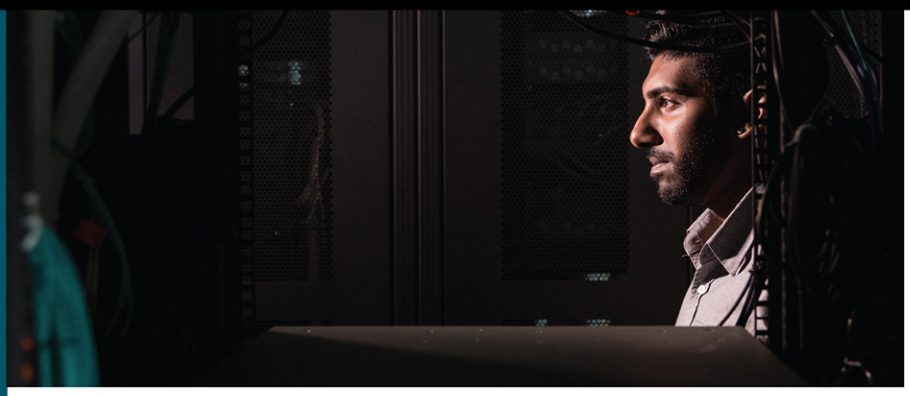

CCIE Professional Development

Integrated Security Technologies and Solutions

Volume II

Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Jamie Sanbower, CCIE® No. 13637
Chad Mitchell, CCIE® No. 44090

ciscopress.com

Integrated Security Technologies and Solutions - Volume II

Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity, and Virtualization

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Jamie Sanbower, CCIE® No. 13637
Chad Mitchell, CCIE® No. 44090

Cisco Press

Integrated Security Technologies and Solutions - Volume II

Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity, and Virtualization

Aaron Woland, Vivek Santuka, Jamie Sanbower, Chad Mitchell

Published by:
Cisco Press
221 River St.
Hoboken, NJ 07030 USA

1 19

Library of Congress Control Number: 2019931156

ISBN-13: 978-1-58714-707-4

ISBN-10: 1-58714-707-6

Warning and Disclaimer

This book is designed to provide information about Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity, and Virtualization. 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 authors, 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 authors 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Product Line Manager: Brett Bartow

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Project Editor: Mandie Frank

Copy Editor: Bill McManus

Technical Editor: Chad Sullivan

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Jeanine Furino

Credits

Figure 2-50 Hariprasad Holla

Table 1-1 Internet Assigned Numbers Authority

About the Authors

Aaron Woland, CCIE® No. 20113, is a principal engineer in Cisco's Advanced Threat Security group and works with Cisco's largest customers all over the world. His primary job responsibilities include security design, solution enhancements, standards development, advanced threat solution design, endpoint security, and futures.

Aaron joined Cisco in 2005 and is currently a member of numerous security advisory boards and standards body working groups. Prior to joining Cisco, Aaron spent 12 years as a consultant and technical trainer.

Aaron's other publications include *Integrated Security Technologies and Solutions - Volume I*; both editions of Cisco ISE for BYOD and Secure Unified Access; *Cisco Next-Generation Security Solutions: All-in-one Cisco ASA FirePOWER Services, NGIPS and AMP; CCNP Security SISAS 300-208 Official Cert Guide;* the *CCNA Security 210-260 Complete Video Course;* and many published white papers and design guides.

Aaron is one of only five inaugural members of the Hall of Fame Elite for Distinguished Speakers at Cisco Live, and he is a security columnist for *Network World*, where he blogs on all things related to security. His other certifications include GHIC, GCFE, GSEC, CEH, MCSE, VCP, CCSP, CCNP, and CCDP, among others.

You can follow Aaron on Twitter: @aaronwoland.

Vivek Santuka, CCIE® No. 17621, is a consulting systems engineer at Cisco and is a security consultant to some of Cisco's largest customers. He has over 13 years of experience in security, focusing on identity management and access control. Vivek is a member of multiple technical advisory groups.

Vivek holds two CCIE certifications: Security and Routing and Switching. In addition, he holds RHCE and CISSP certifications and is a Distinguished Speaker at Cisco Live.

Vivek is also the coauthor of the Cisco Press books *AAA Identity Management Security and Integrated Security Technologies and Solutions – Volume I.*

You can follow Vivek on Twitter: @vsantuka.

Jamie Sanbower, CCIE® No. 13637 (Routing and Switching, Security, and Wireless), is a principal systems engineer for Cisco's Global Security Architecture Team. Jamie has been with Cisco since 2010 and is currently a technical leader and member of numerous advisory and working groups.

With over 15 years of technical experience in the networking and security industry, Jamie has developed, designed, implemented, and operated enterprise network and security solutions for a wide variety of large clients. He is coauthor of the Cisco Press book *Integrated Security Technologies and Solutions - Volume I.*

Jamie is a dynamic presenter and is a Cisco Live Distinguished Speaker. Prior to Cisco, Jamie had various roles, including director of a cyber security practice, senior security consultant, and senior network engineer.

Chad Mitchell, CCIE® No. 44090, is a technical solutions architect at Cisco supporting the Department of Defense and supporting agencies. In his daily role, he supports the sales teams as a technical resource for all Cisco security products and serves as the Identity Services Engine subject matter expert for Cisco's US Public Sector team.

Chad has been with Cisco since 2013 supporting the DoD and other customers and is a contributing member to the Policy & Access Technical Advisors Group. Prior to joining Cisco, Chad spent 7 years as a deployment engineer and systems administrator implementing Cisco security products for customers.

While his primary area of expertise is enterprise network access control with ISE, Chad is well versed on all Cisco security solutions such as ASA firewalls, Firepower NGFW/IPS/IDS, and Stealthwatch, to name a few; he also has first-hand experience deploying these solutions in customer production environments.

Chad's other certifications include CCDA, CCNP, Network+, Security+, and many other industry certifications.

About the Technical Reviewer

Chad Sullivan (3xCCIE® No. 6493: Routing & Switching, Security, and SNA/IP) is the co-founder and President/CEO of Priveon, Inc., a security services-focused, Cisco Partner who globally implements and trains Cisco partners and customers on Cisco technologies. He has been working with Cisco Security and Networking products for decades and has even written and technical edited a handful of Cisco Press books around various endpoint and networking security technologies. You can often find him at an airport, or in front of an audience that is eager to learn from his vast experience in the security industry. When not working to help others secure global organizations, he spends his precious free time with his wife Jennifer and his six children (Avery, Brielle, Celine, Danae, Elliot, and Finley) in their Atlanta area home.

Dedications

First and foremost, this book is dedicated to my amazing best friend, fellow adventurer, and wife, Suzanne. Thank you for your continued support, encouragement, and patience and for putting up with all the long nights and weekends I had to be writing and for always believing in me and supporting me. You are beyond amazing.

To Mom and Pop. You have always believed in me, supported me in absolutely everything I've ever pursued, and showed pride in my accomplishments (no matter how small). I hope I can continue to fill your lives with pride, happiness, and "nachas"; and if I succeed, it will still only be a fraction of what you deserve.

To my four incredible daughters, Eden, Nyah, Netanya, and Cassandra. You girls are my inspiration, pride, and joy! I can only hope that one day you will look back at the ridiculous man that raised you and feel a level of pride.

—*Aaron*

To my beautiful wife. Thank you for your unconditional love and support. Your belief in me keeps me going. From my first CCIE to my third book, you have always encouraged me and have stood with me even when it took so much away from you. Thank you! I couldn't have done any of it without you.

To my son. Thank you for allowing me to miss all those gaming sessions to write this book. I promise to make it up to you. I know you will do much more than your dad and will make me proud. Love you.

—*Vivek*

This book is dedicated to my better half, my soulmate, my Christianna. From CCIEs to babies, we have accomplished so much together, blowing away the status quo. You always told me I could and should write a book, and I know without your support this book would not exist. The fact of the matter is you were as much a part of the writing process as I was. Thank you for putting up with all the late nights and weekends that I was writing and you didn't complain once (except for me being ADD about writing). Your companionship and love motivates me more than you will ever know.

To my amazing kids, Cayden and Lilianna. You are my inspiration and make me want to be a better version of myself. I know you both will amaze the world the way you amaze me each and every day! You make me smile and feel loved in ways that are indescribable.

To Mom and Dad for supporting my interests in technology from the start and certifications during grade school.

—*Jamie*

This book is dedicated to my loving family. To my wife, thank you for dealing with my time away from daily responsibilities, activities, and attention. Your unconditional love and support through the process of my CCIE studies, work travel, and writing this book let me know that I already found my one true love.

To my son, Caelin. You are my main man and the second love of my life. You impress me every day as you grow and always know how to make me smile. I can only hope to mentor and teach you, as others have for me, as you grow into an amazing gentleman.

Finally, to my mom and dad, Curtis and Cindy, for supporting me through my life journey. From multiple high schools to college dropout to trade school and back to college again, you have always been ready to help and guide me down the right path. Your support with watching Caelin while I was off writing this book is greatly appreciated as well. I couldn't have done it without all of your love and support and I am eternally grateful.

—Chad

Acknowledgments

There are so many to acknowledge, and I'm sorry that many will get left out.

Vivek Santuka, for not letting me give up and get out of writing this book and for keeping us all on time and on track.

Jamie Sanbower and Chad Mitchell for agreeing to coauthor this beast of a book with Vivek and I, and to Chad Sullivan for the painstaking job of tech-editing this beast. You guys are amazing!

I am honored to work with so many brilliant and talented people every day. Among those: Al Huger, Moses Frost, Steven Chimes, Andrew Benhase, Jeff Fanelli, Tim Snow, Andrew Ossipov, Mike Storm, Jason Frazier, Mo Sachedina, Eric Howard, Evgeny Mirolyubov, Matt Robertson, Brian McMahon, Adam O'Donnell, TK Keanini, Ben Greenbaum, Dean De Beer, Paul Carco, Karel Simek, Naasief Edross, Eric Hulse, and Craig Williams. You guys truly amaze me—seriously.

Last, but not least: to all those at Pearson, especially Mary Beth Ray, Chris Cleveland, and Mandie Frank, who have worked with me on nearly all of my publications. Thank you and your team of editors for making us look so good. Apparently, it takes an army of folks to do so. I'm sorry for all the times you had to correct our English, grammar, and CapItaLizaTioN.

—*Aaron*

Thank you to my wonderful coauthors, Aaron, Jamie, and Chad. Your efforts through professional and personal challenges are much appreciated. Thank you to our wonderful technical editor, Chad Sullivan, for all the hard work on this book.

To the wonderful people at Pearson—Mary Beth Ray, Chris Cleveland, Mandie Frank, and everyone else involved with this book—thank you for your tremendous work. Every time I opened an edited chapter, I couldn't help but be astonished at the attention to detail that you put into this.

Steven Bardsley and Gary McNiel, thank you for believing in me and for all the support and guidance.

Nirav Sheth, my first manager at Cisco, thank you for encouraging me to submit my first book proposal all those years ago. My professional achievements are rooted in your mentoring.

Finally, thank you to all the wonderful people I work with and learn from. There are too many to name, but you help me grow every day.

—*Vivek*

First and foremost, to the coauthors, Aaron, Vivek, Mason and Chad, together we conquered the two-volume set!

Thanks to our technical editor, Chad Sullivan, for keeping us straight and making Aaron split up his entirely too long chapter.

To Jamey Heary for encouraging me to write this book, and to the entire Global Security Architecture Team at Cisco, including Jeff Fanelli, Gary Halleen, Will Young, Mike Geller, Luc Billot, and, last but not least, the man who keeps the security experts in line, Randy Rivera. You all are inspiring, and together we cannot be beat. Seriously the best team at Cisco.

To Alex Golovin, my first mentor, who taught me what RTFM meant and how to keep learning and growing.

Lastly, to all those at Cisco Press, especially Mary Beth Ray, Chris Cleveland, and Mandie Frank. Thank you and your team of editors for producing a quality product and making the authors look good.

—Jamie

Throughout my career I have met many amazing people and I cannot list them all. I have learned so much from so many, and most don't even know it. If you have crossed my path, trust me, I have learned something from you even if you were there to learn something from me. I thank you all even if I don't mention you by name.

Thank you to my coauthors, Aaron, Vivek, and Jamie, for trusting in my technical aptitude to write this book and joining me on this next adventure of our careers.

Thank you to Chad Sullivan, our technical editor, for keeping us accurate and clear through our technical ramblings.

To Jamie Sanbower, for being a great friend and mentor. I wouldn't be where I am today in my career without your advice and where I am in life without your friendship. Your "Don't ask me questions until you have exhausted all resources or RTFM" method of teaching has helped me grow and learn more than I thought I ever would.

To Tony Pipta, for being a great friend and helping me keep my sanity with fishing trips in the Chesapeake Bay and hazy suds.

To Archie and TJ Guadalupe for being great friends who always go out of the way to help on anything and from time to time turning wrenches in the garage on my many projects.

To my dad, Curtis, for being my first mentor. I would not be the man, father, or engineer that I am today without you teaching me the way to learn from day one, literally.

Finally, to the folks at Cisco Press. I am glad that your editors paid attention during the punctuation and grammar classes, because I didn't. Your ability to take the ramblings of engineers and edit them into meaningful and readable content is unparalleled.

—Chad

Contents at a Glance

Introduction xix

Part I Knock, Knock! Who's There? 1

Chapter 1 Who and What: AAA Basics 3

Chapter 2 Basic Network Access Control 17

Chapter 3 Beyond Basic Network Access Control 149

Chapter 4 Extending Network Access with ISE 193

Chapter 5 Device Administration Control with ISE 307

Part II Spread the Love! 353

Chapter 6 Sharing the Context 355

Chapter 7 APIs in Cisco Security 407

Part III c2889775343d1ed91b 439

Chapter 8 Secure Connectivity 441

Chapter 9 Infrastructure VPN 477

Chapter 10 Remote Access VPN 543

Part IV The Red Pill 597

Chapter 11 Security Virtualization and Automation 599

Index 615

Contents

Introduction **xix**

Part I Knock, Knock! Who's There? 1

Chapter 1 Who and What: AAA Basics 3

Fundamentals of AAA 3

Understanding the Concept of Triple-A in the Real World 4

Compare and Select AAA Options 4

Device Administration 5

Network Access 6

TACACS+ 7

TACACS+ Authentication Messages 8

TACACS+ Authorization and Accounting Messages 10

RADIUS 12

AV Pairs 14

Change of Authorization (CoA) 15

Comparing RADIUS and TACACS+ 15

Summary 16

Chapter 2 Basic Network Access Control 17

What Is Cisco ISE? 17

ISE Architecture for Network Access AAA 18

Personas 18

Network Access AAA Architecture and ISE Personas 19

Configuring ISE for Single/Standalone and Multinode Deployments 23

Standalone 24

Dual Node 25

Distributed Deployment 29

ISE Configuration for Network Access 32

Identity Sources 32

Identity Source Sequences 48

Network Resources 50

802.1X and Beyond 54

EAP Types 56

Not Everything Has a (Configured) Supplicant 62

Configuring Wired Network Access with ISE 71
Configuring Cisco Catalyst Switches 71
Global Configuration for All Catalyst Switches 72
Interface Configuration for Classic and Newer IOS Switches 82
Common Classification Policy Language Switches 88
Configuring ISE for Basic Wired Network Access Control 100
Configuring Wireless Network Access with ISE 115
Introduction to AireOS and Its Versions 116
Authentication Configuration on WLCs 117
Configure the AAA Servers 118
Configure the Airespace ACLs 121
Create the Dynamic Interfaces for the Client VLANs 124
Create the Wireless LANs 127
Configuring ISE for Wireless Network Access Control 138
Verifying Dot1X and MAB 140
Endpoint Supplicant Verification 140
Network Access Device Verification 140
Cisco ISE Verification 147
Summary 148

Chapter 3 Beyond Basic Network Access Control 149
Profiling with ISE 149
ISE Profiler Work Center 153
Profiling Policies 168
Profiling Feed Service 168
Endpoint Profile Policies 170
Context Visibility 171
Logical Profiles 174
ISE Profiler and CoA 175
Global CoA 176
Global Profiler Settings 177
Profiles in Authorization Policies 178
Endpoint Identity Groups 178
Passive Identities and EasyConnect 180
Passive Authentication 181
EasyConnect 183
Summary 191

Chapter 4 Extending Network Access with ISE 193

Get Ready, Get Set, Prerequisites 194

URL Redirection 194

AAA Configuration 197

BYOD Onboarding with ISE 197

Building Blocks of a BYOD Solution 198

Single SSID and Dual SSID Provisioning 200

Configuring ISE for BYOD Onboarding 202

Network Device Configuration for BYOD Onboarding 223

BYOD Onboarding Verification and End-User Experience 229

MDM Onboarding and Enforcement with ISE 236

Posture Assessment and Remediation with ISE 244

Preparing to Configure Posture 247

Configuring AnyConnect Provisioning 249

Configuring Posture Policy 255

Configure Policy Set for Posture 262

Guest Access with ISE 265

Preparing to Configure Guest Access 268

Sponsor Groups and Portal 270

Hotspot Portal 278

Sponsored and Self-Registered Guest Portals 279

Configuring Policy Sets for Guest Access 284

TrustSec with ISE 287

Introducing TrustSec 288

Classification 290

Propagation 292

Enforcement 300

Summary 306

Chapter 5 Device Administration Control with ISE 307

The Case for Centralized AAA 307

RADIUS Versus TACACS+ for Device Administration 308

Using TACACS+ for Device Administration 309

Configuring ISE for TACACS+ 310

TACACS+ with Cisco IOS Routers, Switches, and ISE 318

TACACS+ with Cisco ASA and ISE 331

TACACS+ with Cisco WLC and ISE 335

Using RADIUS for Device Administration 343
RADIUS-Based Device Administration on Cisco FMC 343
RADIUS-Based Device Administration on Cisco WSA/ESA 349
Summary 352

Part II Spread the Love! 353

Chapter 6 Sharing the Context 355
The Many Integration Types of the Ecosystem 356
MDM Integration 356
Rapid Threat Containment 356
Cisco's platform eXchange Grid (pxGrid) 359
pxGrid in Depth 361
pxGrid in Action 362
Context-In 363
Configuring ISE for pxGrid 364
Configuring pxGrid Participants 368
Summary 406

Chapter 7 APIs in Cisco Security 407
APIs 101 407
RESTful APIs 409
Working with APIs 410
Cisco DevNet 412
Firepower Management Center APIs 413
FMC REST API for Configuration 413
Firepower System Remediation API 414
FMC Host Input API 421
FMC Database Access API 422
FMC eStreamer API 423
Identity Services Engine APIs 424
ISE Monitoring REST API 424
ISE External RESTful Services API 426
Advanced Malware Protection APIs 428
Threat Grid APIs 433
Umbrella APIs 435
Summary 437
References 437

Part III c2889775343d1ed91b 439

Chapter 8 Security Connectivity 441

Hashing, Ciphers, Cryptography, and PKI 441

Hashing 441

Cipher Types 444

Encryption Schemes 445

The Keys to the Kingdom 446

Authentication Mechanisms 446

Security Protocols 453

The Bits and Pieces 458

Virtual Private Networks 461

IPsec 461

DMVPN 462

FlexVPN 465

GETVPN 466

SSL Remote Access VPN 469

Layer 2 Encryption: IEEE 802.1AE/MACsec 470

Summary 474

References 474

Chapter 9 Infrastructure VPN 477

IPsec with IKEv1 478

IPsec with IKEv2 484

EzVPN 492

DMVPN 500

DMVPN Phase 1 506

DMVPN Phase 2 508

DMVPN Phase 3 510

Dual-Hub DMVPN 513

FlexVPN 514

GETVPN 532

Summary 541

References 541

Chapter 10 Remote Access VPN 543

Remote Access VPN Overview 543

Clientless versus Client-Based VPNs 545

Cisco AnyConnect Secure Mobility Client 546

AnyConnect Profile Editor 547

Deploying AnyConnect 552

Client-Based Remote Access VPN 554

RAVPN with ASA 554

Group Policies 562

Dynamic Access Policies 565

Posture Assessment 567

RAVPN with Firepower Threat Defense 570

RAVPN with Routers 580

IPsec Remote Access VPN on IOS Using IKEv2 with FlexVPN Example 580

Clientless Remote Access VPN 586

Summary 595

References 595

Part IV The Red Pill 597

Chapter 11 Security Virtualization and Automation 599

Cisco Virtual Solutions and Server Virtualization 599

Virtualization and Automation Solutions 602

Cisco Virtual Security Gateway 602

Service Function Chaining with Network Service Header 603

Network Function Virtualization 605

Application Centric Infrastructure and Micro-Segmentation 608

Summary 613

References 614

Index 615

Reader Services

Register your copy at www.ciscopress.com/title/9781587147074 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9781587147074 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

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

This book is the second and last volume of the *Integrated Security Technologies and Solutions* set in the Cisco CCIE Professional Development Series from Cisco Press. It offers expert-level instruction in security design, deployment, integration, and support methodologies to help security professionals manage complex solutions and prepare for the CCIE Security exams.

This book is an expert-level guide for Cisco security products and solutions, with a strong focus on inter-product integration. Its aim is to help security professionals in their day-to-day jobs as well as in preparing for CCIE written and lab exams.

This volume focuses on the Identity Services Engine, Context Sharing, TrustSec, Application Programming Interfaces (APIs), Secure Connectivity with VPNs, Virtualization, and Automation sections of the CCIE v5 blueprint.

Who Should Read This Book?

This book discusses expert-level topics on Cisco security products and solutions, with a focus on integration between these products. In particular, this volume covers ISE, context sharing, APIs, VPN, virtualization, and automation. The book has been designed with the CCIE Security v5 blueprint as a reference, making it a must-have for CCIE Security candidates.

This book presents real-world deployment scenarios, configuration examples, and troubleshooting steps, so it is invaluable to any network engineer, system administrator, security engineer, or security analyst who wants to configure or manage Cisco security products and solutions.

This book is very important for channel partners and managed security service providers who want to provide technical support to their own customers.

This book is also very useful for network administrators in classified environments, such as the U.S. government, who are not allowed to share their sensitive data and want to design, configure, and troubleshoot on their own.

How This Book Is Organized

This book consists of 11 chapters divided into 4 parts.

Part I, "Knock, Knock! Who's there?"

Chapter 1, "Who and What: AAA Basics"

The book begins with a discussion of the fundamentals of authentication, authorization, and accounting (AAA). This chapter discusses the two common protocols used for AAA: RADIUS and TACACS+.

Chapter 2, "Basic Network Access Control"

This chapter dives deeper into AAA with an introduction to Cisco Identity Services Engine (ISE). It discusses 802.1X, various EAP types, Machine Authentication Bypass (MAB), and how to configure ISE and network devices to use these authentication methods.

Chapter 3, "Beyond Basic Network Access Control"

This chapter discusses profiling features of ISE. It describes various methods available for profiling. It also covers ISE features such as EasyConnect and passive identity.

Chapter 4, "Extending Network Access with ISE"

This chapter discusses advanced ISE topics such as BYOD, mobile device management (MDM) integration, posture validation, and guest services. It describes the use of these features and how to configure ISE and network devices for them. This chapter also discusses components and configuration of TrustSec.

Chapter 5, "Device Administration Control with ISE"

This chapter discusses device administration AAA with ISE using TACACS+ and RADIUS. It describes various methods available to authenticate and authorize device administration requests across various Cisco devices with ISE.

Part II, "Spread the Love!"

Chapter 6, "Sharing the Context"

This chapter discusses context sharing with ISE. It describes ISE features and functions such as pxGrid and Rapid Threat Containment. It describes the various integrations and benefits of such integrations with other Cisco devices such as the Cisco Firepower Management Center (FMC) and Cisco Web Security Appliance (WSA). It also discusses the steps required to accomplish such integration.

Chapter 7, "APIs in Cisco Security"

This chapter describes various APIs available in Cisco security products and the benefits of using them. It also discusses specific examples of APIs available in Cisco security products.

Part III, "c2889775343d1ed91b"

Chapter 8, "Security Connectivity"

This chapter discusses fundamentals of virtual private networks (VPNs) and various types of VPNs available on Cisco products.

Chapter 9, "Infrastructure VPN"

This chapter discusses various types of infrastructure VPN such as site-to-site and Dynamic Multipoint VPN (DMVPN). It describes their features, functionality, and configuration required on various Cisco products.

Chapter 10, "Remote Access VPN"

This chapter discusses different types of remote access VPN solutions available on various Cisco devices. It describes their features, functionality, and configuration.

Part IV, "The Red Pill"

Chapter 11, "Security Virtualization and Automation"

This chapter discusses the virtualization of various Cisco security products. It also discusses the Cisco Virtual Security Gateway (VSG), Cisco Enterprise Network Functions Virtualization (NFV), and micro-segmentation with ACI.

Part II

Spread the Love!

Chapter 6 Sharing the Context

Chapter 7 APIs in Cisco Security

This page intentionally left blank

Chapter 6

Sharing the Context

Because Cisco Identify Services Engine (ISE) is positioned to know exactly who and what is on the network at any given time, as well as assign different levels of access and context assignments with security group tags, it is the perfect security tool to be at the center of a security ecosystem.

There are so many tools that may exist within your "security toolbox": firewalls, next-generation firewalls (NGFWs), intrusion prevention systems (IPSs), NG-IPSs, security information and event management (SIEM) systems, secure web gateways, threat defense tools, vulnerability assessment scanners, mobile device managers, and more. Most of these tools do not know the identity of the user, only the identity of the endpoint. These other tools can be made even more valuable by integrating into a full security ecosystem with ISE.

Wouldn't the reporting in the SIEM be more valuable if it showed which user was involved in the security event, instead of only the IP address or MAC address? What about when your intrusion prevention tools or threat defense solutions identify malicious activity on the network? Wouldn't it be great if they could trigger something that would change the way the endpoint was treated on the network? With a single "trigger," the endpoint's level of network access could be changed, the endpoint's traffic could be inspected deeper as it passes through a Cisco Adaptive Security Appliance (ASA), the Cisco Web Security Appliance (WSA) can apply a different SSL decryption policy, and so much more.

You've already read about ISE integrating with mobile device managers (MDMs) and a little bit on how ISE can provide passive identities to ecosystem partners through technologies like pxGrid, but it can also provide the single point of policy control for threat containment and context setting.

The Many Integration Types of the Ecosystem

An *integration* might be ISE sharing data outbound, or it may be ISE steering traffic toward another solution. The integration method could be with ISE receiving information inbound for use within ISE's own network access policies, or even ISE brokering data exchange between other members of the security system.

MDM Integration

In Chapter 4, "Extending Network Access with ISE," you read about BYOD and the integration between ISE and mobile device management solutions. That integration is twofold: ISE provides the redirection to the MDM service for onboarding, but the MDM service is also able to provide "context-in" to ISE. In other words, the MDM service tells ISE about the mobile endpoints, the endpoint's compliance with the security policies set in the MDM (macro-level compliance), the status of encryption or pin lock, and more (micro-level compliance).

This integration uses a specific bidirectional application programming interface (API) between ISE and the MDM solution (cloud service or appliance). This API is unique and created just for MDM integration.

Note Thanks to industry marketing, endpoint device management platforms may be referred to as Mobile Device Manager (MDM), Unified Endpoint Management (UEM) platforms, or even an Enterprise Mobility Management (EMM) platform. For the purposes of this book, the term MDM is leveraged to cover all the marketing acronyms referring to endpoint device managers.

Rapid Threat Containment

MDM is one of the first and most common integration types for ISE. In true Cisco marketing fashion, this next integration type, Rapid Threat Containment, has gone through several different names and marketing initiatives.

There was a feature added back in ISE 1.1 called *Endpoint Protection Services (EPS)*. EPS provided an API allowing other applications to initiate three actions against an endpoint based on IP address or MAC address:

- **Quarantine:** The quarantine action set the binary flag on the endpoint record to "true," added the endpoint to a list of quarantined endpoints, and allowed the administrator to create authorization policies that used that assignment to assign a different level of network access.
- **Unquarantine:** Removed the endpoint from the list of quarantined endpoints and cleared the binary flag.
- **Shutdown:** Was supposed to send a Change of Authorization (CoA) terminate to the network and shut down the port on the network switch.

Note This option exists in the API, but it is not exposed to the policy and is therefore not usable.

Many of the first integrations with ISE used EPS, including the original integration with Lancope StealthWatch (now Cisco Stealthwatch), where an endpoint was quarantined from the StealthWatch user interface.

Figure 6-1 illustrates a flow with Stealthwatch initiating an EPS quarantine.

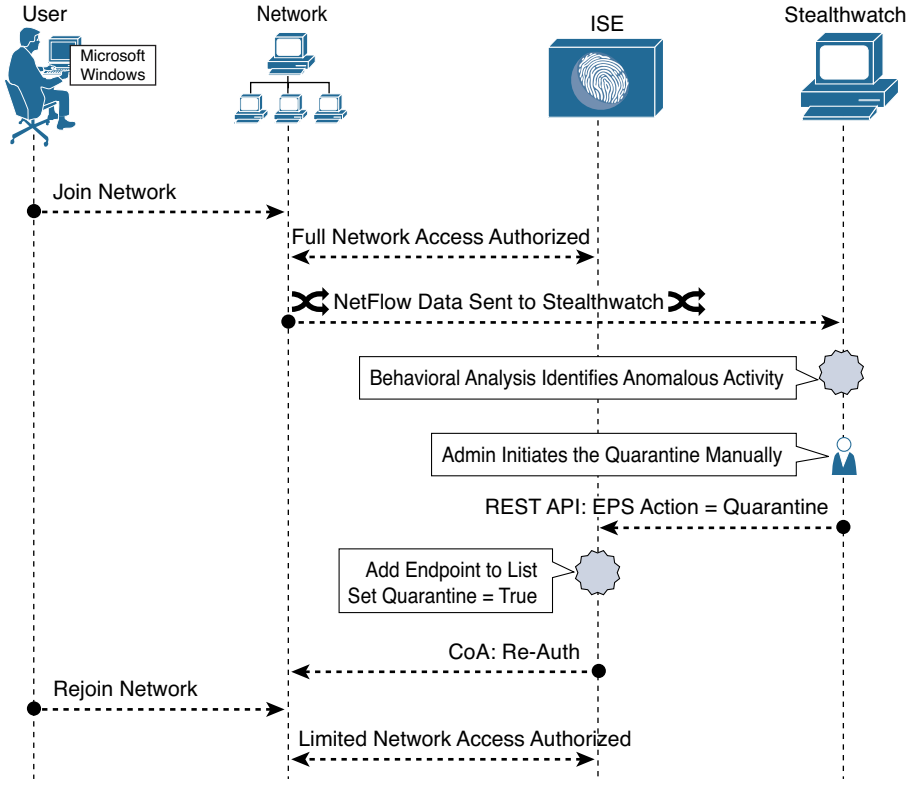

Figure 6-1 *Stealthwatch to ISE: EPS Quarantine*

The flow illustrated in Figure 6-1 shows an endpoint being admitted to the network with full access. The Stealthwatch admin initiates a quarantine, and Stealthwatch connects to ISE using the EPS REST API, telling ISE to quarantine the endpoint with the specific IP address.

ISE then adds the endpoint to the EPS list and sets the flag on the endpoint object and sends a CoA to the network.

When the new access request comes in, a rule created with the EPSStatus condition will be matched. Figure 6-2 shows that condition.

Figure 6-2 *EPSStatus Authorization Condition*

The resulting network authorization may provide for limited access, or even set a new Security Group Tag (SGT) that can be acted upon differently at miscellaneous points in the network, such as the Web Security Appliance.

Well, ultimately EPS was just too rigid. It provided for only a single actionable classification (Quarantine). More flexibility was needed to provide many different options, but also to be integrated into this new-fangled context-sharing technology that Cisco was creating named pxGrid. So, it needed to evolve into "EPS 2.0" or something like it.

So, ISE 1.3 introduced something new named Adaptive Network Control (ANC), which was a huge step forward by simply renaming EPS to ANC. Okay, hopefully the sarcasm was obvious there.

ISE 1.4 actually added new functionality to ANC. While still supporting the old EPS API calls for backward-compatibility purposes, it also added a new API with different labels available, including the ability to create your own label.

ISE refers to these labels as ANC "policies," but there is no policy to them whatsoever. An ANC policy is a tag or a label that gets assigned to an endpoint object and can be used in the authorization policy to invoke some action, such as changing the authorization level and assigning a new SGT.

Although you can add many different labels, there are only three choices for ANC policies: Quarantine, Shut Down, and Port Bounce—which determines the CoA type used when the label is applied to the endpoint.

