



SECURITY

# Cisco ASA

All-in-One Next-Generation Firewall,  
IPS, and VPN Services

Third Edition

# Cisco ASA

---

All-in-One Next-Generation Firewall, IPS, and VPN  
Services, Third Edition

Jazib Frahim, CCIE No. 5459

Omar Santos

Andrew Ossipov, CCIE No. 18483

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

# Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services

## Table of Contents

Contents

Introduction

Chapter 1 Introduction to Security Technologies

Firewalls

Network Firewalls

Packet-Filtering Techniques

Application Proxies

Network Address Translation

Stateful Inspection Firewalls

Demilitarized Zones (DMZ)

Deep Packet Inspection

Next-Generation Context-Aware Firewalls

Personal Firewalls

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Pattern Matching and Stateful Pattern-Matching Recognition

Protocol Analysis

Heuristic-Based Analysis

Anomaly-Based Analysis

Global Threat Correlation Capabilities

Virtual Private Networks

Technical Overview of IPsec

IKEv1 Phase 1

IKEv1 Phase 2

# **Table of Contents**

IKEv2

SSL VPNs

Cisco AnyConnect Secure Mobility

Cloud and Virtualization Security

## **Chapter 2 Cisco ASA Product and Solution Overview**

Cisco ASA Model Overview

Cisco ASA 5505 Model

Cisco ASA 5510 Model

Cisco ASA 5512-X Model

Cisco ASA 5515-X Model

Cisco ASA 5520 Model

Cisco ASA 5525-X Model

Cisco ASA 5540 Model

Cisco ASA 5545-X Model

Cisco ASA 5550 Model

Cisco ASA 5555-X Model

Cisco ASA 5585-X Models

Cisco Catalyst 6500 Series ASA Services Module

Cisco ASA 1000V Cloud Firewall

Cisco ASA Next-Generation Firewall Services (Formerly Cisco  
ASA CX)

Cisco ASA AIP-SSM Module

Cisco ASA AIP-SSM-10

Cisco ASA AIP-SSM-20

Cisco ASA AIP-SSM-40

Cisco ASA Gigabit Ethernet Modules

Cisco ASA SSM-4GE

Cisco ASA 5580 Expansion Cards

# **Table of Contents**

Cisco ASA 5500-X Series 6-Port GE Interface Cards

## **Chapter 3 Licensing**

### **Licensed Features on ASA**

- Basic Platform Capabilities
- Advanced Security Features
- Tiered Capacity Features
- Displaying License Information

### **Managing Licenses with Activation Keys**

- Permanent and Time-Based Activation Keys
- Combining Keys
- Time-Based Key Expiration
- Using Activation Keys

### **Combined Licenses in Failover and Clustering**

- License Aggregation Rules
- Aggregated Time-Based License Countdown

### **Shared Premium VPN Licensing**

- Shared Server and Participants
- Shared License
- Shared Licensing Operation
- Configuring Shared Licensing
- Licensing Server
- Participants
- Backup Licensing Server
- Monitoring Shared Licensing Operation

## **Chapter 4 Initial Setup**

### **Accessing the Cisco ASA Appliances**

- Establishing a Console Connection
- Command-Line Interface

### **Managing Licenses**

# **Table of Contents**

## **Initial Setup**

- Initial Setup via CLI
- Initial Setup of ASDM
- Uploading ASDM
- Setting Up the Appliance
- Accessing ASDM
- Functional Screens of ASDM

## **Device Setup**

- Setting Up a Device Name and Passwords
- Configuring an Interface
- Configuring a Data-Passing Interface
- Configuring a Subinterface
- Configuring an EtherChannel Interface
- Configuring a Management Interface
- DHCP Services

## **Setting Up the System Clock**

- Manual Clock Adjustment
- Time Zone
- Date
- Time
- Automatic Clock Adjustment Using the Network Time Protocol

## **Chapter 5 System Maintenance**

### **Configuration Management**

- Running Configuration
- Startup Configuration
- Removing the Device Configuration

### **Remote System Management**

- Telnet
- Secure Shell (SSH)

