



CCIE Professional Development

Integrated Security Technologies and Solutions

Volume I

Cisco Security Solutions for Advanced Threat
Protection with Next Generation Firewall, Intrusion
Prevention, AMP, and Content Security

Aaron Woland, CCIE® No. 20113

Vivek Santuka, CCIE® No. 17621

Mason Harris, CCIE® No. 5916

Jamie Sanbower, CCIE® No. 13637

Integrated Security Technologies and Solutions - Volume I

Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security

Aaron Woland, CCIE® No. 20113

Vivek Santuka, CCIE® No. 17621

Mason Harris, CCIE® No. 5916

Jamie Sanbower, CCIE® No. 13637

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Integrated Security Technologies and Solutions - Volume I: Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security

Table of Contents

Cover

Title Page

Copyright Page

About the Authors

About the Technical Reviewer

Dedication

Acknowledgments

Contents

Introduction

Part I: Hi There! This Is Network Security

Chapter 1 Lets Talk About Network Security

Know Thy Enemy

Know Thy Self

Security Policy

Security Standards and Frameworks

ISO/IEC 27001 and 27002

NIST Cybersecurity Framework

Regulatory Compliance

Health Insurance Portability and Accountability Act (HIPAA)

Table of Contents

Payment Card Industry Data Security Standard (PCI DSS)

Security Models

Cisco SAFE

SAFE PINs

Secure Domains

Attack Continuum

Integrating Security Solutions

Summary

References

Chapter 2 Infrastructure Security and Segmentation

The Three Planes

Securing the Management Plane

Securing the Command Line

Privilege Levels

Management Plane Protection

CPU and Memory Thresholding

Securing SNMP

SNMP Authentication and Encryption

SNMP with Access Lists

SNMP Views

Securing the Control Plane

Control Plane Policing (CoPP)

Securing Layer 2 Control Plane Protocols

Securing Spanning Tree Protocol (STP)

Securing VLAN Trunking Protocol (VTP)

Securing Layer 3 Control Plane Protocols

Securing Border Gateway Protocol (BGP)

Securing RIPv2 and EIGRP

Securing OSPF

Securing the Data Plane

Security at the Layer 2 Data Plane

The CAM Table and Port Security

Table of Contents

DHCP Snooping
The ARP Table and Dynamic ARP Inspection (DAI)
Segmentation
Attacks Against Segmentation
Traffic Filtering at Layer 2
Security at the Layer 3 Data Plane
Traffic Filtering at Layer 3
Standard ACLs
Extended ACLs
Named ACLs
Time Based ACLs
Reflexive ACLs
Unicast Reverse Path Forwarding
Network Based Application Recognition (NBAR)
TCP Intercept

Visibility with NetFlow

Summary

References

Chapter 3 Wireless Security

What Is Wireless?

Wireless Standards
802.11 Standards
802.11 MAC Frame Formats
Association and Authentication
Autonomous Versus Controller-Based WLANs
WLC Fundamentals
CAPWAP Overview
Access Point Discovery Process
AP Modes
FlexConnect Access Points
Guest Anchor Controllers

Wireless Security Overview

Table of Contents

WEP

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access 2 (WPA2)

WPA Personal Versus WPA Enterprise

Roaming

Securing the WLAN

Configuring Wireless Protection Policies

Rogue AP Detection

Detecting Rogue APs

Classifying Rogue APs

Mitigating Rogue APs

Wireless Threat Detection and Mitigation

Wireless Intrusion Detection Systems

Wireless Intrusion Prevention Systems

Non-802.11 Attacks and Interference

Client Exclusion

Management Frame Protection

Infrastructure MFP

Client MFP

Protected Management Frames

Management and Control Plane Protection

Management Authentication

Management Protocols and Access

CPU ACLs

Access Point Protection

Integrating a WLC with Other Security Solutions

WLC and ISE

WLC and Stealthwatch

WLC and Umbrella

Summary

References

Part II: Deny IP any any

Table of Contents

Chapter 4 Firewalling with the ASA

ASA Fundamentals

- Setting Up a Lab Virtual ASA (ASAv)
- ASA Initial Configuration
- Getting Connected
- ASA Device Manager
- ASA Security Levels
- ASA Security Zones
- ASA Routed and Transparent Mode
- ASA Routed Mode
- Transparent Mode
- ASA Multiple-Context Mode
- Multiple Context Configuration Basics
- Understanding the ASA Classifier
- ASA High Availability Options
- ASA Active/Standby Failover
- ASA Active/Active Failover
- Handling Asymmetric Traffic
- ASA Clustering
- ASA Clustering Troubleshooting
- Enabling Routing Protocol Support on the ASA
- ASA Routing Protocol Troubleshooting
- ASA Clustering Best Practices