To create an ANC policy (a.k.a. label), navigate to **Operations > Adaptive Network Control > Policy List** and click **Add**. Figure 6-3 shows the resulting page with the Action drop-down menu open.

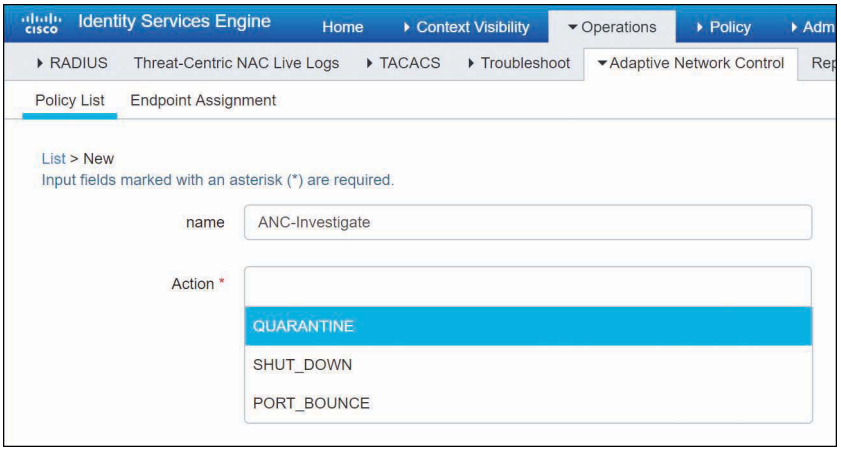

Figure 6-3 *Adding an ANC Policy*

You can create multiple ANC policies, and each policy may contain one or more actions. Each ANC policy can be associated to a different authorization. For example, you can end up with ANC policies such as:

- Investigate
- Phasers on Stun
- Eradicate
- Nuke from Orbit

In addition to a much more flexible approach to classification, or as Cisco's legendary Paul Forbes would call it, "flexible name spaces," ANC also integrates tightly with pxGrid, allowing pxGrid subscribers to trigger the ANC action within the pxGrid connection, not through the point API of the past.

So now you have Endpoint Protection Services which was renamed to Adaptive Network Control. Then Adaptive Network Control gets new functionality in ISE 1.4. Then Cisco security marketing gets involved and comes up with a new naming convention to refer to the entire integrated security system where any Cisco security product may take action through another Cisco security product.

That name is Rapid Threat Containment. You have solutions like: Rapid Threat Containment with Cisco Stealthwatch and the Identity Services Engine and Rapid Threat Containment with Cisco Firepower Management Center and Identity Services Engine.

While ISE is often the center of a security ecosystem, the Rapid Threat Containment portfolio includes more than just integrations with ISE. There are solutions like Rapid Threat Containment with Firepower Management Center and Cisco Stealthwatch, Firepower and Cisco Tetration, and many more. Actions taken using Cisco Threat Response are also part of the Rapid Threat Containment umbrella (no pun intended).

Crystal clear, right?

Cisco's platform eXchange Grid (pxGrid)

Now that you are thoroughly confused about the marketing term "Rapid Threat Containment", let's clear up one thing. Rapid Threat Containment may leverage pxGrid for the integration between two or more Cisco security products, but pxGrid is not a requirement. Many of those integrations are handled by API's or other connection types.

What is this pxGrid thing that we keep talking about?

pxGrid is Cisco's premier publish and subscribe (pub/sub) communication bus that was designed from the ground up to be a scalable, secure data sharing system.

Like most other next-generation AAA solutions, ISE originally started sharing information through the use of APIs. It was quickly recognized that point APIs would not scale to the level of data that needed to be shared and the scale of which it was requested.

Cisco went down the path of a pub/sub bus, similar to the way Cisco Unified Communications Manager (formerly known as Call Manager) and Cisco Jabber work. A *controller* keeps track of all the topics that exist. A *topic* is a list of information that is available. A topic might be session data of who and what is on the network, or it might be a list of vulnerable endpoints and the list of those vulnerabilities.

pxGrid participants can subscribe to any topic of interest and be notified when there is data to be retrieved. Those participants are known as *subscribers*. The true source of the data can be any other pxGrid participant, known as *publishers*. A publisher registers the topic with the controller, who performs the authorization for each subscriber to retrieve the data from the miscellaneous publishers.

Figure 6-4 shows the standard Cisco drawing that is often used to explain pxGrid. In this illustration, you see many different types of products, each of which has different information to publish and needs information from one of the other products.

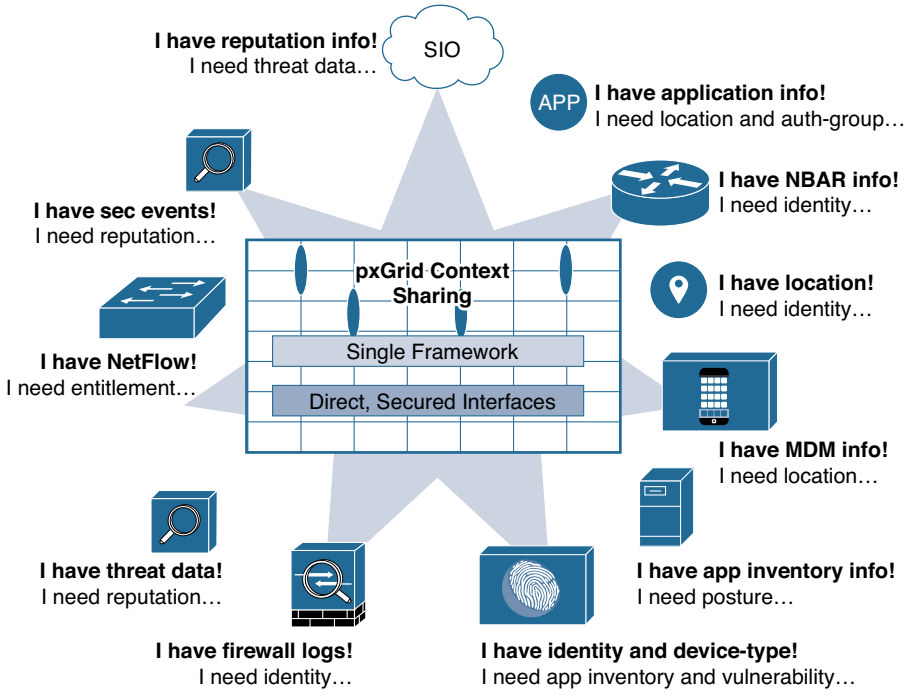

Figure 6-4 *Standard Cisco pxGrid Illustration*

pxGrid was initially added to ISE in version 1.3, so it's been around for a while now and has an ecosystem of partner applications that continue to grow at a very rapid pace.

ISE 2.2 made great strides in enhancing pxGrid. Most of the pxGrid-related enhancements are around ease of use, making it even easier to configure and maintain. ISE 2.2 also added more information into ISE's pxGrid topics for consumption by the

subscribers. A specific example of additional information that was added to pxGrid topics in ISE version 2.2 is the list of groups that each active user is a member of; and that list was shared within the same topic(s) that was used in previous ISE versions, enabling backward compatibility seamlessly.

pxGrid in Depth

pxGrid version 1 was designed by extending the Extensible Messaging and Presence Protocol (XMPP), which is also the communication protocol used by Jabber. In fact, the pxGrid controller itself is a modified Jabber Extensible Communications Platform (XCP) server. (For more on XMPP, see https://xmpp.org.)

The XCP needs a client that knows how to communicate with it. Cisco DevNet partners can create applications that use the pxGrid common library (GCL) to join the pxGrid controller without having to write their own client from scratch.

Beginning in ISE version 2.3, ISE added a modernized WebSocket-based interface to pxGrid, to make it easier to integrate with. DevNet partners no longer are required to integrate a Java or C library into their application; they can use common Representational State Transfer (REST) connections instead.

No matter what the version, always remember that pxGrid is made up of three main components: a controller, publishers, and subscribers. Figure 6-5 is a basic drawing to illustrate this with products.

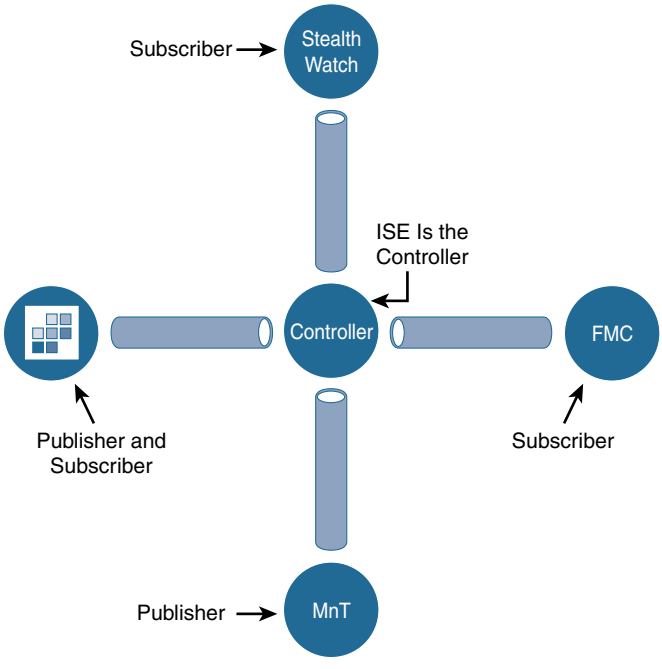

Figure 6-5 *Sample pxGrid Illustration*

pxGrid in Action

pxGrid uses secure communication between the participants, and therefore certificates are of great importance to the success and ease of your deployment. Every participant must trust the controller, and the controller must trust each of the participants.

Examining Figure 6-5 again, the Cisco Firepower Management Center (FMC) will need to speak to the pxGrid controller to learn of the topics that exist and who has published those topics, but then also speak directly to the MnT node to perform bulk downloads of the published session data. If the FMC were to trust the pxGrid controller's certificate but not the MnT's certificate, then the communication would ultimately fail.

Figure 6-6 illustrates this concept. You end up needing a full mesh of trust between pxGrid participants. Each participant must trust the controller as well as each other participant.

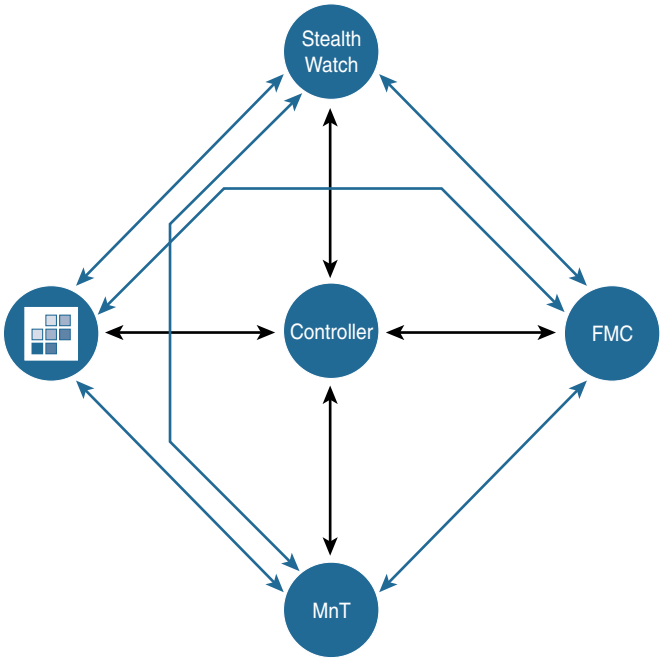

Figure 6-6 *Full Mesh of Trust*

Based on a lot of deployment experience, the resulting best practice is to always use the same certificate authority (CA) to issue the pxGrid certificates for each of the participants. To make that even easier, ISE's built-in CA was enhanced to issue pxGrid certificates in addition to endpoint certificates beginning with ISE version 2.1. In addition to the enhancement to the CA, APIs were added to automate the certificate enrollment from a pxGrid ecosystem partner—these are the exact same APIs and CA that Cisco's flagship DNA Center product uses to integrate with ISE.

Figure 6-7 illustrates a single CA issuing the certificates to all the participants.

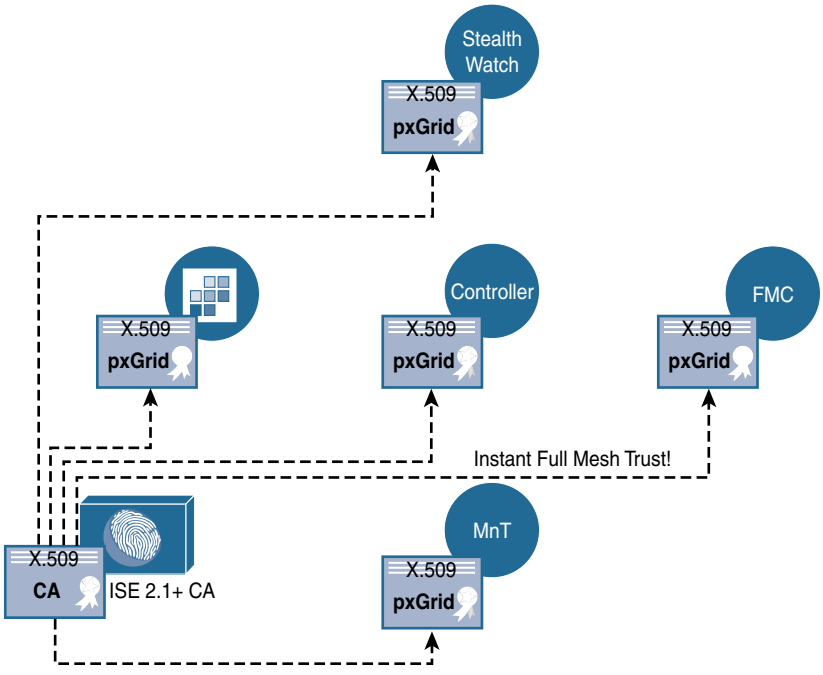

Figure 6-7 *ISE CA Issuing the pxGrid Certificates to All Participants*

Context-In

pxGrid not only shares context from ISE (referred to as *context-out*) but also is used for sharing information between external systems. As of ISE version 2.4, ISE is also able to receive information through pxGrid to help ISE with its own profiling policies. This is referred to as *context-in*.

In Chapter 3, "Beyond Basic Network Access Control," you learned about profiling and the different probes that ISE can use. One of those probes that was introduced in ISE version 2.4 is the pxGrid probe, which is used to learn profiling data about endpoints through pxGrid context-in.

The pxGrid profiling probe was first used with the Cisco Industrial Network Director (IND), which communicates with industrial switches and Internet of Things (IoT) security devices, collecting detailed information about the connected IoT devices.

IND v1.3 adds a pxGrid publisher interface to communicate IoT attributes to ISE, which are leveraged in profiling, as illustrated in Figure 6-8.

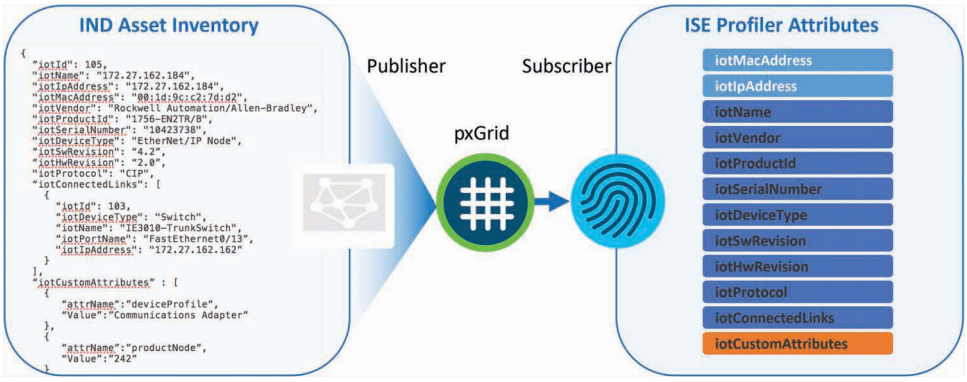

Figure 6-8 *Industrial Network Director Using ISE pxGrid Probe*

Configuring ISE for pxGrid

The pxGrid user interface is located under **Administration > pxGrid Services.** By default, the pxGrid services will not be enabled on any ISE node, and the following message will be displayed:

```
In order to navigate to the pxGrid Services page, pxGrid persona must
be enabled on at least one node in the ISE deployment. Please click on
this link to be redirected to the Deployment page.
```

You need to enable pxGrid on at least one of the policy services nodes in your deployment, but before enabling pxGrid on any of the ISE nodes in the deployment, it's best to ensure that each node in the ISE cube has a pxGrid certificate signed by the same certificate authority.

Beginning in ISE 2.2, each node's pxGrid certificate will be signed automatically by the internal CA. Naturally, you can replace that certificate with one from an external CA of your choosing, but the default certificate will use the internal CA in an attempt to simplify the setup and follow best practices. Truly, recommended practice dictates that you use the CA built into ISE for all pxGrid communications to keep things easy and working well. The steps are as follows:

Step 1. Navigate to **Administration > System > Certificates**, as shown in Figure 6-9.

Step 2. Select the pxGrid certificate of one of the nodes, by selecting the checkbook on the left end of the row.

Step 3. Click **View**.

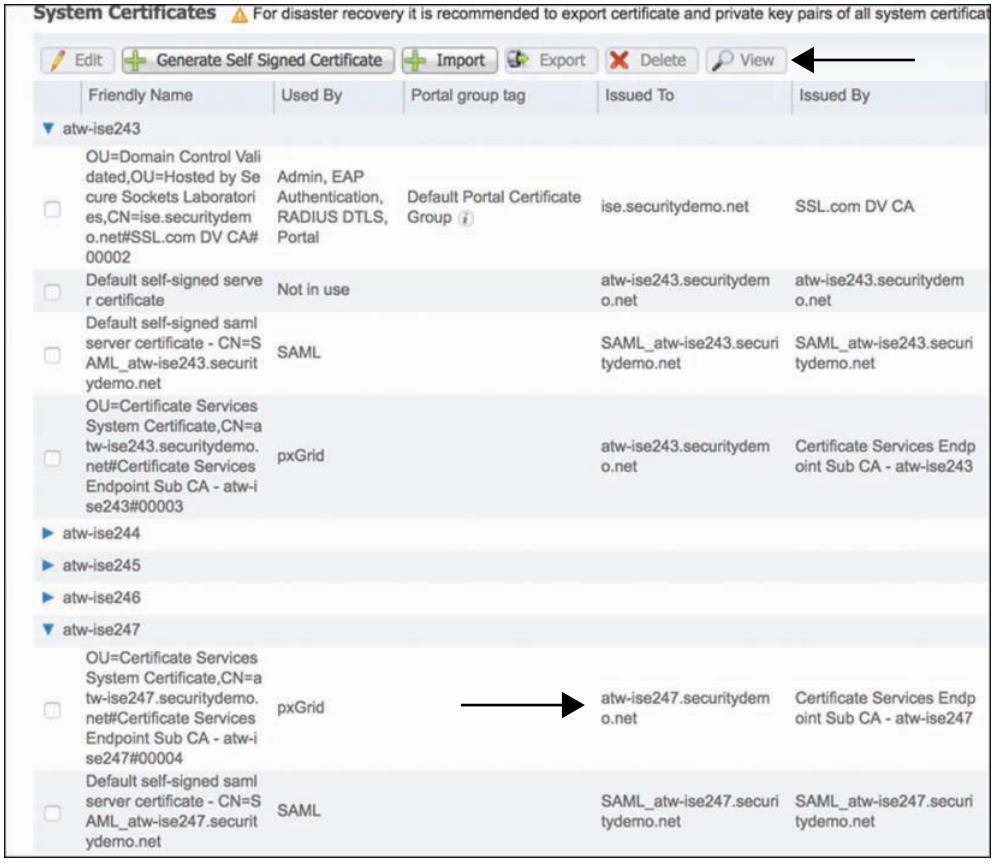

Figure 6-9 *Viewing a pxGrid Certificate*

Step 4. Check that the root signer of the certificate is the primary PAN of the ISE cube (the root CA), as shown in Figure 6-10.

Once you're sure the certificates in use are all issued by the same PKI, then it's time to enable them. Experienced-based recommendation is to have a pxGrid certificate on every single node in the ISE deployment, even if the node will not run the pxGrid controller function.

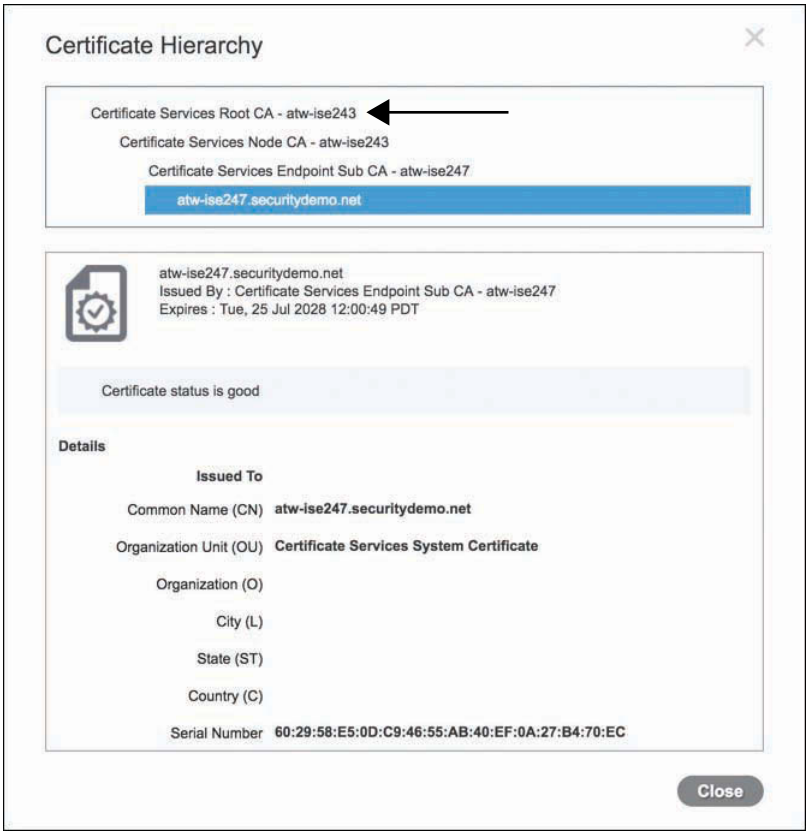

Figure 6-10 *Checking the Root Signer of Certificate in Certificate Hierarchy*

Note Beginning in ISE version 2.2, all pxGrid communications occur within the secure pxGrid channel; in other words, all communication occurs leveraging the pxGrid certificate of the ISE node. In prior versions, all bulk downloads from the MnT node occurred using the admin certificate, not the pxGrid certificate. This caused many TAC cases and confusion and needed to change. If you are implementing pxGrid on any ISE version less than ISE 2.2, you must ensure that the participant trusts the issuing CA of the admin certificate as well as the pxGrid certificate.

To enable pxGrid on a PSN, follow these steps:

Step 1. Navigate to **Administration > System > Deployment**.

Step 2. The pxGrid controller function must run on a PSN. Select one of the PSNs from the list.

Step 3. Check the **pxGrid** check box, as shown in Figure 6-11.

Step 4. Click **Save**.

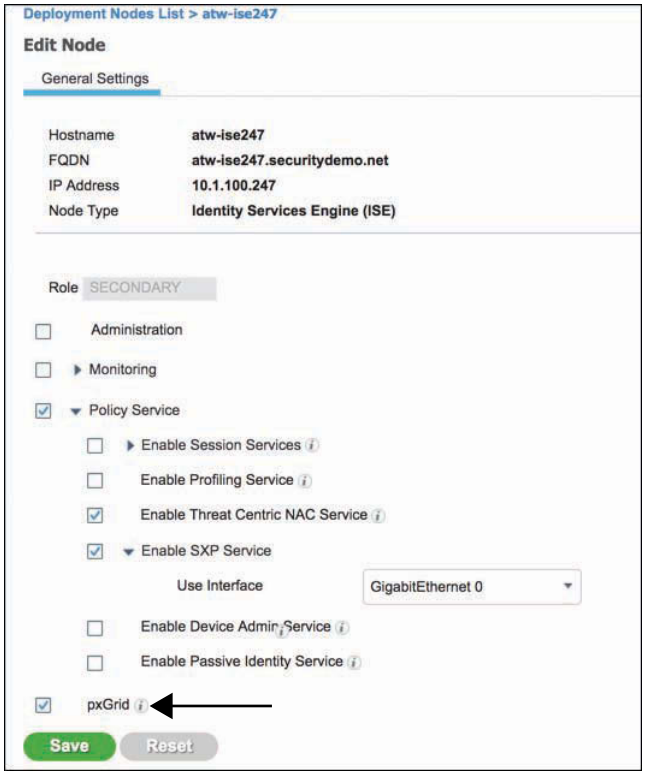

Figure 6-11 *Enabling the pxGrid Controller Function*

This enables the pxGrid controller function on the PSN. You may have up to two pxGrid controllers per ISE cube to provide redundancy.

Once the pxGrid services are all up and running, the PAN and MnT will automatically register and publish their respective topics into the grid, as shown in Figure 6-12.

Notice in Figure 6-12 the way the topics are listed under the pxGrid participant, as well as the role that node plays with the topic (Pub or Sub).

By default, only ISE nodes will be registered automatically; all others require approval, or they require you to enable auto-registration.

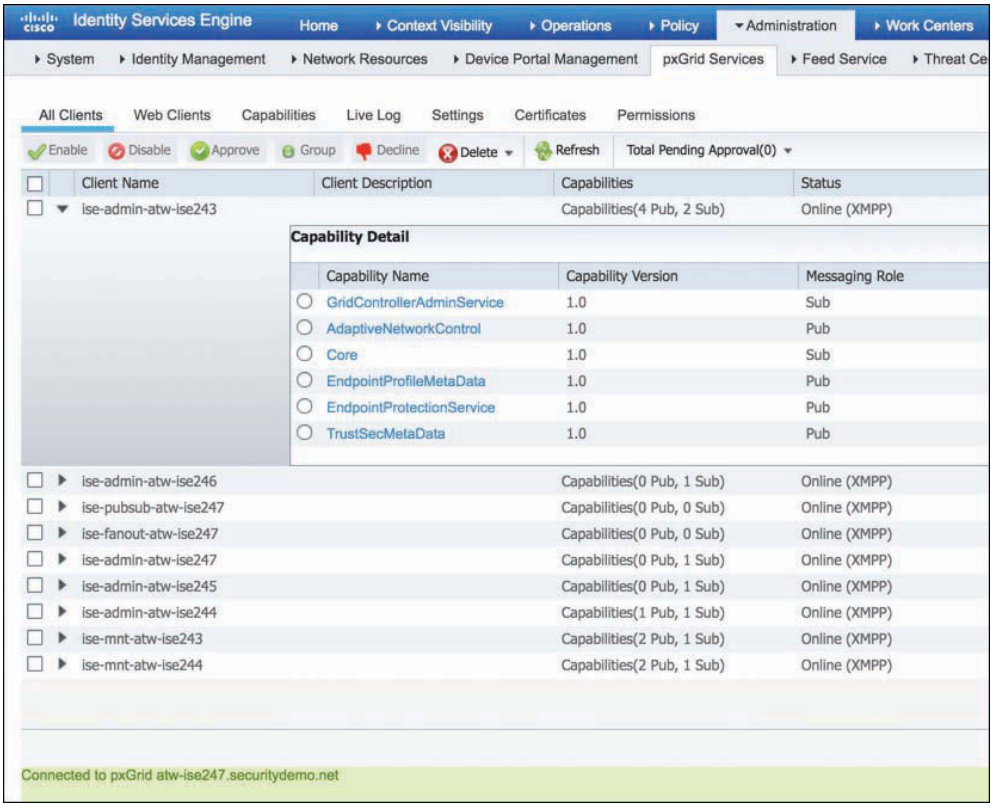

Figure 6-12 *Default pxGrid Services after Enabling*

Configuring pxGrid Participants

There are many different subscribers and publishers that can participate in the ecosystem with pxGrid. Each one will use the information in its own way, and the integration UI is bound to be unique per product, but the basic requirements and configuration steps will always remain the same:

Step 1. Trust the ISE certificate authority.

Step 2. Install a pxGrid certificate for its own identity.

Step 3. Configure the IP or FQDN of the pxGrid controller.

For the most part, that is all that you really need to do on each participant. Some will make things easier than others. Let's take a look at configuring some of the main pxGrid participants: Cisco Firepower Management Center, Cisco Stealthwatch, and Cisco Web Security Appliance.

Configuring Firepower Management Center for Identity with pxGrid

The Cisco Firepower Management Center (FMC) is the enterprise-class device manager and security monitoring tool for Cisco's Firepower line of NGFWs and NGIPSs, described in detail in Chapter 5, "Next-Gen Firewalls," of *Integrated Security Technologies and Solutions -Volume I*, which also covers the Firepower Device Manger (FDM) used for individual device management.

The FMC has had pxGrid integration with ISE for a while, but version 6.2 added an even better integration, with the ability to use the TrustSec data independent of user identities. The FMC can use context information provided by pxGrid, such as endpoint profiles, TrustSec tags, and both passive and active user identities.

Much like the FMC, the FDM solution is also capable of integrating with ISE using pxGrid, but this section is only focused on the FMC integration.

The Firepower Management Center leverages pxGrid to learn the context of who and what is on the network and the mapping of those devices to IP addresses. However, the FMC leverages the LDAP-based realms to learn about what users and groups exist in Active Director for the creation of access policy.

We will begin by configuring the pxGrid integration, and then follow up with the realm configuration.

Configuring Firepower Management Center for pxGrid

Before configuring pxGrid on the FMC, generate a pxGrid certificate for the FMC to use. Beginning with ISE 2.2, an administrator can download the CA's certificates and generate certificates directly from the pxGrid Services user interface.

To generate a pxGrid certificate for the FMC:

Step 1. Navigate to **Administration > pxGrid Services > Certificates**, as shown in Figure 6-13.

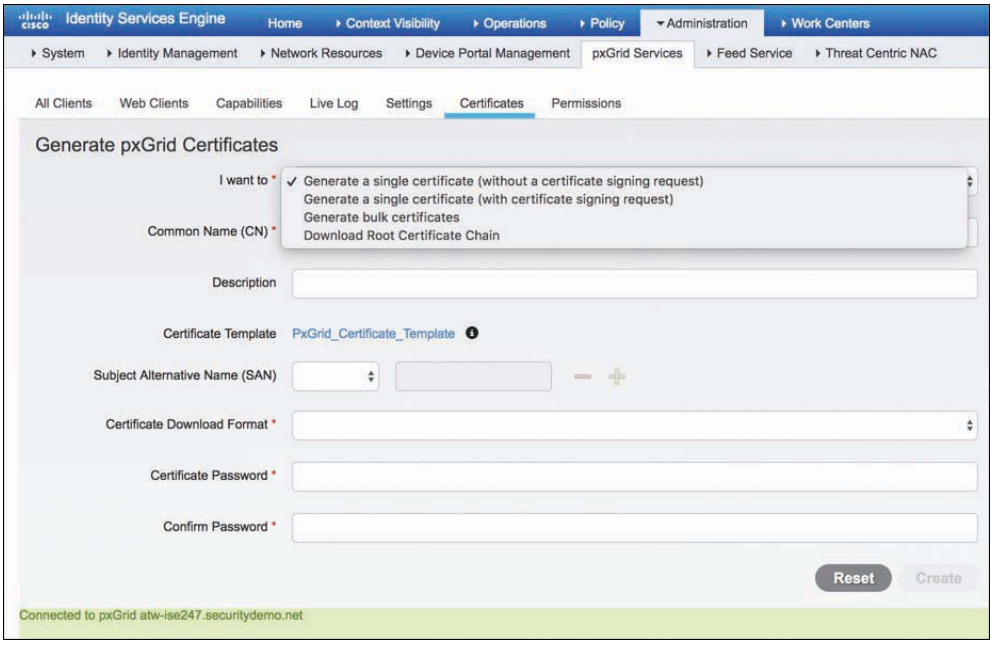

Figure 6-13 *Generating a pxGrid Certificate for the FMC*

Examining Figure 6-13, from this screen you can generate a single certificate, sign a certificate signing request (CSR), generate bulk certificates from a CSV file, or download the certificate authority chain for import into the trust store of the pxGrid participant. For the FMC, we need to generate a certificate-key pair.

