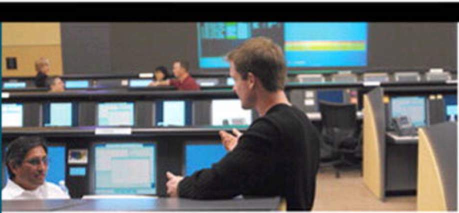

CCIE Professional Development

Network Security Technologies and Solutions

A comprehensive, all-in-one reference for Cisco network security

ciscopress.com

Yusuf Bhaiji, CCIE No. 9305

CCIE Professional Development

Network Security Technologies and Solutions

Yusuf Bhaiji, CCIE No. 9305

Cisco Press

Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

Network Security Technologies and Solutions (CCIE Professional Development Series)

Table of Contents

Contents

Foreword

Introduction

Part I: Perimeter Security

Chapter 1 Overview of Network Security

Fundamental Questions for Network Security

Transformation of the Security Paradigm

Principles of SecurityThe CIA Model

Policies, Standards, Procedures, Baselines, Guidelines

Security Models

Perimeter Security

Security in Layers

Security Wheel

Summary

References

Chapter 2 Access Control

Traffic Filtering Using ACLs

IP Address Overview

Subnet Mask Versus Inverse Mask Overview

ACL Configuration

Understanding ACL Processing

Types of Access Lists

Summary

Table of Contents

References

Chapter 3 Device Security

Device Security Policy

Hardening the Device

Securing Management Access for Security Appliance

Device Security Checklist

Summary

References

Chapter 4 Security Features on Switches

Securing Layer 2

Port-Level Traffic Controls

Private VLAN (PVLAN)

Access Lists on Switches

Spanning Tree Protocol Features

Dynamic Host Configuration Protocol (DHCP) Snooping

IP Source Guard

Dynamic ARP Inspection (DAI)

Advanced Integrated Security Features on High-End Catalyst Switches

Control Plane Policing (CoPP) Feature

CPU Rate Limiters

Layer 2 Security Best Practices

Summary

References

Chapter 5 Cisco IOS Firewall

Router-Based Firewall Solution

Context-Based Access Control (CBAC)

CBAC Functions

How CBAC Works

CBAC-Supported Protocols

Table of Contents

Configuring CBAC

IOS Firewall Advanced Features

Zone-Based Policy Firewall (ZFW)

Summary

References

Chapter 6 Cisco Firewalls: Appliance and Module

Firewalls Overview

Hardware Versus Software Firewalls

Cisco PIX 500 Series Security Appliances

Cisco ASA 5500 Series Adaptive Security Appliances

Cisco Firewall Services Module (FWSM)

Firewall Appliance Software for PIX 500 and ASA 5500

Firewall Appliance OS Software

Firewall Modes

Stateful Inspection

Application Layer Protocol Inspection

Adaptive Security Algorithm Operation

Security Context

Security Levels

Redundant Interface

IP Routing

Network Address Translation (NAT)

Controlling Traffic Flow and Network Access

Modular Policy Framework (MPF)

Cisco AnyConnect VPN Client

Redundancy and Load Balancing

Firewall Module Software for Firewall Services Module (FWSM)

Firewall Module OS Software

Network Traffic Through the Firewall Module

Installing the FWSM

Table of Contents

Router/MSFC Placement

Configuring the FWSM

Summary

References

Chapter 7 Attack Vectors and Mitigation Techniques

Vulnerabilities, Threats, and Exploits

Mitigation Techniques at Layer 3

Mitigation Techniques at Layer 2

Security Incident Response Framework

Summary

References

Part II: Identity Security and Access Management

Chapter 8 Securing Management Access

AAA Security Services

Authentication Protocols

Implementing AAA

Configuration Examples

Summary

References

Chapter 9 Cisco Secure ACS Software and Appliance

Cisco Secure ACS Software for Windows

Advanced ACS Functions and Features

Configuring ACS

Cisco Secure ACS Appliance

Summary

References

Chapter 10 Multifactor Authentication

Identification and Authentication

Two-Factor Authentication System

Table of Contents

Cisco Secure ACS Support for Two-Factor Authentication Systems

Summary

References

Chapter 11 Layer 2 Access Control

Trust and Identity Management Solutions

Identity-Based Networking Services (IBNS)

IEEE 802.1x

Deploying an 802.1x Solution

Implementing 802.1x Port-Based Authentication

Summary

References

Chapter 12 Wireless LAN (WLAN) Security

Wireless LAN (WLAN)