Traffic with the ASA

- Network Address Translation (NAT)
- ASA 8.3+ NAT Configuration Changes
- NAT Terminology
- Types of NAT
- Applying NAT
- NAT and IPv6
- Dynamic NAT
- Dynamic PAT
- Static NAT

Table of Contents

Identity NAT

NAT and IPv6

NAT66

ASA NAT Troubleshooting

Service Policies and Application Inspection

Application Inspection

Commonly Used Application Inspection Engines

ASA Advanced Features

Identity Firewall

Identity Firewall Configuration

Security Group Tags (SGTs)

TrustSec Configuration

Advanced Firewall Tuning

TCP State Bypass

Policy Based Routing (PBR)

Threat Detection

Troubleshooting the ASA

Packet Capture

Summary

References

Chapter 5 Next-Gen Firewalls

Firepower Deployment Options

What Is the Firepower Management Console?

Configuring Firepower Threat Defense

FTD Initial Configuration

Routed Mode

Transparent Mode

Adding a Device to the FMC

Interface Configuration

Security Zones

Interface Addressing

High Availability

Table of Contents

- NGFW Interface High Availability
- NGFW System High Availability
- High-Availability Configuration
- Routing in FTD
- Network Address Translation (NAT)

Access Control Policies

- Prefilter Policy
- Objects
- Network Discovery Policy
- Identity Firewall
- Active Authentication
- Passive Authentication
- Application Visibility and Control (AVC)
- Custom Application Detectors
- URL Filtering
- Network Reputation
- SSL Inspection

Analysis and Reporting

- Dashboards
- Context Explorer
- Connection Events
- User Activity

Summary

References

Chapter 6 Next-Gen Intrusion Detection and Prevention

NGIPS Overview

- Legacy IDSs/IPSs Versus NGIPSs
- Contextual Awareness
- Impact Assessment
- Security Intelligence
- Indications of Compromise (IOCs)
- Automated Tuning

Cisco NGIPS Appliances

Table of Contents

- Firepower Clustering
- Firepower Stacking
- Firepower Management Center (FMC)
- NGIPS Deployment Options

Snort

- Snort Rules
- Options, Keywords, and Arguments in Rules
- Custom Intrusion Rules
- Preprocessors and Network Analysis

Configuring a NGIPS

- Intrusion Policies
- System-Provided Intrusion Policies
- Policy Layers
- Advanced Settings
- Committing Changes
- Variables
- Access Control Policies
- Performance Settings
- Security Intelligence
- Monitoring Security Intelligence

Operationalizing a NGIPS

- Dashboards and Custom Dashboards
- Context Explorer
- Reporting
- Intrusion Event Workflows
- Correlation Engine
- IPS Tuning
- Updating Rules and the Vulnerability Database (VDB)

Summary

References

Chapter 7 IOS Firewall and Security Features

- Network Address Translation (NAT)

Table of Contents

- NAT Terminology
- NAT Configuration
- NAT Overload
- Dynamic NAT
- Static NAT
- Troubleshooting NAT
- NAT Virtual Interface (NVI)
- ACLs and NAT
- Helpful Troubleshooting Commands

Zone-Based Firewall (ZBF)

- ZBF Configuration Steps
- Defining Zones
- Configuring Zone Pairs
- Defining the Class Map(s)
- Defining the Policy Map(s)
- Configuring ZBF
- Nested Class Maps
- The Self-Zone
- Self-Zone Configuration
- Proper Use of the Self-Zone
- Port-to-Application Mapping (PAM)
- Verifying ZBF
- Troubleshooting ZBF
- Unsupported Features with ZBF