Step 2. Select **Generate a single certificate (without a certificate signing request)**.

Step 3. In the Common Name (CN) field, enter a common name for the subject of your certificate.

The CN is normally the FQDN of the host (e.g., atw-fmc.securitydemo.net). However, a common practice is to add a prefix to your CN, such as *pxGrid-*, which will help you avoid installation errors that can sometimes occur when you try to install more than one certificate with the same FQDN.

Step 4. In the Subject Alternative Name (SAN) spin box, add a SAN, if needed.

If you use anything other than the true FQDN for the device, then you need to enter a SAN in this field. Per RFC 6125, anytime you use a SAN, it must also contain the CN. Add an entry for the FQDN of the host. Adding a SAN for the IP address is helpful, just in case one of the pxGrid peers is sent to the host via the IP address instead of the FQDN.

Step 5. In the Certificate Download Format spin box, choose **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format.**

All options will include the internal CA's certificates, for the entire PKI hierarchy. There is also an option to download it as a PKCS12 chain file, where the public certificate + private key + signing chain are all in a single file. For the FMC, the download format needs to be separate PEM files, not the PKCS12 chain.

Step 6. In the Certificate Password field, add a password for the private key (and then confirm it).

ISE will never issue private keys without a password to encrypt the key.

Step 7. Click **Create** and download the resulting ZIP file.

Figure 6-14 shows the completed certificate form, and Figure 6-15 shows the contents of the ZIP file.

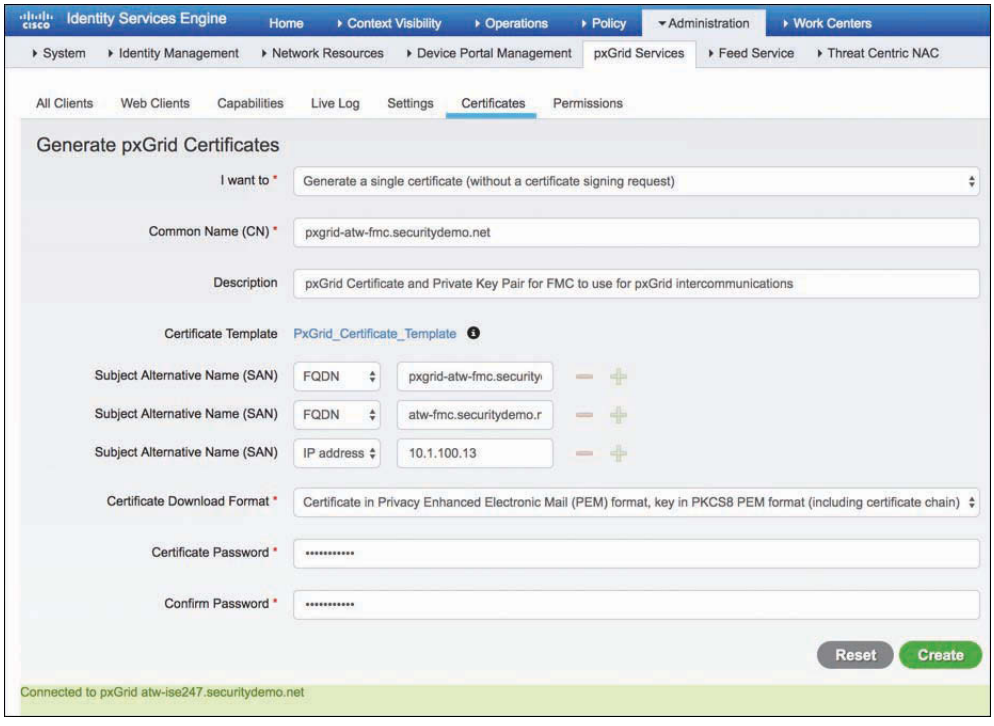

Figure 6-14 *Completed Certificate Form*

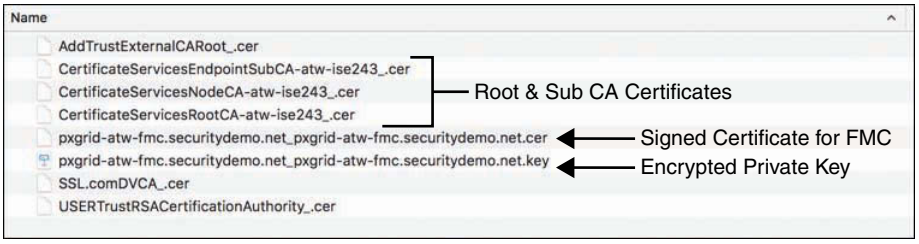

Figure 6-15 *Contents of the Resulting ZIP File*

Examining Figure 6-15, the ZIP file contains the signed certificate, the encrypted private key, and all the signing certificates in the PKI hierarchy for the issued certificate. Additionally, the signing certificates in the PKI hierarchy for the admin certificate are also included for good measure. Beginning with ISE 2.2, they should not be required, but are included in the ZIP file anyway.

Now you have all the required certificates and the private key for the FMC. To configure pxGrid on the FMC:

Step 1. Navigate to **System > Integration > Identity Sources**, as shown in Figure 6-16.

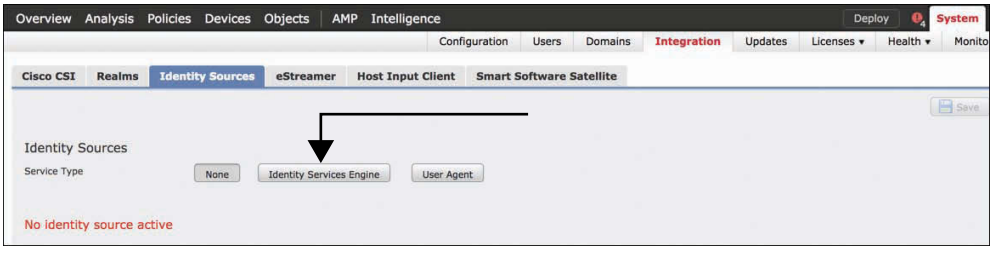

Figure 6-16 *FMC Identity Sources*

Step 2. Click the **Identity Services Engine** button.

Step 3. In the Primary Host Name/IP Address field, enter the FQDN or IP address of the primary pxGrid controller.

Step 4. If there is a secondary controller, add its FQDN or IP address in the Secondary Host Name/IP Address field.

Step 5. Click the green **+** button to the right of the pxGrid Server CA field to add the ISE root CA certificate.

This adds the root CA certificate to the list of trusted CAs in the FMC. In the Name field, give the certificate a name that makes sense to you, similar to what you see in Figure 6-17.

Step 6. Click **Browse** and select the root CA certificate from the expanded ZIP file you downloaded earlier, as shown in Figure 6-17.

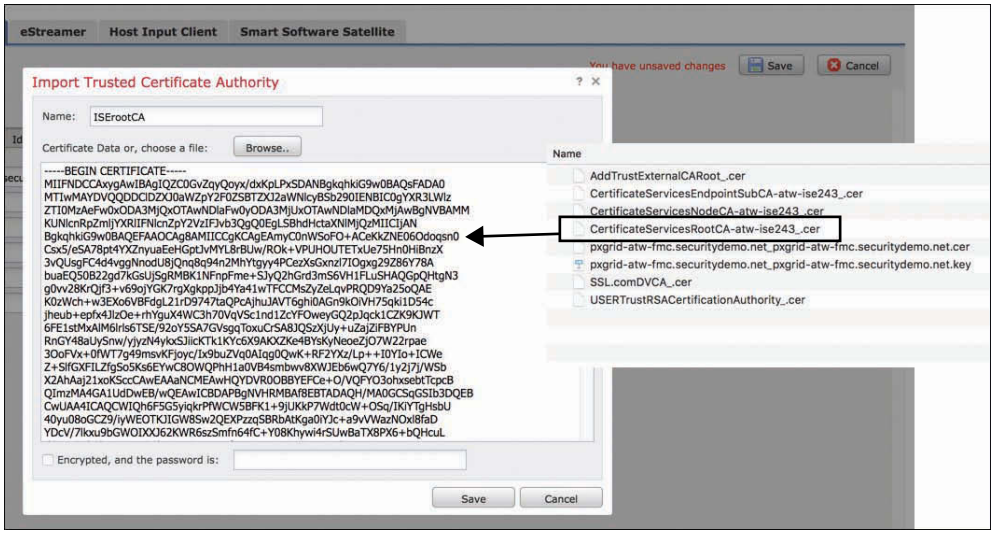

Figure 6-17 *Import Trusted Certificate Authority: ISE Root CA*

Step 7. Click **Save**.

Step 8. Ensure that the newly imported root CA certificate is listed in both the pxGrid Server CA and the MNT Server CA fields, as shown in Figure 6-19.

Note The separate MnT certificate is there just in case you are not using a single CA for all pxGrid clients, but you now know that you should always use the same CA for all participants.

Step 9. Add the signed certificate and private key for the FMC by clicking the green **+** button to the right of the FMC Server Certificate field.

This adds to the FMC the PEM-encoded certificate that was signed by ISE's endpoint CA and the encrypted private key. In the Name field, give the internal certificate a name that makes sense to you, similar to what you see in Figure 6-18.

Step 10. Click **Browse** for Certificate Data and select the PEM certificate from the expanded ZIP file you downloaded earlier, as shown in Figure 6-18.

Step 11. Click **Browse** for Key and select the PKCS8 key file from the expanded ZIP file you downloaded earlier, as shown in Figure 6-18.

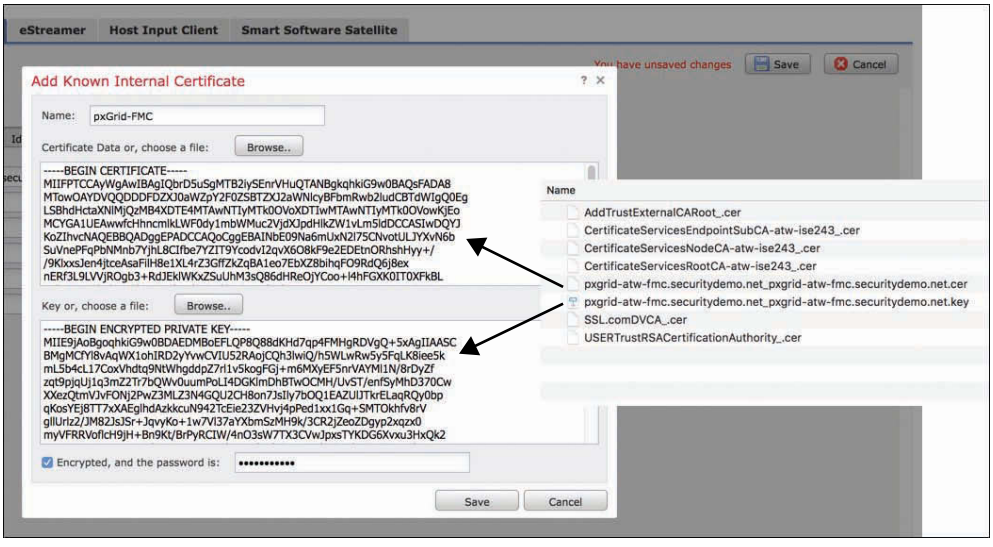

Figure 6-18 *Adding the Internal Certificate*

Step 12. Click **Save** in the upper right corner of the screen. Figure 6-19 shows the completed form.

Figure 6-19 *Completed ISE Identity Source Form*

Step 13. Click **Test** to verify a successful connection.

The test will most likely fail the first time you try unless ISE is configured to automatically approve new participants.

Step 14. In the ISE UI, navigate to **Administration > pxGrid Services > Clients**.

If ISE is not configured to auto-approve participants, you need to accept the FMC's agent and test agent.

Step 15. Check the corresponding check box for the iseagent client for the FMC, as shown in Figure 6-20, and click **Approve**.

Step 16. Check the firesightisetest client check box and click **Approve**.

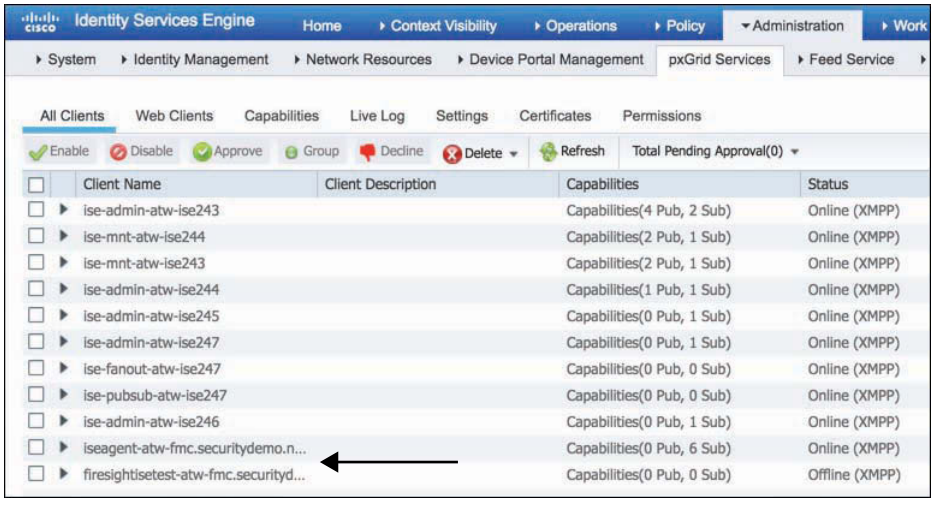

Figure 6-20 *pxGrid Clients*

Step 17. Return to the FMC UI and click **Test** to attempt the test again. This test should be successful.

Manually approving each and every pxGrid participant and their test accounts can be time consuming and somewhat confusing. Alternatively, you may enable the automatic approval of certificate-based accounts in the pxGrid Settings, as shown in Figure 6-21. Just remember to disable it again after you are finished.

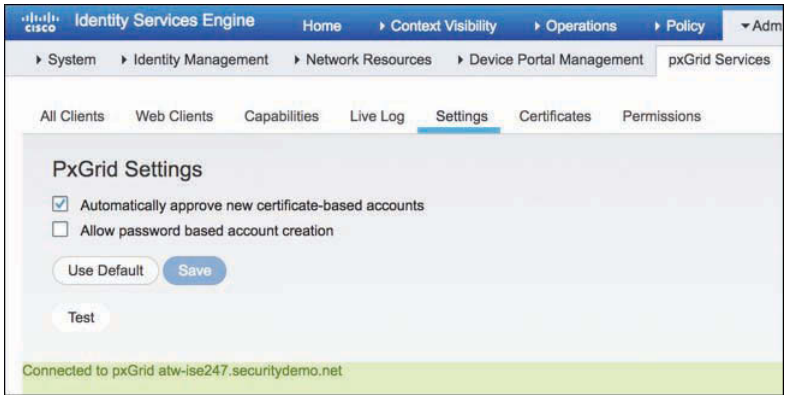

Figure 6-21 *Enabling Automatic Approval of Certificate-Based Accounts in pxGrid Settings*

Note The option in the pxGrid Settings to allow password-based account creation is an alternative to the certificate-based accounts that are shown in this chapter, where a password is leveraged instead and then tokens are assigned for authorization. At the time of writing, there are not any pxGrid client applications leveraging this account method. Also, in the Settings screen is a Test button to verify that pxGrid is working as expected within ISE. It is very useful for checking that ISE trusts its own certificates.

Configuring Realms for Identity in Access Rules

The FMC may download all the users and IP address bindings to its heart's content, but none of the data that is downloaded will be used in the policy until there is a realm configured to determine which groups and users to use in the firewall policies.

Realms leverage LDAP or LDAP/S to communicate to query the data from Active Directory. Within the FMC:

Step 1. Navigate to **System > Integration > Realms**.

Step 2. Click **New Realm**.

Step 3. Provide a name for the realm and then choose **AD** from the Type drop-down list.

Step 4. In the AD Primary Domain field, enter the IP address of the domain controller that the FMC should use to query AD.

Step 5. In the AD Join Username field, provide a UPN (user principal name) for an AD user with enough permissions to join the FMC to the domain, such as administrator@securitydemo.net (used in this example).

Step 6. In the AD Join Password field, enter the password for the AD user.

Step 7. In the Directory Username field, provide a UPN for an AD user account for performing the LDAP queries, such as administrator@securitydemo.net.

Step 8. In the Base DN field, enter the base distinguished name to begin the user account LDAP queries, such as ou=users,dc=securitydemo,dc=net.

Step 9. Enter the base DN (distinguished name) to begin the group LDAP queries, such as ou=groups,dc=securitydemo,dc=net.

Hint If you aren't getting the result you want, try backing up in the DN an extra level, such as dc=securitydemo,dc=net, which will then examine all organizational units (OUs).

Step 10. Click **OK**.

Figure 6-22 shows the completed Add New Realm form.

Figure 6-22 *Completed Add New Realm Form*

After the realm has been created, you will need to add a "directory," which is another way of saying you need to add an LDAP server to perform the queries against.

Step 1. From the Realm configuration screen, click **Add directory**.

Step 2. In the Hostname/IP Address field, enter the IP address for the AD domain controller that the FMC should use for LDAP queries.

Step 3. In the Port field, enter the port for LDAP; **389** is the default port for unencrypted LDAP.

Step 4. If you are using secure LDAP, choose the encryption method and the certificate to trust.

Step 5. Click **OK**.

Figure 6-23 shows the completed directory entry.

Figure 6-23 *Completed Directory Entry*

Now that the realm is configured along with an LDAP server, it is time to download users and groups for use in the policies:

Step 1. Click the **User Download** tab.

Step 2. Check the **Download users and groups** check box.

Step 3. Select the interesting groups from the Available Groups list and use the **Add to Include** and **Add to Exclude** buttons to assign them for inclusion for use or exclusion from use within Firepower policies, as shown in Figure 6-24.

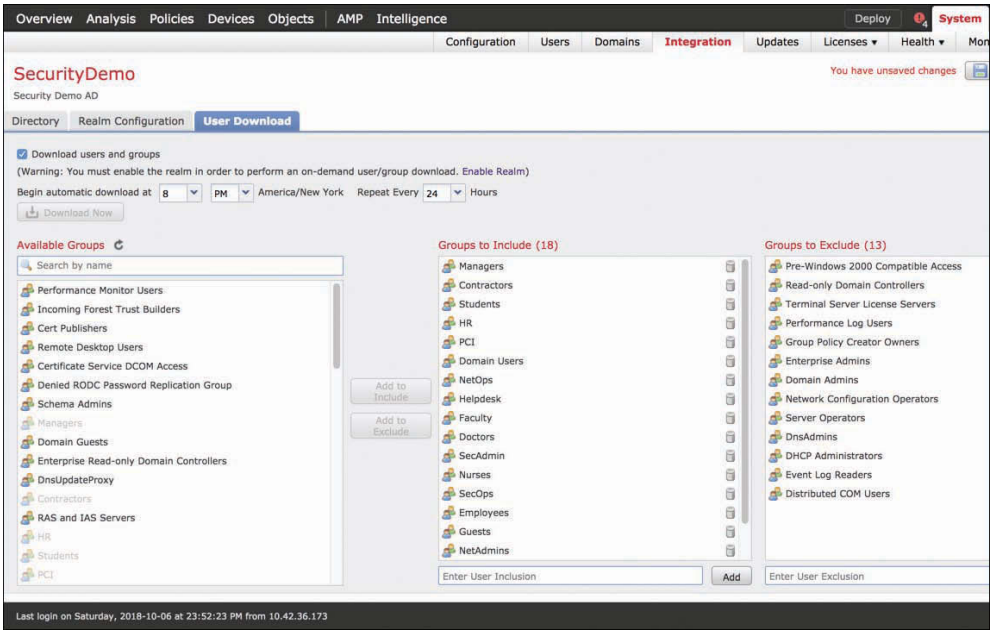

Figure 6-24 *Included and Excluded Groups*

Selective inclusion of AD groups is a key item for performance, as AD may have thousands of groups, most of which will not be relevant for identity policies in the firewalls, nor would it perform very well if all groups were candidates for identity rules.

Step 4. Click **Save**.

Step 5. **Enable** the Realm, as shown in Figure 6-25.

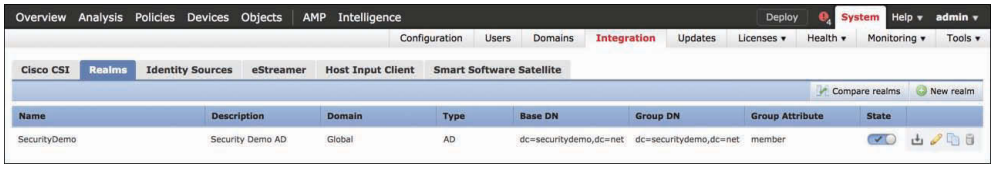

Figure 6-25 *Enabled Realm*

The realm is now fully configured for rule creation, along with the pxGrid integration for learning what IP addresses belong to which users and devices. Now you are ready to add identity information to the access policy rules in the FMC.

Configuring Firepower Access Rules with Context from pxGrid

Before you can add user identities or groups to the access-policy rule, you must first create an identity rule:

Step 1. Navigate to **Policies > Access Control > Identity**.

Step 2. Click **New Policy**.

Step 3. In the New Identity policy dialog box, shown in Figure 6-26, enter a name and, optionally, a description.

Step 4. Click **Save**.

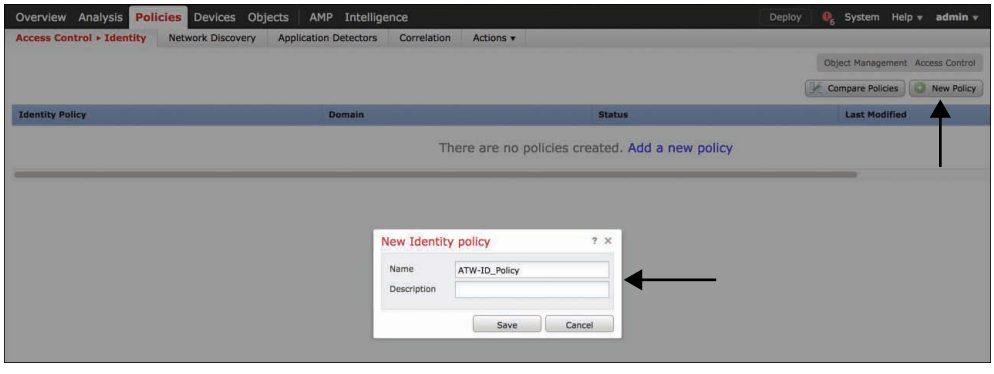

Figure 6-26 *Creating a New Identity Policy*

Step 5. Click **Add Rule** to configure an identity rule.

Step 6. In the Name field, enter a name.

Step 7. Keep the Enabled check box checked.

Step 8. In the Action drop-down list, select **Passive Authentication**.

Step 9. Click the **Realm & Settings** tab.

Step 10. From the Realm drop-down list, select your AD realm.

Step 11. Click **Add**.

Figure 6-27 shows the new rule being added to the identity policy.

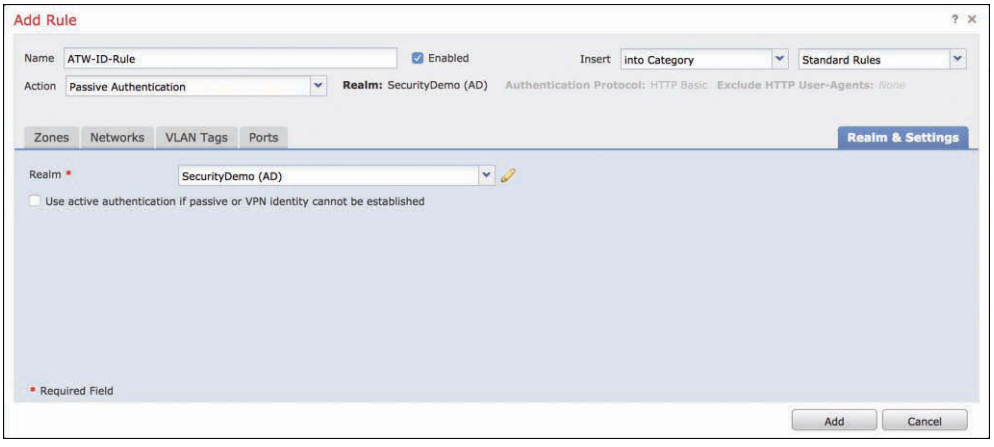

Figure 6-27 *Adding the Identity Rule to the Identity Policy*

Now that an identity policy has been created, you can attach it to the access policy.

Step 12. Navigate to **Access Policy > Access Policy**.

Step 13. Click the link in Identity Policy field.

Step 14. In the Identity Policy dialog box, choose your identity policy from the drop-down list.

Step 15. Click **OK**.

Figure 6-28 shows the identity policy being selected in the access policy.

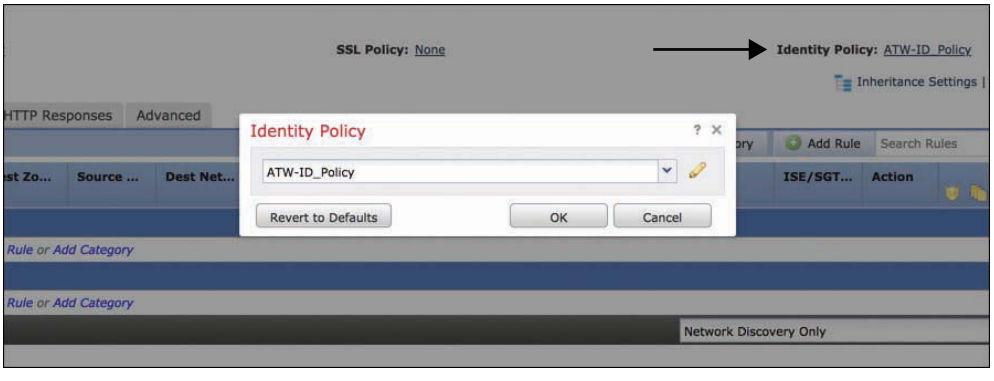

Figure 6-28 *Selecting the Identity Policy in the Access Policy*

Now that an identity policy has been attached to the access policy, you can add identities to the access rule.

Step 16. Navigate to **Access Policy > Access Policy**.

Step 17. Either click **Add Policy** to create a new policy or click **Edit** to add an existing policy.

Step 18. Click the **Users** tab.

Step 19. In the Available Realms column, select the realm you created.

Step 20. In the Available Users column, select the groups or users to match in this access rule.

Step 21. Click **Add to Rule** to transfer them to the Selected Users column.

Figure 6-29 shows the user group Employees being added to the access rule.

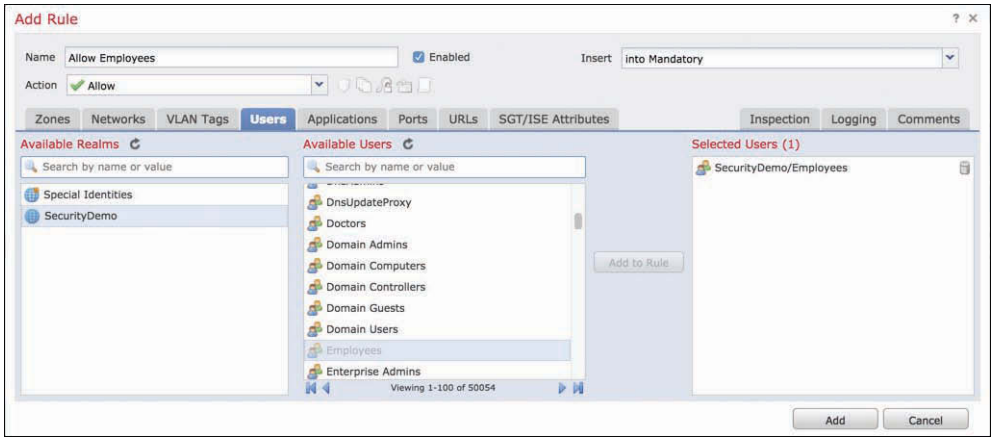

Figure 6-29 *Adding AD Groups to an Access Policy Rule*

Because we have integrated Firepower Management Center with ISE, we also have access to other bits of contextual data to build our policy on, such as endpoint profiles and TrustSec tags (also known as Scalable Group Tags or Security Group Tags).

Step 22. Click the **SGT/ISE Attributes** tab.

Step 23. In the Available Attributes column, select **Security Group Tag**.

Step 24. In the Available Metadata column, select one of the SGTs from ISE and click **Add to Rule**.

Figure 6-30 shows the SGT named Employees being added to the access rule.

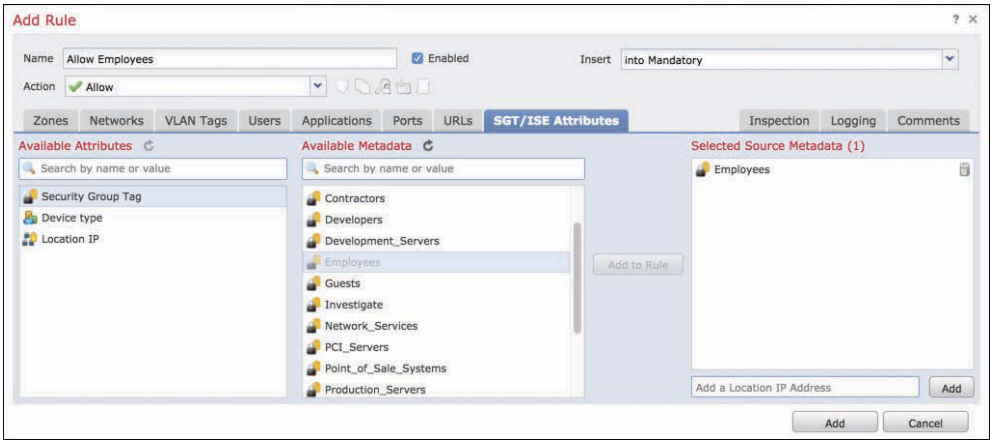

Figure 6-30 *Adding SGTs to an Access Policy Rule*

Step 25. In the Available Attributes column, select **Device Type**.

Step 26. In the Available Metadata column, select the endpoint profiles and click **Add to Rule** to add them to the policy.

Step 27. Click **Add** to save the access policy rule to the policy.

Step 28. Click **Save** to save the policy.

Figure 6-31 shows device type groups being added to the access rule.

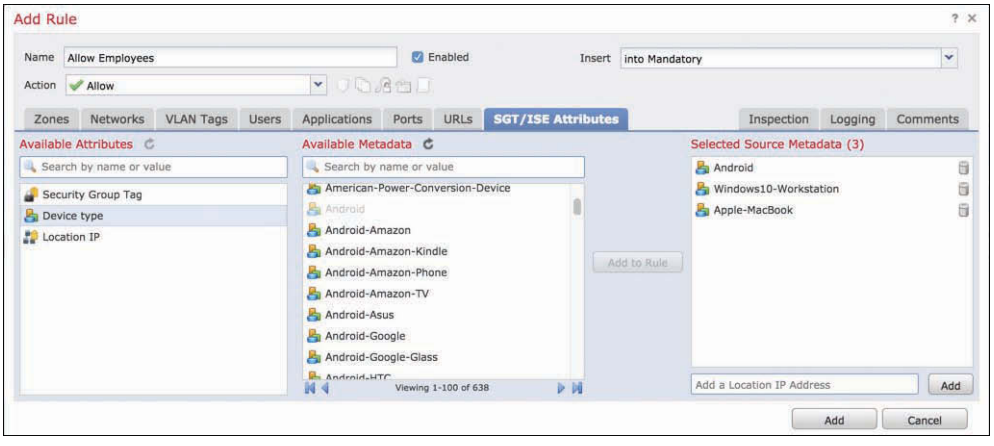

Figure 6-31 *Adding Endpoint Profiles to an Access Policy Rule*

Viewing Active Users

You've completed all the configuration steps for the identity integration with the FMC and ISE, but how do you know that the FMC is learning about the active and passive online users and devices?

Navigate to **Analysis > Users > Active Sessions** and you should start seeing domain logons, such as what you see in Figure 6-32.

Figure 6-32 shows the online users that ISE has learned about through either active or passive identity mappings. See Chapter 3, "Beyond Basic Network Access Control," for more on active versus passive identities.

