration, 357
- CUSM (Cisco Unified Service Monitor), 513**

CUSSM (Cisco Unified Service Statistics Manager), 514
customization, COR partitions, 381
CUVA (Cisco Unified Video Advantage), 446
CWSS (Cisco Wireless Security Suite), 457
cycles, security, 25

D

DAI (Dynamic ARP Inspection), 116
damages, costs of, 81-82
databases, audit (logs), 291
data centers
 access authorization, 71
 Access Policy, 73
 ASAs, 182-203
 proxy servers, 201-203
 zones, 183
 connectivity schemes, 52
 distribution layers, 38
 end-to-end security, 50
 physical security, 74-75, 97-101
 remote, backups, 102
 security controls, 54-56
 services, 52
Data Encryption Standard. *See* DES
data gathering, 25
data manipulation attacks, 524
Daytime service, 142
DC (Domain Controller), 368
DCRouters, 150
DDoS (distributed denial of service) attacks, 10
decapsulation, 110
dedicated VLANs, Layer 2 security best practices, 132

defaults
 authentication, 249
 level of security, cost of, 83
 passwords, modifying, 438
 policies, CSA, 237
 SBD. *See* SBD
 voice gateway toll fraud, 379-380
 website properties, 314
defense constructs, 35
defining
 ACLs, 567
 CAPF servers, 433
 class maps, 570
 CME trustpoints, 431
 CSS, 381
 security, 4-8
 trustpoints, 397
delay (SRTP), 548
deleting RSA keys, 495
demarcation points, CUBE, 414
Demilitarized Zone. *See* DMZ
denial of service attacks. *See* DoS attacks
denying external traffic, 427
deployment, 22
 applications, 63
 authentication, 240
 best practices
 HTTPS, 500
 RDP, 506
 SCP, 508
 SFTP, 508
 SSH, 495
 Syslog, 490
 TFTP, 508
 VNC, 501

- Cisco IPS 4200 series appliances, 572-574
- CUBE, 415
- encryption, 203
- firewalls, 30
- in-band network management, 475
- models, 50
- OOB management, 476
- SNMP best practices, 485
- de-registering phones, 29**
- DES (Data Encryption Standard), 522**
- design, 63**
 - architecture, 23
 - security, 35
 - enabling, 37-39*
 - layers, 35-39*
 - networks, 473-478*
- destination IP addresses, adding, 379**
- destruction of equipment, 28**
- details, navigating CDP, 144**
- detection**
 - controls, 40
 - systems, 551
- development**
 - culture of security, 6
 - policies, 62-63, 64-80
 - components, 69-74*
 - risk assessment, 65-69*
 - strategies, 64-65*
 - security policies, 24-26
- devices**
 - assessments, 62
 - authentication, 539, 541
 - encryption, 543
 - lockdown, 75
 - maintenance, 74
 - MTP, enabling, 279
 - NIPS, 571
 - physical security, 74-75
 - security controls, 43-44
 - SSH configuration, 492-494
 - Syslog, 488-490
 - third-party SIP Phones, 237-267
- Device Security Mode drop-down, 262**
- DHCP (Dynamic Handshake Challenge Protocol)**
 - spoofing, 113-114
 - starvation attacks, 120-122
- dialog boxes**
 - Export Cisco Unity Root Certificate, 320
 - Properties, 315
 - TFTP Server, 319
- dial-peers**
 - COR, 380, 382
 - SRTP configuration, 397
- dictionary-based attacks, 312**
- Digest Authentication, enabling, 265**
- Digest Credentials, 267**
- directed broadcasts, disabling, 146**
- directory number. *See* DN**
- disabling**
 - automatic grant of certificates, 386
 - auto-registration, 428
 - AUX security, 139
 - BootP servers, 143
 - CDP, 143-145
 - classless routing, 148
 - configuration autoloading, 148-149
 - console port logins, 138
 - directed broadcasts, 146
 - finger services, 143

- mask replies, ICMP, 154
- password recovery, 166-167
- Proxy ARP, 145
- redirects, ICMP, 154-155
- requests, ICMP, 156
- SELinux, 582
- small servers, 143
- small services, 142-143
- source routing, 147
- unnecessary IOS services, 142-149
- unreachable messages, ICMP, 154
- disaster recovery, physical security, 97, 100-101
- Discard service, 142
- discovery, 9, 25
- Discovery (GRQ) messages, 407
- distributed denial of service attacks. *See* DDoS attacks
- distribution
 - CDA, 39
 - layers, data centers, 38
- DMZs (Demilitarized Zones), 36
 - ASA firewall interfaces, 174
 - assigning, 178
- DN (directory number), 270, 383, 424
- DNS (Domain Name Service), 175
- Domain Controller. *See* DC
- domains
 - name configuration, 493
 - SIP Phones, 267
- DoS (denial of service) attacks, 11, 29, 62
 - CIPC, 464
 - DHCP spoofing, 113-114
 - endpoints, 442
 - tools, 14-15

- double tagging (802.1Q), 110-111
- downloading
 - CSA, 311
 - CTL Client, 241
 - TFTP authentication, 249-250
- drops, 559
 - conferencing restrictions, 281
- DSPFarm configuration, 395
- DTP (dynamic trunking protocol), 110
- dumps, conversations, 14
- duration of IP Phone conversations, 237
- DWORD values, 369
- Dynamic ARP Inspection. *See* DAI
- Dynamic Handshake Challenge Protocol. *See* DHCP
- Dynamic Secure MAC addresses, 117
- dynamic trunking protocol. *See* DTP

E

- EAdmin (Example Admin), 318
- EAP (Extensible Authentication Protocol), 125, 457
- earthquake protection, 102
- eavesdropping, 10, 11, 13, 62, 313
- Echo service, 142
- EDI (Enhanced Directory Integration), 368
- editing signatures, 579
- egress traffic inspection,
- EIGRP (Enhanced Interior Gateway Routing Protocol), 152
- electrical security, LANs, 77
- electromagnetic intrusion detection systems, 98

- electronic fences, 98
- EM (Extension Mobility), 466
- emergency equipment, 102
- enable secret command, 156
- enabling
 - AAA, 158-160
 - audit (logs), 292
 - authentication, 152-153, 541.
 - See also* authentication
 - AUX security, 139
 - BGP authentication, 153
 - Call Source Authentication, 379
 - CA servers, 430
 - console port logins, 138
 - CP routers, 496-498
 - CUCM cluster security, 240
 - CUCME HTTPS, 427
 - CUE, 437
 - Digest Authentication, 265
 - encrypted configuration files, 543
 - ephone security, 434
 - FIPS, 352
 - FTP support, 149
 - hardening (wireless IP Phones), 456
 - HTTP, 141, 430, 497
 - IOS routers, 142
 - LDAPS, 259-261
 - local authentication, 157-158
 - MGCP SRTP packages, 392
 - MOTD, 163
 - multiple inspections, 558
 - protected devices, 269
 - Secure Tone, 269
 - security, 37-39, 61-64
 - SELinux, 583
 - SSH access on ASAs, 494
 - SSL, 316
 - SSO (Cisco Unity Connection), 338
 - TACACS+ (Cisco), 158-160
 - TLS proxy, 203
 - transparency, 145
 - TRP, 279
 - VTY logins, 140
- encapsulation, 110
 - Layer 3 security, 30
 - SCCP, 240
- Encrypted Security Profile, 268
- encryption, 519
 - calls, 544
 - CIPC, 465-466
 - deployment, 203, 240
 - impact of, 548
 - IP Phones, 264
 - Layer 3 traffic, 168
 - media, 70, 416-417
 - overview of, 522-523, 542-547
 - passwords, 138
 - PKI, 524-525
 - policies, 71
 - RTP, 391
 - Secure Tone, 268
 - SNMPv3 authentication options, 479
 - SSL, 314
 - standards, 90
 - TFTP, 250, 449
 - wireless IP Phones, 456
 - X.509 v3 certificates, 534
- End of Life. *See* EOL
- End of Support. *See* EOS
- endpoints, 35
 - assessments, 62
 - Block OffNet to OffNet Transfers, 281

- CIPC, 463-469
- Cisco Gatekeeper configuration, 408
- CUCM ports, 188-190
- CUPS, 191
- firewalls, transiting, 186
- H.323 (Cisco Gatekeeper), 406
- layered security design, 37
- lockouts, 29
- protected devices, 269
- protocols, 31
- rogue, 123-131, 406
- security, 441
 - controls*, 46
 - importance of*, 442-443
 - IP Phones*, 443-449
- voice (802.1x), 126
- wireless IP Phones
 - conversations*, 456
 - network admission*, 457-463
- wireless security, 450
- Endpoint Security Policy, 79-80**
- end-to-end security, 50-52**
- end users**
 - CAPF profiles, 284
 - CUCM, 287
- enforcement**
 - minimum password lengths, 166
 - policies, 62-63
 - Trusted QoS Enforcement, 277
- Enhanced Directory Integration.**
 - See EDI*
- Enhanced Interior Gateway Routing Protocol.** *See EIGRP*
- enrollment**
 - CA (Certificate Authority), 386
 - CUCM, 388, 401
 - routers, 386
- enterprise parameters, 247**
- enterprise security policies, 165-167**
- entrance security, 98**
- enumeration, 9, 14**
- environmental challenges, 16**
- environmental factors, physical security, 102**
- EOL (End of Life), 237**
 - Cisco Unity 8.x, 310
 - CSA, 311
- EOS (End of Support), 237**
 - Cisco Unity 8.x, 310
 - CSA, 311
- ephones**
 - configuration, 433
 - security, enabling, 434
- equipment**
 - acceptable use, 70
 - emergency, 102
 - LAN, 76
 - locking down, 101-102
 - maintenance, 74
 - physical security, 74-75
- erasing switches, 29**
- errors**
 - certificates, 505
 - configuration, troubleshooting, 270
 - UTIM-TFTP, 319
- estimations**
 - likelihood of attacks, 68
 - values, 67
- ethical challenges, 16**
- eTokens, 240**
 - certificates, 243
 - CTL Client, 244

