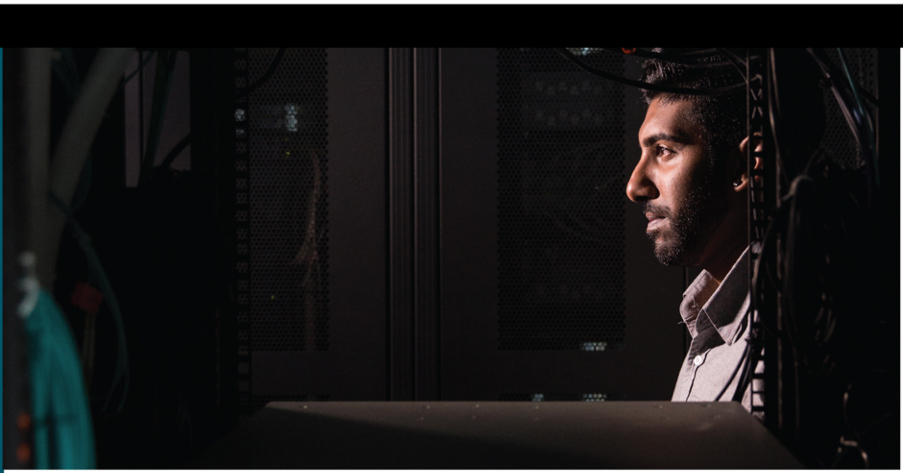

CCIE Professional Development

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

Table of Contents

Cover

Title Page

Copyright Page

About the Authors

About the Technical Reviewer

Dedications

Acknowledgments

Contents at a Glance

Contents

Introduction

Part I: Knock, Knock! Whos There?

- Chapter 1 Who and What: AAA Basics
  - Fundamentals of AAA
  - Understanding the Concept of Triple-A in the Real World
  - Compare and Select AAA Options
    - Device Administration
    - Network Access
  - TACACS+

Pearson

Table of Contents

TACACS+ Authentication Messages

TACACS+ Authorization and Accounting Messages

RADIUS

AV Pairs

Change of Authorization (CoA)

Comparing RADIUS and TACACS+

Summary

Chapter 2 Basic Network Access Control

What Is Cisco ISE?

ISE Architecture for Network Access AAA

Personas

Network Access AAA Architecture and ISE Personas

Configuring ISE for Single/Standalone and Multinode Deployments

Standalone

Dual Node

Distributed Deployment

ISE Configuration for Network Access

Identity Sources

Identity Source Sequences

Network Resources

802.1X and Beyond

EAP Types

Not Everything Has a (Configured) Supplicant

Configuring Wired Network Access with ISE

Configuring Cisco Catalyst Switches

Global Configuration for All Catalyst Switches

Interface Configuration for Classic and Newer IOS Switches

Common Classification Policy Language Switches

Configuring ISE for Basic Wired Network Access Control

Configuring Wireless Network Access with ISE

Introduction to AireOS and Its Versions

Authentication Configuration on WLCs

Table of Contents

Configure the AAA Servers

Configure the Airespace ACLs

Create the Dynamic Interfaces for the Client VLANs

Create the Wireless LANs

Configuring ISE for Wireless Network Access Control

Verifying Dot1X and MAB

Endpoint Supplicant Verification

Network Access Device Verification

Cisco ISE Verification

Summary

Chapter 3 Beyond Basic Network Access Control

Profiling with ISE

ISE Profiler Work Center

Profiling Policies

Profiling Feed Service

Endpoint Profile Policies

Context Visibility

Logical Profiles

ISE Profiler and CoA

Global CoA

Global Profiler Settings

Profiles in Authorization Policies

Endpoint Identity Groups

Passive Identities and EasyConnect

Passive Authentication

EasyConnect

Summary

Chapter 4 Extending Network Access with ISE

Get Ready, Get Set, Prerequisites

URL Redirection

AAA Configuration

BYOD Onboarding with ISE

Table of Contents

- Building Blocks of a BYOD Solution
- Single SSID and Dual SSID Provisioning
- Configuring ISE for BYOD Onboarding
- Network Device Configuration for BYOD Onboarding
- BYOD Onboarding Verification and End-User Experience