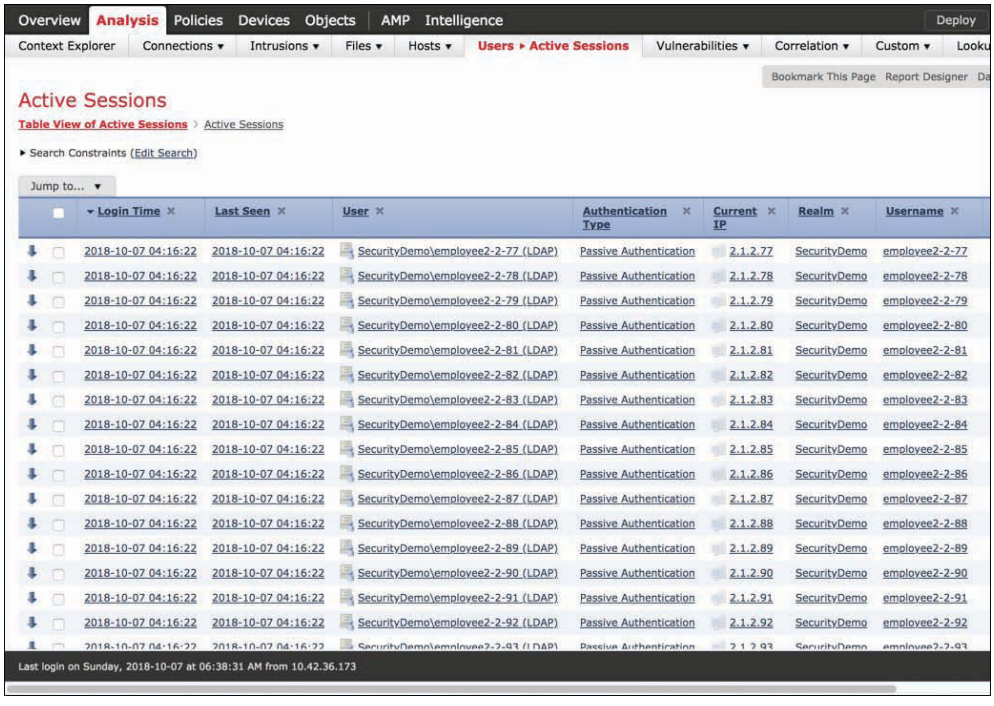

Figure 6-32 *Online Users Learned from ISE*

For the CLI-oriented CCIE or CCIE candidate, there is also a great way to see the user identities from the command line, **adi_cli session**, as shown in Example 6-1.

Example 6-1 *Viewing Online Users from the FMC CLI*

```
admin@atw-fmc:~$ sudo adi_cli session | more
input 'q' to quit
received realm information: operation REALM_DELETE_ALL, Null realm info
received realm information: operation REALM_ADD, realm name securitydemo.net, sh
ort name SECURITYDEMO, id 3
ADI is connected
received security group operation: DELETE ALL
received security group operation: ADD id: 92bb1950-8c01-11e6-996c-525400b48521
name: ANY fullyQualifiedName: Any Security Group tag: 65535
received security group operation: ADD id: 934557f0-8c01-11e6-996c-525400b48521
name: Auditors fullyQualifiedName: Auditor Security Group tag: 9
received security group operation: ADD id: 935d4cc0-8c01-11e6-996c-525400b48521
name: BYOD fullyQualifiedName: BYOD Security Group tag: 15
received security group operation: ADD id: 9370d4c0-8c01-11e6-996c-525400b48521
name: Contractors fullyQualifiedName: Contractor Security Group tag: 5
received security group operation: ADD id: 93837260-8c01-11e6-996c-525400b48521
name: Developers fullyQualifiedName: Developer Security Group tag: 8
received security group operation: ADD id: 9396d350-8c01-11e6-996c-525400b48521
```

Configuring Rapid Threat Containment with Firepower and ISE

Learning about the online users and endpoints is only one of the use cases when integrating the FMC with ISE. Another common use case of the integration is to act when a malicious activity has occurred, as you learned about in the "Rapid Threat Containment" section earlier in this chapter.

Figure 6-33 illustrates how the FMC works with correlation rules and remediation modules, to aid your understanding of how all the pieces fit together.

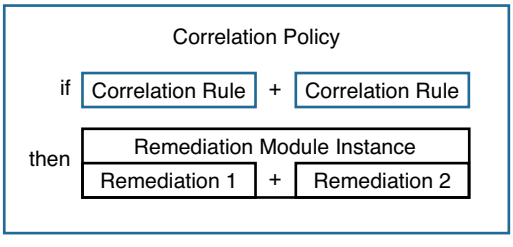

Figure 6-33 *Illustration of Correlation Policies and Components*

The parts that make up the response are as follows:

- **Correlation policy:** The policy construct that is made up of correlation rules and configured remediations.

- **Correlation rule:** An individual rule housed inside of a correlation policy that is configured to look for one or more security events. There can be one or many correlation rules in each correlation policy.
- **Remediation module:** Modules of the FMC that understand how to communicate to an external system; for example, the pxGrid module knows how to use EPS on ISE to quarantine endpoints.
- **Remediation instance:** A specific instance of a remediation module, as there can be many instances, each with a different configuration.
- **Remediation:** A specific action that is configured, such as quarantine. There can be many remediations in each instance of the remediation module.

The pxGrid mitigation module is built into the FMC, and that module can be used to take an EPS quarantine action when a correlation rule is triggered. Let's start by configuring the built-in pxGrid mitigation module:

Note If you are following along only in the book, the following steps may seem a little strange. However, if you are following along with a live Firepower Management Center user interface, these steps will seem much more clear.

Step 1. Navigate to **Policies > Actions > Remediation > Modules**, which brings you to the Installed Remediation Modules screen, as shown in Figure 6-34.

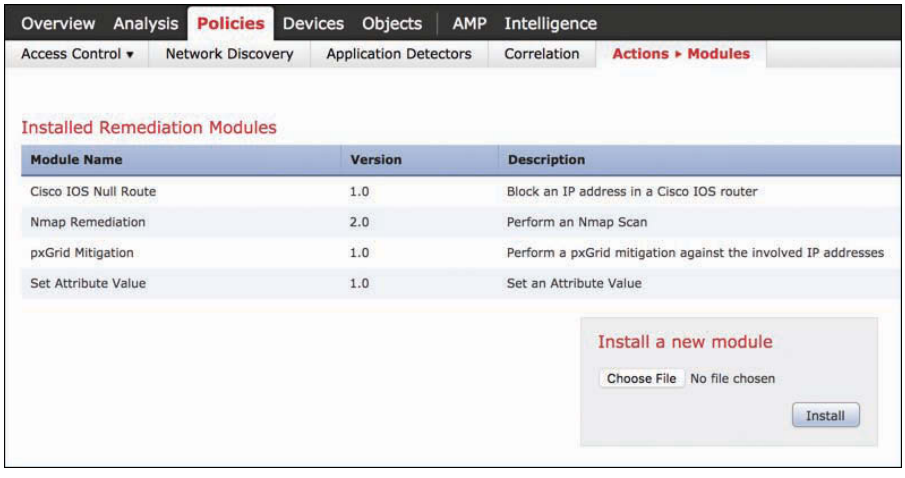

Figure 6-34 *Remediation Modules*

Step 2. Click the **magnifying glass icon** (not shown in Figure 6-34) at the right end of the pxGrid Mitigation module row.

Step 3. Click **Add** to create a new instance of the module.

Step 4. Provide a name for the instance and an optional description, as shown in Figure 6-35.

Step 5. Click **Create**.

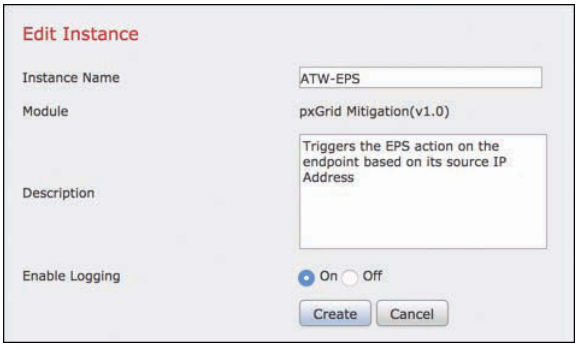

Figure 6-35 *Creating a New Instance of the pxGrid Mitigation Module*

Step 6. Choose **Mitigate Source** in the Configured Remediations drop-down list, as shown in Figure 6-36.

Step 7. Click **Create**.

Figure 6-36 *Select Mitigate Source*

After clicking Create, you are brought automatically to the window where you create a remediation action for the module.

Step 8. Provide a name for the remediation and an optional description, as shown in Figure 6-37.

Step 9. Set the Mitigation Action to **quarantine**, as shown in Figure 6-36.

Step 10. Click **Create**.

Step 11. Click **Save**.

Step 12. Click **Done**.

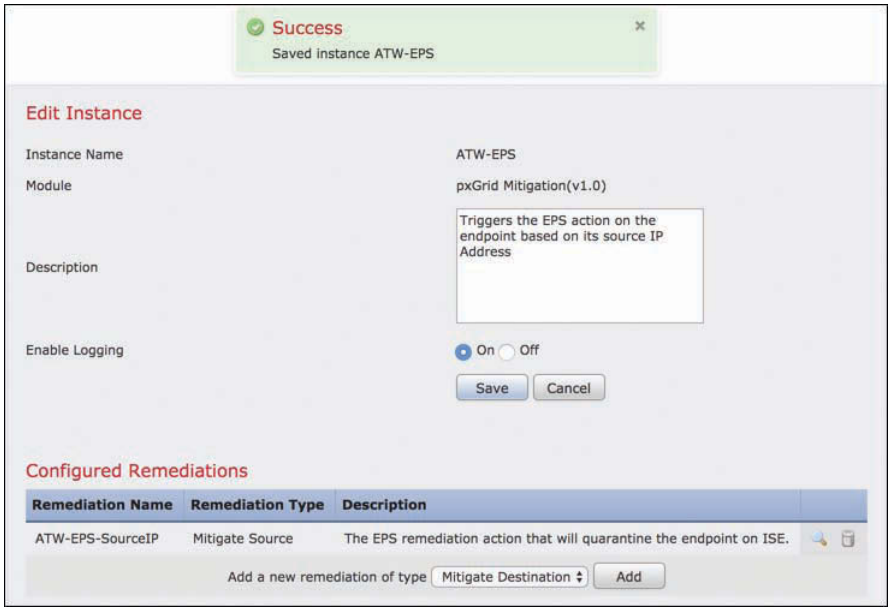

Figure 6-37 *Creating the Remediation*

Step 13. Click **Save** to save the module instance.

Figure 6-38 shows the completed instance of the pxGrid mitigation module.

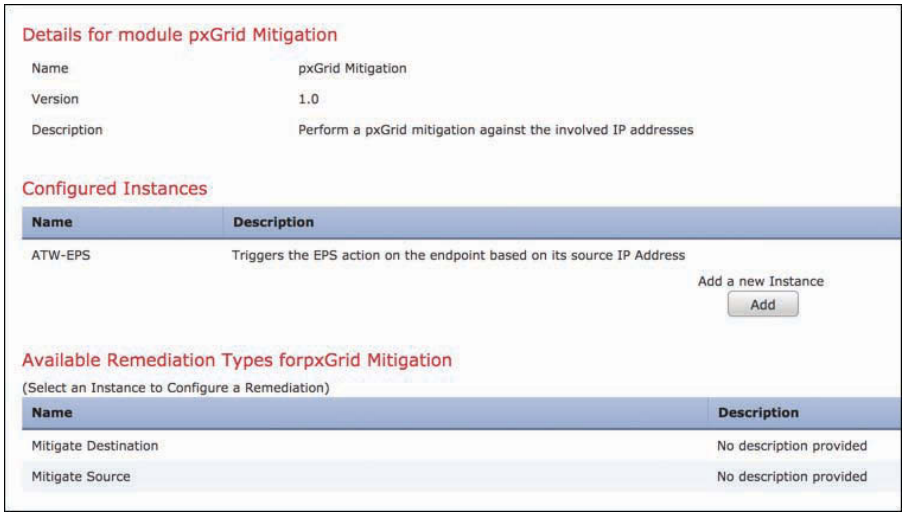

Figure 6-38 *Completed pxGrid Mitigation Module*

The remediation module is ready for use, so now we need to create a correlation rule that will use the remediation module whenever that correlation rule is matched.

Step 14. Navigate to **Policies > Correlation > Rule Management**.

Step 15. Click **Create Rule**.

Figure 6-39 shows a completed correlation rule that looks for an AMP for endpoints event where a cloud recalled file is unable to be quarantined.

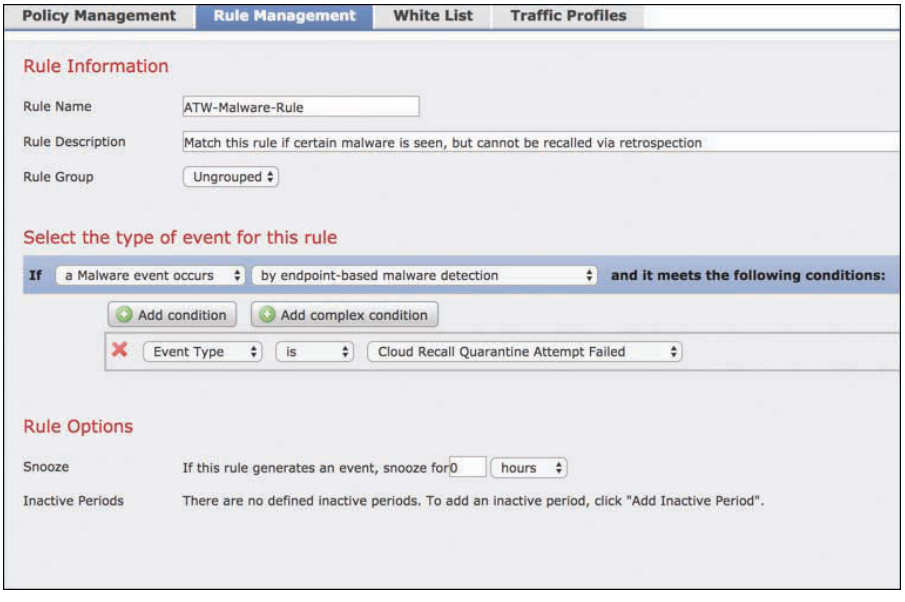

Figure 6-39 *Completed Correlation Rule*

Now that rule exists, we can add it to the correlation policy.

Step 16. Navigate to **Policies > Correlation > Policy Management**.

Step 17. Click **Create Policy**.

Step 18. Provide a policy name and an optional description in the corresponding fields.

Step 19. Click **Add Rules**.

Step 20. Select the correlation rule you created.

Figure 6-40 shows a correlation policy, with the correlation rule added; however, there is no remediation action configured yet.

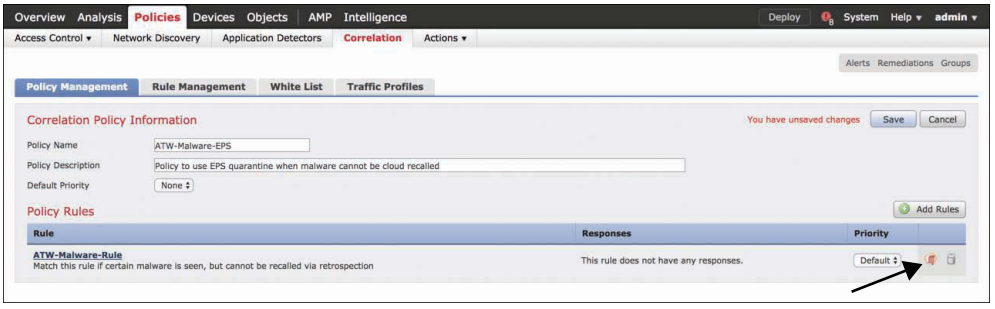

Figure 6-40 *Correlation Policy without a Remediation Action*

Let's add that remediation action.

Step 21. Click the response icon, pointed to in Figure 6-40.

Step 22. Assign the remediation action you created, as shown in Figure 6-41.

Step 23. Click **Update**.

Figure 6-41 *Assigning the Remediation Action*

Step 24. Click **Save**.

Step 25. Enable the policy, as shown in Figure 6-42.

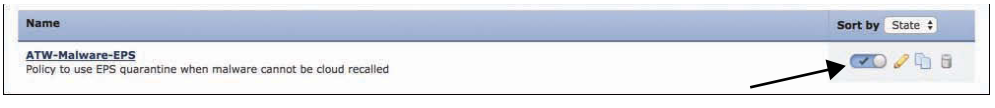

Figure 6-42 *Final Policy, Enabled*

Configuring the Web Security Appliance for Identity with pxGrid

The Cisco Web Security Appliance (WSA) was one of the first pxGrid partner applications in the security ecosystem. The WSA may use pxGrid to ascertain both passive and active user identities, as well as TrustSec tags; however, at the time of writing, the WSA (version 11.5.1) is unable to combine Active Directory group membership with the identity information gathered from pxGrid, which means that TrustSec tagging is realistically the only scalable approach when using pxGrid.

Integrating the WSA and ISE with pxGrid

All pxGrid participants should be using certificates that are issued from the ISE internal CA. This is not a requirement, but it is certainly a best practice to ensure things always work optimally. So, before you continue to the following steps, create a certificate private-key pair, just like you did for the FMC in the "Configuring Firepower Management Center for pxGrid" section earlier in the chapter.

To configure pxGrid on the WSA, we will first add the ISE root certificates to the trusted certificate store:

Step 1. Navigate to **Network > Certificate Management**.

Step 2. Click **Manage Trusted Root Certificates**, as indicated in Figure 6-43.

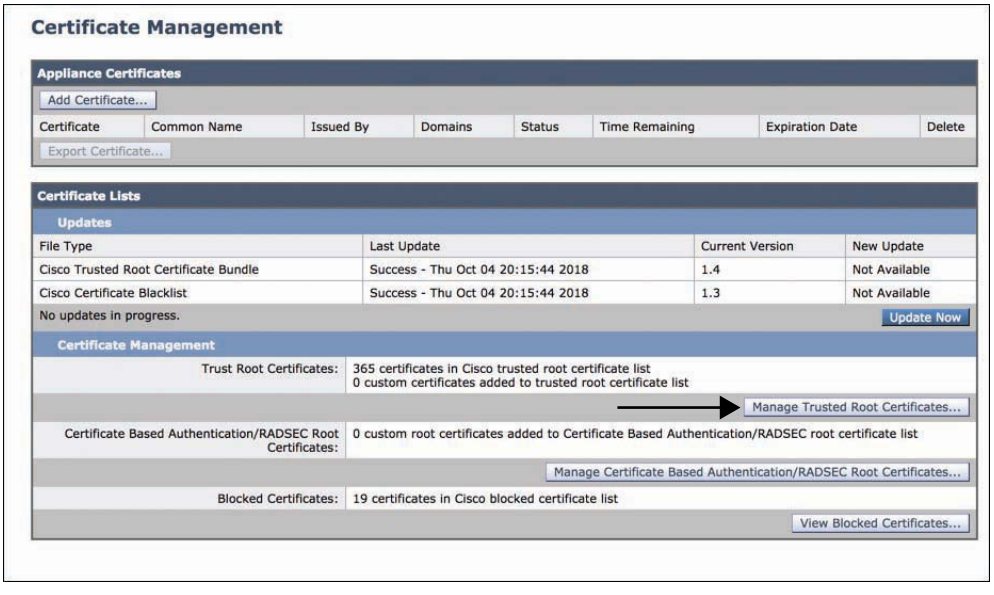

Figure 6-43 *Network > Certificate Management*

Step 3. Click **Import**, as shown at the top of Figure 6-44.

Step 4. Browse for each of the ISE CA certificates (Root, Node, and Endpoint) and click **Submit**, one at a time.

Step 5. When all of the signing certificates are uploaded, click **Submit**, as indicated in Figure 6-44.

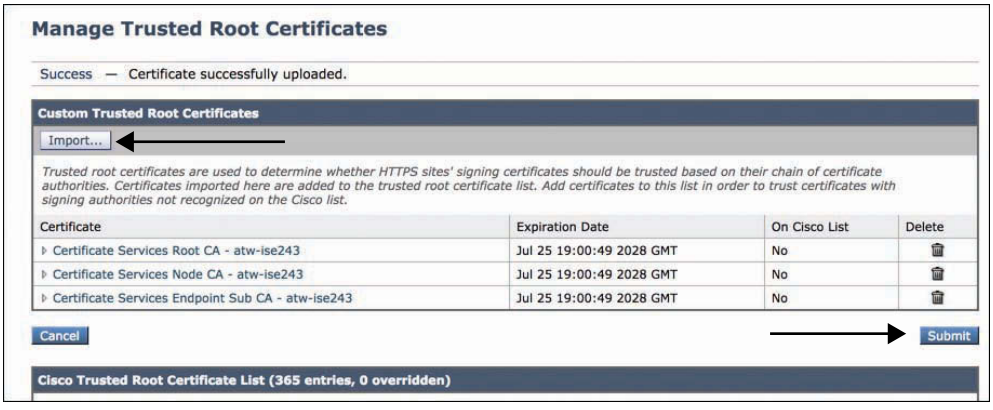

Figure 6-44 *Manage Trusted Root Certificates*

Step 6. Click **Commit Changes** to save the WSA configuration.

Now that the ISE root certificates will be trusted, it is time to configure the WSA for pxGrid:

Step 1. Navigate to **Network > Identification Services > Identity Services Engine**.

Step 2. Click **Enable and Edit Settings**, as shown in Figure 6-45.

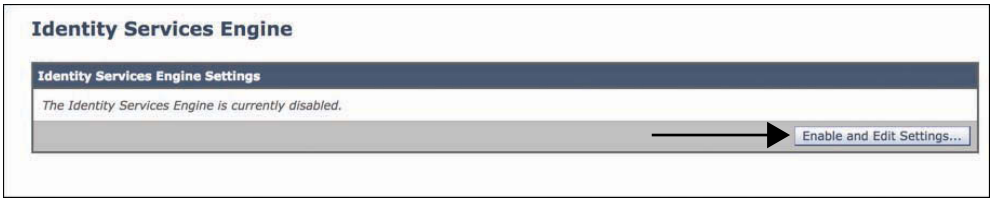

Figure 6-45 *Identification Servers > Identity Services Engine*

In the Primary ISE pxGrid Node section:

Step 3. In the Hostname or IPv4 address field, enter the FQDN for the primary pxGrid controller.

Step 4. Click **Choose File** and select the ISE root CA certificate.

Step 5. Click **Upload File**.

Figure 6-46 shows the completed Primary ISE pxGrid Node section.

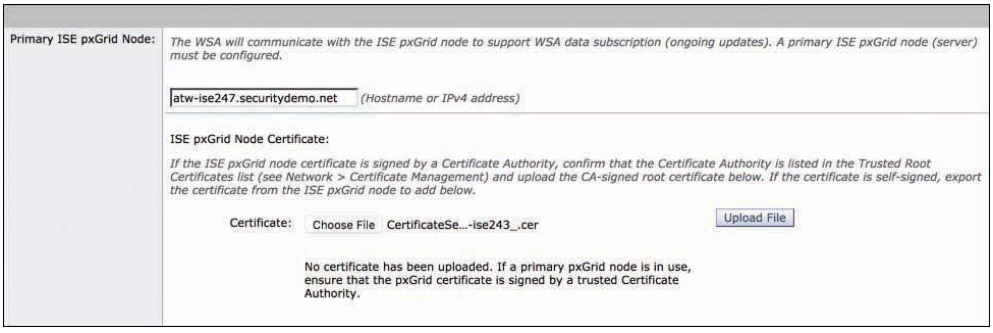

Figure 6-46 *Primary ISE pxGrid Node*

Step 6. In the ISE Monitoring Node Admin Certificates section, click **Upload File** and upload the ISE root CA certificate for both the Primary and Secondary ISE Monitoring nodes.

Figure 6-47 shows the completed ISE Monitoring Node Admin Certificates section.

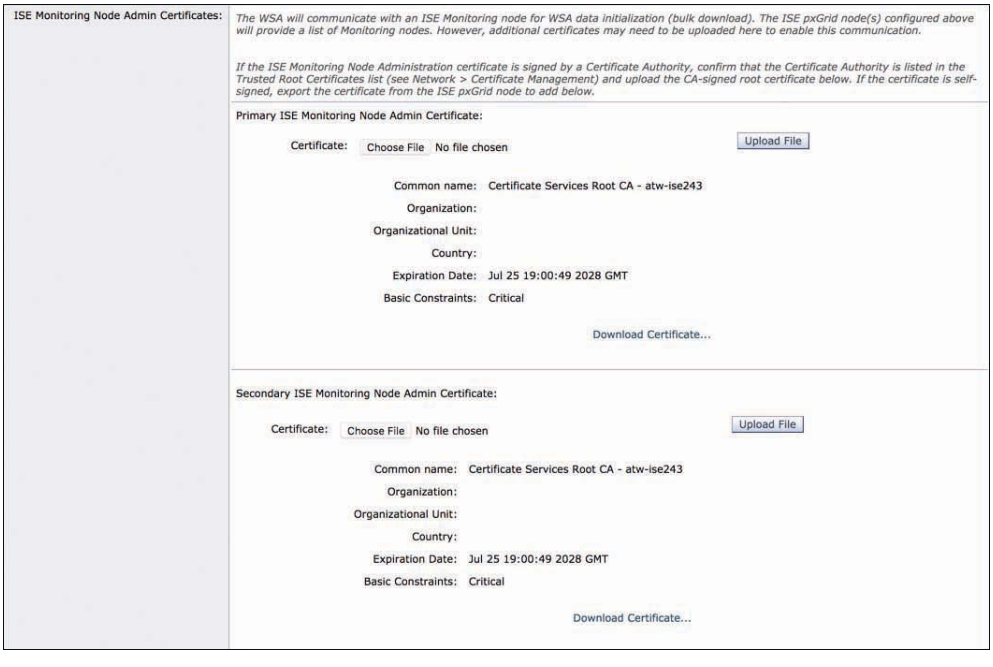

Figure 6-47 *ISE Monitoring Node Admin Certificates*

In the WSA Client Certificate Section:

Step 7. Click **Use Uploaded Certificate and Key**.

Step 8. Click **Choose File** in the Certificate field and select the WSA's certificate from the ISE CA.

Step 9. Click **Choose File** in the Key field and select the WSA's private key from the ISE CA.

Step 10. Check the **Key is Encrypted** check box.

Step 11. In the Password field, enter the password that you used to encrypt the key.

Step 12. Click **Upload Files**.

Figure 6-48 shows the WSA certificate and key selected and ready for upload.

Figure 6-48 *WSA Client Certificate Section*

Step 13. Click **Submit** to complete the configuration.

Step 14. Click **Commit Changes** twice.

Step 15. To test the connection, click **Edit Settings**.

Step 16. Click **Start Test** at the bottom of the screen, as shown in Figure 6-49. If auto-approval is enabled, then the test should be successful. If it is not enabled, the test will fail until you manually approve the two WSA accounts on the pxGrid controller.

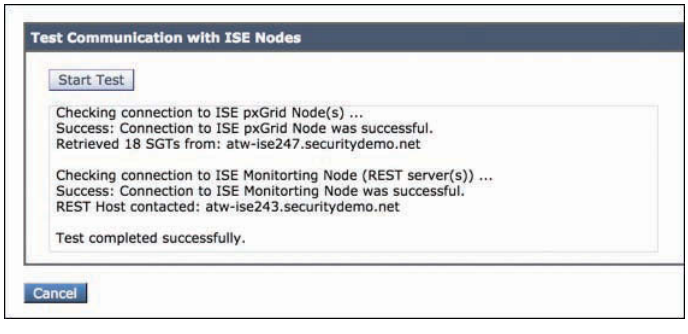

Figure 6-49 *Test Communication with ISE Nodes*

Example 6-2 shows an example of the test output.

Example 6-2 *Example Output for Testing Communication with ISE Nodes*

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved 'atw-ise247.securitydemo.net' address: 10.1.100.247

Validating WSA client certificate ...
Success: Certificate validation successful

Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful

Validating ISE Monitorting Node Admin certificate(s) ...
Success: Certificate validation successful

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 18 SGTs from: atw-ise247.securitydemo.net

Checking connection to ISE Monitorting Node (REST server(s)) ...
Success: Connection to ISE Monitorting Node was successful.
REST Host contacted: atw-ise243.securitydemo.net