- passwords, 245
- requests, 243
- evaluation**
 - costs, 80-83
 - security, 8, 61
- events**
 - monitoring, 581
 - troubleshooting, 508-515
 - Violations and Security Incident Reporting and Handling Policy, 74
- Example Admin.** *See* EAdmin
- exchanges, certificates (CUCM), 396**
- EXEC prompt, 159**
- existing security concerns, 61**
- exploits, 9**
 - impersonation, 442
 - vulnerabilities, 30
- explosion protection, 102**
- Export Cisco Unity Root Certificate dialog box, 320**
- exporting**
 - Certificate Export Wizard, 259
 - certificates, 387
 - CUCM certificates, 396-397
- Extensible Authentication Protocol.** *See* EAP
- Extensible Messaging and Presence Protocol.** *See* XMPP
- Extension Mobility.** *See* EM
- external CAs**
 - CUCM, applying, 253-256
 - signed certificates (PKI), 526
 - with Tomcat, 256-258
- external traffic, denying, 427**

F

- FAC (Forced Authentication Code), 300**
- Failed Login report, 336**
- failover**
 - active command, 552
 - ASA, 552-554
- failures rates, authentication, 166**
- fallback (CallManager), 401**
- FAST (Flexible Authentication with Secure Tunneling), 457**
- Fast Ethernet, RFC 2827 filtering, 161**
- Federal Information Processing Standard.** *See* FIPS
- Federation Routing Parameters configuration, 352**
- Fighting Internet and Wireless Spam (FISA) Act, 90**
- files**
 - authentication of Unified IP Phones, 540
 - CTL, 246
 - ITL, 252
 - TFTP encryption, 250
- File Transfer Protocol.** *See* FTP
- filtering**
 - ACLs, 565
 - RFC 2827, 161-162, 475, 478
 - routes, 282
 - traffic
 - ACL call control, 378*
 - CUBE, 416*
- finger services, disabling, 143**
- FIPS (Federal Information Processing Standard), 352, 456**

Firefox. *See* Mozilla Firefox

fire protection, 102

firewalls, 37, 551-583

access restrictions, 71

ASAs, 54, 172-173, 181-182, 426

interfaces, 174-177

security levels, 177-178

stateful, 174

CUBE, 415, 417-418

CUCME, 426

deployment, 30

endpoints, transiting, 186

enhanced inspection for voice
protocols, 558-564

failover, 552-554

in-band network management, 475

IOS firewalls, 564-570

QoS, 557-558

service deployment, 203

Syslog, 489

transparency, 179

ZFWs, 568-570

firmware

authentication, 539

Unified IP Phone, 539-540

**FISA (Fighting Internet and Wireless
Spam) Act, 90**

**Flexible Authentication with Secure
Tunneling.** *See* FAST

flooding

attacks, 10

protection, 102

tools, 14-15

flow, calls (SRTP), 546-547

foot printing, 9-15

Forced Authentication Code.

See FAC

formats

passwords, 156

administration, 71

minimum lengths, 165-166

modifying, 438

wireless IP Phones, 455

SRTP packets, 536

X.509 v3 certificates, 534

forwarding

calls, 280, 383-384, 424-425

CEF, 162

PSPF, 453

uRPF, 162

VRF, 282

**FQDN (fully qualified domain name),
504**

frames, tagging, 111

frameworks

CSF, 371

security, completion of, 87-91

front-end server certificates, 349

FTP (File Transfer Protocol)

ASAs, 175

support, enabling, 149

fully qualified domain name. *See*
FQDN

functionality

CUPS, 342

span-to-PC port, 446

functions, PTMTUD, 155

fundamentals, PKI, 525-537

Fuzzy Packet, 15

G

GARP (Gratuitous Address Resolution Protocol), 445

gatekeepers. *See also* Cisco Gatekeeper
 H.323, 271
 security controls, 44

gateways, 4
 H.323, 271, 394-396
 voice. *See also* voice
 conferencing, 384-390
 conversations, 390-398
 COR, 380-383
 monitoring, 402-403
 platform security, 377-378
 preventing toll fraud, 378-384
 security controls, 45
 SRST, 399-402

GC (Global Catalog), 368

general guidelines, policies, 72

Global Catalog. *See* GC

global configuration, 395, 397. *See also* configuration

global-policies, configuration, 361

goals of risk management, 65

Gold Mine phase, 10

graphical user interfaces. *See* GUIs

Gratuitous Address Resolution Protocol. *See* GARP

groups, adding users, 288

guards, 28, 98

guest VLANs, 126

guidelines
 policies, 72
 purchasing, 71
 remote-access users, 74
 sensitive areas, 99

GUIs (graphical user interfaces)

access, 426-427
 CUE, 440
 HTTP/HTTPS, 495

H

H.225
 ASAs, 175
 ICTs, 271-273
 regreject, 15

H.235 intra-domain security, 410

H.323
 Cisco Gatekeeper, 406
 gateways, SRTP support
 configuration, 394-396
 RAS, ASAs, 175

HA (high-availability), 552.
See also availability

hackers, 5, 8
 attack techniques, 8-10
 countermeasures, 10
 Layer 2 security, 29

hard-coded access modes, configuration, 111

hardening
 CIPC, 464-465
 in-band network management, 475
 IP Phones, 443-448
 servers, 237
 Cisco Unity, 312-313
 CUPS, 340
 wireless IP Phones, 454-456

hard phones, acceptable use, 70

hardware
 Cisco IOS platform security, 137
 failures, 68, 552
 PKI, 523-525

hashes

- adding, 520
- authentication, 544
- SNMPv3 authentication options, 479

headers (TCP), 548**headquarters, end-to-end security, 50****high-availability. *See* HA****High-based Message Authentication Codes. *See* HMACs****high security, cost of, 83****hijacking calls, 10, 11****HIPS (Host Intrusion Prevention System), 40, 551, 582-583**

- Cisco Security Agent, 237
- Cisco Unity, 311
- hybrid network management, 478
- policies, 71

HMACs (High-based Message Authentication Codes), 520**hopping, 9, 109-111****Host Intrusion Prevention System. *See* HIPS****hostname validation, 417****hosts**

- authorization (CUPS), 351
- discovery, 9
- TFTP, adding, 319

Hot Standby Routing Protocol. *See* HSRP**HSRP (Hot Standby Routing Protocol), 153, 413****HTTP (Hypertext Transfer Protocol), 137, 478**

- ASAs, 175
- GUI access security, 426-427

security

- interfaces, 140-142*
- networks, 495-500*

servers, enabling, 430**HTTPS (Secure HTTP), 426, 478**

- CUE, 440
- network security, 495-500

hub rooms, 76**hybrid network management, 474, 477-478****Hypertext Transfer Protocol. *See* HTTP****I****IBNS (Identity Based Network Service), 123****ICMP (Internet Control Message Protocol), 154-156**

- ASAs, 175
- Smurf attacks, 146

ICTs (Inter-Cluster trunks)

- H.225, 271-273
- security, 275

identification

- badges, 98
- critical systems/sensitive information, 67
- MCID, 289
- potential threats, 67-68
- spoofing, 442
- verification, 150.
- See also* access; management

identity, 520

- traffic, 570
- X.509 v3 certificates, 534

Identity Based Network Service. *See* IBNS

- IDM (IPS Device Manager), 575
- IDS (Intrusion Detection Systems), 30, 31, 40
- IEEE (Institute of Electrical and Electronics Engineers)
 - 801.1x, 126-131
 - 802.1x, 123-125
- IIS (Internet Information Services), 314, 349
- IM (Instant Messaging), 4
- images, Unified IP Phone, 539-540
- IMAP (Internet Message Access Protocol), 317
- IME (IPS Manager Express), 576
- imitation, credentials, 10
- impact of encryption, 548
- impersonation, 11, 442.
 - See also* imitation
- implementation, 4
 - applications, 23
 - Cisco VPN Phone, 224-227
 - COR, 380-383, 425
 - costs, 81
 - countermeasures, 69
 - failover, 552
 - security, 26-30, 31-32
 - controls*, 41-50
 - life cycles*, 61-64
- importing
 - CAs
 - Root certificates*, 358
 - signed certificates*, 360
 - certificates, 387
 - CUCM certificates, 396-397
 - CUPS certificates, 357
- in-band network management, 474-475
- incidents. *See also* attacks
 - management, 101
 - Violations and Security Incident Reporting and Handling Policy, 74
- information
 - analysis, 26
 - privacy, 30
 - security, 29. *See also* security
- infrared, 98
- infrastructure
 - design, 35
 - layered security design, 37
 - networks, 4. *See also* networks
 - routing, 54, 56
 - security, 7
 - switches, 54, 56
 - wireless, 54
- inside attacks, 67
- Inside Interfaces, 176
- inspection
 - application protocols, 175
 - enhanced inspection for voice protocols, 558-564
 - incoming/outgoing materials, 98
 - options, 568
 - packets, 173
 - traffic, 36
 - untrusted interfaces, 567
- installations
 - CA signed certificates, 315
 - CTL Client, 241
 - MCS servers, 310
- instances (TLS Proxy), 360
- Instant Messaging. *See* IM

integration

CUPS, 341-345

EDI, 368

UTIM, 319

integrity, 520

attacks, 30

authentication, 539

conversations, 20

messages, 541

voice call signaling, 541-542

interactions, components, 4**Inter-Cluster trunks. *See* ICTs****inter-domain security (Cisco Gatekeeper), 411-413****interfaces**