WLAN Security

Mitigating WLAN Attacks

Cisco Unified Wireless Network Solution

Summary

References

Chapter 13 Network Admission Control (NAC)

Building the Self-Defending Network (SDN)

Network Admission Control (NAC)

Cisco NAC Appliance Solution

Cisco NAC Framework Solution

Summary

References

Part III: Data Privacy

Chapter 14 Cryptography

Secure Communication

Virtual Private Network (VPN)

Table of Contents

Summary

References

Chapter 15 IPsec VPN

Virtual Private Network (VPN)

IPsec VPN (Secure VPN)

Public Key Infrastructure (PKI)

Implementing IPsec VPN

Summary

References

Chapter 16 Dynamic Multipoint VPN (DMVPN)

DMVPN Solution Architecture

DMVPN Deployment Topologies

Implementing DMVPN Hub-and-Spoke Designs

Implementing Dynamic Mesh Spoke-to-Spoke DMVPN Designs

Summary

References

Chapter 17 Group Encrypted Transport VPN (GET VPN)

GET VPN Solution Architecture

Implementing Cisco IOS GET VPN

Summary

References

Chapter 18 Secure Sockets Layer VPN (SSL VPN)

Secure Sockets Layer (SSL) Protocol

SSL VPN Solution Architecture

Implementing Cisco IOS SSL VPN

Cisco AnyConnect VPN Client

Summary

References

Chapter 19 Multiprotocol Label Switching VPN (MPLS VPN)

Table of Contents

Multiprotocol Label Switching (MPLS)
MPLS VPN (Trusted VPN)
Comparison of L3 and L2 VPNs
Layer 3 VPN (L3VPN)
Implementing L3VPN
Layer 2 VPN (L2VPN)
Implementing L2VPN
Summary
References
Part IV: Security Monitoring
Chapter 20 Network Intrusion Prevention
Intrusion System Terminologies
Network Intrusion Prevention Overview
Cisco IPS 4200 Series Sensors
Cisco IDS Services Module (IDSM-2)
Cisco Advanced Inspection and Protection Security Services Module (AIP-SSM)
Cisco IPS Advanced Integration Module (IPS-AIM)
Cisco IOS IPS
Deploying IPS
Cisco IPS Sensor OS Software
Cisco IPS Sensor Software
IPS High Availability
IPS Appliance Deployment Guidelines
Cisco Intrusion Prevention System Device Manager (IDM)
Configuring IPS Inline VLAN Pair Mode
Configuring IPS Inline Interface Pair Mode
Configuring Custom Signature and IPS Blocking
Summary
References
Chapter 21 Host Intrusion Prevention

Table of Contents

Securing Endpoints Using a Signatureless Mechanism

Cisco Security Agent (CSA)

CSA Architecture

CSA Capabilities and Security Functional Roles

CSA Components

Configuring and Managing CSA Deployment by Using CSA MC

Summary

References

Chapter 22 Anomaly Detection and Mitigation

Attack Landscape

Anomaly Detection and Mitigation Systems

Cisco DDoS Anomaly Detection and Mitigation Solution

Cisco Traffic Anomaly Detector

Cisco Guard DDoS Mitigation

Putting It All Together for Operation

Configuring and Managing the Cisco Traffic Anomaly Detector

Configuring and Managing Cisco Guard Mitigation

Summary

References

Chapter 23 Security Monitoring and Correlation

Security Information and Event Management

Cisco Security Monitoring, Analysis, and Response System (CS-MARS)

Deploying CS-MARS

Summary

References

Part V: Security Management

Chapter 24 Security and Policy Management

Cisco Security Management Solutions

Cisco Security Manager

Table of Contents

Cisco Router and Security Device Manager (SDM)

Cisco Adaptive Security Device Manager (ASDM)

Cisco PIX Device Manager (PDM)

Cisco IPS Device Manager (IDM)

Summary

References

Chapter 25 Security Framework and Regulatory Compliance

Security Model

Policies, Standards, Guidelines, and Procedures

Best Practices Framework

Compliance and Risk Management

Regulatory Compliance and Legislative Acts

GLBAGramm-Leach-Bliley Act

HIPAAHealth Insurance Portability and Accountability Act

SOXSarbanes-Oxley Act

Worldwide Outlook of Regulatory Compliance Acts and Legislations

Cisco Self-Defending Network Solution

Summary

References

Index

Pearson