Test completed successfully.
```

Configuring WSA Policies That Leverage the Data from ISE

Now that you have configured the WSA to work with ISE and to subscribe to the interesting pxGrid topics, it is time to configure policies. The first step is to create an identification profile:

Step 1. Navigate to **Web Security Manager > Identification Profiles**.

Step 2. Click **Add Identification Profile**.

Step 3. In the Name field, provide a name for the profile.

Step 4. In the User Identification Method section, in the Identification and Authentication spin box, select **Transparently identify users with ISE**.

Step 5. Click **Submit**.

Step 6. Click **Commit Changes** to save the WSA configuration.

Figure 6-50 shows the completed identification profile.

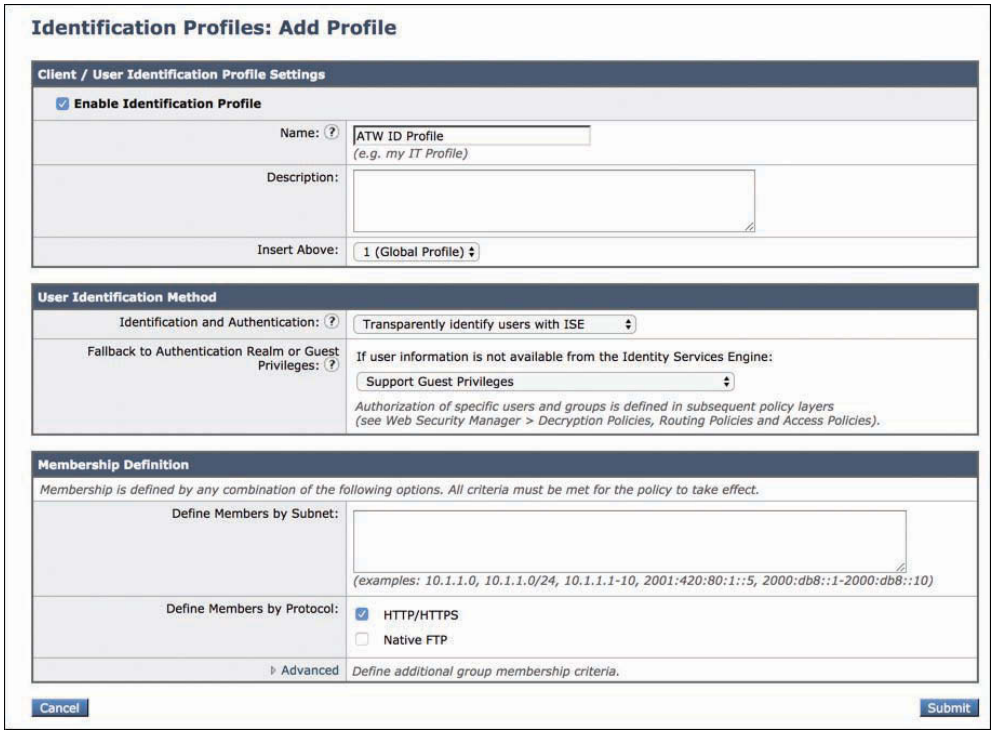

Figure 6-50 *Identification Profile*

To add an access policy leveraging security group tags from ISE:

Step 7. Navigate to **Web Security Manager > Access Policies**.

Step 8. Click **Add Policy**.

Step 9. In the Policy Name field, provide a name for the policy, as shown in Figure 6-51.

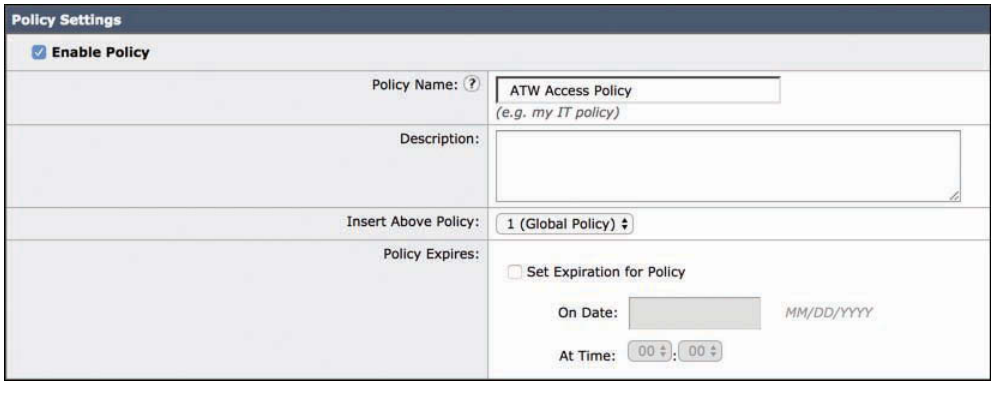

Figure 6-51 *Naming the Access Policy*

Step 10. In the Identification Profiles and Users section, choose **Select One or More Identification Profiles** in the top spin box.

Step 11. In the Identification Profile column, choose the configured ID profile in the spin box.

Step 12. In the Authorized Users and Groups column, click the **Selected Groups and Users** radio button.

Step 13. Select SGTs in the ISE Secure Group Tags area directly below the radio button.

Step 14. Click **Submit**.

Figure 6-52 shows the completed access policy that will apply to all users with the Employees SGT assigned.

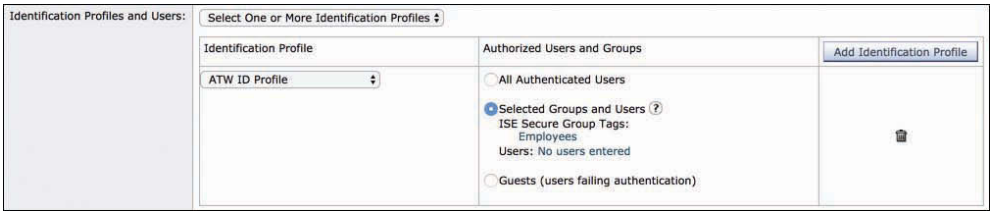

Figure 6-52 *Access Policy with Employees SGT*

To add a decryption policy that will decrypt SSL traffic from users with a specific SGT:

Step 15. Navigate to **Web Security Manager > Decryption Policies**.

Step 16. Click **Add Policy**.

Step 17. In the Policy Name field, provide a name for the policy.

Step 18. In the Identification Profiles and Users section, choose **Select One or More Identification Profiles** in the top spin box.

Step 19. In the Identification Profile column, choose the configured ID profile in the spin box.

Step 20. In the Authorized Users and Groups column, click the **Selected Groups and Users** radio button.

Step 21. Select SGTs in the ISE Secure Group Tags area directly below the radio button.

Step 22. Click **Submit**.

Figure 6-53 shows the completed access policy that will apply to all users with the Investigate SGT assigned.

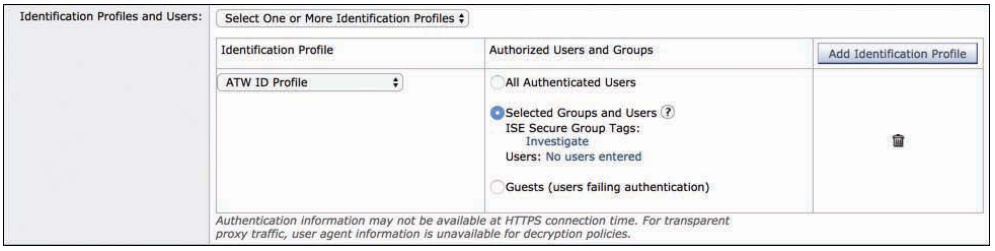

Figure 6-53 *Decryption Policy*

Integrating Stealthwatch and ISE for Identity and Rapid Threat Containment with pxGrid

For years, Cisco had a proven solution known as Cyber Threat Defense (CTD), the main components of which were Cisco ISE and a product called StealthWatch from Lancope. Lancope was acquired by Cisco in December of 2016, and Cisco proceeded to rebrand the product Cisco Stealthwatch. That's right, folks. Please don't capitalize that W, as Cisco branding would not be happy.

Regardless of what the product is called, what remains 100 percent true is that Stealthwatch is phenomenal at security analytics and visibility. It works primarily by analyzing NetFlow records from the network and providing analytics around the traffic, hosts, and other telemetry used to decorate the flows.

Why Integrate Stealthwatch and ISE?

Flow analysis itself is incredibly useful for pre- and post-attack analytics. Figure 6-54 shows a basic host report for a client PC in Stealthwatch before integrating it to ISE. This report is just a small taste of what Stealthwatch is able to provide to your security organization and security operations center (SOC) for incident response and alerting.

Beginning with version 6.9, Cisco Stealthwatch uses ISE as the primary source for learning passive and active user identities to merge into the flow records used for security analytics. The mechanisms used are exactly the same, whether it is full ISE or the ISE Passive Identity Connector (ISE-PIC), which provides only passive identities (see Chapter 3, "Beyond Basic Network Access Control," for more information on ISE and passive identity).

Just as with the WSA, the context provided to Stealthwatch can be much richer with full ISE and therefore provide more value by adding endpoint profiles and TrustSec data.

After integrating ISE, the flows will contain much more context about the hosts, including the logged-in user data. Figure 6-55 shows the populated Users & Sessions table after ISE integration.

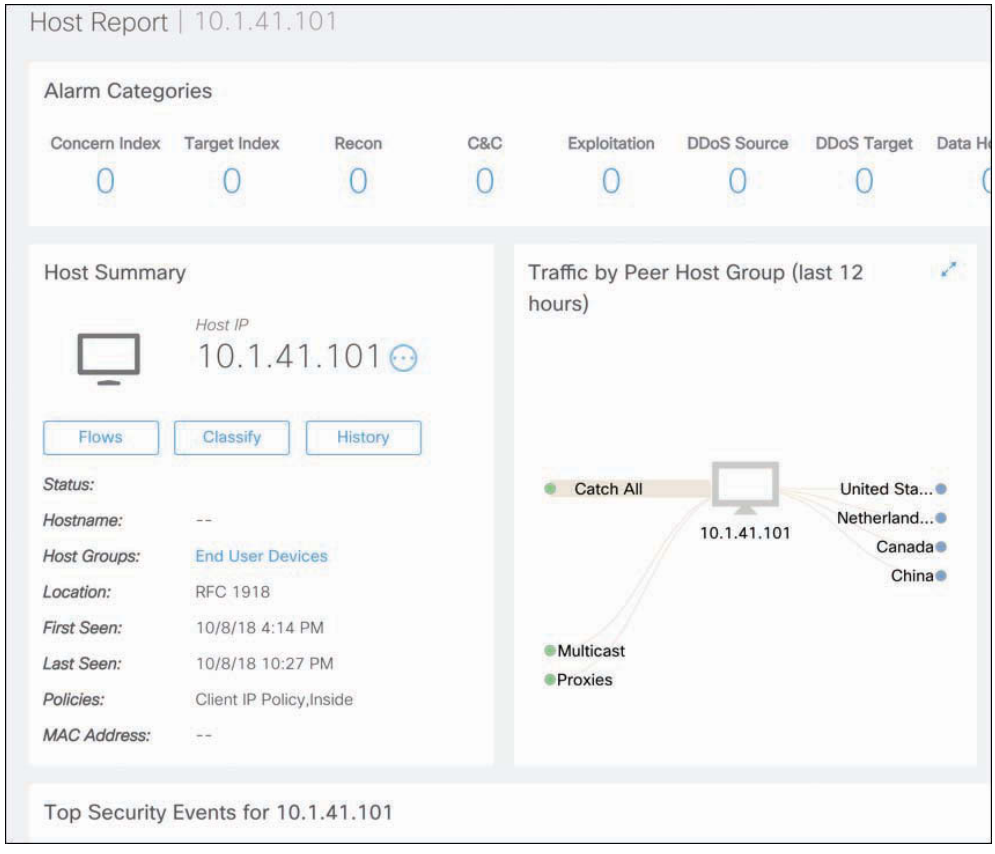

Figure 6-54 *Host Report—Pre-ISE Integration*

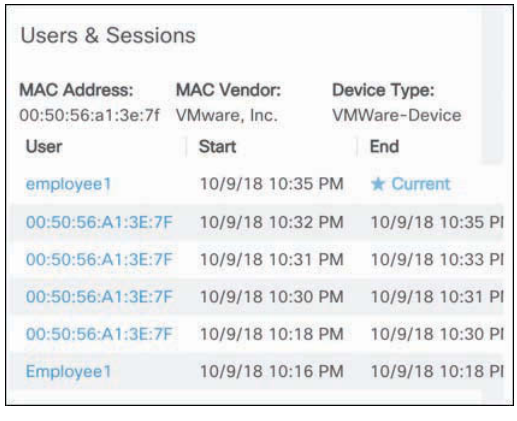

Figure 6-55 *Host Report—Post ISE-Integration*

Preparing Stealthwatch for pxGrid

To start configuring Stealthwatch for pxGrid, we will generate an "Additional TLS Identity" for the Stealthwatch Management Center (SMC); which is to say we will get a pxGrid certificate from ISE and install it on the SMC.

Unlike the FMC and the WSA, Stealthwatch uses the PKCS12 chain files instead of individual certificates. In other words, it requires the private key, signed certificate, and all the signing root certificates in a single encrypted file.

Note All steps in this book are for Cisco Stealthwatch version 7.0. To see the integration with version 6.x, check out *Cisco ISE for BYOD and Secure Unified Access, Second Edition* (Cisco Press, 2017).

Step 1. Click the **settings** cog in the upper-right corner and select **Central Management**, as shown in Figure 6-56.

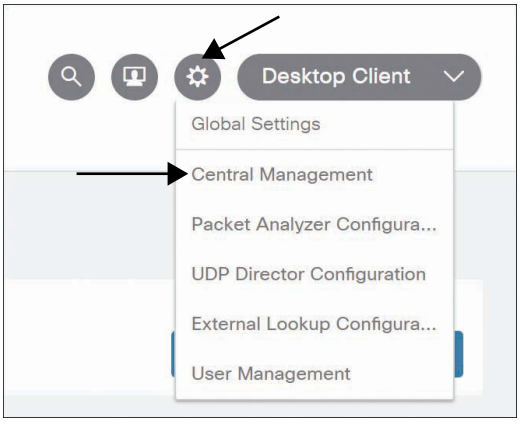

Figure 6-56 *Settings > Central Management*

Step 2. The Stealthwatch Central Management tab or window will open.

Step 3. In the Actions column, click the circle icon next to your Stealthwatch Management Center and click **Edit Appliance Configuration**, as shown in Figure 6-57.

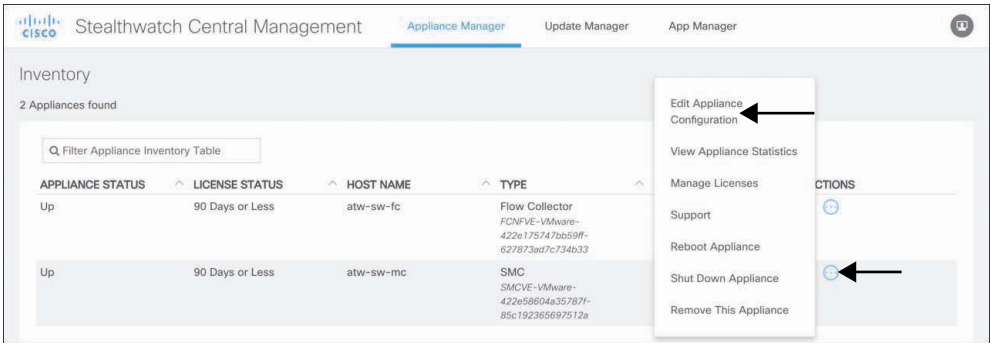

Figure 6-57 *Choosing to Edit the Appliance Configuration*

Step 4. Scroll down to the section titled Additional SSL/TLS Client Identities.

Step 5. Click **Add New**.

Step 6. Click **Generate CSR**.

Step 7. In the Generate a CSR section, fill out the fields for the certificate signing request, as shown in Figure 6-58.

Step 8. Click **Generate CSR**, as indicated in Figure 6-58.

Figure 6-58 *Generating the CSR*

Step 9. Save the resulting CSR file to a location where you can easily retrieve it.

Step 10. Open the CSR in your favorite text editor.

Step 11. Copy the contents of the CSR to your clipboard.

In the ISE user interface:

Step 12. Navigate to **Administration > pxGrid Services > Certificates**.

Step 13. In the *I want to* spin box, select **Generate a single certificate (with certificate signing request).**

Step 14. In the Certificate Download format spin box, choose **PKCS12 format (including certificate chain; one file for both the certificate chain and key).**

Step 15. Enter and confirm a certificate password for the encrypted resulting file.

Step 16. Click **Create**.

Step 17. Save the resulting p12 file to a location where you can easily retrieve it.

Figure 6-59 shows the completed certificate generation screen in ISE.

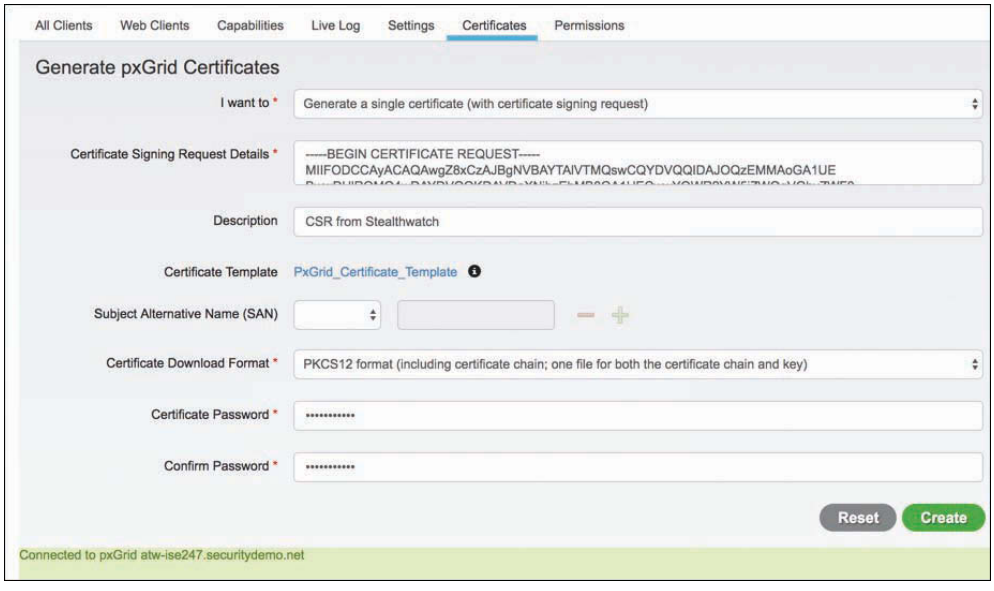

Figure 6-59 *Generating the Certificate Chain for Stealthwatch*

Back in the Stealthwatch User Interface:

Step 18. In the **Friendly Name** field, enter a simplified name for the identity certificate.

Step 19. Click **Choose File** and select the downloaded p12 chain file.

Step 20. After the UI recognizes the chain file, the Bundle Password field appears; enter and confirm the bundle password.

Step 21. Click **Add Client Identity**.

Figure 6-60 shows the import of the PKCS certificate chain into Stealthwatch.

Figure 6-60 *Importing the Signed CSR Chain File*

Step 22. Click **Apply Changes** to save the new identity certificate.

Configuring Stealthwatch for ISE

Now that the pxGrid client identity certificate is imported to Stealthwatch, it is time to configure the ISE integration:

Step 1. On the main Stealthwatch screen, navigate to **Deploy > Cisco ISE Configuration**, as shown in Figure 6-61.

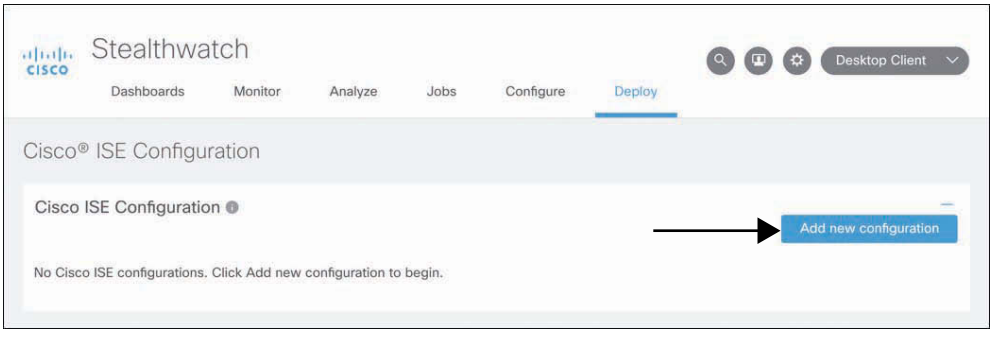

Figure 6-61 *Deploy > Cisco ISE Configuration*

Step 2. Click **Add new configuration.**

Step 3. In the Cluster Name field, enter a friendly name for the ISE cube.

Step 4. In the Certificate field, select the pxGrid certificate from the drop-down list.

Step 5. Enter the IP addresses for the primary and secondary pxGrid controllers.

Step 6. Create a username to uniquely identity Stealthwatch in the ISE pxGrid UI.

Step 7. Under Integration options, check the **Adaptive Network Control**, **Static SGT Classifications**, and **User sessions** check boxes.

Step 8. Click **Save**.

Figure 6-62 shows the completed Cisco ISE Configuration Setup screen.

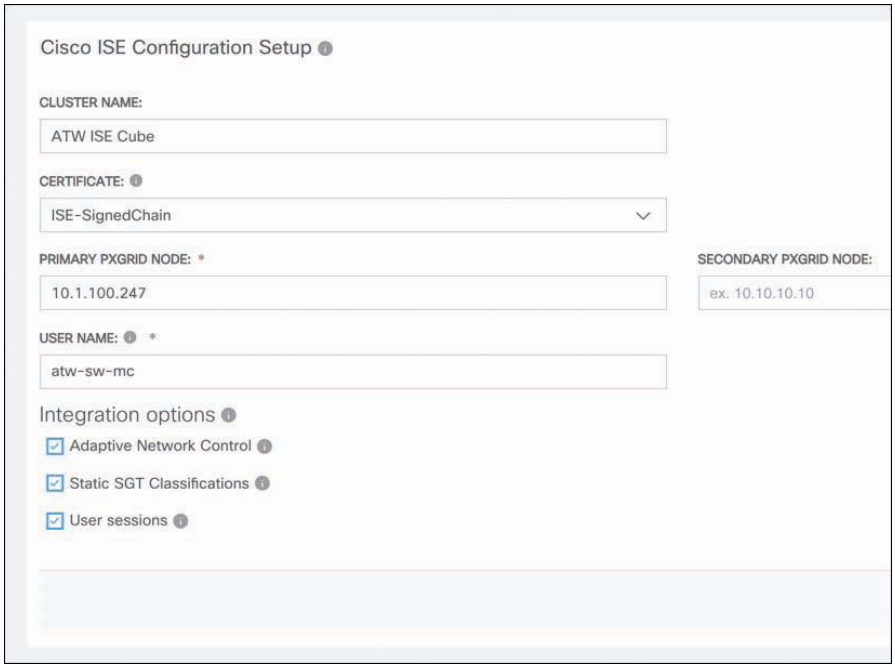

Figure 6-62 *Configuring the pxGrid Connection*

After a bit of time, the Status indicator for the pxGrid connection should change from yellow to green to symbolize that the connection to pxGrid is up and running, as shown in Figure 6-63.

Figure 6-63 *Connected Status for pxGrid Connection*

Figure 6-64 shows the final pxGrid clients screen, where you can see the FMC, WSA, and Stealthwatch clients in the list.

The integration is not only for providing telemetry to Stealthwatch; you can also act during an investigation in Stealthwatch for enforcement through ISE. Stealthwatch 7.0 uses Adaptive Network Control (ANC), whereas previous versions used EPS.

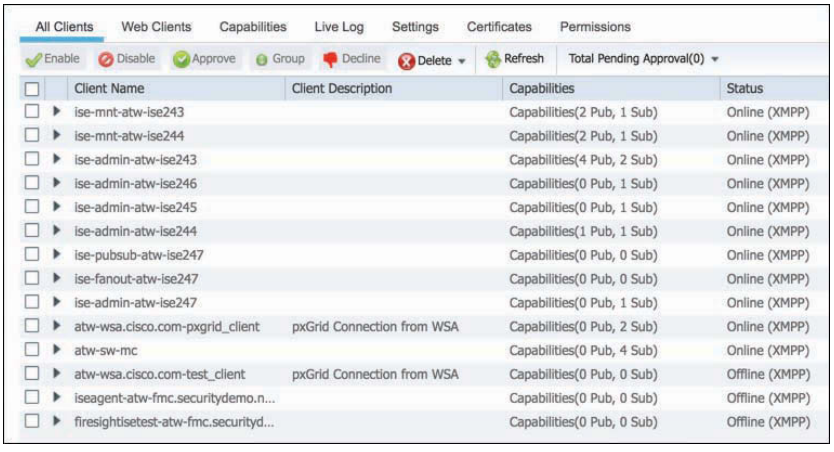

Figure 6-64 *Final pxGrid Clients Screen*

Unlike EPS, which had only two options (Quarantine & Unquarantine), ANC allows you to create many different labels of your choosing, for a variety of actions.

From the ISE user interface:

Step 1. Navigate to **Operations > Adaptive Network Control > Policy List**.

Step 2. Click **Add** to create a new label (called a policy).

Step 3. In the Name field, give the policy a name, such as Investigate.

Step 4. In the Action drop-down list, choose the type of CoA that ISE will issue: SHUT_DOWN, PORT_BOUNCE, or QUARANTINE).

Step 5. Click **Save**.

Figure 6-65 shows two configured ANC labels.

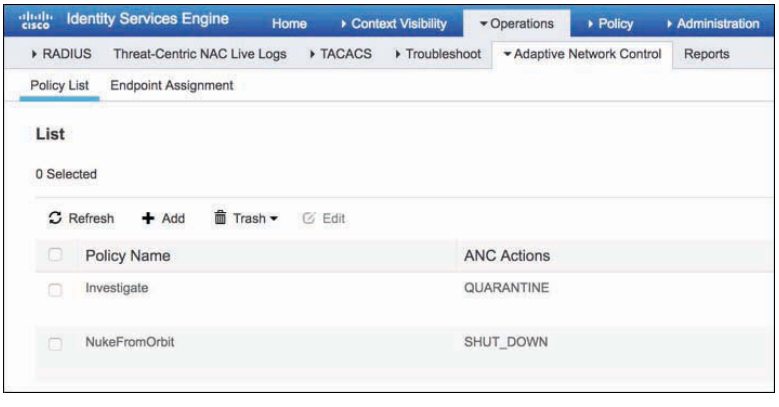

Figure 6-65 *ANC Labels*

After your labels exist, you can include them as conditions in your authorization rules, as shown in Figure 6-66.

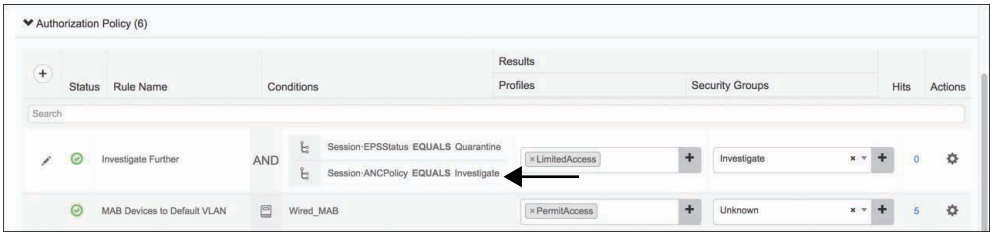

Figure 6-66 *ANC Labels in the Authorization Policy*

Now when something looks awry during an incident response, you can assign the ANC label to a host right in the Stealthwatch interface and have ISE take action.

From the Stealthwatch user interface:

Step 1. Click **Edit** for ISE ANC Policy, as shown in Figure 6-67.

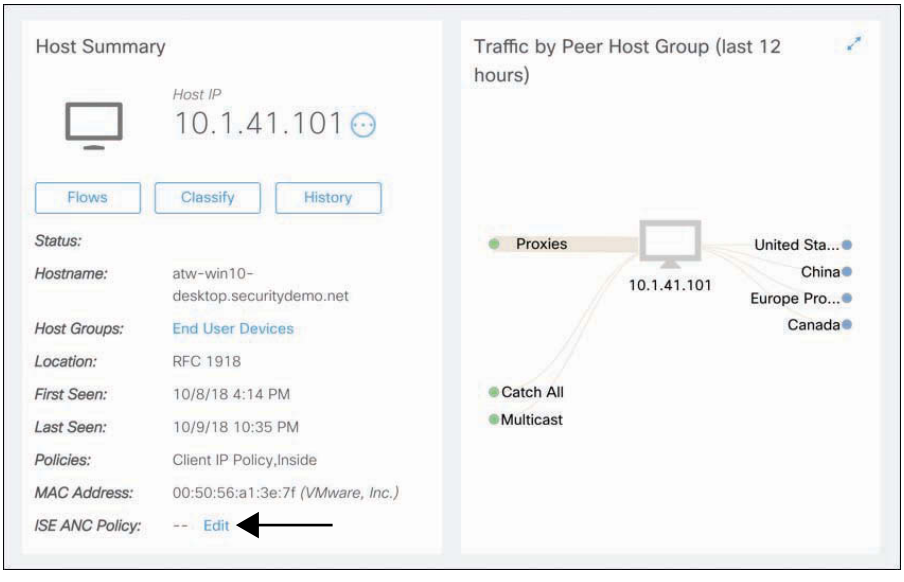

Figure 6-67 *Editing the ISE ANC Policy*

Step 2. In the Applying ANC policy screen, select your chosen label from the ANC Policy drop-down list, as shown in Figure 6-68.

Step 3. Click **Save**.

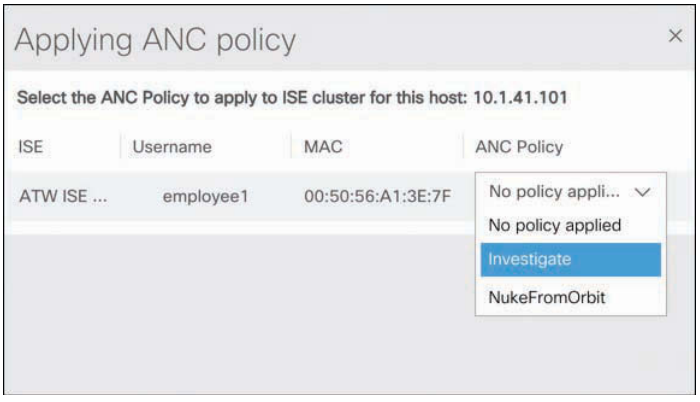

Figure 6-68 *Assigning ISE ANC Policy*

Summary

In this chapter, you learned about the many different ways of sharing context out of ISE to other security solutions, about Rapid Threat Containment, and about the Platform Exchange Grid (pxGrid). In addition to sharing context from ISE to other systems, ISE is able to learn contextual data from those systems as well, creating a true symbiotic ecosystem.

You integrated Firepower with ISE and Active Directory for identity-based firewalling and Rapid Threat Containment using endpoint protection services (EPS). You integrated the Web Security Appliance and Stealthwatch for pxGrid integration with ISE to enhance their capabilities as well.

Index

Numbers

802.1AE, 470–473

802.1X, 199

authentication servers, 55

authenticators, 55

C3PL switch configuration, 95–96

Catalyst switch configuration, 79

components of, 54–56

EAP (Extensible Authentication Protocol)

authentication type identity stores, 61

types of, 57–61

EasyConnect as stepping-stone to, 183–186

MAB (MAC Authentication Bypass), 62–65

supplicants, 55

verification

with Cisco WLC (Wireless LAN Controller), 145–147

endpoint supplicant verification, 140

network access device verification, 140–145

overview of, 140

Web Authentication

CWA (Centralized Web Authentication), 69–71

LWA (Local Web Authentication), 66–69

overview of, 65–66

A

AAA (authentication, authorization, and accounting). *See also* device administration; network access control; policies; posture assessment; profiles

centralized, 307–308

commands, 73–74

concept of, 3–4

configuration, 197

credentials, 4

definition of, 4

protocols, 4–5

RADIUS (Remote Authentication Dial-In User Service)

accounting messages, 14–15

accounting servers, 119–120

authentication messages, 13–14

authentication servers, 118–119

authorization messages, 13–14
AV (attribute-value) pairs, 15
on Cisco ESA (Email Security Appliance), 343–349
on Cisco FMC (Firepower Management Center), 343–349
on Cisco WSA (Web Security Appliance), 343–349
CoA (Change of Authorization), 14–15
definition of, 4–5
Layer 2 EAP communication, 12–13
Live Authentications Log, 147–148
overview of, 343
purpose of, 6–7
RADIUS-Proxy, 54
TACACS+ compared to, 16, 308–309
Token service, 33
TACACS+ (Terminal Access Controller Access Control System Plus)
accounting messages, 11–12
authentication messages, 8–10
authorization messages, 10–11
with Cisco ASA (Adaptive Security Appliance), 331–335
with Cisco IOS devices, 318–331
with Cisco WLC (Wireless LAN Controller), 335–343
client-server communication, 8
data flow, 309–310
definition of, 4–5
ISE (Identity Services Engine) configuration for, 310–318
RADIUS compared to, 16, 308–309
support for, 7–8
aaa accounting command, 329
aaa accounting dot1x default start-stop group radius command, 74, 92
aaa accounting update newinfo periodic 1440 command, 74
aaa authentication dot1x default group radius command, 74, 92
aaa authentication login command, 321
aaa authorization command, 333
aaa authorization config-commands command, 326
aaa authorization console command, 321
aaa authorization network command, 304
aaa authorization network default group radius command, 74, 92
aaa new-model command, 74, 91, 319
aaa server radius dynamic-author command, 75
AAA Servers tab
Corporate WLANs, 137
Guest WLANs, 130–131
aaa session-id common command, 91
aaa-server command, 332
ACCEPT message (TACACS+), 9
acceptable use policy (AUP), 67
access control lists. *See* ACLs (access control lists)
access rules (FMC), 379–382
Access-Accept message (RADIUS), 13
Access-Challenge message (RADIUS), 14
Access-Reject message (RADIUS), 14
Access-Request message (RADIUS), 13
accounting. *See* AAA (authentication, authorization, and accounting)
Accounting-Request message (RADIUS), 14
Accounting-Response message (RADIUS), 14
Accounts menu
API Credentials command, 429
Audit Log command, 432
ACEs (access control entries), 287
ACI (Application Centric Infrastructure)
application network profiles, 610
contracts, 612
device packages, 609–610

EPGs (endpoint groups), 610–611
object models, 609–610
service graphs, 612–613
spine-and-leaf topology, 608–609
ACL (Filter-ID) setting, 106
ACLs (access control lists)
Airespace
Google URLs for ACL bypass, 122–123
overview of, 121
Web Authentication Redirection ACLs, 121–122
application profile settings, 106
applying to ports, 88
C3PL switch configuration, 94–95
Catalyst switch configuration, 78–79
dACLs (downloadable ACLS), 103–104, 287
FlexVPN, 520–521
GETVPN (Group Encrypted Transport VPN), 536–538
redirect, 195–196
tag-based, 305
ACS (Access Control System), 5, 7
Actions command (Policies menu), 419
active authentication, 181–183
Active Directory. *See* AD (Active Directory)
active FMC users, viewing, 383–384
AD (Active Directory)
Active Directory Sites and Services, 37
configuration
advanced settings, 44–47
attributes, 44
groups, 42–44
joining to domains, 37–40
PassiveID, 41
whitelisted domains, 41
ISE profiling probes, 164–165
overview of, 32–33
Adaptive Network Control (ANC), 358–359, 403–406, 427
Adaptive Security Appliance. *See* ASA (Adaptive Security Appliance)
Add New Realm form, 376–378
Add Source command, 421
AD-Host-Exists attribute, 164
adi_cli session command, 383–384
AD-Join-Point attribute, 165
Adleman, 442
AD-Operating-System attribute, 165
AD-OS-Version attribute, 165
AD-Service-Pack attribute, 165
Advanced Attribute Settings (authorization profiles), 107
Advanced Malware Protection. *See* AMP (Advanced Malware Protection)
Advanced Settings tab (Network Access work center), 44–47
Advanced tab
Corporate WLANs, 137–138
Guest WLANs, 132–134
AES-GCM (Galois/Counter Mode Advanced Encryption Standard).471
Aggressive mode (IKEv1), 454, 478–479
AH (Authentication Header) packets, 459
AireOS, 116–117
Airespace ACL Name setting (authorization profiles), 107
Airespace ACLs (access control lists)
authorization profile setting, 107
Google URLs for ACL bypass, 122–123
overview of, 121
Web Authentication Redirection ACLs, 121–122
algorithms, hashing, 441–443. *See also* ciphers
ALL role (WLC), 335
ALL_ACCOUNTS group, 271
Allowed Protocols policy element, 314

AMP (Advanced Malware Protection)
AMP4E (Advanced Malware Protection for Endpoints), 416–420
APIs, 428–432, 546
Enabler, 546
Analysis menu
Correlation command, 415
Intrusion Events command, 423
Vulnerabilities command, 422
ANC (Adaptive Network Control), 358–359, 403–406, 427
AnyConnect provisioning, 246, 546–547
AnyConnect VPN Wizard, 554–570
configuration, 246, 249–255
deployment, 552–554
Profile Editor, 547–552
AnyConnect VPN Wizard, 554–570
API Credentials command (Accounts menu), 429
APIC-EM (Cisco Application Policy Infrastructure Controller Enterprise Module), 604
APIs (application programming interfaces)
accessing, 410
advantages of, 407–409
AMP (Advanced Malware Protection), 428–432
Cisco DevNet, 412
definition of, 407
FMC (Firepower Management Center)
Database Access API, 422–423
eStreamer API, 423–424
Host Input API, 421–422
overview of, 413
remediation API, 414–420
REST API, 413–414
ISE (Identity Services Engine)
ERS (External RESTful Services) API, 426–428
Monitoring REST API, 424–425
overview of, 424
ODBC (Open Database Connectivity), 33
Postman tool, 410–412
RESTful, 409–410
Threat Grid, 433–435
Umbrella, 435–437
Application Centric Infrastructure. *See* ACI (Application Centric Infrastructure)
application network profiles, 610
Application Policy Infrastructure Controller Enterprise Module (APIC-EM), 604
application programming interfaces. *See* APIs (application programming interfaces)
ASA (Adaptive Security Appliance)
ASAv, 601
CDA (Cisco Context Directory Agent), 181
device administration with TACACS+331–335
FlexVPN
ASA configuration, 515–516
ASA verification, 518–519
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
ASA VTI router routing and ping test, 523
ASA VTI validation, 522–523
dual-hub, dual-cloud hub configurations, 524–527
dual-hub, dual-cloud spoke configurations, 527–528
hub virtual access interface verification, 529
spoke routing and interface verification, 530
spoke-to-spoke tunnel verification, 530–532
traffic problem with crypto map ACLs, 520
IKEv1 ASA configuration, 484

IPsec with IKEv2, 489–491
RAVPN (Remote Access VPN) with
AnyConnect VPN Wizard, 554–561
DAP (dynamic access policies), 565–566
group policies, 562–565
posture assessment, 567–570
tag-based ACLs on, 305
ASA VPN setting (authorization profiles), 107
assigning SGTs (Security Group Tags)
dynamically, 290–291
manually, 291–292
asymmetric encryption, 445–446
Attribute Details setting (authorization profiles), 107
attributes, AD (Active Directory), 44
attribute-value (AV) pairs, 15
Audit Log command (Accounts menu), 432
AUP (acceptable use policy), 67
authentication display legacy command, 88
authentication display new-style command, 88, 91
authentication event server command, 85
Authentication Header (AH) packets, 459
authentication host-mode multi-auth command, 86
authentication mechanisms. ***See also*** **AAA (authentication, authorization, and accounting)**
certificate expiration, 451–452
certificate revocation, 452–453
certificate trust relationship, 449–450
OTPs (one-time passwords), 447
PSKs (preshared keys), 447
username/password combinations, 447
X.509 PKI (Public Key Infrastructure), 448–449
authentication open command, 87
authentication order dot1x mab command, 85
authentication priority dot1x mab command, 84
Authentication Redirection ACLs, 121–122
authentication servers, 802.1X, 55. ***See also*** **AAA (authentication, authorization, and accounting)**
authentication timers, 87–88
authentication violation restrict command, 86
authentications logs, 147–148
Authenticator, 33
authenticators
definition of, 55
NDAC (Network Device Admission Control), 472
authorization. ***See*** **AAA (authentication, authorization, and accounting)**
Auto SmartPot setting (authorization profiles), 107
auto-enable option (aaa authorization command), 333
automation, 606–607. ***See also*** **virtualization**
AV (attribute-value) pairs, 15

B

BGP (Border Gateway Protocol), 463
blacklisting domains, 435–437
block ciphers, 444
blogs, Network World, 44
Border Gateway Protocol (BGP), 463
bring your own device. ***See*** **BYOD (bring your own device) onboarding**
built-in groups, 43
business partners, 545. ***See also*** **RAVPN (Remote Access VPN)**

BYOD (bring your own device) onboarding
building blocks of BYOD solutions, 198–200
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
Dual SSID provisioning, 200–202
end-user experience, 229–235
network device configuration, 223–228
NSPs (Native Supplicant Profiles), 204, 207–208
overview of, 197–198
policy sets and rules, 216–223
portals for, 212–216
SCEP (Simple Certificate Enrollment Protocol) RA profiles, 205–207
Single SSID provisioning, 200–202
SPWizards, 203, 209–210
verification, 229–235
bypass
Google URLs for ACL bypass, 122–123
MAB (MAC Authentication Bypass), 62–65, 89, 150

C

C3PL switches, configuration of
802.1X commands, 95–96
advantages of, 89–90
configuration hierarchy, 96
enabling switches, 88
global configuration, 91–92
local access control lists, 94–95
policies
control class configuration, 97–98
control policy application, 99–100
control policy configuration, 98–99
overview of, 97
RADIUS commands for, 92–94
service templates, 95
cache, MAR, 46
CAPs (Certificate Authentication Profiles), 47–48
Captive Network Assistant Bypass option (WLC), 130
Captive Network Assistant (CNA), 227
CAs (certificate authorities), 205–206, 362–363, 448–450
Catalyst switches, configuration of
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
switch types, 71–72
verification
show aaa servers command, 140–141
show authentication session interface command, 142–143
syslog messages, 143–145
test aaa servers command, 141–142
CDA (Cisco Context Directory Agent), 181
centralized AAA (authentication, authorization, and accounting), 307–308
Centralized Web Authentication (CWA), 69–71, 99

centralized web portals, local web authentication with, 67–69
Certificate Authentication Profiles (CAPs), 47–48
certificate authorities (CAs), 205–206, 362–363, 448–450
certificate signing request (CSR), 370, 399–402
certificates, 384–389
CAs (certificate authorities), 205–206, 362–363, 448–450
on Catalyst switches, 72–73
certificate SCEP enrollment, 487–489
expiration, 451–452
ISE root, 390–394
MDM server, 239–240
pxGrid, 364–365, 369–375
ISE root certificates, 390–394
StealthWatch CSR, 399–402
RAVPN with FTD, 571
revocation, 452–453
templates, 205–207
trust relationship, 449–450
Certification Revocation Lists (CRLs), 448, 452
chaining, SFC (service function chaining), 603–605
Change of Authorization (CoA), 356, 425
CHAP (Challenge/Handshake Authentication Protocol), 6
ciphers
block, 444
definition of, 444
stream, 444
Cisco 4000 Series Integrated Services Routers (ISR), 606
Cisco 5000 Enterprise Network Compute System (ENCS), 606
Cisco Adaptive Security Appliance. *See* ASA (Adaptive Security Appliance)
Cisco AnyConnect. *See* AnyConnect provisioning
Cisco Application Centric Infrastructure. *See* ACI (Application Centric Infrastructure)
Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), 604
Cisco Catalyst switches. *See* Catalyst switches, configuration of
Cisco Content Security Virtual Appliances, 601
Cisco Context Directory Agent, 181
Cisco DevNet, 412
Cisco Email Security Appliance. *See* ESA (Email Security Appliance)
Cisco Enterprise Service Automation, 606–607
Cisco Firepower Management Center. *See* FMC (Firepower Management Center)
Cisco Identity Services Engine. *See* ISE (Identity Services Engine)
***Cisco Identity Services Engine Administrator Guide*, 189**
Cisco Industrial Network Director, 363
Cisco IOS devices
device administration with TACACS+
accounting, 329
command authorization, 325–329
debugging, 331
live logs, 330–331
login authentication and authorization, 319–325
overview of, 318–319
privilege levels, 319–325
Shell Profiles, 322–323
verification, 329–331
NTP and CA configuration, 484–486
***Cisco ISE for BYOD and Secure Unified Access, Second Edition*, 18, 25, 148, 191**
Cisco Jabber, 360

Cisco Network Functions Virtualization. ***See*** **NFV (Network Functions Virtualization)**
Cisco Network Setup Assistant, 203
Cisco Next Generation Firewalls, 305–306
Cisco NGIPSv, 602
Cisco Prime Network Services Controller, 602–603
Cisco pxGrid. ***See*** **pxGrid**
Cisco Secure Access Control System, 5, 7
Cisco Security Architecture APIs. ***See*** **APIs (application programming interfaces)**
Cisco Sourcefire Firepower, 181
Cisco StealthWatch. ***See*** **StealthWatch**
Cisco Threat Grid APIs, 433–435
Cisco UCS, 606
Cisco UCS (Unified Computing System), 606
Cisco Umbrella APIs, 435–437
Cisco Unified Communications Manager, 360
Cisco Virtual Internet Routing Lab, 477
Cisco Virtual Security Gateway, 602–603
Cisco vPath, 603
Cisco Web Security Appliance. ***See*** **WSA (Web Security Appliance)**
Cisco Wireless LAN Controller. ***See*** **WLC (Wireless LAN Controller)**
classification, SGTs (Security Group Tags), 288–290
class-map type control subscriber match-all DOT1X-FAILED command, 98
class-map type control subscriber match-any AAA-DOWN command, 97
Client Provisioning Policy (CPP), 203–204, 210–212
client VLANs, dynamic interfaces for
  employee interfaces, 124–125
  guest interfaces, 125–127
  overview of, 124
  PCI interfaces, 127
client-based VPNs (virtual private networks)
  definition of, 545–546
  IPsec IKEv2 VPN example, 580–586
  RAVPN with ASA
    AnyConnect VPN Wizard, 554–561
    DAP (dynamic access policies), 565–566
    group policies, 562–565
    posture assessment, 567–570
  RAVPN with FTD, 570–579
    access control, 577–579
    authentication method, 574
    authentication servers, 571
    certificates, 571
    group policies, 574
    interface and certificate configuration, 575–576
    VPN client images, 573
    VPN pool, 572
    VPN profile, 572
  RAVPN with routers, 580
Clientless SSL VPN Wizard, 587–594
  bookmarks, 589–590
  DAP (dynamic access policies), 594
  group policies, 592
  login screen and home page, 590–592