ASA firewalls, 174-177

CDP, disabling, 145

Cisco IPS 4200 series appliances, 576

configuration, 178

GUIs

*access security, 426-427**HTTP/HTTPS, 495*

HTTP security, 140-142

ICMP unreachable messages, 154

JTAPI, 283-286

management, 177

RFC 2827 filtering, 161

SSO configuration, 306-307

TUIs, 318

untrusted, inspection, 567

internal firewalls, 37**internal security, 99****Internet**

access (Cisco Unity servers), 312

searching, 9

Internet Control Message Protocol. *See* ICMP**Internet Explorer, SSO configuration, 306****Internet Information Services. *See* IIS****Internet Message Access Protocol. *See* IMAP****Internet Service Providers. *See* ISPs****intra cluster ports, 188****intra-domain security (Cisco Gatekeeper), 410-411****intruder alarms, 98****intrusion**

attempts, 30

prevention, 551

Intrusion Detection Systems. *See* IDS**Intrusion Prevention Systems. *See* IPS****inventory management**

equipment, 102

LANs, 77

IOS

Firewalls, 564-570

*CBAC, 565-568**CUCME, 426**telecommuters, 57*

routers

*remote management, 140**security, 136**unnecessary services, disabling, 142-149*

Voice Gateway, 383

Zone-Based Policy Firewalls. *See* ZFWs**IP (Internet Protocol)**

addresses, trust, 379

Source Guard, 120

spoofing, 10, 29, 119-120

IP Phones, 4, 37auto-registration, disabling, 428
configuration, 543

CSS, assigning, 280
 CUCM security, 261-267
 hardening, 443-448
 IOS Voice Gateway, calls to/from, 383
 remote data centers, 56
 secure network admission, 448
 Secure Tone, 267
 security, 54, 443-449
 SIP, 262
 strict registration, 427
 support, 107
 TFTP encryption, 449
 voice conversation security, 448
 wired, 443-448
 wireless, 449-463, 456. *See also*
 wireless IP Phones
IPS (Intrusion Prevention Systems),
 30, 31, 172
ip scp server enable command, 508
IPS Device Manager. *See* IDM
IPSec (IP Security), 395
 ASA configuration, 395
 in-band network management, 475
 LANs, 555
 tunnels, 271, 393
IPS Manager Express. *See* IME
ip source-address command, 427
IP Telephony, 4. *See also* networks
IP Telephony Network Maintenance
 Policy, 74
IPTRouter, 164
 isolation of access areas, 98
ISPs (Internet Service Providers), 552
ITL files, 252
IT service provider. *See* ITSP
ITSP (IT service provider),
 52, 410, 413

J

J2EE Agent Profile configuration,
 301-302
Java Telephony Application
 Programming Interface. *See* JTAPI
JTAPI (Java Telephony Application
 Programming Interface), 283-286

K

keys
 encryption/decryption, 522
 RSA. *See* RSA key pairs
keywords
 matchrequest method, 559
 parameters, 560

L

LANs (local-area networks), 5
 IPSec, 555
 sniffing, 29
LANs (local-area networks)
 Security Policy, 76-77
latency, low, 38
law enforcement requirements, 71
Layer 2
 controls, 41
 security, 29, 54, 105
 ARP spoofing, 114-116
 best practices, 131-133
 CAM table overflow attacks,
 120-122
 DHCP spoofing, 113-114
 in-band network management,
 475
 IP spoofing, 119-120

- MAC address spoofing, 116-119*
- overview of, 105-108*
- rogue endpoints, 123-131*
- STP manipulation, 112*
- VLAN hopping attacks/mitigation, 109-111*
- switches, 37
- topology overview, 106-107
- Layer 3**
 - controls, 41
 - security, 29-30, 135-136
 - anti-spoofing measures, 160-162*
 - AUX security, 139*
 - best practices, 168-169*
 - blocking ports, 165*
 - Cisco IOS platform, 136-137*
 - console port security, 138-139*
 - disabling unnecessary IOS services, 142-149*
 - encryption, 168*
 - enterprise security policies, 165-167*
 - HSRP, 153*
 - HTTP interface security, 140-142*
 - ICMP attacks, 154-156*
 - IOS routers, 136*
 - NTP, 164*
 - passwords, 156*
 - restricting management access, 137-142*
 - RIPv2, 151-152*
 - router banner messages, 163-164*
 - routing protocol security, 150-153*
 - user access/privilege levels, 157-160*
 - VTY port security, 139-140*
- switches, 37
- layers**
 - access, 106. *See also* Layer 2
 - coherence, 39
 - components, 27
 - cores, 38
 - design, 35-39
 - distribution, 38
 - networks, 37. *See also* Layer 3
 - TLS, 535
- LDAP (Lightweight Directory Access Protocol), 258**
 - CUPC connectivity, 368-369
 - CUPS, 345, 369
 - servers (SSL), 369
- LDAPS (Secure LDAP), 258-261**
 - CUPS, 345
 - enabling, 259-261
- levels**
 - privileges (Layer 3 security), 157-160
 - security, 84-87
 - ASA firewalls, 177-178*
 - requirements, 22*
- licenses (ASAs), 202**
- life cycles, security, 60-64**
- Lightweight Directory Access Protocol. *See* LDAP**
- likelihood of attacks, estimations, 68**
- limitations**
 - access, line VTYS using ACLs, 140
 - CBAC, 565
 - console port timeouts, 139
- Line Console. *See* CTY**
- line passwords, assigning, 138**

- Link Layer Discovery Protocol.**
See LLDP
- Link Layer Discovery Protocol - Media Endpoint Discover.** *See* LLDP-MED
- links, integrity, 520**
- Linux**
 - CUCM, 237-238
 - platform security (Cisco Unity Connection), 313
 - Security Modules. *See* LSMs
- lists**
 - COR, assigning to voice dial peers, 382
 - CTL, 204, 239. *See also* CTL
 - IP addresses trust, 379
 - time zones, 385
- LLDP (Link Layer Discovery Protocol), 447**
- LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discover), 447**
- LLQs (low latency queues), 557**
- load-balancing, Active/standby failover, 552**
- local authentication, enabling, 157-158**
- Locally Significant Certificates.** *See* LSC
- local survivability, 50**
- lockdown devices, 75, 101-102, 467-468**
- Lock icon, 269**
- lockouts, 29**
 - accounts, 328
 - temporary, 438
- locks, 28, 99**
- log audit status command, 292**
- logging, 567**
 - applications, 291
 - audits. *See* audits
 - authentication failure parameters, 166
 - Cisco Unity/Unity Connection, 335-337
 - CUCME, 428
 - CUCM security, 290-295
 - databases, 291
 - OSs, 291-292
 - remote support accounting, 292-294
 - signatures, 581
 - viewing, 447
- logical controls, 40**
- logical security**
 - Cisco Gatekeeper, 405-406
 - CUBE, 405-406
- logical zones (ASA firewalls), 177**
- logins**
 - AAA, 138
 - blocking, 166
 - console port, enabling, 138
 - CUCME, 436
 - PCs, 436
 - router banner messages, 163
 - TTY restrictions, 436
 - TUIs, 336
 - VTY, enabling, 140
- loop prevention, 112**
- losses**
 - availability, 71
 - critical systems as potential threats, 68
 - security controls, 40
- low latency**
 - optimization, 38
 - queues. *See* LLQs
- low security, cost of, 83**
- LSC (Locally Significant Certificates), 126, 525, 533**
 - CIPC, 465
 - PKI topologies, 528
- LSMs (Linux Security Modules), 582**

M

MAB (MAC Authentication By-Pass),
126

MAC (Media Access Control)
addresses

ARP spoofing, 115

CIPC, 467-468

spoofing, 116-119

MAC Authentication By-Pass.
See MAB

MACs (Message Authentication Codes), 520

mailstores (CUPC),
configuration, 373

main data centers, 52.
See also data centers

maintenance

IP Telephony Network Maintenance
Policy, 74

policies, 71

software, 311

Malicious Call Identification.
See MCID

malware, 30

management, 35, 64

access

Layer 3 restrictions, 137-142

restrictions, 132

certificates, 347

CSM, 511

CTIManager, 283

CUCM. *See* CUCM

CUPM, 515

CUSSM, 514

IDM, 575

incidents, 101

interfaces, 177

messages, 313

networks, 473. *See also* networks

risk, 65-69

SME, 275-276

stations, 194

support, 90

switches (SSH), 132

UTIM, 319

UTM, 36, 551

VNC, 500-501

vulnerabilities, 71

wireless infrastructure, 454

man-in-the-middle attack. *See* MITM

manipulation, 11

STP, 112

tools, 15

**Manufacturing Installed
Certificates.** *See* MIC

maps

class maps

configuration, 361

defining, 570

commands (SELinux), 582

policy configuration, 570

marking

clarifying, 99

security, 75

traffic, 557

masks, replies, 154

matchprequest method
keywords, 559

maximum level of security,
cost of, 83

**MCID (Malicious Call
Identification),** 289

MCS (Media Convergence Server),
236, 310

MD5 (Message Digest), 520

- authentication, 150
- OSPF authentication, 152-153

MDA (Multi Domain Authentication), 127**media**

- CIPC, 465-466
- CUCM. *See* CUCM
- encryption, 70, 415, 416-417, 543
- manipulation, 10
- resources, 38
- retention, 70
- SIP trunk security, 273
- tools, 15
- TRP, 277

Media Access Control addresses. *See* MAC addresses**Media Convergence Server. *See* MCS****Media Gateway Control Protocol. *See* MGCP****Media Termination Points. *See* MTPs****medium security, cost of, 83****memory**

- CAM tables, 120
- NVRAM, 251

Message Authentication Codes. *See* MACs**Message Digest. *See* MD5****Message of the Day. *See* MOTD****messages**

- AMIS, 318
- ARQ, 407
- authentication, 536, 539, 541
- Cisco Unity/Unity Connection, 332-335
- Discovery (GRQ), 407
- encryption, 522
- integrity, 520, 541

management, 313

- router banners, 163-164
- third-party SIP Phones, 265
- unreachable, disabling ICMP, 154

methodologies, security, 19-22

- encryption, 522
- overview of, 19-21
- strategies, 21-22

MGCP (Media Gateway Control Protocol), 270, 391-394**MIC (Manufacturing Installed Certificates), 525, 527, 533****Microsoft. *See also* Windows**