IOS Advanced Security Features

- TCP Intercept
- TCP Intercept Configuration
- Unicast Reverse Path Forwarding
- uRPF Configuration
- Policy-Based Routing (PBR)
- PBR Operation
- PBR Configuration
- PBR Troubleshooting

Table of Contents

Web Cache Communication Protocol (WCCP)

WCCP Protocol Capabilities

Forwarding Method

Return Method

WCCP Configuration

WCCP Troubleshooting

Summary

References

Part III: <HTML> EHLO. You have threat in content </HTML>

Chapter 8 Content Security and Advanced Threat Protection

Content Security Overview

Cisco Async Operating System (AsyncOS)

Web Security Appliance

Proxy Basics

Explicit Forward Mode

Transparent Mode

Transparent Proxy Traffic Redirection with WCCP

Transparent Proxy Traffic Redirection with PBR

Web Proxy IP Spoofing

WSA System Setup

WSA Policy Configuration

Identification Policies

Access Policies

Decryption Policies

Outbound Malware Policies

Data Security Policies and DLP Policies

WSA Reporting

Email Security Appliance

Email Basics

ESA System Setup

ESA Policy Configuration

Incoming and Outgoing Mail Policies

Table of Contents

- Host Access Table
- Mail Flow Policies
- Recipient Access Table
- Data Loss Prevention
- SMTP Authentication and Encryption
- ESA Reporting

Security Management Appliance

Summary

References

Chapter 9 Umbrella and the Secure Internet Gateway

Umbrella Fundamentals

- nslookup dnsbasics.securitydemo.net

- Umbrella Architecture

- Secure Internet Gateway

Umbrella Overview Dashboard

Deploying Umbrella

- Identities

- Forwarding DNS Traffic to Umbrella

- Umbrella Virtual Appliances

- Active Directory

- Roaming Devices

- Cisco Security Connector

- Policies

- Reporting

Cisco Investigate

Summary

References

Chapter 10 Protecting Against Advanced Malware

Introduction to Advanced Malware Protection (AMP)

Role of the AMP Cloud

Doing Security Differently

Table of Contents

The Prevention Framework

One-to-One Signatures

Ethos Engine

Spero Engine

Indicators of Compromise

Device Flow Correlation

Advanced Analytics

Dynamic Analysis with Threat Grid

The Retrospective Framework

The Cloud

Private Cloud

Cloud Proxy Mode

Air Gap Mode

Threat Grid

Threat Grid Cloud

Threat Grid Appliance

The Clean Interface

The Administrative Interface

The Dirty Interface

Comparing Public and Private Deployments

AMP for Networks

What Is That Manager Called?

Form Factors for AMP for Networks

What AMP for Networks Does

Where Are the AMP Policies?

File Rules

Advanced

AMP for Endpoints

What Is AMP for Endpoints?

Connections to the AMP Cloud

U.S. and North American Cloud

European Union Cloud

Table of Contents

Asia Pacific, Japan, and Greater China Cloud

Outbreak Control

Custom Detections

Simple Custom Detections

Advanced Custom Detections

Android Custom Detections

Network IP Blacklists and Whitelists

Application Control

Exclusions

The Many Faces of AMP for Endpoints

AMP for Windows

Windows Policies

The General Tab

The File Tab

The Network Tab

AMP for macOS

Mac Policies

The General Tab

The File Tab

The Network Tab

AMP for Linux

Linux Policies

The General Tab

The File Tab

The Network Tab

AMP for Android

Installing AMP for Endpoints

Groups, Groups, and More Groups

The Download Connector Screen

Distributing via Cisco AnyConnect

Installing AMP for Windows

Installing AMP for Mac

Table of Contents

Installing AMP for Linux

- Installing AMP for Android

- Android Activation Codes

- Deploying the AMP for Android Connector

Proxy Complications

- Proxy Server Autodetection

- Incompatible Proxy Security Configurations

AMP for Content Security

- Content Security Connectors

- Configuring AMP for Content Security Appliances

Configuring the Web Security Appliance (WSA) Devices

Configuring the Email Security Appliance (ESA) Devices

AMP Reports

Summary

Index