  plug-ins, 593
  portal customization, 594
  profile and interface configuration, 587–588
  smart tunnels, 593
  user authentication, 588
  virtual desktop support, 593
clientless VPNs (virtual private networks)
  configuration, 586–594
    bookmarks, 589–590
    DAP (dynamic access policies), 594

group policies, 592
login screen and home page, 590–592
plug-ins, 593
portal customization, 594
profile and interface, 587–588
smart tunnels, 593
user authentication, 588
virtual desktop support, 593
definition of, 545–546
clients
EzVPN (Easy VPN)
client validation tunnel down, 497
client validation tunnel up, 497–498
configuration, 495–497
hub ICMP debug, 499
hub validation tunnel up, 498
monitoring, 145–146
Clients UI (Cisco WLC), 145–146
cloud FlexVPN configurations
dual-hub, dual-cloud hubs, 524–527
dual-hub, dual-cloud spokes, 527–528
CN (Common Name) field, 370
CNA (Captive Network Assistant), 227
CoA (Change of Authorization), 14–15, 175–177, 356, 425
command authorization, Cisco IOS devices, 325–329
command sets, 5
commands. *See individual commands*
Common Classification Policy Language switches. *See* C3PL switches, configuration of
Common Name (CN) field, 370
Comodo, 450
conditions
BYOD (bring your own device) onboarding, 220–223
differentiated access policy, 108–112
guest access, 285–286
MDM (mobile device management) onboarding, 242–244
posture assessment, 256–258, 264–265
posture requirements, 260–261
prebuilt, 257
remediation actions, 258–260
TACACS+ (Terminal Access Controller Access Control System Plus), 314, 318
Config Wizard or Supplicant Provisioning Wizards. *See* SPWizards
configuration
C3PL switches
802.1X commands, 95–96
advantages of, 89–90
configuration hierarchy, 96
enabling switches, 88
global configuration, 91–92
local access control lists, 94–95
policies, 97–100
RADIUS commands for, 92–94
service templates, 95
Catalyst switches
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
switch types, 71–72

clientless RAVPN (Remote Access VPN), 586–594
DMVPN (Dynamic Multipoint VPN)
crypto keyrings, 501
dual-hub configuration, 513–514
hub interface configuration, 501–502
hub tunnel interface, 502
ISAKMP and transform set, 501
NHRP configuration, 505–506
Phase 1, 506–507
Phase 2, 508–510
Phase 3, 510–513
sample network, 500
show dmvpn command, 504–505
spoke configuration, 503–504
VRF configuration, 500–501
EzVPN (Easy VPN)
client configuration, 495–497
client validation tunnel down, 497
client validation tunnel up, 497–498
dynamic VTI network, 492–493
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498
FlexVPN
ASA configuration, 515–516
ASA verification, 518–519
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
ASA VTI router routing and ping test, 523
ASA VTI validation, 522–523
dual-hub, dual-cloud hub configurations, 524–527
dual-hub, dual-cloud spoke configurations, 527–528
hub virtual access interface verification, 529
INSIDE router configuration, 515
IOS virtual access interface, 518
spoke routing and interface verification, 530
SPOKE1 configuration, 516–517
spoke-to-spoke tunnel verification, 530–532
traffic problem with crypto map ACLs, 520
verification ping, 517
FMC (Firepower Management Center) for pxGrid, 369–376
access rules, 379–382
active users, viewing, 383–384
correlation rules, 384–389
Rapid Threat Containment, 384–389
realms, 376–379
remediation modules, 384–389
GETVPN (Group Encrypted Transport VPN)
group member configuration, 535
group member validation, 538–540
key server and group member status validation, 535–536
key server policy and ACL validation, 536–538
primary key server configuration, 532–534
guest access
guest types, 268–270
hotspot portals, 278–279
network devices, 268
policy sets for, 284–287
self-registered portals, 279–284
sponsor groups, 270–273
sponsor portals, 274–276
identity sources
advanced settings, 44–47
attributes, 44

CAPs (Certificate Authentication Profiles), 47–48
groups, 42–44
joining to domains, 37–40
passive identity, 41
sequences, 48–50
whitelisted domains, 41
IPsec with IKEv1, 478–484
Aggressive mode, 478–479
ASA configuration, 484
basic IPsec network, 478
crypto map sets, 479–480
debugging, 481–484
interesting traffic ACL, 479
ISAKMP policy, 478
transform set, 479
tunnel establishment, 480
validation, 480–481
IPsec with IKEv2
Cisco IOS NTP and CA configuration, 484–486
IKEv2 configuration for ASA, 489–491
IKEv2 peer NTP synchronization and certificate SCEP enrollment, 487–489
validation, 491–492
ISE for BYOD onboarding
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
end-user experience, 229–235
network device configuration, 223–228
NSPs (Native Supplicant Profiles), 204, 207–208
policy sets and rules, 216–223
portals for, 212–216
SCEP (Simple Certificate Enrollment Protocol) RA profiles, 205–207
SPWizards, 203, 209–210
verification, 229–235
ISE for network access
distributed deployment, 22–23, 29–32
dual-node deployment, 19–20, 25–28
multinode deployment, 21–22
standalone deployment, 19, 24–25
ISE for pxGrid, 364–367
ISE for TACACS+
network devices, adding, 312–313
overview of, 310
policy elements, 314–316
policy sets and rules, 316–318
TACACS+, enabling, 310–312
ISE profiling, 153–155
Active Directory probes, 164–165
CoA (Change of Authorization), 176–177
context visibility, 171–174
DHCP and DHCPSPAN probes, 157–158
endpoint policies, 170–171
HTTP probes, 165–167
HTTP profiling without probes, 167
logical policies, 174–175
NETFLOW probes, 167–168
NMAP probes, 160–162
profiling feed service, 168–170
pxGrid probes, 168
RADIUS probes, 159
SNMPQUERY and SNMPTRAP probes, 164
MDM (mobile device management) onboarding
MDM server, adding in ISE, 236–240
policy sets and rules, 240–244

posture assessment
AnyConnect provisioning, 246, 249–255
policy sets, 262–265
posture policy, 255–262
prerequisites, 247–249
pxGrid. *See* pxGrid
RADIUS on Cisco ESA (Email Security Appliance)
ESA configuration, 349–351
ISE configuration, 351
overview of, 343–344
verification, 351
RADIUS on Cisco WSA (Web Security Appliance)
ISE configuration, 351
overview of, 343–344
verification, 351
WSA configuration, 349–351
RADIUS on on Cisco FMC (Firepower Management Center)
FMC configuration, 344–346
ISE configuration, 346–348
verification, 349
RAVPN with ASA
AnyConnect VPN Wizard, 554–570
DAP (dynamic access policies), 565–566
group policies, 562–565
posture assessment, 567–570
RAVPN with FTD, 570–579
access control, 577–579
authentication method, 574
authentication servers, 571
certificates, 571
group policies, 574
interface and certificate configuration, 575–576
VPN client images, 573
VPN pool, 572
VPN profile, 572
RAVPN with routers, 580–586
REST API preferences, 413
StealthWatch
advantages of, 397–398
configuration for ISE, 402–406
CSR (certificate signing request), 399–402
TACACS+ with Cisco ASA (Adaptive Security Appliance), 331–335
TACACS+ with Cisco IOS devices
accounting, 329
command authorization, 325–329
debugging, 331
live logs, 330–331
login authentication and authorization, 319–325
privilege levels, 319–325
Shell Profiles, 322–323
verification, 329–331
TACACS+ with Cisco WLC (Wireless LAN Controller)
ISE configuration, 338–342
roles, 335–336
Shell Profiles, 335, 339–340
verification, 342–343
WLC configuration, 336–337
TrustSec
inline tagging, 294–295
policy configuration in ISE, 300–302
policy download, 302–305
SXP (SGT Exchange Protocol), 295–300
tag-based ACLs, 305
tag-based policies on Cisco NGFW, 305–306
wired network access control

default policy sets and rules, 100–102
differentiated access policy, creating, 102–115
wireless network access control
802.1X and MAB verification, 140–148
AAA server configuration, 118–121
AireOS, 116–117
Airespace ACLs, 121–123
Corporate WLANs, 134–138
dynamic interfaces for client VLANs, 124–127
Guest WLANs, 127–134
ISE configuration, 138–140
overview of, 115–116
RADIUS accounting servers, 119–120
RADIUS authentication servers, 118–119
RADIUS fallback, 120–121
WMI (Windows Management Instrumentation), 187–190
WSA (Web Security Appliance)
ISE root certificates, 390–394
overview of, 390
policies, 394–397
WSA and ISE integration, 390–394
configure command, 318
console keyword, 332
Content Security Virtual Appliances, 601
context sharing. *See also* pxGrid
MDM (mobile device management), 356
Rapid Threat Containment, 356–359
configuration, 384–389
StealthWatch, 397–406
context visibility, ISE profiling, 171–174
context-in, 363
context-out, 363
CONTINUE message (TACACS+), 8, 9, 11
contractors, 545. *See also* RAVPN (Remote Access VPN)
contracts, 612
controllers, 360
COOP key servers, GETVPN with, 468
group member configuration, 535
group member validation, 538–540
key server and group member status validation, 535–536
key server policy and ACL validation, 536–538
primary key server configuration, 532–534
Corporate WLANs
AAA Servers tab, 137
Advanced tab, 137–138
General tab, 135–136
Layer 2 Security tab, 136
Layer 3 Security tab, 136–137
overview of, 134–135
Correlation command
Analysis menu, 415
Policies menu, 420
correlation rules (FMC), 384–389
CPP (Client Provisioning Policy), 203–204, 210–212
create, read, update, and delete (CRUD) operations, 426–428
Create Client command (Host Input Client menu), 421
credentials
AMP (Advanced Malware Protection) APIs, 429–431
definition of, 4
Critical MAB, 89
CRLs (Certification Revocation Lists), 448, 452
CRUD (create, read, update, and delete) operations, 426–428
crypto isakmp key command, 478

crypto map sets, 461, 479–480, 520
cryptography. *See also* VPNs (virtual private networks)
AH (Authentication Header) packets, 459
asymmetric encryption, 445–446
authentication mechanisms
certificate expiration, 451–452
certificate revocation, 452–453
certificate trust relationship, 449–450
OTPs (one-time passwords), 447
PSKs (preshared keys), 447
username/password combinations, 447
X.509 PKI (Public Key Infrastructure), 448–449
ciphers
block, 444
definition of, 444
stream, 444
crypto keyrings, 501
Diffie-Hellman, 458–459
ESP (Encapsulating Security Payload) packets, 460
hashing, 441–443
overview of, 441
protocols
DTLS (Datagram Transport Layer Security), 460
IKEv1 (Internet Key Exchange version 1), 453–456
IKEv2 (Internet Key Exchange version 2), 456–458
IPsec, 453, 459–460, 461–462
ISAKMP (Internet Security Association and Key Management Protocol), 459
SSL (Secure Sockets Layer), 460
TLS (Transport Layer Security), 460
symmetric encryption, 445
Transport mode encryption, 459
Tunnel mode encryption, 459
CSR (certificate signing request), 370, 399–402
cts authorization list command, 304
cts credentials id command, 304
cts manual command, 294
cts role-based enforcement command, 294
cts role-based sgt-map command, 292
cts sxp connection peer command, 295
cts sxp default password command, 295
cts sxp enable command, 295
curl command, 410
CWA (Centralized Web Authentication), 69–71, 99

D

DACL Name setting (authorization profiles), 104
dACLs (downloadable ACLS), 103–104, 287
Dagenhardt, Frank, 608–609
DAP (dynamic access policies), 565–566, 594
DART (Diagnostic and Reporting Tool), 547
data flow, FMC remediation API, 415
Database Access API (FMC), 422–423
Datagram Transport Layer Security (DTLS), 460, 576
debug aaa accounting command, 331, 335
debug aaa authentication command, 331, 334
debug aaa authorization command, 331, 335
debug client command, 146–147
debug crypto ipsec command, 481
debug crypto isakmp command, 481
debug dot1x command, 146

debug ip icmp command, 499
debug nhrp packet command, 511–512
debug tacacs command, 331, 334
debugging
EzVPN (Easy VPN), 499
IPsec with IKEv1, 481–484
with Live Log, 147–148
TACACS+ (Terminal Access Controller Access Control System Plus), 331, 334
WLC (Wireless LAN Controller), 146–147
default devices, 53–54
default method lists, 326
DELETE requests (HTTP), 409
deny statement, 195–196
***Deploying ACI* (Dagenhardt, Moreno, and Dufresne), 608–609**
deployment. *See also* configuration
AnyConnect, 552–554
ISE (Identity Services Engine)
distributed, 22–23, 29–32
dual-node, 19–20, 25–28
multinode, 21–22
standalone, 19, 24–25
Details command (User menu), 433
Device Admin policy sets, 316–318, 324, 341
Device Admin Policy Sets command (Device Administration menu), 324, 341
Device Admin Service, 310–312
device administration
BYOD (bring your own device) onboarding, 197–198
building blocks of BYOD solutions, 198–200
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
Dual SSID provisioning, 200–202
end-user experience, 229–235
network device configuration, 223–228
NSPs (Native Supplicant Profiles), 207–208
overview of, 197–198
policy sets and rules, 216–223
portals for, 212–216
SCEP RA profiles, 205–207
Single SSID provisioning, 200–202
SPWizards, 209–210
verification, 229–235
concept of, 5–6
configuration for BYOD onboarding, 223–228
definition of, 4
MDM (mobile device management) onboarding
MDM server, adding in ISE, 236–240
overview of, 236–238
policy sets and rules, 240–244
RADIUS (Remote Authentication Dial-In User Service)
accounting messages, 14–15
authentication messages, 13–14
authorization messages, 13–14
AV (attribute-value) pairs, 15
on Cisco ESA (Email Security Appliance), 343–349
on Cisco FMC (Firepower Management Center), 343–349
on Cisco WSA (Web Security Appliance), 343–349
CoA (Change of Authorization), 14–15
definition of, 4–5
Layer 2 EAP communication, 12–13
overview of, 343

purpose of, 6–7
TACACS+ compared to, 16, 308–309
TACACS+ (Terminal Access Controller Access Control System Plus), 4–5
accounting messages, 11–12
authentication messages, 8–10
authorization messages, 10–11
with Cisco ASA (Adaptive Security Appliance), 331–335
with Cisco IOS devices, 318–331
with Cisco WLC (Wireless LAN Controller), 335–343
client-server communication, 8
data flow, 309–310
ISE (Identity Services Engine) configuration for, 310–318
RADIUS compared to, 16, 308–309
Shell Profiles, 315
support for, 7–8
device packages, 609–610
device-sensor accounting command, 82
device-sensor filter-list command, 81
device-sensor filter-spec command, 81
device-sensor notify all-changes command, 82
DevNet, 412
DHCP (Dynamic Host Control Protocol) probes, 155–158
configuration, 157–158
DHCP logical design, 155
DHCP SPAN logical design, 156–157
WLC considerations, 157
DHCPSPAN probes, 155–158
Diagnostic and Reporting Tool (DART), 547
DIAMETER, 7
Dictionaries section (Network Access work center), 36
differentiated access policy, creating
authorization results, 103–109
least privilege access rules example, 102–103
policy conditions, 108–112
policy sets, 112–115
Diffie-Hellman, 458–459
disable command, 319
disaster recovery, 544–545. ***See also*** **RAVPN (Remote Access VPN)**
distributed ISE deployment, 22–23, 29–32
DMVPN (Dynamic Multipoint VPN), 462–465. ***See also*** **FlexVPN**
crypto keyrings, 501
dual-hub configuration, 513–514
FlexVPN compared to, 514
hub interface configuration, 501–502
hub tunnel interface, 502
ISAKMP and transform set, 501
NHRP configuration, 505–506
Phase 1
hub routing verification, 506
overview of, 506–507
spoke routing verification, 506–507
spoke-to-spoke trace route, 507
Phase 2
hub EIGRP configuration, 508
overview of, 508–510
spoke CEF adjacency, 508–509
spoke CEF punt, 509
spoke DMVPN and NHRP verification, 510
spoke routing configuration, 508
spoke-to-spoke trace route, 509
tunnel interface changes, 508
Phase 3
DMVPN and NHRP verification, 512–513
NHRP redirect and summary address, 510–511
NHRP routes verification, 512

NHRP shortcut and routing verification, 511
overview of, 510–513
trace route and NHRP redirect, 511–512
sample network, 500
show dmvpn command, 504–505
spoke configuration, 503–504
VRF configuration, 500–501
DNS (Domain Name System), 197
AD (Active Directory) and, 37
ISE profiling probe, 162
Umbrella APIs, 435–437
domain local groups, 43
Domain Name System. *See* DNS (Domain Name System)
domains. *See also* DNS (Domain Name System)
joining ISE to, 37–40
white/blacklisting, 435–437
whitelisted, 41
dot1x pae authenticator command, 87
dot1x system-auth-control command, 79, 95
downlink MACsec, 472
downloadable ACLS (dACLs), 103–104, 287
downloading
SPWizards, 209–210
TrustSec policy, 302–305
DTLS (Datagram Transport Layer Security), 460, 576
Dual SSID provisioning, 200–202
dual-hub DMVPN (Dynamic Multipoint VPN), 513–514
dual-hub FlexVPN
dual-hub, dual-cloud hubs, 524–527
dual-hub, dual-cloud spokes, 527–528
hub virtual access interface verification, 529
spoke routing and interface verification, 530
spoke-to-spoke tunnel verification, 530–532
dual-node ISE deployment, 19–20, 25–28
Dufresne, Bill, 608–609
Duo Security MFA, 33
dynamic access policies (DAP), 565–566, 594
dynamic interfaces for client VLANs
employee interfaces, 124–125
overview of, 124
PCI interfaces, 127
Dynamic Multipoint VPN. *See* DMVPN (Dynamic Multipoint VPN)

E

EAP (Extensible Authentication Protocol), 7. *See also* 802.1X
authentication type identity stores, 61
EAP-GTC (Generic Token Card), 58, 59, 125–127
types of, 57–61
Easy VPN. *See* EzVPN (Easy VPN)
EasyConnect, 183–186
overview of, 183–186
WMI (Windows Management Instrumentation)
configuration, 187–190
logoff detection, 190–191
overview of, 185–186
Edit OS and Identity Sources menu, Add Source command, 421
EIGRP (Enhanced Interior Gateway Routing Protocol), 463, 508
Email Security Appliance. *See* ESA (Email Security Appliance)
EMM (Enterprise Mobility Management). *See* MDM (mobile device management) onboarding

employee dynamic interfaces, 124–125
enable command, 309, 319, 322
Enable ERS for Read/Write button, 426
Encapsulating Security Payload (ESP) packets, 460
encryption. *See* cryptography
ENCS (Enterprise Network Compute System), 606
Endpoint Identity Groups, 178–179
Endpoint Protection Services (EPS), 356–359
endpoints
attribute filtering, 177–178
EPGs (endpoint groups), 178–179, 610–611
EPS (Endpoint Protection Services), 356–359
probes, 190–191
profile policies, 170–171
supplicant verification, 140
end-user experience, BYOD (bring your own device) onboarding, 229–235
enforcement
Enforcement API, 435
TrustSec
overview of, 300
policy configuration in ISE, 300–302
policy download, 302–305
tag-based ACLs, 305
tag-based policies on Cisco NGFW, 305–306
Enhanced Interior Gateway Routing Protocol (EIGRP), 463
Enterprise Mobility Management (EMM). *See* MDM (mobile device management) onboarding
Enterprise Network Compute System (ENCS), 606
EPGs (endpoint groups), 610–611
epm logging command, 144
ePO (ePolicy Orchestrator) ports, 160
EPS (Endpoint Protection Services), 356–359
ERROR message (TACACS+), 9, 11
ERS (External RESTful Services) API, 426–428
ESA (Email Security Appliance)
ESA configuration, 349–351
ESAv, 601
ISE configuration, 351
overview of, 343–344
verification, 351
ESA (Enterprise Service Automation), 606–607
ESP (Encapsulating Security Payload) packets, 460
eStreamer API (FMC), 423–424
event agent-found match-all command, 99
event authentication-failure match-all command, 99
event session-started match-all command, 98
exit command, 328
expiration of certificates, 451–452
Ext Id Sources section (Network Access work center), 35
extending network access. *See* network access, extending
Extensible Authentication Protocol. *See* EAP (Extensible Authentication Protocol)
Extensible Communications Platform (XCP), 361
Extensible Messaging and Presence Protocol (XMPP), 361
External Authentication command (Users menu), 344
external RADIUS servers, 54
External RESTful Services (ERS) API, 426–428
EZC. *See* EasyConnect
EzVPN (Easy VPN)

client configuration, 495–497
client validation tunnel down, 497
client validation tunnel up, 497–498
dynamic VTI network, 492–493
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498

F

FAIL message (TACACS+), 10
fallback, RADIUS, 120–121
FAST (Flexible Authentication via Secure Tunneling), 59, 61
feed service, ISE Profiler, 168–170
files, module.template, 417–418
filtering endpoint attributes, 177–178
Firepower Management Center. *See* FMC (Firepower Management Center)
Firepower Threat Defense (FTD), 413
FlexAuth
FAST (Flexible Authentication via Secure Tunneling), 59, 61
overview of, 83–86
Flexible Authentication via Secure Tunneling (FAST), 59, 61
FlexVPN
ASA configuration, 515–516
ASA verification, 518–519
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
ASA VTI router routing and ping test, 523
ASA VTI validation, 522–523
DMVPN compared to, 514
dual-hub, dual-cloud hub configurations, 524–527
dual-hub, dual-cloud spoke configurations, 527–528
hub virtual access interface verification, 529
INSIDE router configuration, 515
IOS virtual access interface, 518
overview of, 465–466
spoke routing and interface verification, 530
SPOKE1 configuration, 516–517
spoke-to-spoke tunnel verification, 530–532
traffic problem with crypto map ACLs, 520
verification ping, 517
FMC (Firepower Management Center), 362
configuration for pxGrid, 369–376
access rules, 379–382
active users, viewing, 383–384
Rapid Threat Containment, 384–389
realms, 376–379
Database Access API, 422–423
device administration with RADIUS
FMC configuration, 344–346
ISE configuration, 346–348
overview of, 343–344
verification, 349
eStreamer API, 423–424
Host Input API, 421–422
overview of, 413
RAVPN Policy Wizard, 570–579
access control, 577–579
authentication method, 574
authentication servers, 571
certificates, 571
group policies, 574
interface and certificate configuration, 575–576
VPN client images, 573
VPN pool, 572
VPN profile, 572
remediation API, 414–420

built-in remediation modules, 415–416
custom AMP4E remediation module, 416–420
data flow, 415
instance configuration, 419–420
module.template file, 417–418
REST API, 413–414
FOLLOW message (TACACS+), 11
FQDNs (fully qualified domain names), 162
FTD (Firepower Threat Defense), RAVPN with, 413, 570–579
access control, 577–579
authentication method, 574
authentication servers, 571
certificates, 571
group policies, 574
interface and certificate configuration, 575–576
VPN client images, 573
VPN pool, 572
VPN profile, 572
fully qualified domain names (FQDNs), 162
functions, Cisco NFV (Network Functions Virtualization), 605–607

G

Galois Method Authentication Code (GMAC), 471
Galois/Counter Mode Advanced Encryption Standard (AES-GCM), 471
gateways, Cisco VSG (Virtual Security Gateway), 602–603
GBLA (Gramm-Leach-Bliley Act), 466
GDOI (Group Domain of Interpretation), 466
General tab
Corporate WLANs, 135–136
Guest WLANs, 128–129
GeoTrust, 450
GET requests (HTTP), 409
GETVPN (Group Encrypted Transport VPN)
GMs (group members), 535
group member validation, 538–540
key server and group member status validation, 535–536
key server policy and ACL validation, 536–538
overview of, 466–469
primary key server configuration, 532–534
global CoA (Change of Authorization), 176–177
global groups, 42
global profiler settings, 177–178
endpoint attribute filtering, 177–178
NMAP Scan Subnet Exclusions, 178
SNMP settings, 177
GMAC (Galois Method Authentication Code), 471
GMs (group members)
configuration, 535
overview of, 467–468
validation, 535–536, 538–540
GoDaddy, 450
Google
Authenticator, 33
domains, 227
URLs for ACL bypass, 122–123
Gramm-Leach-Bliley Act (GBLA), 466
graphs, service, 612–613
Group Domain of Interpretation (GDOI), 466
Group Encrypted Transport VPN (GETVPN), 466–469
GROUP_ACCOUNTS group, 271
groups
AD (Active Directory), 42–44

EPGs (endpoint groups), 178–179, 610–611
GMs (group members)
configuration, 535
overview of, 467–468
validation, 535–536, 538–540
group policy
clientless VPNs (virtual private networks), 592
RAVPN with ASA, 562–565
RAVPN with FTD, 574
NDGs (Network Device Groups), 50–51
SGTs (Security Group Tags), 108–109, 288–292
sponsor, 270–273
guest access
guest types, 268–270
hotspot portals, 278–279
network device configuration, 268
overview of, 265–268
policy sets for, 284–287
self-registered portals, 279–284
sponsor groups, 270–273
sponsor portals, 274–276
guest dynamic interfaces, 125–127
guest types, 268–270
Guest VLANs, 67
Guest WLANs
AAA Servers tab, 130–131
Advanced tab, 132–134
General tab, 128–129
Layer 2 Security tab, 129
Layer 3 Security tab, 130
overview of, 127–128

H

hashing, 441–443
Health Insurance Portability and Accountability Act (HIPAA), 466
high availability
configuration, 83–86
RADIUS fallback, 120–121
HIPAA (Health Insurance Portability and Accountability Act), 466
Host Input API (FMC), 421–422
Host Input Client menu, Create Client command, 421
Host Scan module, 566–570
hotspot portals, 278–279
HTTP (Hypertext Transfer Protocol). ***See also*** **RESTful APIs (application programming interfaces)**
profiling
with probes, 165–167
without probes, 167
redirection, 197
requests, 409
server configuration, 73
HTTPS (HTTP Secure), 73
hub-and-spoke design
DMVPN (Dynamic Multipoint VPN), 503–504, 513–514
hub EIGRP configuration, 508
hub interface configuration, 501–502
hub routing verification, 506
hub tunnel interface, 502
show dmvpn command, 504–505
spoke CEF adjacency, 508–509
spoke CEF punt, 509
spoke configuration, 503–504
spoke DMVPN and NHRP verification, 510
spoke routing configuration, 508
spoke routing verification, 506–507
spoke-to-spoke trace route, 507, 509

EzVPN (Easy VPN)
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498
FlexVPN
dual-hub, dual-cloud hubs, 527–528
dual-hub, dual-cloud spokes, 527–528
hub virtual access interface verification, 529
spoke routing and interface verification, 530
SPOKE1 configuration, 516–517
spoke-to-spoke tunnel verification, 530–532
Hyper-V Live Migration, 602–603

I

IBM Tivoli Identity Manager (TIM), 33
ICMP (Internet Control Message Protocol), 499
Id Groups section (Network Access work center), 35
Identities section (Network Access work center), 34
Identity PSK (IPSK), 447
Identity Resolution setting, 47
Identity Rewrite setting, 47
Identity Services Engine. *See* ISE (Identity Services Engine)
Identity Source Sequences tab (Network Access work center), 48–50
identity sources
AD (Active Directory), 32–33
configuration
advanced settings, 44–47
attributes, 44
CAPs (Certificate Authentication Profiles), 47–48
groups, 42–44
joining to domains, 37–40
passive identity, 41
whitelisted domains, 41
Identity Groups, 178–179
inner, 59
LDAP (Lightweight Directory Access Protocol), 33
ODBC (Open Database Connectivity), 33
outer, 59
overview of, 29–32
passive, 41, 47, 180–181
RADIUS Token service, 33
RSA SecurID, 34
rules, 379–382
SAML (Security Assertion Markup Language) ID providers, 34
sequences, 48–50
identity stores, 48
IEEE (Institute of Electrical and Electronics Engineers), 7, 470–473. *See also* 802.1X
IKE_AUTH messages, 457
IKE_SA_INIT messages, 457
IKEv1 (Internet Key Exchange version 1)
IPsec with, 478–484
Aggressive mode, 478–479
ASA configuration, 484
basic IPsec network, 478
crypto map sets, 479–480
debugging, 481–484
interesting traffic ACL, 479
ISAKMP policy, 478
transform set, 479
tunnel establishment, 480
validation, 480–481
PFS (Perfect Forward Secrecy), 455–456
Phase 1, 453–454
Phase 2, 455
IKEv2 (Internet Key Exchange version 2)

IPsec IKEv2 VPN example, 580–586
IPsec with
Cisco IOS NTP and CA configuration, 484–486
IKEv2 configuration for ASA, 489–491
IKEv2 peer NTP synchronization and certificate SCEP enrollment, 487–489
validation, 491–492
overview of, 456–458
IND (Industrial Network Director), 363
infrastructure VPNs. *See* VPNs (virtual private networks)
inline tagging, 294–295
inner identities, 59
INSIDE router configuration (FlexVPN), 515