- Access Edge Servers, 360
- Active Directory. *See* AD
- Office Client. *See* MOC
- support, 311

migration (CUCM), 237**minimum lengths, passwords, 165-166****mirroring traffic, 572****mitigation**

- ARP spoofing, 116
- attacks, 90
- CAM table overflow attacks, 122
- DHCP spoofing, 114
- eavesdropping, 314
- IP spoofing attacks, 120
- MAC address spoofing, 117-119
- risk, 26
- STP manipulation, 112
- TFTP authentication, 149
- VLANs, 109-111

MITM (man-in-the-middle) attacks, 7, 11, 30

- attacks, 540
- CIPC, 464
- GARP packets, 445

- as potential threats, identification, 68
- root bridges, 112
- SSH, 491
- mixed mode**
 - clusters, 217
 - CUCM, 239, 240-249
- MOC (Microsoft Office Client), 347**
- models**
 - ASA availability, 172-173
 - Cisco Unity Connection, 310
 - CUBE, 415
 - deployment, 50
- moderate level of security, cost of, 83**
- modes**
 - ASAs, 179
 - Cisco IPS 4200 series appliances, 572-574, 575-578
 - CUCM/CCM Cluster Security Mode, 319
 - FIPS, 456
 - hard-coded access configuration, 111
 - promiscuous, 572
 - security, 239
- modification**
 - accounts, 327
 - configuration, 71
 - passwords, 313, 438
 - policies, 60
 - Profile option, 455
 - source routing, 147
- modules, Windows Desktop SSO Authentication Module, 300**
- monitoring, 23, 60, 64**
 - CUSM, 513
 - events, 581
 - RTMT, 294

- software, 76
- voice gateways, 402-403
- MOTD (Message of the Day), 163**
- movement detectors, 98**
- Mozilla Firefox, SSO configuration, 306**
- MTPs (Media Termination Points), 278**
- Multi context mode, 179**
- Multi Domain Authentication. *See* MDA**

N

- NAC (Network Access Control), 469**
- names**
 - domain configuration, 493
 - FQDNs, 504
- Nastysip, 9, 15**
- NAT (Network Address Translation), 179, 180, 354**
- negotiation, trunks, 109-110**
- Nessus, 9, 14**
- NETBIOS protocol, 175**
- Network Access Control. *See* NAC**
- Network Address Translation. *See* NAT**
- Network Intrusion Detection Systems. *See* NIDS**
- Network Intrusion Prevention Systems. *See* NIPS**
- Network Management Systems. *See* NMSs**
- Network Operation Center. *See* NOC**
- networks**
 - ACLs, 565
 - cores, 38
 - device assessments, 62
 - IBNS, 123
 - IP Telephony Network Maintenance Policy, 74

- Layer 3 security, 29-30
 - layers, 37. *See also* Layer 3
 - overview of, 3
 - perimeters, 43
 - resources, access, 73
 - routers, 41
 - safeguards, 7-8
 - security, 473
 - controls*, 42
 - design*, 473-478
 - HTTP/HTTPS*, 495-500
 - implementation*, 26-30
 - protocols*, 478-479
 - RDP*, 501-507
 - SCP*, 507-508
 - SFTP*, 507-508
 - SNMP*, 479-485
 - SSH*, 491-495
 - Syslog*, 485-490
 - TFTP*, 507-508
 - troubleshooting*, 508-515
 - VNC management access*, 500-501
 - threats, 8-12
 - WANs (ASA failover), 552
 - wired IP Phones, 448
 - wireless
 - IP Phone endpoint admission*, 457-463
 - security controls*, 41
 - Network Time Protocol. *See* NTP
 - NIDS (Network Intrusion Detection Systems), 571
 - NIPS (Network Intrusion Prevention Systems), 551, 571-582
 - hybrid network management, 477
 - Nmap, 9, 14
 - NMSs (Network Management Systems), 475, 476, 508
 - NOC (Network Operation Center), 75
 - no cdp run command, 144
 - noconfirm option, 495
 - nodes, rebooting clusters, 255
 - no failover active command, 552
 - non-default call-restriction rules, adding, 318
 - nonprotected devices, 268
 - non-repudiation, 520
 - non-secure clusters to secure cluster conversions, 240
 - non-volatile RAM. *See* NVRAM
 - notification, Cisco Notification Service, 137
 - NTP (Network Time Protocol), 164
 - numbers, restrictions, 318
 - NVRAM (non-volatile RAM), 251
-
- ## O
- objectives of security assessments, 62
 - OCS server configuration, 347, 361
 - one-time passwords. *See* OTPs
 - OOB (Out-Of-Band) management method, 138, 139, 474, 475-477
 - OpenAM SSO server configuration, 297-299
 - Open Shortest Path First. *See* OSPF
 - OpenSSO server configuration, 301-302
 - operating systems. *See* OSs
 - operations, 23, 64
 - optimization of low latency, 38

options

- authentication, 125
- Cisco Gatekeeper security, 410
- inspection, 568
- noconfirm, 495
- parameters, 560
- Profile, 455
- SIP, 9
- SNMPv3, 479

organization processes, 90**OSI layers (ASAs), 174****OSPF (Open Shortest Path First), 152-153****OSs (operating systems)**

- audit (logs), 291-292
- Cisco IOS platform security, 136
- CUCM, 236
- CUPS, 339
- Linux. *See* Linux
- passwords, modifying, 313
- upgrading, 237
- Windows. *See* Windows

OTPs (one-time passwords), 123**out-dial Auto Attendants, 439****Out-Of-Band. *See* OOB****outside attacks, 67****Outside Interfaces, 176****P****packages, enabling MGCP SRTP, 392****packets**

- BPDUs, 112
- GARP, 445
- inspection, 173
- integrity, 520
- PSPF, 453

source routing, disabling, 147**TLS, 535-536****uRPF, 162****pairs, zones, 570****parameters**

- Cisco Unity authentication, 329
- enterprise, cluster security mode, 247
- Federation Routing Parameter configuration, 352
- keywords, 560

partitions, 280**COR, 380****Time of Day Routing, 280-281****passwords**

- administration, 71
- administrator, 237
- Authentication Policy, 73
- Cisco Unity/Unity Connection, 327-330
- conferencing, 386
- eTokens, 245
- LANs, 76
- Layer 3 security, 156
- line, assigning, 138
- minimum lengths, 165-166
- modifying, 313, 438
- OTPs, 123
- port security, 139
- recovery, disabling, 166-167
- restrictions, 327
- server hardening, 312
- SIP Phones, 267
- sniffing for, 29
- SSO, 295
- wireless IP Phones, 455

patches

OSs, 237

Windows (Cisco Unity), 311

Path MTU Discovery. *See* PTMTUD**Patriot Act, 90****patterns**

calls, tracking, 10

routes, 282

table restrictions, 318

payloads, adding hashes, 520**PCA (Personal Communication Assistant)**

Cisco Unity, 313-317, 329

Cisco Unity Connection, 317

PCs (personal computers), 436

ports, 445, 447

span-to-PC port functionality, 446

Peer Firmware Sharing. *See* PFS**penetrations, estimations of likelihood, 68****performance**

ASAs, 173

TLS, 548

Perimeter network defenses, 5**perimeters**ASAs, 171. *See also* ASAs

case studies, 184-201

firewalls, 37

networks, 43

physical security, 97, 98

security, 30

WAN and Perimeter Security Policy, 77-78

permissions, assigning, 287**Personal Communication Assistant.** *See* PCA**personal computers.** *See* PCs**PFS (Peer Firmware Sharing), 447****phases.** *See also* life cycles

monitoring, 60

of security, 22-24

testing, 60

Phone proxy (ASAs), 212-222**phones**

acceptable use, 70

placement, 43

Soft. *See* Soft Phones

VPN, 57

phreakers, 8

countermeasures, 10

physical security, 28-29, 95

access restrictions, 97-100

Cisco Gatekeeper, 405-406

CUBE, 405-406

data centers, 97-101

disaster recovery, 100-101

environmental factors, 102

equipment, 74-75, 101-102

overview of, 95-97

perimeters, 98

survivability, 100-101

training, 100

voice gateways, 378

physical zones (ASA firewalls), 177**PIN codes, 98****ping sweeps, 9****PKI (Public Key Infrastructure)**

CTL Client, 529-533

CUCM, 238

encryption, 542

external CA signed certificates, 526

fundamentals, 525-537

LSC, 528

overview of, 523-525

- self-signed certificates, 526
- unified IP Phone certificates, 533
- X.509 v3 certificates, 533-534
- placement of phones/servers, 43**
- Plain Old Telephony System. *See* POTS**
- plain text authentication, 150**
- planning, 22, 26, 63, 71.**
See also management
- platforms. *See also* OSs**
 - Cisco Unity/Unity Connection, 310-313
 - CUCM, 236-238
 - CUCME, 422
 - CUE, 435-437
 - CUPS, 339-341
 - voice gateways, 377-378
- plug-ins (CTL Client), 529-533**
- PoE (Power over Ethernet), 107**
- policies**
 - Acceptable Usage Policy, 73
 - Access Policy, 73-74
 - Accountability Policy, 72
 - Authentication Policy, 72-73
 - backups, 101
 - Cisco Unity accounts, 327-328
 - Cisco Unity Connection, 330
 - configuration, 570
 - CSA, 237
 - development, 62-63, 64-80
 - components, 69-74*
 - risk assessment, 65-69*
 - strategies, 64-65*
 - encryption, 71
 - Endpoint Security Policy, 79-80
 - enterprise security, 165-167
 - general guidelines, 72
 - global-policy configuration, 361
 - IP Telephony Network Maintenance Policy, 74
 - LAN Security Policy, 76-77
 - Layer 3, 38
 - maintenance, 71
 - map configuration, 570
 - modifying, 60
 - NAC, 469
 - physical security of equipment, 74-75
 - PKI, 523-525
 - security, 22
 - core, 72-74*
 - CUCM, 287*
 - development, 24-26*
 - Server Security Policy, 78-79
 - summaries, 71
 - Violations and Security Incident Reporting and Handling Policy, 74
 - Voice Application Security Policy, 79
 - WAN and Perimeter Security Policy, 77-78
- ports**
 - ACL usage (Cisco ASA firewalls), 188
 - blocking, 165
 - Cisco Unity (CUCM), 321-322
 - configuration, 110
 - consoles, 138-139
 - CUCM endpoints, 188-190
 - intra cluster, 188
 - LANs, 76
 - LLDP, 447
 - PCs, 445
 - scanning, 9
 - security, 132
 - servers, 193