MDM Onboarding and Enforcement with ISE

Posture Assessment and Remediation with ISE

- Preparing to Configure Posture
- Configuring AnyConnect Provisioning
- Configuring Posture Policy
- Configure Policy Set for Posture

Guest Access with ISE

- Preparing to Configure Guest Access
- Sponsor Groups and Portal
- Hotspot Portal
- Sponsored and Self-Registered Guest Portals
- Configuring Policy Sets for Guest Access

TrustSec with ISE

- Introducing TrustSec
- Classification
- Propagation
- Enforcement

Summary

Chapter 5 Device Administration Control with ISE

The Case for Centralized AAA

RADIUS Versus TACACS+ for Device Administration

Using TACACS+ for Device Administration

- Configuring ISE for TACACS+
- TACACS+ with Cisco IOS Routers, Switches, and ISE
- TACACS+ with Cisco ASA and ISE
- TACACS+ with Cisco WLC and ISE

Using RADIUS for Device Administration

Table of Contents

RADIUS-Based Device Administration on Cisco FMC

RADIUS-Based Device Administration on Cisco WSA/ESA

Summary

Part II: Spread the Love!

Chapter 6 Sharing the Context

The Many Integration Types of the Ecosystem

MDM Integration

Rapid Threat Containment

Ciscos platform eXchange Grid (pxGrid)

pxGrid in Depth

pxGrid in Action

Context-In

Configuring ISE for pxGrid

Configuring pxGrid Participants

Summary

Chapter 7 APIs in Cisco Security

APIs 101

RESTful APIs

Working with APIs

Cisco DevNet

Firepower Management Center APIs

FMC REST API for Configuration

Firepower System Remediation API

FMC Host Input API

FMC Database Access API

FMC eStreamer API

Identity Services Engine APIs

ISE Monitoring REST API

ISE External RESTful Services API

Advanced Malware Protection APIs

Threat Grid APIs

Table of Contents

- Umbrella APIs
- Summary
- References

Part III: c2889775343d1ed91b

- Chapter 8 Security Connectivity
  - Hashing, Ciphers, Cryptography, and PKI
    - Hashing
    - Cipher Types
    - Encryption Schemes
    - The Keys to the Kingdom
    - Authentication Mechanisms
    - Security Protocols
    - The Bits and Pieces
  - Virtual Private Networks
    - IPsec
    - DMVPN
    - FlexVPN
    - GETVPN
    - SSL Remote Access VPN
  - Layer 2 Encryption: IEEE 802.1AE/MACsec
  - Summary
  - References
- Chapter 9 Infrastructure VPN
  - IPsec with IKEv1
  - IPsec with IKEv2
  - EzVPN
  - DMVPN
    - DMVPN Phase 1
    - DMVPN Phase 2
    - DMVPN Phase 3
    - Dual-Hub DMVPN

Table of Contents

- FlexVPN
- GETVPN
- Summary
- References

Chapter 10 Remote Access VPN

- Remote Access VPN Overview
  - Clientless versus Client-Based VPNs
- Cisco AnyConnect Secure Mobility Client
  - AnyConnect Profile Editor
  - Deploying AnyConnect
- Client-Based Remote Access VPN
  - RAVPN with ASA
  - Group Policies
  - Dynamic Access Policies
  - Posture Assessment
  - RAVPN with Firepower Threat Defense
  - RAVPN with Routers
  - IPsec Remote Access VPN on IOS Using IKEv2 with FlexVPN Example
- Clientless Remote Access VPN
- Summary
- References

Part IV: The Red Pill

Chapter 11 Security Virtualization and Automation

- Cisco Virtual Solutions and Server Virtualization
- Virtualization and Automation Solutions
  - Cisco Virtual Security Gateway
  - Service Function Chaining with Network Service Header
  - Network Function Virtualization
  - Application Centric Infrastructure and Micro-Segmentation
- Summary
- References

Table of Contents

Index