Institute of Electrical and Electronics Engineers. *See* IEEE (Institute of Electrical and Electronics Engineers)
Integrated Services Routers (ISR), 606
integration
MDM (mobile device management), 356
Rapid Threat Containment, 356–359
Integrations command (Policies menu), 436
interesting traffic ACL, 479
interface range command, 83
interfaces
for client VLANs
employee interfaces, 124–125
guest interfaces, 125–127
overview of, 124
PCI interfaces, 127
configuring as switch ports, 83
Interim Updates option (Cisco WLC), 137
intermediate CAs (certificate authorities), 449–450
Internet Security Association and Key Management Protocol (ISAKMP)
Aggressive mode, 478–479
IPsec with IKEv1, 478
overview of, 459
"Introduction to DevNet" Learning Lab, 412
Intrusion Events command (Analysis menu), 423
Investigate API, 436
IOS Catalyst switches, configuration of
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
verification
show aaa servers command, 140–141
show authentication session interface command, 142–143
syslog messages, 143–145
test aaa servers command, 141–142
IOS device administration
accounting, 329
command authorization, 325–329
debugging, 331
live logs, 330–331
login authentication and authorization, 319–325
overview of, 318–319
privilege levels, 319–325

Shell Profiles, 322–323
verification, 329–331
IOS validation of VPN sessions, 568–586
IOS virtual access interface, 518
ip access-list command, 78
ip access-list ext command, 78–79, 94–95
ip access-list extended ACL-ALLOW command, 94
ip device tracking command, 79, 96, 141, 197
IP Device Tracking (IPDT), 197
ip domain-name command, 73, 91
ip helper-address command, 155–157
ip http active-session-modules none command, 91
ip http secure-active-session-modules none command, 91
ip http secure-server command, 73, 91, 196
ip http server command, 73, 91, 196
ip nhrp shortcut command, 511
ip radius source-interface command, 78
IPDT (IP Device Tracking), 197
IPsec
AH (Authentication Header) packets, 459
crypto map sets, 461
ESP (Encapsulating Security Payload) packets, 460
with IKEv1, 478–484
Aggressive mode, 478–479
ASA configuration, 484
basic IPsec network, 478
crypto map sets, 479–480
debugging, 481–484
interesting traffic ACL, 479
ISAKMP policy, 478
transform set, 479
tunnel establishment, 480
validation, 480–481
with IKEv2
Cisco IOS NTP and CA configuration, 484–486
IKEv2 configuration for ASA, 489–491
IKEv2 peer NTP synchronization and certificate SCEP enrollment, 487–489
IPsec IKEv2 VPN example, 580–586
validation, 491–492
overview of, 453
Transport mode encryption, 459
Tunnel mode encryption, 459
VPNs (virtual private networks), 461–462
ipsec-isakmp command, 462
ipsec-manual command, 462
IPSK (Identity PSK), 447
ISAKMP (Internet Security Association and Key Management Protocol), 459
Aggressive mode, 478–479
DMVPN (Dynamic Multipoint VPN), 501
IPsec with IKEv1, 478
ISE (Identity Services Engine). *See also* device administration; network access control; pxGrid
APIs (application programming interfaces)
ERS (External RESTful Services) API, 426–428
Monitoring REST API, 424–425
overview of, 424
BYOD (bring your own device) onboarding, 197–198
building blocks of BYOD solutions, 198–200
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
Dual SSID provisioning, 200–202
end-user experience, 229–235

network device configuration, 223–228
NSPs (Native Supplicant Profiles), 204, 207–208
overview of, 197–198
policy sets and rules, 216–223
portals for, 212–216
SCEP (Simple Certificate Enrollment Protocol) RA profiles, 205–207
Single SSID provisioning, 200–202
SPWizards, 203, 209–210
verification, 229–235
C3PL switch configuration
802.1X commands, 95–96
advantages of, 89–90
configuration hierarchy, 96
enabling switches, 88
global configuration, 91–92
local access control lists, 94–95
policies, 97–100
RADIUS commands for, 92–94
service templates, 95
Catalyst switch configuration
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
switch types, 71–72
centralized AAA, case for, 307–308
EasyConnect
overview of, 183–186
WMI (Windows Management Instrumentation), 185–191
guest access
guest types, 268–270
hotspot portals, 278–279
network device configuration, 268
overview of, 265–268
policy sets for, 284–287
self-registered portals, 279–284
sponsor groups, 270–273
sponsor portals, 274–276
identity sources
AD (Active Directory), 32–33
advanced settings, 44–47
attributes, 44
CAPs (Certificate Authentication Profiles), 47–48
groups, 42–44
joining to domains, 37–40
LDAP (Lightweight Directory Access Protocol), 33
ODBC (Open Database Connectivity), 33
overview of, 29–32
passive identity, 41
RADIUS Token service, 33
RSA SecurID, 34
SAML (Security Assertion Markup Language) ID providers, 34
sequences, 48–50
whitelisted domains, 41
MDM (mobile device management) onboarding
MDM server, adding, 239–240
overview of, 236–238
MNT (Monitoring Node), 143
network access architecture

distributed deployment, 22–23, 29–32
dual-node deployment, 19–20, 25–28
multinode deployment, 21–22
personas, 18–19
standalone deployment, 19, 24–25
Network Access work center
Active Directory configuration, 37–47
Identity Source Sequences tab, 48–50
Network Resources, 50–54
overview of, 34–36
network resources
default devices, 53–54
external RADIUS servers, 54
NADs (network access devices), 51–53
NDGs (Network Device Groups), 50–51
overview of, 50
overview of, 5, 17–18, 435–437
passive authentication
active authentication versus, 181–183
EasyConnect, 183–186
passive identities, 180–181
posture assessment
AnyConnect provisioning, 246, 249–255
overview of, 244–246
policy sets, 262–265
posture policy configuration, 255–262
prerequisite configuration tasks, 247–249
Profiler
Active Directory probes, 164–165
CoA (Change of Authorization), 175–177
context visibility, 171–174
DHCP and DHCPSPAN probes, 155–158
DNS probes, 162
Endpoint Identity Groups, 178–179
endpoint probe, 190–191
endpoint profile policies, 170–171
global settings, 177–178
HTTP probes, 165–167
HTTP profiling without probes, 167
logical profiles, 174–175
NETFLOW probes, 167–168
NMAP probes, 159–162
overview of, 149–152
passive authentication, 181–183
probe configuration, 153–155
profiling feed service, 168–170
pxGrid probes, 168
RADIUS probes, 158–159
SNMPQUERY and SNMPTRAP probes, 163–164
work center, 153
root certificates, 390–394
StealthWatch, 357
advantages of, 397–398
configuration for ISE, 402–406
CSR (certificate signing request), 399–402
syslog messages, 143–145
TrustSec
enforcement, 300–306
overview of, 287–288
propagation, 292–300
SGTs (Security Group Tags), 288–292
verification, 147–148
wired network access control

default policy sets and rules, 100–102
differentiated access policy, creating, 102–115
wireless network access control
AAA server configuration, 118–121
AireOS, 116–117
Airespace ACLs, 121–123
Corporate WLANs, 134–138
dynamic interfaces for client VLANs, 124–127
Guest WLANs, 127–134
ISE configuration for, 138–140
overview of, 115–116
ISR (Integrated Services Routers), 606
ISSs (identity source sequences), 48–50

J

Jabber, 360
join points, 37
joining to domains, 37–40

K

KEK (key encryption key), 466
key servers. *See* KSs (key servers)
keys. *See also* cryptography
API
AMP (Advanced Malware Protection) APIs, 429–431
Threat Grid APIs, 433
Umbrella APIs, 436
authentication
certificate expiration, 451–452
certificate revocation, 452–453
certificate trust relationship, 449–450
OTPs (one-time passwords), 447
PSKs (preshared keys), 447
username/password combinations, 447
X.509 PKI (Public Key Infrastructure), 448–449
crypto keyrings, 501
Diffie-Hellman key exchange, 458–459
KEK (key encryption key), 466
private, 445–446
public, 445–446
TEK (traffic encryption key), 466
keywords. *See individual keywords*
KSs (key servers), 535
group member configuration, 535
group member validation, 538–540
key server and group member status validation, 535–536
key server policy and ACL validation, 536–538
overview of, 467
primary key server configuration, 532–534

L

Lancope, 167, 357
LANs (local area networks). *See* WLANs (wireless LANs)
Layer 2 Security tab
Corporate WLANs, 136
Guest WLANs, 129
Layer 3 Security tab
Corporate WLANs, 136
Guest WLANs, 130
LDAP (Lightweight Directory Access Protocol), 33
least privilege access rules, 102–103
lists, method, 320–321
default, 326
named, 321

Live Authentications Log, 147–148
Lobby role (WLC), 335
local access control lists
Catalyst switch configuration, 78–79
local access control lists, 94–95
Local Web Authentication (LWA)
with centralized web portals, 67–69
overview of, 66–67
logging commands, 79–80, 144–145
logical profiles, 174–175
logins, Cisco IOS devices
authentication and authorization, 319–325
debugging, 331
privilege levels, 319–325
Shell Profiles, 322–323
logoff detection, WMI (Windows Management Instrumentation), 190–191
logs
Live Authentications Log, 147–148
TACACS+ (Terminal Access Controller Access Control System Plus), 330–331
LWA (Local Web Authentication)
with centralized web portals, 67–69
overview of, 66–67

M

MAB (MAC Authentication Bypass), 62–65, 150
Critical MAB, 89
verification
with Cisco WLC (Wireless LAN Controller), 145–147
endpoint supplicant verification, 140
network access device verification, 140–145
overview of, 140
MAC address management (MAM) model, 179
MAC Authentication Bypass. *See* MAB (MAC Authentication Bypass)
Machine Access Restrictions (MAR), 45–47
Machine Authentication, 44
MacOsXSPWizard, 210
MACsec, 470–473
macsec access-control command, 472
MACSec Policy setting (authorization profiles), 105
Main mode (IKEv1), 454
malicious destinations, blocking, 435–437
malware, protection against
AMP (Advanced Malware Protection) APIs, 428–432
Threat Grid APIs, 433–435
MAM (MAC address management) model, 179
mapping, VLAN, 563
MAR (Machine Access Restrictions), 45–47
McAfee, 160
MD5 algorithm, 57, 442
MDM (mobile device management) onboarding
MDM integration, 356
MDM server, adding in ISE, 236–240
overview of, 236–238
policy sets and rules, 240–244
messages
CoA (Change of Authorization), 14–15
syslog, 143–145
TACACS+ (Terminal Access Controller Access Control System Plus), 8–10
method lists, 320–321
default, 326
named, 321
MFA (Multifactor authentication) systems, 33

mGRE (Multipoint GRE), 462–463
micro-segmentation, ACI and
application network profiles, 610
contracts, 612
device packages, 609–610
endpoint groups, 610–611
object models, 609–610
overview of, 608–609
service graphs, 612–613
Microsoft AD (Active Directory). *See* AD (Active Directory)
Microsoft CHAP (MS-CHAP), 6
mismatched authentication errors, 482–483
mismatched ISAKMP policy, 482–483
MNT (Monitoring Node), 18, 143
mobile device management. *See* MDM (mobile device management) onboarding
mobile workers, 544. *See also* RAVPN (Remote Access VPN)
modules, remediation, 415–420
module.template file, 417–418
monitoring clients, 145–146
Monitoring Node (MNT), 18, 143
monitoring persona, 18
Monitoring REST API (ISE), 424–425
Moreno, Jose, 608–609
MS-CHAP (Microsoft CHAP), 6, 57, 59
multifactor authentication (MFA) systems, 33
multinode ISE deployment, 21–22
Multipoint GRE (mGRE), 462–463
Murray, Chris, 44

N

NADs (network access devices)
overview of, 6, 50, 51–53
verification
show aaa servers command, 140–141
show authentication session interface command, 142–143
syslog messages, 143–145
test aaa servers command, 141–142
named method lists, 321
native EAP types, 57–58
Native Supplicant Profiles (NSPs), 204, 207–208
NDAC (Network Device Admission Control), 472–473
NDGs (Network Device Groups), 50–51
NDS (Novell Directory Services), 33
NETFLOW, 167–168
NetIQ eDirectory, 33
netsh ras set tracing * enable command, 140
network access control, 6–7. *See also* ISE (Identity Services Engine); network access, extending
802.1X
authentication servers, 55
authenticators, 55
components of, 54–56
EAP (Extensible Authentication Protocol), 56–61
MAB (MAC Authentication Bypass), 62–65
supplicants, 55
Web Authentication, 65–71
C3PL switch configuration
802.1X commands, 95–96
advantages of, 89–90
configuration hierarchy, 96
enabling switches, 88
global configuration, 91–92
local access control lists, 94–95
policies, 97–100
RADIUS commands for, 92–94
service templates, 95

Catalyst switch configuration
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
switch types, 71–72
concept of, 6–7
definition of, 4
EasyConnect
overview of, 183–186
WMI (Windows Management Instrumentation), 185–191
identity sources
AD (Active Directory), 32–33
advanced settings, 44–47
attributes, 44
CAPs (Certificate Authentication Profiles), 47–48
groups, 42–44
joining to domains, 37–40
LDAP (Lightweight Directory Access Protocol), 33
ODBC (Open Database Connectivity), 33
overview of, 32
passive identity, 41
RADIUS Token service, 33
RSA SecurID, 34
SAML (Security Assertion Markup Language) ID providers, 34
sequences, 48–50
whitelisted domains, 41
ISE APIs (application programming interfaces)
ERS (External RESTful Services) API, 426–428
Monitoring REST API, 424–425
overview of, 424
ISE deployments
distributed, 22–23, 29–32
dual-node, 19–20, 25–28
multinode, 21–22
personas, 18–19
standalone, 19, 24–25
Network Access work center
Active Directory configuration, 37–47
Identity Source Sequences tab, 48–50
Network Resources, 50–54
overview of, 34–36
network resources
default devices, 53–54
external RADIUS servers, 54
NADs (network access devices), 51–53
NDGs (Network Device Groups), 50–51
overview of, 50
passive authentication
active authentication versus, 181–183
EasyConnect, 183–186
passive identities, 180–181
profiling
Active Directory probes, 164–165
CoA (Change of Authorization), 175–177
context visibility, 171–174
DHCP and DHCPSPAN probes, 155–158

DNS probes, 162
Endpoint Identity Groups, 178–179
endpoint probes, 190–191
endpoint profile policies, 170–171
global settings, 177–178
HTTP probes, 165–167
HTTP profiling without probes, 167
logical profiles, 174–175
NETFLOW probes, 167–168
NMAP probes, 159–162
overview of, 149–152
passive authentication, 181–183
probe configuration, 153–155
profiling feed service, 168–170
pxGrid probes, 168
RADIUS probes, 158–159
SNMPQUERY and SNMPTRAP probes, 163–164
work center, 153
RADIUS (Remote Authentication Dial-In User Service), 4–5
accounting messages, 14–15
authentication messages, 13–14
authorization messages, 13–14
AV (attribute-value) pairs, 15
CoA (Change of Authorization), 14–15
Layer 2 EAP communication, 12–13
purpose of, 6–7
TACACS+ compared to, 16
URL redirection, 189
wired
default policy sets and rules, 100–102
differentiated access policy, creating, 102–115
wireless
802.1X and MAB verification, 140–148
AAA server configuration, 118–121
AireOS, 116–117
Airespace ACLs, 121–123
Corporate WLANs, 134–138
dynamic interfaces for client VLANs, 124–127
Guest WLANs, 127–134
ISE configuration for, 138–140
overview of, 115–116
network access devices (NADs), 6, 50, 51–53
network access, extending. ***See also*** **network access control**
BYOD onboarding with ISE
building blocks of BYOD solutions, 198–200
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
Dual SSID provisioning, 200–202
end-user experience, 229–235
network device configuration, 223–228
NSPs (Native Supplicant Profiles), 204, 207–208
overview of, 197–198
policy sets and rules, 216–223
portals for, 212–216
SCEP (Simple Certificate Enrollment Protocol) RA profiles, 205–207
Single SSID provisioning, 200–202
SPWizards, 203, 209–210
verification, 229–235
guest access
guest types, 268–270
hotspot portals, 278–279

network device configuration, 268
overview of, 265–268
policy sets for, 284–287
self-registered portals, 279–284
sponsor groups, 270–273
sponsor portals, 274–276
MDM (mobile device management) onboarding
MDM server, adding, 239–240
overview of, 236–238
posture assessment
AnyConnect provisioning, 249–255
overview of, 244–246
policy sets, 262–265
posture policy configuration, 255–262
prerequisite configuration tasks, 247–249
prerequisites
AAA configuration, 197
BYOD onboarding with ISE, 197–198
URL Redirection, 194–197
TrustSec
enforcement, 300–306
overview of, 287–288
propagation, 292–300
SGTs (Security Group Tags), 288–292
Network Access work center
Active Directory configuration
Advanced Settings tab, 44–47
attributes, 44
groups, 42–44
joining domains, 37–40
PassiveID tab, 41
Whitelisted Domains tab, 41
Identity Source Sequences tab, 48–50
overview of, 34–36
Network Device Admission Control (NDAC), 472–473
Network Device Groups (NDGs), 50–51
Network Device Registration API, 435
Network Discovery command (Policies menu), 421
Network Functions Virtualization (NFV), 605–607
Network Mapper. *See* NMAP (Network Mapper)
Network Policy mode (service graphs), 612
network resources
default devices, 53–54
external RADIUS servers, 54
NADs (network access devices), 51–53
NDGs (Network Device Groups), 50–51
overview of, 50
Network Resources command (Device Administration menu), 312
Network Resources (Network Access work center)
default devices, 53–54
external MDM servers, 54
external RADIUS servers, 54
NADs (network access devices), 51–53
NDGs (Network Device Groups), 50–51
overview of, 50
Network Resources section (Network Access work center), 35
Network Scan (NMAP) probes
configuration, 160–162
considerations with, 160
overview of, 159–160
Network Service Header (NSH), 603–605
Network Services Controller (NSC), 602–603
Network Setup Assistant (NSA), 122
Network Time Protocol. *See* NTP (Network Time Protocol)
Network Visibility Module, 546

Network World blog, 44
New API Credential command, 429
Next Hop Resolution Protocol. ***See*** **NHRP (Next Hop Resolution Protocol)**
Nexus 1000V Virtual Supervisor Module (VSM), 602–603
NFV (Network Functions Virtualization), 605–607
NGIPSv, 602
NHRP (Next Hop Resolution Protocol)
DMVPN NHRP configuration
Phase 1, 505–506
Phase 2, 510
Phase 3, 510–513
overview of, 463
NMAP (Network Mapper)
NMAP Scan Subnet Exclusions, 178
probes
configuration, 160–162
considerations with, 160
overview of, 159–160
No CoA option, 176
no server command, 320
nodes
ISE deployments
distributed, 22–23, 29–32
dual-node, 19–20, 25–28
multinode, 21–22
personas, 18–19
standalone, 19, 24–25
MNT (Monitoring Node), 18, 143
PANs (policy admin nodes), 18
PSNs (Policy Services Nodes), 18–19
TC-NAC (Threat-Centric NAC), 19
Novell Directory Services (NDS), 33
NSA (Network Setup Assistant), 122
NSC (Network Services Controller), 602–603
NSH (Network Service Header), 603–605
NSPs (Native Supplicant Profiles), 204, 207–208
NTP (Network Time Protocol)
IKEv2 configuration, 484–486
IKEv2 peer NTP synchronization and certificate SCEP enrollment, 487–489

O

object models, 609–610
OCSP (Online Certificate Status Protocol), 448, 452
ODBC (Open Database Connectivity), 33
ODR (On-Demand Routing), 463
OGS (Optimal Gateway Selection), 550
OIM (Oracle Identity Manager), 33
Okta Universal Directory (UD), 33
onboarding
BYOD (bring your own device), 197–198
building blocks of BYOD solutions, 198–200
certificate templates, 205–207
CPP (Client Provisioning Policy), 203–204, 210–212
Dual SSID provisioning, 200–202
end-user experience, 229–235
network device configuration, 223–228
NSPs (Native Supplicant Profiles), 207–208
overview of, 197–198
policy sets and rules, 216–223
portals for, 212–216
SCEP RA profiles, 205–207
Single SSID provisioning, 200–202
SPWizards, 209–210
verification, 229–235
MDM (mobile device management)
MDM server, adding in ISE, 236–240

overview of, 236–238
policy sets and rules, 240–244
On-Demand Routing (ODR), 463
one-time passwords (OTPs), 447
one-way encryption, 483
Online Certificate Status Protocol (OCSP), 448, 452
online users (FMC), viewing, 383–384
Open Authentication, 86–87
Open Database Connectivity (ODBC), 33
Open Shortest Path First (OSPF), 463
Optimal Gateway Selection (OGS), 550
Oracle Identity Manager (OIM), 33
OSPF (Open Shortest Path First), 463
OTA (over-the-air) provisioning, 203
OTPs (one-time passwords), 447
outer identities, 59
over-the-air (OTA) provisioning, 203
Overview command (Device Administration menu), 312, 330
Overview section (Network Access work center), 34
OWN_ACCOUNTS group, 271

P

packages, device, 609–610
packets
AH (Authentication Header), 459
ESP (Encapsulating Security Payload), 460
PACs (Protected Access Credentials), 59
PANs (policy admin nodes), 18
PAP (Password Authentication Protocol), 6
participants (pxGrid)
FMC (Firepower Management Center) configuration, 369–376
access rules, 379–382
active users, viewing, 383–384
correlation rules, 384–389
Rapid Threat Containment, 384–389
realms, 376–379
remediation modules, 384–389
overview of, 368–369
PASS_ADD message (TACACS+), 11
PASS_REPL message (TACACS+), 11
passive authentication
active authentication versus, 181–183
EasyConnect, 183–186
passive identities, 180–181
passive identities, 41, 47, 180–181
Passive Identity Tracking setting (authorization profiles), 106
PassiveID, 41, 47
Password Authentication Protocol (PAP), 6
passwords
certificate expiration, 451–452
certificate revocation, 452–453
certificate trust relationship, 449–450
OTPs (one-time passwords), 447
PAP (Password Authentication Protocol), 6
username/password combinations, 447
X.509 PKI (Public Key Infrastructure), 448–449
PATCH requests (HTTP), 409
PCI DSS (Payment Card Industry Data Security Standard), 466
PCI dynamic interfaces, 127
PEAP (Protected EAP), 58–59, 61
peer routers (FlexVPN), 522
Perfect Forward Secrecy (PFS), 455–456
permit statement, 121, 195–196
personas
distributed deployment, 22–23, 29–32
dual-node deployment, 19–20, 25–28

multinode deployment, 21–22
overview of, 18–19
standalone deployment, 19, 24–25
PFS (Perfect Forward Secrecy), 455–456
Phase 1 (DMVPN)
hub routing verification, 506
overview of, 506–507
spoke routing verification, 506–507
spoke-to-spoke trace route, 507
Phase 2 (DMVPN)
hub EIGRP configuration, 508
overview of, 508–510
spoke CEF adjacency, 508–509
spoke CEF punt, 509
spoke DMVPN and NHRP verification, 510
spoke routing configuration, 508
spoke-to-spoke trace route, 509
tunnel interface changes, 508
Phase 3 (DMVPN)
DMVPN and NHRP verification, 512–513
NHRP redirect and summary address, 510–511
NHRP routes verification, 512
NHRP shortcut and routing verification, 511
overview of, 510–513
trace route and NHRP redirect, 511–512
ping command
EzVPN (Easy VPN), 499
FlexVPN, 517, 520, 523, 530
IKEv1 tunnel establishment, 477
IKEv2 validation, 491
PingID, 33
PKI (Public Key Infrastructure), 445–446, 448–449
plain old telephone service (POTS), 6
platform exchange grid. *See* pxGrid
plug-ins, 593
Point-to-Point Protocol (PPP), 12
policies. *See also* configuration
ANC (Adaptive Network Control), 358–359, 403–406
BYOD (bring your own device) onboarding
CPP (Client Provisioning Policy), 203–204, 210–212
policy sets and rules, 216–223
C3PL switch configuration
control class configuration, 97–98
control policy application, 99–100
control policy configuration, 98–99
overview of, 97
clientless VPNs (virtual private networks), 592, 594
differentiated access, 112–115
FMC (Firepower Management Center) for pxGrid, 379–382
guest access, 284–287
IKEv1 ISAKMP, 478
MDM (mobile device management) onboarding, 240–244
policy admin persona, 18
policy services persona, 18–19
posture assessment
policy rules, 261–262
posture conditions, 256–258
posture requirements, 260–261
remediation actions, 258–260
required elements, 255
primary key servers, 536–538
profiling
context visibility, 171–174
endpoint, 170–171
global CoA (Change of Authorization), 176–177
logical, 174–175
overview of, 168
profiling feed service, 168–170

RAVPN with ASA
DAP (dynamic access policies), 565–566
group policies, 562–565
RAVPN with FTD, 574
TACACS+ (Terminal Access Controller Access Control System Plus)
Allowed Protocols, 314
Conditions, 314, 318
policy elements, creating, 314–316
policy sets and rules, creating, 316–318
Results, 314, 318
TACACS+ Profiles, 315
TrustSec
policy configuration in ISE, 300–302
policy download, 302–305
tag-based ACLs, 305
tag-based policies on Cisco NGFW, 305–306
wired network access control, 100–102
default policy sets and rules, 100–102
differentiated access policy, creating, 102–115
WSA (Web Security Appliance), 394–397

Policies menu
Actions command, 419
Correlation command, 420
Integrations command, 436
Network Discovery command, 421

Policy Elements command (Device Administration menu), 314

Policy Elements section (Network Access work center), 35

Policy Service, 310–312

Policy Services Node (PSNs), 18–19

Policy Sets section (Network Access work center), 36

policy static sgt command, 294

policy-map type control subscriber DOT1X-DEFAULT command, 98

Port Bounce CoA option, 176–177

port command, 320

portals
for BYOD (bring your own device) onboarding, 212–216
customization of, 594
hotspot, 278–279
self-registered, 279–284
sponsor, 274–276

ports
configuring interfaces as, 83
ePO (ePolicy Orchestrator) ports, 160
TCP port 49, 8

POST requests (HTTP), 409

Postman tool, 410–412

posture assessment
AnyConnect provisioning, 246, 249–255
overview of, 244–246
posture policy configuration
policy rules, 261–262
policy sets, 262–265
posture conditions, 256–258
posture requirements, 260–261
remediation actions, 258–260
required elements, 255
prerequisite configuration tasks, 247–249
RAVPN with ASA, 567–570

Posture module, 566–570

POTS (plain old telephone service), 6

PPP (Point-to-Point Protocol), 12

preshared keys (PSKs), 447

primary key servers
configuration, 532–534
policies, 536–538

private keys, 445–446

privilege levels, Cisco IOS devices, 319–325

probes, profiling

Active Directory probes, 164–165
configuration, 153–155
DHCP and DHCPSPAN
DHCP logical design, 155
DHCP SPAN logical design, 156–157
overview of, 155–158
probe configuration, 157–158
WLC considerations, 157
DNS, 162
endpoint, 190–191
HTTP, 165–167
HTTP profiling without probes, 167
NETFLOW, 167–168
NMAP
configuration, 160–162
considerations with, 160
overview of, 159–160
pxGrid, 168
RADIUS, 158–159
SNMPQUERY and SNMPTRAP, 163–164
Profiler Editor (AnyConnect), 547–552
profiles. *See also* policies
AnyConnect, 246, 249–255
application network, 610
authorization, 178–179
creating, 103–109
RADIUS (Remote Authentication Dial-In User Service), 346–347
CAPs (Certificate Authentication Profiles), 47–48
CoA (Change of Authorization), 175–177
commands, 81–82
EasyConnect
overview of, 183–186
WMI (Windows Management Instrumentation), 185–191
global profiler settings, 177–178
endpoint attribute filtering, 177–178
NMAP Scan Subnet Exclusions, 178
SNMP settings, 177
NSPs (Native Supplicant Profiles), 204, 207–208
overview of, 149–152
passive authentication
active authentication versus, 181–183
EasyConnect, 183–186
passive identities, 180–181
probes
Active Directory probes, 164–165
configuration, 153–155
DHCP and DHCPSPAN, 155–158
DNS, 162
HTTP, 165–167
NETFLOW, 167–168
NMAP, 159–162
overview of, 153
pxGrid, 168
RADIUS, 158–159
SNMPQUERY and SNMPTRAP, 163–164
SCEP (Simple Certificate Enrollment Protocol) RA profiles, 205–207
Shell Profiles
Cisco IOS devices, 322–323
WLC (Wireless LAN Controller), 339–340
propagation (TrustSec)
inline tagging, 294–295
overview of, 292–294
SXP (SGT Exchange Protocol) configuration, 295–300
Protected Access Credentials (PACs), 59
protocols. *See individual protocols*
provisioning
AnyConnect, 246, 249–255
Dual SSID, 200–202
Single SSID, 200–202

proxies, RADIUS-Proxy, 54
PSKs (preshared keys), 447