- span-to-PC port functionality, 446
- switches
 - configuration*, 128
 - LLDP-MED*, 447
- trust, 114
- violation rule configuration, 118
- Voice Gateways, 189
- voicemail port security
 - Cisco Unity/Unity Connection*, 318-327
 - CUCM*, 324-327
- workstations, 192
- Port VLAN Identifiers.** *See* PVIDs
- post-deployment risk**, 90
- postings, blogs**, 9
- potential threat identification**, 67-68
- POTS (Plain Old Telephony System)**, 280, 377
 - call transfer restrictions, 423-424
 - network management security, 473
- power failures**, 552
- Power over Ethernet.** *See* PoE
- precautionary controls**, 40
- pre-deployment risk**, 90
- preparation**, 22
- prerequisites, Cisco VPN Phone**, 223
- Presence (CUPS)**, 54, 345-368. *See also* Cisco Presence Foundation
- prevention**
 - controls, 40
 - loops, 112
 - toll fraud, 279-282
 - Cisco Unity/Unity Connection*, 317-318
 - CUCME*, 422-425
 - CUE*, 438-439
 - voice gateways*, 378-384
- privacy**, 30, 520
- private keys**, 525, 529-533
- private messaging**, 332-335
- privilege levels (Layer 3 security)**, 157-160
- procedures (PKI)**, 523-525
- processes**
 - 802.1x, 124
 - authentication, 521, 538. *See also* authentication
 - encryption, 522. *See also* encryption
 - organization, 90
 - PKI, 523-525
- Profile option**, 455
- profiles**
 - conferencing, 389
 - Encrypted Security Profile, 268
 - IP Phones, 262
 - J2EE Agent Profile configuration, 301-302
 - SCCP, 262, 389
 - SIP Trunk Security, 273, 322
 - Voice Mail configuration, 374
 - wireless IP Phones, 456
- promiscuous mode**, 572
 - Cisco IPS 4200 series appliances, 575-578
- properties, website defaults**, 314
- Properties dialog box**, 315
- protected devices**, 268
 - enabling, 269
 - endpoints, 269
- protection**
 - replay, 536
 - security policies, 70
- protect option**, 118

protocols

- application inspection, 175
- ARP, 10
 - disabling Proxy ARP, 145*
 - spoofing, 114-116*
- CDP, 107, 143-145
- defining, 567
- DHCP
 - spoofing, 113-114*
 - starvation attacks, 120-122*
- EAP, 125, 457
- EIGRP, 152
- endpoints, 31
- enhanced inspection for voice, 558-564
- GARP, 445
- HSRP, 153, 413
- HTTP, 137, 478
 - GUI access security, 426-427*
 - network security, 495-500*
- HTTPS, 478, 495-500
- ICMP, 146, 175
- IMAP, 317
- IP, 119-120
- LDAP, 258
 - CUPC, 368-369*
 - synchronization, 345*
- LDAPS, 258-261
- LLDP, 447
- MGCP, 270, 391-394
- NETBIOS, 175
- network security, 478-479
- NTP, 164
- RDP, 478, 501-507
- RIPv2, 151-152
- routing, 150-153
- RTP, 180, 391, 536
- RTSP, 175
- SCCP, 175, 240
 - Cisco Unity, 319-321*
 - Cisco Unity Connection, 323-324*
 - profiles, 389*
 - wireless IP Phones, 456*
- SCP, 149, 478, 507-508
- SFTP, 478, 507-508
- SIP, 175, 559
 - auto-registration restrictions, 428*
 - Cisco Unity Connection, 324-327*
 - CUBE, 418-419*
 - Presence Foundation, 345-368*
- SLDAP (Cisco Unity Connection), 327
- SNMP, 40, 137, 478-485
- SQLNET, 175
- SRTP, 239, 536-537
 - authentication, 544*
 - CUCME voice traffic, 429-434*
 - H.323 gateways, 394-396*
 - SIP, 396-398*
 - termination, 271*
 - wireless IP Phones, 456*
- STP, manipulation, 112
- Syslog. *See* Syslog
- TCP, 548
- TFTP, 478
 - authentication, 149*
 - encryption, 449*
 - network security, 507-508*
 - SBD, 249-250*
 - security, 149*

servers, 543
UTIM-TFTP errors, 319
wireless IP Phones, 456, 463

TLS, 535
 UDP, 143
 voice gateways, monitoring, 403
 XMPP, 345-368

provisioning (CUPM), 515

Proxy ARP, disabling, 145

proxy servers

ASAs, 201-203
 TLS Proxy configuration, 360

PSPF (Public Secure Packet Forwarding), 453

PSTNs (public switched telephone networks), 318

call transfer restrictions, 423-424
 restriction tables, 439
 toll fraud, 378. *See also* toll fraud

PTMTUD (Path MTU Discovery)
 functions, 155

Public Key Infrastructure. *See* PKI

public keys, 525

CTL Client, 529-533

Public Secure Packet Forwarding.
See PSPF

public switched telephone networks.
See PSTNs

purchasing guidelines, 71

PVIDs (Port VLAN Identifiers), 126

Q

QoS (quality of service)

ASAs, 186
 CIPC, 469
 firewalls, 557-558

Trusted QoS Enforcement, 277

voice traffic, 106

WLC, 453

R

racks, 99

RADIUS, 157

Cisco Gatekeeper, 407

WLC, 450

RAM (random access memory), 251

rates

failures, authentication, 166

limiting, 560

RDP (Remote Desktop Protocol),
 478, 501-507

Real Time Monitoring Tool.
See RTMT

Real Time Protocol. *See* RTP

Real Time Streaming Protocol.
See RTSP

RealVNC, 500

rebooting nodes, clusters, 255

recommendations, 26

reconnaissance, 524

reconstructions, conversations, 13

records

CDRs. *See* CDRs

WHOIS, 9

recovery, passwords, 166-167

redirection

calls, 10

ICMP, disabling, 154-155

REGISTER message, 265

registration

auto-registration, disabling, 428

Cisco Gatekeeper security (HSRP),
 413

- CUBE, 415
- lockouts, 29
- removal, 10
- strict ephone, 427
- subnet restrictions, 407
- Registry (CIPC), 468**
- regulations, 90**
- rejection, registration, 10**
- relationships, layers, 39**
- reliability (ASAs), 173**
- remediation, 26, 40**
- remote access (Cisco ASA Phone proxy), 213**
- remote data centers, 50**
 - ASAs, 195-201
 - backups, 52, 102
 - security controls, 54-56
- Remote Desktop Protocol. *See* RDP**
- remote management (Cisco IOS routers), 140**
- Remote SPAN. *See* RSPAN**
- remote support accounting logs, 292-294**
- remote users, Access Policy, 73**
- remote workers (ASAs), 227-231**
- removing registration, 10**
- replay protection, 536**
- replies, masks, 154**
- reports**
 - Failed Login, 336
 - Violations and Security Incident Reporting and Handling Policy, 74
- requests**
 - ARQ, 406
 - CSRs, 359, 459
 - DHCP, 114
 - eTokens, 243
 - ICMP, disabling, 156
- requirements**
 - law enforcement, 71
 - security, 22
 - SSO, 296-297
 - training, 91
- resets, 559**
- resetting**
 - NVRAM, 167
 - passwords, 138
 - SIP trunks, 325
- resilience, 4**
- resources**
 - media, 38
 - network access, 73
- responses, security, 15-16**
- restating OCS front end services, 352**
- restore policies, 101**
- restrictions**
 - access, 71, 99
 - administration, 286-288*
 - physical security, 97-100*
 - protocols from user VRF, 282*
 - after-hours calling, 422
 - calls, 71
 - forwarding, 424-425*
 - transfers, 383-384, 423-424*
 - CIPC, 467
 - conferencing, 281
 - COR, 380-383
 - data centers (Access Policy), 73
 - IP Phone registration, 427
 - Layer 3, 137-142
 - management access, 132
 - passwords, 327

- SIP auto-registration, 428
- SSH, 494
- subnet registration, 407
- tables
 - CUE*, 439
 - patterns*, 318
- toll fraud prevention, 425
- TTY logins, 436
- restrict option**, 118
- retention, media**, 70
- Return On Investment**. *See* ROI
- revealing controls**, 40
- RFC 2827 filtering**,
 - 161-162, 475, 478
- RFID-based badge access**, 99
- RIPv2 (Routing Information Protocol v2)**, 151-152
- risk**
 - architecture, 23
 - assessment, 24, 61-62
 - cost evaluation, 80-83
 - mitigation, 26
 - policies
 - development*, 65-69
 - modifying*, 60
 - post-deployment, 90
 - pre-deployment, 90
 - security controls, 40
- rogue endpoints, 123-131, 406**
 - 801.1x configuration, 126-131
- ROI (Return On Investment)**, 3, 80
- roles**
 - adding, 288
 - assigning, 287
 - Cisco Unity/Unity Connection, 331
 - CUCM administrators, 287
- root bridges, 29**
 - MITM, 112
- Root certificates, 255, 257**
 - CA, importing, 358
 - Cisco Unity, 320
 - Cisco Unity Connection, 323
 - importing, 387
 - wireless IP Phones, 457
- root guard configuration**, 113
- Routed mode**, 179
- routers, 37**
 - assessments, 62
 - banners, messages, 163-164
 - Cisco CP tool, 141
 - configuration
 - CA, 385
 - erasing*, 29
 - controls, 41
 - CP, enabling, 496-498
 - DCRouters, 150
 - enrollment, 386
 - enterprise security policies, 165-167
 - networks, security controls, 41
 - remote management, 140
 - Secure CFB, 386
 - security, 136
 - SNMP, 483-485
 - SSH, 491
 - Syslog configuration, 489
 - unnecessary services, disabling, 142-149
- routes**
 - filtering, 282
 - poisoning attacks, 30
- routing**
 - alternative, 99
 - APR, 13
 - classless, disabling, 148

- Federation Routing Parameter configuration, 352
 - infrastructure, 54, 56
 - protocols, 150-153
 - source, disabling, 147
 - Time of Day Routing, 280-281
 - VRF, 282
 - Routing Information Protocol v2.**
See **RIPv2**
 - RSA keys, 217**
 - deleting, 495
 - SSH, 491
 - RSPAN (Remote SPAN), 574**
 - Cisco Catalyst Switch configuration, 575
 - RTMT (Real Time Monitoring Tool), 294**
 - RTP (Real Time Protocol), 180, 391, 536**
 - RTP Flooder, 14**
 - RTP Injector, 15**
 - RTSP (Real Time Streaming Protocol), 175**
 - rules**
 - COR, 380-383
 - non-default call-restriction, adding, 318
 - PKI, 524
 - violation, configuration, 118
-
- S**
- SA (System Administrator), 313-317**
 - sabotage protection, 102**
 - safeguards, 7-8. *See also* security**
 - Safenet, 240**
 - same-security-traffic permit interface command, 178**
 - SBC (Session Border Controller), 38, 414**
 - SBD (Security by Default), 249-253, 379**
 - scalability, 4**
 - scanning, 9, 14**
 - SCCP (Skinny Client Control Protocol), 175, 240**
 - Cisco Unity, 319-321
 - Cisco Unity Connection, 323-324
 - IP Phones, 262
 - profiles, 262, 389
 - wireless IP Phones, 456
 - schedules, partitions, 280**
 - schemes, IBNS, 123**
 - SCP (Secure Copy Protocol), 149, 478, 507-508**
 - searching Internet, 9**
 - Secure CFB routers, 386**
 - Secure Copy Protocol. *See* SCP**
 - Secure File Transfer Protocol. *See* SFTP**
 - Secure Hash Algorithm. *See* SHA**
 - Secure HTTP. *See* HTTPS**
 - secure inter-working. *See* TLS proxy**
 - Secure LDAP. *See* LDAPS**
 - Secure Real Time Protocol. *See* SRTP**
 - secure signaling (Call Control), 535**
 - Secure Sockets Layer. *See* SSL**
 - Secure Tone, 267-270**
 - security. *See also* perimeters**
 - architecture, 22-24
 - assessment, 24-26
 - breaches, cost of, 81-82
 - building blocks, 19
 - challenges, 15-16
 - Cisco Gatekeeper, 405-406-414
 - accounting*, 407-409
 - HSRP*, 413

- inter-domain*, 411-413
- intra-domain*, 410-411
- options*, 410
- restricted subnet registration*, 407
- Cisco Presence Foundation, 345-368
- Cisco Security Agent (HIPS), 237
- Cisco Unity
 - messages*, 332-335
 - platforms*, 310-313
- Cisco Unity Connection, 309
- components, 32-33
- conferencing, voice gateways, 384-390
- controls, 40-50
 - components*, 52-57
 - implementation*, 41-50
 - overview of*, 40
- conversations, 390-398
- costs, 80-83
- cryptography, overview of, 519-523
- CTIManager, 283
- CUBE, 414-419
- CUCM, 235-236
 - audit (logs)*, 290-295
 - CAPF*, 238-249, 253-256
 - CTI/JTAPI*, 283-286
 - IP Phones*, 261-267
 - LDAPS*, 258-261
 - mixed mode*, 240-249
 - platforms*, 237-238
 - SBD*, 249-253
 - Secure Tone*, 267-270
 - SPIT*, 288-290
 - SSO*, 295-307
 - TRP*, 277-279
 - trunks*, 271-276
- CUCM/CCM Cluster Security Mode, 319
- CUCME
 - disabling auto-registration*, 428
 - platforms*, 422
 - strict ephone registration*, 427
 - voice traffic*, 429-434
- CUE
 - GUI access*, 440
 - platforms*, 435-437
- culture of, 6
- CUPC, 368-374
- CUPS, 339
 - LDAPS*, 345
 - platforms*, 339-341
- cycles, 25
- defining, 4-8
- design, 35
 - enabling*, 37-39
 - layers*, 35-39
- enabling, 61-64
- Encrypted Security Profile, 268
- endpoints, 441
 - importance of*, 442-443
 - IP Phones*, 443-449
- ephones, enabling, 434
- firewalls, 551. *See also* firewalls
- frameworks, completion of, 87-91
- GUI access, 426-427
- ICTs, 275
- implementation, 26-30, 31-32
- IP Phones
 - voice conversation*, 448
 - wireless*, 449-463
- IPSec. *See* IPSec
- Layer 2, 29, 54, 105

- ARP spoofing*, 114-116
- best practices*, 131-133
- CAM table overflow attacks*, 120-122
- DHCP spoofing*, 113-114
- IP spoofing*, 119-120
- MAC address spoofing*, 116-119
- overview of*, 105-108
- rogue endpoints*, 123-131
- STP manipulation*, 112
- VLAN hopping attacks/mitigation*, 109-111
- Layer 3, 29-30, 135-136
 - anti-spoofing measures*, 160-162
 - AUX security*, 139
 - best practices*, 168-169
 - blocking ports*, 165
 - Cisco IOS platform*, 136-137
 - console port security*, 138-139
 - disabling unnecessary IOS services*, 142-149
 - encryption*, 168
 - enterprise security policies*, 165-167
 - HSRP*, 153
 - HTTP interface security*, 140-142
 - ICMP attacks*, 154-156
 - IOS routers*, 136
 - NTP*, 164
 - passwords*, 156
 - restricting management access*, 137-142
 - RIPv2*, 151-152
 - router banner messages*, 163-164
 - routing protocol security*, 150-153
 - user access/privilege levels*, 157-160
 - VTY port security*, 139-140
- levels, 84-87, 177-178
- life cycles, 60-64
- marking, 75
- methodologies, 19-22
 - overview of*, 19-21
 - strategies*, 21-22
- modes, 239
- networks, 473
 - design*, 473-478
 - HTTP/HTTPS*, 495-500
 - protocols*, 478-479
 - RDP*, 501-507
 - SCP*, 507-508
 - SFTP*, 507-508
 - SNMP*, 479-485
 - SSH*, 491-495
 - Syslog*, 485-490
 - TFTP*, 507-508
 - troubleshooting*, 508-515
 - VNC management access*, 500-501
- overview of, 4-6, 50-57
- perimeters, 30, 171
- physical, 28-29, 95
 - access restrictions*, 97-100
 - data centers*, 97-101
 - disaster recovery*, 100-101
 - environmental factors*, 102
 - locking down equipment*, 101-102
 - overview of*, 95-97
 - perimeters*, 98

- survivability, 100-101*
- training, 100*
- policies, 22. *See also* policies
 - core, 72-74*
 - CUCM, 287*
 - development, 24-26*
- ports, 132
- rationale for, 6-7
- requirements, 22
- responses, 15-16
- SIP, trunks, 273-275
- SRST, voice gateways, 399-402
- strategies, 19
- TFTP, 149
- third-party SIP Phones, 264-267
- threats, 7, 8-12
- TLS, 535-536
- token-based, 410
- voice gateways, 377-378
- voicemail port security
 - Cisco Unity/Unity Connection, 318-327*
 - CUCM, 324-327*
- VoIP tools, 12-15
- wireless IP Phones, 454, 456
- WLC, 450-454
- Security by Default.** *See* SBD
- Security Enhanced Linux.**
 - See* SELinux
- Security Event Management Systems.** *See* SEMSs
- Security Operations.** *See* SOC
- self-signed certificates**
 - ASAs, 356
 - PKI, 526
- SELinux, 40, 582**
 - disabling, 582
 - enabling, 583
 - status, 583
- SEMSs (Security Event Management Systems), 164, 509-511**
- send-lifetime command, 151**
- sensitive area guidelines, 99**
- sensitive information**
 - identification, 67
 - value estimations, 67
- sensors**
 - adding, 577
 - break glass alarm, 99
 - Cisco IPS 4200 series appliances, 572-574
 - virtual, configuration, 577
- servers**
 - ACs, 461
 - authentication (TLS proxy), 205
 - BootP, disabling, 143
 - CA
 - enabling, 430*
 - trustpoints, 358*
 - CAPF, defining, 433
 - Cisco Presence Foundation, 345-368
 - Cisco Unity/Unity Connection, 310-313
 - CUCM, 525
 - CUPS, 339
 - LDAPS, 345*
 - platforms, 339-341*
 - front-end certificates, 349
 - hardening, 237
 - Cisco Unity, 312-313*
 - CUPS, 340*
 - HTTP, enabling, 141, 430
 - LANs, 77
 - LDAP (SSL), 369