PSNs (Policy Services Nodes), 18–19
PSStatus conditions, 357
Public Key Infrastructure (PKI), 445–446, 448–449
publishers (pxGrid), 360
PUT requests (HTTP), 409
pxGrid
CAs (certificate authorities), 362–363
certificates
ISE root certificates, 390–394
overview of, 364–365, 369–375
StealthWatch CSR, 399–402
components of, 361
context-in, 363
context-out, 363
controllers, 360
FMC (Firepower Management Center) configuration, 369–376
access rules, 379–382
active users, viewing, 383–384
correlation rules, 384–389
Rapid Threat Containment, 384–389
realms, 376–379
remediation modules, 384–389
ISE configuration for, 364–367
ISE profiling probes, 168
overview of, 359–361
participant configuration, 368–369
publishers, 360
StealthWatch
advantages of, 397–398
configuration for ISE, 402–406
CSR (certificate signing request), 399–402
subscribers, 360
topics, 360
trust between participants, 362–363
WSA (Web Security Appliance) configuration
ISE root certificates, 390–394
overview of, 390
policies, 394–397
WSA and ISE integration, 390–394

Q-R

RADIUS (Remote Authentication Dial-In User Service), 4–5
accounting messages, 14–15
authentication messages, 13–14
authorization messages, 13–14
AV (attribute-value) pairs, 15
on Cisco ESA (Email Security Appliance)
ESA configuration, 349–351
ISE configuration, 351
overview of, 343–344
verification, 351
on Cisco FMC (Firepower Management Center)
FMC configuration, 344–346
ISE configuration, 346–348
overview of, 343–344
verification, 349
on Cisco WSA (Web Security Appliance)
ISE configuration, 351
overview of, 343–344
verification, 351
WSA configuration, 349–351
CoA (Change of Authorization), 14–15
commands
C3PL switches, 92–94
Catalyst switches, 74–78
external RADIUS servers, 54
ISE profiling probes, 158–159
Layer 2 EAP communication, 12–13
Live Authentications Log, 147–148

overview of, 343
purpose of, 6–7
RADIUS-Proxy, 54
server configuration
accounting servers, 119–120
authentication servers, 118–119
RADIUS fallback, 120–121
TACACS+ compared to, 16, 308–309
Token service, 33
RADIUS-Proxy, 54
radius-server attribute command, 77
radius-server dead-criteria time command, 75
radius-server host command, 75
Rapid Threat Containment
configuration, 384–389
overview of, 356–359
StealthWatch
advantages of, 397–398
configuration for ISE, 402–406
CSR (certificate signing request), 399–402
RAs (registration authorities), 448
RAVPN (Remote Access VPN)
with ASA (Adaptive Security Appliance)
AnyConnect VPN Wizard, 554–561
DAP (dynamic access policies), 565–566
group policies, 562–565
posture assessment, 567–570
Cisco AnyConnect Secure Mobility Client
deployment, 552–554
overview of, 546–547
Profile Editor, 547–552
clientless
configuration, 586–594
definition of, 545–546
with FTD (Firepower Threat Defense), 570–579
access control, 577–579
authentication method, 574
authentication servers, 571
certificates, 571
group policies, 574
interface and certificate configuration, 575–576
VPN client images, 573
VPN pool, 572
VPN profile, 572
overview of, 469–470, 543–545
with routers, 580
use cases, 544–545
RA-VPN (remote-access virtual private networks), 7
reactivation-mode timed command, 332
realms, 376–379
Reauth CoA option, 177
redirection
DMVPN (Dynamic Multipoint VPN), 510–512, 580–586
redirect ACLs (access control lists), 195–196
URL, 194–197
Web Authentication Redirection ACLs, 121–122
registration authorities (RAs), 448
REJECT message (TACACS+), 9
relationships, trust, 41
remediation (FMC)
built-in remediation modules, 415–416
configuration, 384–389
custom AMP4E remediation module, 416–420
data flow, 415
instance configuration, 419–420
module.template file, 417–418
overview of, 258–260, 414–420
Remote Access VPN. *See* RAVPN (Remote Access VPN)

Remote Authentication Dial-In User Service. *See* RADIUS (Remote Authentication Dial-In User Service)
remote-access virtual private networks (RA-VPN), 7
REPLY message, 8
Reports section (Network Access work center), 36
Representational State Transfer (REST), 361, 413–414
requests
HTTP (Hypertext Transfer Protocol), 409
TACACS+ (Terminal Access Controller Access Control System Plus), 10, 11
resolution, identity, 47
RESPONSE message (TACACS+), 10, 11
REST (Representational State Transfer), 361, 413–414
RESTful APIs (application programming interfaces)
accessing, 410
Cisco DevNet, 412
FMC (Firepower Management Center)
Database Access API, 422–423
eStreamer API, 423–424
Host Input API, 421–422
overview of, 413
remediation API, 414–420
REST API, 413–414
HTTP request types, 409–410
ISE (Identity Services Engine)
ERS (External RESTful Services) API, 426–428
Monitoring REST API, 424–425
overview of, 424
Postman tool, 410–412
results (TACACS+), 314, 318
revocation of certificates, 452–453
RIP (Routing Information Protocol), 463
Rivest, Ron, 442
roles, WLC (Wireless LAN Controller), 335–336
root CAs (certificate authorities), 449
Routing Information Protocol (RIP), 463
RSA SecurID, 34
rules
BYOD (bring your own device) onboarding, 216–223
FMC (Firepower Management Center)
correlation rules, 384–389
identity rules, 379–382

S

SAML (Security Assertion Markup Language), 34
SAN (Subject Alternative Name), 370
sandboxing, 433–435
Santuka, Vivek, 168
Save and Reboot command, 342
Scalable Group Tags. *See* SGTs (Security Group Tags)
Scan Subnet Exclusions (NMAP), 178
SCEP (Simple Certificate Enrollment Protocol), 205–207, 487–489
Secure Access Control Server, 7
Secure Hash Algorithm, 442
Secure Sockets Layer. *See* SSL (Secure Sockets Layer)
security. *See also* VPNs (virtual private networks)
cryptography
AH (Authentication Header) packets, 459
asymmetric encryption, 445–446
cipher types, 444
Diffie-Hellman, 458–459
ESP (Encapsulating Security Payload) packets, 460
hashing, 441–443
overview of, 441

symmetric encryption, 445
Transport mode encryption, 459
Tunnel mode encryption, 459
protocols
Diffie-Hellman, 458–459
DTLS (Datagram Transport Layer Security), 460
IKEv1 (Internet Key Exchange version 1), 453–456
IKEv2 (Internet Key Exchange version 2), 456–458
IPsec, 453, 459–460, 461–462
ISAKMP (Internet Security Association and Key Management Protocol), 459
SSL (Secure Sockets Layer), 460
TLS (Transport Layer Security), 460
SGTs (Security Group Tags), 563
assigning dynamically, 290–291
assigning manually, 291–292
classification, 288–290
inline tagging, 294–295
overview of, 288–290
preconfigured, 108–109
SXP (SGT Exchange Protocol) configuration, 295–300
virtualization
ACI (Application Centric Infrastructure), 608–613
advantages and limitations, 599–602
NFV (Network Functions Virtualization), 605–607
NSH (Network Service Header), 603–605
SFC (service function chaining), 603–605
VSG (Virtual Security Gateway), 602–603
Security Assertion Markup Language (SAML), 34
Security Group setting (authorization profiles), 106
Select Directory Groups, 42–44
Select Groups From Directory window, 42
self-registered portals, 279–284
sequences, identity source, 48–50
server command, 320
server name command, 320
servers. ***See also*** **ISE (Identity Services Engine); RADIUS (Remote Authentication Dial-In User Service); TACACS+ (Terminal Access Controller Access Control System Plus)**
802.1X authentication servers, 55
KSs (key servers), 535
group member configuration, 535
group member validation, 538–540
key server and group member status validation, 535–536
key server policy and ACL validation, 536–538
overview of, 467
primary key server configuration, 532–534
MDM (mobile device management), 236–240
monitoring, 140–141
virtualization
ACI (Application Centric Infrastructure), 608–613
advantages and limitations, 599–602
NFV (Network Functions Virtualization), 605–607
NSH (Network Service Header), 603–605
SFC (service function chaining), 603–605
VSG (Virtual Security Gateway), 602–603
service function chaining (SFC), 603–605

service graphs, 612–613
Service Manager mode (service graphs), 612
Service Policy mode (service graphs), 612
service set identifiers. ***See*** **SSID (service set identifier) provisioning**
service-policy command, 99
services
Device Admin Service, 310–312
Policy Service, 310–312
Session Service, 310–312
templates, 95
Session Service, 310–312
sets, policy. ***See*** **policies**
Settings section (Network Access work center), 36
SFC (service function chaining), 603–605
SFUA (Source Fire User Agent), 181
SGTs (Security Group Tags)
assigning dynamically, 290–291
assigning manually, 291–292
classification, 288–290
inline tagging, 294–295
overview of, 288–290, 563
preconfigured, 108–109
SXP (SGT Exchange Protocol) configuration, 295–300
sh crypto gdoi detail command, 538–540
sh crypto gdoi ks ac command, 537
sh crypto gdoi ks acl command, 537–538
sh crypto gdoi ks command, 535–536
sh crypto gdoi ks members summary command, 536
sh crypto gdoi ks policy command, 537
sh crypto ikev2 sa command, 491
sh crypto ipsec client ezvpn command, 497–498
sh crypto ipsec sa command, 492
sh derived-config interface Virtual-Access 1 command, 518
sh dmvpn command, 504–505
sh int Virtual-Access 1 command, 531
sh ip eigrp neighbors command, 506
sh ip int brief command, 529, 530, 531
sh ip interface brief command, 518
sh ip local pool command, 529
sh ip route command, 506, 508, 512, 518, 520, 523, 530, 531–532
sh run int tunn0 command, 513
SHA1 algorithm, 442
SHA2 algorithm, 442
Shamir, Adi, 442
Shell Profiles
Cisco IOS devices, 322–323
definition of, 315
WLC (Wireless LAN Controller), 335, 339–340
show aaa servers command, 140–141
show adjacency command, 509
show authentication session interface command, 142–143
show crypto ca certificates command, 488
show crypto ikev2 sa detail command, 585–586
show crypto ipsec sa command, 480–481, 483, 498, 540
show crypto isakmp policy command, 483
show crypto isakmp sa command, 498
show crypto isakmp sa detail command, 480–481
show crypto pki certificates command, 452
show crypto session command, 498
show crypto session detail command, 568–585
show cts environment-data command, 304–305
show cts interface command, 295

show cts sxp connections command, 296, 297
show dmvpn command, 504–505, 508, 510, 512–513
show interface Virtual-Access 1 command, 529
show interfaces command, 530
show ip cef command, 509
show ip nhrp command, 505, 508, 510, 512–513
show ip route command, 506–507
show ip route vrf INTERNET command, 506
show vpn-sessiondb detail anyconnect command, 558
show vpn-sessiondb detail l2l command, 518–519, 522–523
Simple Certificate Enrollment Protocol (SCEP), 205–207, 487–489
Simple Network Management Protocol. ***See*** **SNMP (Simple Network Management Protocol)**
single sign on (SSO), 34
Single SSID provisioning, 200–202
smart tunnels, 593
SNMP (Simple Network Management Protocol)
global profiler settings, 177
SNMPQUERY and SNMPTRAP probes, 163–164
snmp-server community command, 82
snmp-server enable traps mac-notification change move threshold command, 82
snmp-server host command, 82
snmp-server source-interface informs command, 78
snmp-server trap-source command, 78
Source Fire User Agent (SFUA), 181
Sourcefile Firepower, 181
spine-and-leaf topology, 608–609
split tunneling
EzVPN (Easy VPN)
client configuration, 495–497
client validation tunnel down, 497
client validation tunnel up, 497–498
dynamic VTI network, 492–493
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498
group policies, 563–564
spokes. ***See*** **hub-and-spoke design**
Sponsor_Portal_Sequence ID sequence group, 275
sponsors
groups, 270–273
portals, 274–276
SPWizards, 203, 209–210
SSID (service set identifier) provisioning
Dual, 200–202
Single, 200–202
SSL (Secure Sockets Layer), 460, 469–470
SSO (single sign on), 34
standalone ISE deployment, 19, 24–25
START message (TACACS+), 8, 11
statements
deny, 195–196
permit, 121, 195–196
StealthWatch, 357
advantages of, 397–398
configuration for ISE, 402–406
CSR (certificate signing request), 399–402
STOP message (TACACS+), 11
stores, identity, 48
stream ciphers, 444
Subject Alternative Name (SAN), 370
subscribers (pxGrid), 360
SUCCESS message (TACACS+), 11
sudo adi_cli session command, 383–384
summary address (DMVPN), 510–511

summary-address command, 507
supplicants
definition of, 55
NDAC (Network Device Admission Control), 472
verification of, 140
SVI (switch virtual interface), 196
switch configuration
C3PL switches
802.1X commands, 95–96
advantages of, 89–90
configuration hierarchy, 96
enabling, 88
global configuration, 91–92
local access control lists, 94–95
policies, 97–100
RADIUS commands for, 92–94
service templates, 95
Catalyst switches
802.1X commands, 79
AAA commands, 73–74
authentication settings, 86–87
authentication timers, 87–88
certificates on switch, 72–73
enabling authentication, 88
Flexible Authentication, 83–86
high availability, 83–86
HTTP/HTTPS server, 73
interfaces as switch ports, 83
local access control lists, 78–79
logging commands, 79–80
profiling commands, 81–82
RADIUS commands, 74–78
show aaa servers command, 140–141
show authentication session interface command, 142–143
switch types, 71–72
syslog messages, 143–145
test aaa servers command, 141–142
switch virtual interface (SVI), 196
switchport command, 83
switchport host command, 83
SXP (SGT Exchange Protocol) configuration, 295–300
symmetric encryption, 445
synchronization, IKEv2 peer NTP, 487–489
syslog messages, 143–145

T

TACACS Command Accounting command (Device Administration menu), 343
TACACS Livelogs command (Overview menu), 330
TACACS+ (Terminal Access Controller Access Control System Plus)
accounting messages, 11–12
authentication messages, 8–10
authorization messages, 10–11
with Cisco ASA (Adaptive Security Appliance), 331–335
with Cisco IOS devices
accounting, 329
command authorization, 325–329
debugging, 331
live logs, 330–331
login authentication and authorization, 319–325
overview of, 318–319
privilege levels, 319–325
Shell Profiles, 322–323
verification, 329–331
with Cisco WLC (Wireless LAN Controller)
ISE configuration, 338–342
roles, 335–336
verification, 342–343
WLC configuration, 336–337
client-server communication, 8

Command Sets policy element, 316
data flow, 309–310
ISE (Identity Services Engine) configuration for
network devices, adding, 312–313
overview of, 310
policy elements, 314–316
policy sets and rules, 316–318
TACACS+, enabling, 310–312
overview of, 4–5
Profiles policy element, 315
RADIUS compared to, 16, 308–309
Shell Profiles, 315
support for, 7–8

tags
SGTs (Security Group Tags)
assigning dynamically, 290–291
assigning manually, 291–292
classification, 288–290
inline tagging, 294–295
overview of, 288–290
preconfigured, 108–109
SXP (SGT Exchange Protocol) configuration, 295–300
tag-based ACLs (access control lists), 305
tag-based policies on Cisco NGFW, 305–306

TC-NAC (Threat-Centric NAC), 19
TCP (Transmission Control Protocol) ports, 8
TEK (traffic encryption key), 466
teleworkers, 544. *See also* RAVPN (Remote Access VPN)
templates
certificate, 205–207
service, 95

Terminal Access Controller Access Control System Plus. *See* TACACS+ (Terminal Access Controller Access Control System Plus)
test aaa servers command, 141–142
Third-Party Vulnerabilities command (Vulnerabilities menu), 422
Threat Grid APIs, 433–435
threat prevention
AMP (Advanced Malware Protection) APIs, 428–432
Threat Grid APIs, 433–435

Threat-Centric NAC (TC-NAC), 19
TIM (Tivoli Identity Manager), 33
timeout command, 320
timers, authentication, 87–88
Tivoli Identity Manager (TIM), 33
TLS (Transport Layer Security), 57, 59, 61, 460
TND (Trusted Network Detection), 550
topics (pxGrid), 360
traceroute command, 507, 509, 512
Track Movement setting (authorization profiles), 106
traffic encryption key (TEK), 466
transform set
DMVPN (Dynamic Multipoint VPN), 501
IPsec with IKEv1, 479

Transport Layer Security (TLS), 460
Transport mode encryption, 459
Transportation Security Administration (TSA), 3
Triple-A. *See* AAA (authentication, authorization, and accounting)
Troubleshoot section (Network Access work center), 36
troubleshooting. *See* debugging
trust relationships, 41, 449–450
trusted keyword, 294
Trusted Network Detection (TND), 550
TrustSec
ACI policy plane integration, 610–611
enforcement
overview of, 300
policy configuration in ISE, 300–302

policy download, 302–305
tag-based ACLs, 305
tag-based policies on Cisco NGFW, 305–306
overview of, 287–288
propagation
inline tagging, 294–295
overview of, 292–294
SXP (SGT Exchange Protocol) configuration, 295–300
SGTs (Security Group Tags)
assigning dynamically, 290–291
assigning manually, 291–292
classification, 288–290
overview of, 288–290
preconfigured, 108–109
TSA (Transportation Security Administration), 3
Tunnel mode encryption, 459
tunnel-group commands, 554
tunneling
DMVPN (Dynamic Multipoint VPN), 508
EzVPN (Easy VPN)
client validation tunnel down, 497
client validation tunnel up, 497–498
FlexVPN, 530–532
IPsec with IKEv1, 480
smart, 593
split
client configuration, 495–497
client validation tunnel down, 497
client validation tunnel up, 497–498
dynamic VTI network, 492–493
group policies, 563–564
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498
tunneled EAP types, 58–60
VTI (Virtual Tunnel Interface), FlexVPN with
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
router routing and ping test, 523
validation, 522–523

U

UCS (Unified Computing System), 606
UD (Universal Directory), 33
Umbrella APIs, 435–437
Umbrella Roaming Security, 546
Unified Communications Manager, 360
Unified Endpoint Management. *See* MDM (mobile device management) onboarding
Universal Directory (UD), 33
universal groups, 42
uplink MACsec, 472
URLs
for ACL bypass, 122–123
redirection, 194–197
User menu, Details command, 433
User-Agent field (HTTP packets), 165–166
username command, 319
usernames, 447
users, viewing active, 383–384

V

validation. *See also* verification
EzVPN (Easy VPN)
client validation tunnel down, 497
hub ICMP debug, 499
hub validation tunnel up, 498
FlexVPN, 522–523

GETVPN (Group Encrypted Transport VPN)
key server policy and ACLs, 536–538
key servers and group member status, 535–536
GMs (group members), 538–540
IPsec with IKEv1, 480–481
validation authorities (VAs), 448
VAs (validation authorities), 448
verification. *See also* validation
DMVPN (Dynamic Multipoint VPN)
DMVPN and NHRP verification, 512–513
DMVPN NHRP configuration, 505–506
hub routing, 506
NHRP routes, 512
NHRP shortcut and routing, 511
spoke routing, 506–507
EzVPN (Easy VPN), 497–498
FlexVPN, 517
ASA (Adaptive Security Appliance), 518–519
hub virtual access interface, 529
spoke routing and interface, 530
spoke-to-spoke tunnel, 530–532
IPsec with IKEv2, 489–491
Verisign, 450
VIRL (Virtual Internet Routing Lab), 477
virtual private networks. *See* VPNs (virtual private networks)
Virtual Security Gateway (GSG), 602–603
Virtual Supervisor Module (VSM), 602–603
virtualization. *See also* VLANs (virtual LANs); VPNs (virtual private networks)
ACI (Application Centric Infrastructure)
application network profiles, 610
contracts, 612
device packages, 609–610
EPGs (endpoint groups), 610–611
object models, 609–610
service graphs, 612–613
spine-and-leaf topology, 608–609
advantages and limitations, 599–602
NFV (Network Functions Virtualization), 605–607
NSH (Network Service Header), 603–605
SFC (service function chaining), 603–605
VIRL (Virtual Internet Routing Lab), 477
virtual desktop support, 593
Virtual Security Gateway, 602–603
Virtual Supervisor Module, 602–603
VSG (Virtual Security Gateway), 602–603
Virtual-Template 1 command, 518
VLANs (virtual LANs)
dynamic interfaces for client VLANs
employee interfaces, 124–125
guest interfaces, 125–127
overview of, 124
PCI interfaces, 127
Guest, 67
mapping, 563
vMotion, 602–603
VNID (VXLAN Instance ID), 608–609
Voice Domain Permission setting (authorization profiles), 106
vPath, 603
VPN Client, 546
VPN Posture (HostScan) module, 566–570
VPNs (virtual private networks). *See also* IPsec
802.1AE/MACsec, 470–473
DMVPN (Dynamic Multipoint VPN)
crypto keyrings, 501
dual-hub configuration, 513–514
FlexVPN compared to, 514

hub interface configuration, 501–502
hub tunnel interface, 502
ISAKMP and transform set, 501
NHRP configuration, 505–506
overview of, 462–465
Phase 1, 506–507
Phase 2, 508–510
Phase 3, 510–513
sample network, 500
show dmvpn command, 504–505
spoke configuration, 503–504
VRF configuration, 500–501
EzVPN (Easy VPN)
client configuration, 495–497
client validation tunnel down, 497
client validation tunnel up, 497–498
dynamic VTI network, 492–493
hub configuration, 493–495
hub ICMP debug, 499
hub validation tunnel up, 498
FlexVPN
ASA configuration, 515–516
ASA verification, 518–519
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
ASA VTI router routing and ping test, 523
ASA VTI validation, 522–523
DMVPN compared to, 514
dual-hub, dual-cloud hub configurations, 524–527
dual-hub, dual-cloud spoke configurations, 527–528
hub virtual access interface verification, 527–528
INSIDE router configuration, 515
IOS virtual access interface, 518
overview of, 465–466
spoke routing and interface verification, 530
SPOKE1 configuration, 516–517
spoke-to-spoke tunnel verification, 530–532
traffic problem with crypto map ACLs, 520
verification ping, 517
GETVPN (Group Encrypted Transport VPN)
GMs (group members), 535
group member validation, 538–540
key server and group member status validation, 535–538
overview of, 466–469
primary key server configuration, 532–534
IPsec with IKEv1
Aggressive mode, 478–479
ASA configuration, 484
basic IPsec network, 478
crypto map sets, 479–480
debugging, 481–484
interesting traffic ACL, 479
ISAKMP policy, 478
transform set, 479
tunnel establishment, 480
validation, 480–481
IPsec with IKEv2
Cisco IOS NTP and CA configuration, 484–486
IKEv2 configuration for ASA, 489–491
IKEv2 peer NTP synchronization and certificate SCEP enrollment, 487–489
validation, 491–492
overview of, 461
RAVPN (Remote Access VPN)
with ASA (Adaptive Security Appliance), 554–570

Cisco AnyConnect Secure Mobility Client, 546–554
clientless, 545–546, 586–594
with FTD (Firepower Threat Defense), 570–579
IPsec IKEv2 VPN example, 580–586
overview of, 543–545
with routers, 580
use cases, 544–545
RA-VPN (remote-access virtual private networks), 7
SSL RAVPN (Remote Access VPN), 469–470
VPN Client, 546
VPN Posture (HostScan) module, 566–570
VRF (virtual routing and forwarding), 500–501
VSG (Virtual Security Gateway), 602–603
VSM (Virtual Supervisor Module), 602–603
VTEP (VXLAN Tunnel Endpoints), 608–609
VTI (Virtual Tunnel Interface), FlexVPN with
ASA VTI changes, 520–521
ASA VTI peer router changes, 522
router routing and ping test, 523
validation, 522–523
Vulnerabilities command (Analysis menu), 422
VXLAN Instance ID (VNID), 608–609
VXLAN Tunnel Endpoints (VTEP), 608–609

W

WAAS (Wide Area Application Service), 604
Web Authentication
CWA (Centralized Web Authentication), 69–71
LWA (Local Web Authentication)
with centralized web portals, 67–69
overview of, 66–67
overview of, 65–66
Redirection ACLs, 121–122
Web Redirection setting (authorization profiles), 107
Web Security Appliance. *See* WSA (Web Security Appliance)
wget command, 410
whitelisted domains, 41, 435–437
Whitelisted Domains tab (Network Access work center), 41
Wide Area Application Service (WAAS), 604
Windows Management Instrumentation. *See* WMI (Windows Management Instrumentation)
WinSPWizard, 210
wired network access control
default policy sets and rules, 100–102
differentiated access policy, creating
authorization results, 103–109
least privilege access rules example, 102–103
policy conditions, 108–112
policy sets, 112–115
Wireless LAN Controller. *See* WLC (Wireless LAN Controller)
wireless LANs. *See* WLANs (wireless LANs)
wireless network access control
802.1X and MAB verification
with Cisco WLC (Wireless LAN Controller), 145–147
endpoint supplicant verification, 140
network access device verification, 140–145
overview of, 140
AAA server configuration

RADIUS accounting servers, 119–120
RADIUS authentication servers, 118–119
RADIUS fallback, 120–121
AireOS, 116–117
Airespace ACLs
Google URLs for ACL bypass, 122–123
overview of, 121
Web Authentication Redirection ACLs, 121–122
Cisco ISE verification, 147–148
Corporate WLANs
AAA Servers tab, 137
Advanced tab, 137–138
General tab, 135–136
Layer 2 Security tab, 136
Layer 3 Security tab, 136–137
overview of, 134–135
dynamic interfaces for client VLANs
employee interfaces, 124–125
guest interfaces, 125–127
overview of, 124
PCI interfaces, 127
Guest WLANs
AAA Servers tab, 130–131
Advanced tab, 132–134
General tab, 128–129
Layer 2 Security tab, 129
Layer 3 Security tab, 130
overview of, 127–128
ISE configuration for, 138–140
overview of, 115–116
wizards
AnyConnect VPN Wizard, 554–570
Clientless SSL VPN Wizard, 587–594
bookmarks, 589–590
DAP (dynamic access policies), 594
group policies, 592
login screen and home page, 590–592
plug-ins, 593
portal customization, 594
profile and interface configuration, 587–588
smart tunnels, 593
user authentication, 588
virtual desktop support, 593
FMC RAVPN Policy Wizard, 570–579
access control, 577–579
authentication method, 574
authentication servers, 571
certificates, 571
group policies, 574
interface and certificate configuration, 575–576
VPN client images, 573
VPN pool, 572
VPN profile, 572
WLANs (wireless LANs). ***See also*** **WLC (Wireless LAN Controller)**
Corporate
AAA Servers tab, 137
Advanced tab, 137–138
General tab, 135–136
Layer 2 Security tab, 136
Layer 3 Security tab, 136–137
overview of, 134–135
Guest
AAA Servers tab, 130–131
Advanced tab, 132–134
General tab, 128–129
Layer 2 Security tab, 129
Layer 3 Security tab, 130
overview of, 127–128
WLC (Wireless LAN Controller). ***See also*** **wireless network access control**
802.1X and MAB verification

with Cisco WLC (Wireless LAN Controller), 145–147
endpoint supplicant verification, 140
network access device verification, 140–145
overview of, 140
AireOS, 116–117
authentication configuration
Airespace ACLs, 121–123
RADIUS accounting servers, 119–120
RADIUS authentication servers, 118–119
RADIUS fallback, 120–121
Cisco ISE verification, 147–148
Corporate WLAN, creating
AAA Servers tab, 137
Advanced tab, 137–138
General tab, 135–136
Layer 2 Security tab, 136
Layer 3 Security tab, 136–137
overview of, 134–135
device administration with TACACS+
ISE configuration, 338–342
roles, 335–336
Shell Profiles, 335, 339–340
verification, 342–343
WLC configuration, 336–337
dynamic interfaces for client VLANs
employee interfaces, 124–125
guest interfaces, 125–127
overview of, 124
PCI interfaces, 127
Guest WLAN, creating
AAA Servers tab, 130–131
Advanced tab, 132–134
General tab, 128–129
Layer 2 Security tab, 129
Layer 3 Security tab, 130
overview of, 127–128
ISE profiling probes with, 157
verifying authentications with, 146–147
WMI (Windows Management Instrumentation)
configuration, 187–190
logoff detection, 190–191
overview of, 185–186
Woland, Aaron, 44, 168
work centers
ISE Profiler, 153
Network Access
joining domains, 37–40
overview of, 34–36
PassiveID tab, 41
Whitelisted Domains tab, 41
WSA (Web Security Appliance)
configuration
ISE root certificates, 390–394
overview of, 390
policies, 394–397
WSA and ISE integration, 390–394
device administration with RADIUS
ISE configuration, 351
overview of, 343–344
verification, 351
WSA configuration, 349–351
WSAv, 601

X-Y-Z

X.509 PKI (Public Key Infrastructure), 448–449
XCP (Extensible Communications Platform), 361
XMPP (Extensible Messaging and Presence Protocol), 361
Yubico YubiKey, 33