- MCS, 236, 310
- Microsoft Access Edge Servers, 360
- OCS configuration, 347
- OpenAM SSO configuration, 297-299
- placement, 43
- ports, 193
- proxy (ASAs), 201-203
- RDP configuration, 502-504
- Server Update Wizard, 311
- TFTP, 543
 - access*, 216
 - adding hosts*, 319
 - enumeration*, 9
 - SBD*, 249-250
- TLS, 535-536
- UCS, 236
- workstations, 192
- Server Security Policy, 78-79**
- Server Update Wizard, 311**
- service password-encryption command, 156**
- services, 4, 26, 52**
 - access, 70
 - assessments, 62
 - Cisco Advance Services, 61
 - Cisco Notification Service, 137
 - CTL, 241
 - CUSM, 513
 - finger, disabling, 143
 - firewalls, deployment, 203
 - IBNS, 123
 - NAT. *See* NAT
 - Smart Card Service, 241
 - SRST credentials, 399
 - TVS, 249, 251-253
 - unnecessary IOS, disabling, 142-149
- Service Units. *See* SUs**
- Session Border Controller. *See* SBC**
- Session Initiation Protocol. *See* SIP**
- Session Management Edition. *See* SME**
- sessions**
 - CBAC limitations, 565
 - SSH, 493. *See also* SSH
 - TLS, 206
- settings, access, 445. *See also* configuration**
- SFTP (Secure File Transfer Protocol), 478, 507-508**
- SHA (Secure Hash Algorithm), 520**
- sharing**
 - contexts, 179
 - PFS, 447
- show commands, 119**
 - show cdp neighbors detail, 144
 - show version command, 137
 - Syslog configuration, 489
- shunt locks, 99**
- shutdown option, 118**
- signaling**
 - ACL configuration, 378
 - authentication, 539
 - Call Control, 535
 - CIPC, 465-466
 - CUBE, 415, 416-417
 - CUCM, 283. *See also* CUCM
 - encryption, 543
 - manipulation, 10
 - protection for, 70
 - SIP trunk security, 273
 - sniffing, 406
 - SRTP call flow, 546-547
 - TLS, wireless IP Phones, 456

- tools, 15
- voice, 109, 541-542
- signatures**
 - Cisco IPS 4200 series appliances, 578-582
 - external CA with CAPF, 253-256
- signed certificates, CAs, 360**
- Simple Network Management Protocol. *See* SNMP**
- Single Sign-On. *See* SSO**
- SIP (Session Initiation Protocol), 175, 559**
 - auto-registration restrictions, 428
 - Cisco Unity Connection, 324-327
 - CUBE, 415, 418-419
 - IP Phones, 262
 - options, 9
 - Presence Foundation, 345-368
 - SRTP, support configuration, 396-398
 - third-party SIP Phones, 264-267
 - trunks, 273-275, 325
 - Trunk Security profiles, adding, 322
- SIP-Kill, 15**
- SIPVicious, 9, 14**
- Skinny Client Control Protocol. *See* SCCP**
- Small Office Home Office. *See* SOHO**
- small services, disabling, 142-143**
- smart cards, 98**
- Smart Card Service, 241**
- SME (Session Management Edition), 275-276, 414**
- Smurf attacks, 146**
- sniffing**
 - conversations, 109
 - LANs, 29
 - signaling, 406
 - tools, 13-14
- SNMP (Simple Network Management Protocol), 40, 137, 478**
 - ASAs, 175
 - enumeration, 9
 - network security, 479-485
 - sweeps, 9
 - voice gateways, monitoring, 403
- snmpwalk, 9**
- snooping, 114**
- SOC (Security Operations), 509**
- social engineering, 282**
- Soft key templates, 269**
- Soft Phones, 37**
 - acceptable use, 70
 - remote data centers, 56
 - security controls, 49, 54
 - telecommuters, 52, 57
- Softphones, 463, 464. *See also* CIPC**
- software**
 - antivirus. *See* antivirus programs
 - CTL Client, 529-533
 - CUCM. *See* CUCM
 - failures, 68, 552
 - maintenance, 311
 - monitoring, 76
 - NIPS, 571
 - patches, 237
 - PKI, 523-525
- SOHO (Small Office Home Office), 172**
- solution challenges, 15**
- Source Guard (IP), 120**
- source routing, disabling, 147**
- sources of certificates, 534**
- SPAM, 12**

Spam over Internet Telephony.*See* SPIT**SPAN (Switched Port Analyzer), 574**Cisco Catalyst Switch configuration,
574**span-to-PC port functionality, 446****speakerphones, 444****SPIT (Spam over Internet Telephony),
12, 288-290****spoofing, 524**

anti-spoofing measures, 160-162

ARP, 114-116

DHCP, 113-114

identification, 442

IP, 10, 29, 119-120

MAC addresses, 116-119

SQLNET protocol, 175**SRST (Survivable Remote Site
Telephony), 383, 399-402****SRTP (Secure Real Time Protocol),
239, 536-537**

authentication, 544

call flow, 546-547

CUCME voice traffic, 429-434

delay, 548

MGCP gateways, 270

MGCP support configuration,
391-394

support

*H.323 gateways, 394-396**SIP, 396-398*

termination, 271

wireless IP Phones, 456

SSH (Secure Shell), 132, 139, 478

ASAs, enabling access on, 494

best practices, 495

device configuration, 492-494

network security, 491-495

ssh scopy enable command, 508**SSL (Secure Sockets Layer)**

enabling, 316

encryption, 314

HTTP/HTTPS, 495

LDAP servers, 369

RDP, 502

SLDAP, 327

SSO (Single Sign-On), 295-307

Cisco Unity Connection, 338

interface configuration, 306-307

J2EE Agent Profile configuration,
301-302

Windows Desktop SSO

Authentication Module, 300

standards, encryption, 90**starvation attacks (DHCP), 120-122****stateful failover, 552****statements**

availability, 71, 72

policies, 70, 72. *See also* policies**static routes (CUPS), 350****Static Secure MAC addresses, 117****stations, management, 194****statistics (CUSSM), 514****status**

CSA, 237

CUE, 435

CUPS, 341

SELinux, 583

SSH, 492, 494

Status Monitor

Cisco Unity authentication, 329

Cisco Unity Web service security,
313-317**Sticky Secure MAC addresses, 117****STP (Spanning Tree Protocol),
manipulation, 112**

strategies

- policy development, 64-65, 69-74

- security, 19

- methodologies, 21-22*

- policy development, 24-26*

- streams, voice (CIPC), 469

- strict ephone registration, 427

- strong passwords, 156. *See also*

- passwords

- subnet restrictions, registration, 407

- summaries, policies, 71

- supplicants, 124

- authentication, 125

support

- antivirus programs, 312

- EOS, 237

- FTP, enabling, 149

- IP Phones, 107

- management, 90

- Microsoft, 311

- remote support accounting logs, 292-294

- SNMPv3 applications, 480-483

- SRTP

- configuration, 391-394*

- H.323 gateways, 394-396*

- SIP, 396-398*

- SSH, 492

- video (CUVA), 446

- supporting information, 71, 72

- survivability, physical security, 97, 100-101

- Survivable Remote

- Site Telephony, 37

- SUs (Service Units), 237

sweeps

- ping, 9

- SNMP, 9

- Switched Port Analyzer. *See* SPAN

switches

- access, 38

- address tables, 117

- assessments, 62

- Catalyst 3550, 106

- Cisco Catalyst Switch configuration, 574

- connections, 110

- controls, 41

- erasing, 29

- infrastructure, 54, 56

- Layer 2 security, 37

- Layer 3 security, 37

- ports

- configuration, 128*

- LLDP-MED, 447*

- SNMP, 483-485

- SSH, 132

- user-facing access, 132

- symmetric (secret-key) encryption, 522

- synchronization (LDAP), 345

- Syslog, 40, 478

- applications, 486

- ASAs, 488-490

- network security, 485-490

- voice gateways, monitoring, 403

- System Administrator. *See* SA

- System Health Dashboard, 576

- system requirements (SSO), 296-297

T**tables**

- addresses, switches, 117

- ARP, 115. *See also* ARP

- CAM table overflow attacks, 120-122
- patterns, restrictions, 318
- TACACS+ (Terminal Access Control Access Control Server), 157, 158-160**
 - accounting configuration, 159-160
 - authorization configuration, 159
 - Cisco Gatekeeper, 408
 - configuration, 129
- tags, double tagging (802.1Q), 110-111
- TCO (Total Cost of Ownership), 3**
- TCP (Transmission Control Protocol)**
 - headers, 548
 - ping scans, 9
 - small servers, disabling, 143
- technical challenges, 16**
- technical controls, 40**
- technology, security frameworks, 90**
- telecommuters, 50**
 - ASAs, 195-201, 227-231
 - security controls, 56-57
 - soft phones, 52
- Telephony User Interfaces. *See* TUIs**
- telnets, 132**
 - CUE, 435
- templates, Soft key, 269**
- temporary lockouts, accounts, 438**
- Terminal Access Control Access Control Server. *See* TACACS+**
- termination (SRTP), 271**
- testing, 60, 402**
- text**
 - CSR, 459
 - management (SSH), 132
 - plain, authentication, 150
- TFTP (Trivial FTP), 478**
 - ASAs, 175
 - authentication, mitigation, 149
 - encryption, 449
 - enumeration, 9
 - network security, 507-508
 - SBD, 249-250
 - security, 149
 - servers, 216, 543
 - UTIM-TFTP errors, 319
 - wireless IP Phones, 456, 463
- TFTP Server dialog box, 319**
- theft of equipment, 28**
- third-party**
 - certificates, 457
 - SIP Phone security, 264-267
- threats, 7, 8-12**
 - countermeasures, 68
 - CUPS, upgrading, 340
 - Layer 2 security, 29, 105
 - Layer 3 security, 30
 - physical security, 28
 - potential, identification of, 67-68
 - router management, 137-142
 - security
 - controls, 40*
 - countermeasures, 10-11, 12*
 - tracking, 62
 - UTM, 36
- time**
 - NTP, 164
 - zones, 385
- Time of Day Routing, 280-281, 422**
- timeouts**
 - console port limitations, 139
 - SSH, 493

TLS (Transport Layer Security), 239, 535-536

- context, 344
- CUCME voice traffic, 429-434
- EAP, 457
- HTTP/HTTPS, 495
- in-band network management, 475
- performance, 548
- sessions, 206
- static routes for CUPS, 350
- third-party SIP Phones, 264
- wireless IP Phones, 456

TLS Proxy

- ASAs, 203-212
- configuration, 360

token-based security, 410**tokenless authentication, 410****toll fraud, 10-11, 62, 279-282**

- Cisco Unity/Unity Connection, 317-318
- conferencing restrictions, 281
- COR, 380-383
- CUCME, 422-425
- CUE, 438-439
- endpoints, 442
- voice gateways, 378-384

TOLLFRAUD_APP, 380**Tomcat**

- certificates, 370
- external CAs, 256-258
- HTTP/HTTPS, 496

tools

- assessment, 13
- Cisco CP, 141
- DoS, 14-15
- enumeration, 14

flooding, 14-15

- media, 15
- RTMT, 294
- scanning, 9, 14
- signaling, 15
- sniffing, 13-14
- spoofing, 10
- VoIP, 9, 12-15

topologies

- CTL Client, 529-533
- external CA signed certificates PKI, 526
- Layer 2, 106-107
- loops, 112
- LSC PKI, 528
- MIC PKI, 527
- routing (authentication), 150
- self-signed certificates PKI, 526

Total Cost of Ownership. *See* TCO**tracking, 10, 281****traffic**

- ACL configuration, 378
- analyzers, 14
- CUCME, 429-434
- denying, 427
- DMZ, 36
- egress, inspection,
- filtering
 - ACL call control, 378*
 - CUBE, 416*
- identity, 570
- in-band network management, 475
- Layer 3 encryption, 168
- marking, 557
- mirroring, 572
- voice, 106

training

- physical security, 97, 100
- requirements, 91

transactions, 520**transcoding, 38****transfer max-length command, 423****transfer-pattern command, 423****transfers**

- Block OffNet to OffNet Transfers, 281
- calls, 383-384, 423-424
- IP Phone configuration, 543

transiting firewall endpoints, 186**transparency**

- enabling, 145
- firewalls, 179

Transparent mode, 179**Transport Layer Security. *See* TLS****Trojan horses, 10, 30**

- as potential threats, identification, 68

troubleshooting

- administrator logins, 336
- certificate errors, 505
- configuration errors, 270
- network security, 508-515
- toll fraud, 378. *See also* toll fraud
- voice, 447

TRP (Trusted Relay Point), 277-279**trunks**

- CUCM security, 271-276
- negotiation, 109-110
- SIP
 - resetting*, 325
 - security*, 273-275, 322

trust

- conditions, 30
- CTL, 239. *See also* CTL

CTL Client, 529-533

CUCM, 205-206

images, 539

IP addresses, 379

ports, 114

Trusted QoS Enforcement, 277**Trusted Relay Point. *See* TRP****trustpoints**

- authentication, 431
- CA servers, 358
- CME, defining, 431
- CUCM certificates, 400
- CUPS configuration, 357
- defining, 397

Trust Verification Service. *See* TVS**TTLS (Tunneled Transport Layer Security), 457****TTY (Asynchronous Line), 137**

CUE, 435

TUIs (Telephony User Interfaces), 318, 336**Tunneled Transport Layer Security. *See* TTLS****tunneling**

- EAP authentication methods, 125
- FAST. *See* FAST
- in-band network management, 475
- IPSec, 271
 - LAN-to-LAN*, 554
 - voice gateways*, 393

TurboVNC, 501**TVS (Trust Verification Service), 249, 251-253****Type 3 codes, ICMP, 155****types**

- of access, 137
- of controls, 40
- of failover, 552

U

UCS (Unified Computing System), 236, 310
UCSniff, 13
UDP (User Datagram Protocol), 143
UDP Flooder, 15
UltraVNC, 501
unauthorized access, 28, 62, 466.
See also security
Unicast Reverse Packet Forwarding.
See uRPF
Unified Computing System. *See UCS*
Unified IP Phone
 certificates, 533
 configuration, authentication, 540
 firmware image verification, 539-540
Unified Threat Management.
See UTM
Uninterruptible Power Supply.
See UPS
unnecessary IOS services, disabling, 142-149
unreachable messages, ICMP, 154
untrusted interfaces, inspection, 567
updating
 Cisco Notification Service, 137
 Server Update Wizard, 311
upgrading
 CUPS, 340
 OSs, 237
 Windows (Cisco Unity), 311
uploading
 ASA certificates, 224
 signed Tomcat certificates, 257
UPS (Uninterruptible Power Supply), 100

uRPF (Unicast Reverse Packet Forwarding), 162
USB (universal serial bus) security tokens, 531
U.S. Communications Assistance for Law Enforcement Act (CALEA), 90
User Datagram Protocol. *See UDP*
user-facing access switches, 132
users
 access (Layer 3 security), 157-160
 Access Policy, 73
 applications (CUCM), 287
 authentication, enabling IOS router HTTP servers, 142
 CAPF profiles, 284
 credentials, 10
 CTIManager, 283
 CUCM, 287
 facing access layers, 37
 groups, adding, 288
 TUIs, 318
 VRF, 282
UTIM (Cisco Unity Telephony Integration Management), 319
UTM (Unified Threat Management), 36, 172, 180, 551

V

validating hostnames, 417
values
 business, 7
 DWORD, 369
 estimations, 67
verification, 520
 commands (CUCME), 434
 identification, 150. *See also* access; management

- Syslog configuration, 489
- TVS, 249, 251-253
- Unified IP Phone, 539-540
- versions (SSH), 493
- Vice President. *See* VP
- video (CUVA), 446
- viewing logging, 447
- violation rule configuration, 118
- virtual LANs. *See* VLANs
- Virtual Network Computing. *See* VNC
- virtual sensors (Cisco IPS 4200 series appliances), 577
- Virtual Terminal Line. *See* VTY
- viruses, 30, 40
 - as potential threats, identification, 68
- visual alarms, 98, 99
- VLANs (virtual LANs)
 - access, 445, 447
 - Auth-Fail, 126
 - bridging, 215
 - CIPC, 469
 - critical, 126
 - dedicated, 132
 - guest, 126
 - hopping attacks/mitigation, 109-111
 - layer 2 topology overview, 106
 - TRP, 277
- VNC (Virtual Network Computing), 478
 - management access, 500-501
- voice
 - ASA QoS, 557
 - calls
 - encryption*, 543
 - signaling*, 541-542
- Cisco Unity
 - CCM Cluster Security Mode*, 319
 - CUCM*, 321-322
- conversation security (IP Phones), 448
- CUCME, 429-434
- endpoints (802.1x), 126
- enhanced inspection for voice protocols, 558-564
- gatekeepers, 44
- gateways, 37
 - conferencing*, 384-390
 - conversations*, 390-398
 - COR*, 380-383
 - CUCME*. *See* CUCME
 - monitoring*, 402-403
 - platform security*, 377-378
 - ports*, 189
 - preventing toll fraud*, 378-384
 - security controls*, 45, 54
 - SRST*, 399-402
- messaging
 - access switches*, 38
 - data centers*, 54
 - remote data centers*, 56
- signaling, 109
- streams (CIPC), 469
- traffic, 106
- troubleshooting, 447
- Voice Application Security Policy, 79
- voicemail, 4
 - acceptable use, 70
 - CUPC connectivity, 372-374

port security
 Cisco Unity/Unity Connection, 318-327
 CUCM, 324-327

Voice over IP. *See* **VoIP**

Voice Transmission Quality. *See* **VTQ**

Voice VLAN Identifiers. *See* **VVIDs**

VoIP (Voice over IP), 4, 180
 call transfer restrictions, 423-424
 tools, 9, 12-15

VoIP Hopper, 14

VoIPong, 14

VOMIT, 13

VP (Vice President), 135

VPNs (virtual private networks)
 Cisco VPN Phones, 222-227
 Client, telecommuters, 57
 phones, 57
 Routing and Forwarding. *See* **VRF**

VRF (VPN Routing and Forwarding), 282

VT Advantage, 37

VTQ (Voice Transmission Quality), 513

VTY (Virtual Terminal Line), 137
 port security, 139-140
 SSH restrictions, 494

vulnerabilities, 4, 8
 countermeasures, 68
 exploits, 30
 identification, 67-68
 management, 71
 policies, modifying, 60

VVIDs (Voice VLAN Identifiers), 126

W

WAN and Perimeter Security Policy, 77-78

WANs (wide-area networks), 5

 ASA failover, 552

 clusters, 554-557

WAP (Wireless Access Point), 449

Web

 access, 446

 Server Certificate Wizard, 314

 services

Cisco Unity Connection, 317

Cisco Unity/Unity Connection, 313-317

websites

 property defaults, 314

 vulnerabilities, 9

wheels, security, 60

WHOIS records, 9

Wi-Fi Multi Media. *See* **WMM**

windows, physical security, 98

Windows Desktop SSO

 Authentication Module, 300

Windows platform security (Cisco Unity), 311-313

wired IP Phones, 443-448

 secure network admission, 448

 TFTP encryption, 449

 voice conversation security, 448

Wireless Access Point. *See* **WAP**

wireless infrastructure, 54

 IP Phones, 449-463

 management, 454

wireless IP Phones

endpoints

conversations, 456

network admission, 457-463

hardening, 454-456

security, 454, 456

TFTP, 463

Wireless LAN Controller. *See* WLC

wireless networks, 41

Wireshark, 14

wiring (LANs), 76

wizards

Certificate Export Wizard, 259

CTL Client, 246

Web Server Certificate Wizard, 314

WLANs (wireless LANs)

configuration, 450

phones, acceptable use, 70

WLC (Wireless LAN Controller), 449

security, 450-454

WMM (Wi-Fi Multi Media), 453

workstations

LANs, 76

ports, servers, 192

worms, 30

as potential threats, identification, 68

X

X.509 certificates, 259

X.509 v3 certificates, 533-534

XMPP (Extensible Messaging and Presence Protocol), 345-368

Z

ZFWs (IOS Zone-Based Policy Firewalls), 426, 568-570

zones

ASAs

data centers, 183

firewalls, 177

CUCM, 272

pairs, 570

time, 385