### **System Maintenance**

# **Table of Contents**

Software Installation

Image Upgrade via Cisco ASDM

Image Upgrade via the Cisco ASA CLI

Image Upload Using ROMMON

Password Recovery Process

Disabling the Password Recovery Process

## **System Monitoring**

System Logging

Enabling Logging

Defining Event List

Logging Types

Defining a Syslog Server

Defining an Email Server

Storing Logs Internally and Externally

Syslog Message ID Tuning

NetFlow Secure Event Logging (NSEL)

Step 1: Define a NetFlow Collector

Step 2: Define a NetFlow Export Policy

Simple Network Management Protocol (SNMP)

Configuring SNMP

SNMP Monitoring

## **Device Monitoring and Troubleshooting**

CPU and Memory Monitoring

Troubleshooting Device Issues

Troubleshooting Packet Issues

Troubleshooting CPU Issues

## **Chapter 6 Cisco ASA Services Module**

### **Cisco ASA Services Module Overview**

Hardware Architecture

Host Chassis Integration

# **Table of Contents**

## **Managing Host Chassis**

- Assigning VLAN Interfaces

- Monitoring Traffic Flow

## **Common Deployment Scenarios**

- Internal Segment Firewalling

- Edge Protection

## **Trusted Flow Bypass with Policy Based Routing**

- Traffic Flow

- Sample PBR Configuration

## **Chapter 7 Authentication, Authorization, and Accounting (AAA) Services**

### **AAA Protocols and Services Supported by Cisco ASA**

- RADIUS

- TACACS+

- RSA SecurID

- Microsoft Windows NTLM

- Active Directory and Kerberos

- Lightweight Directory Access Protocol

### **Defining an Authentication Server**

### **Configuring Authentication of Administrative Sessions**

- Authenticating Telnet Connections

- Authenticating SSH Connections

- Authenticating Serial Console Connections

- Authenticating Cisco ASDM Connections

### **Authenticating Firewall Sessions (Cut-Through Proxy Feature)**

- Authentication Timeouts

### **Customizing Authentication Prompts**

### **Configuring Authorization**

- Command Authorization



# **Table of Contents**

Configuring Downloadable ACLs

## **Configuring Accounting**

RADIUS Accounting

TACACS+ Accounting

## **Troubleshooting Administrative Connections to Cisco ASA**

Troubleshooting Firewall Sessions (Cut-Through Proxy)

ASDM and CLI AAA Test Utility

## **Chapter 8 Controlling Network Access: The Traditional Way**

### **Packet Filtering**

Types of ACLs

Standard ACLs

Extended ACLs

EtherType ACLs

Webtype ACLs

Comparing ACL Features

Through-the-Box-Traffic Filtering

To-the-Box-Traffic Filtering

### **Advanced ACL Features**

Object Grouping

Object Types

Configuration of Object Types

Object Grouping and ACLs

Standard ACLs

Time-Based ACLs

Downloadable ACLs

ICMP Filtering

### **Deployment Scenario for Traffic Filtering**

Using ACLs to Filter Inbound Traffic

Configuration Steps with ASDM

# **Table of Contents**

Configuration Steps with CLI

Monitoring Network Access Control

Monitoring ACLs

## **Chapter 9 Implementing Next-Generation Firewall Services with ASA CX**

CX Integration Overview

Logical Architecture

Hardware Modules

Software Modules

High Availability

ASA CX Architecture

Data Plane

Eventing and Reporting

User Identity

TLS Decryption Proxy

HTTP Inspection Engine

Application Inspection Engine

Management Plane

Control Plane

Preparing ASA CX for Configuration

Managing ASA CX with PRSM

Using PRSM

Configuring User Accounts

CX Licensing

Component and Software Updates

Signatures and Engines

System Software

Configuration Database Backup

Defining CX Policy Elements

# **Table of Contents**

Network Groups

Identity Objects

URL Objects

User Agent Objects

Application Objects

Secure Mobility Objects

Interface Roles

Service Objects

Application-Service Objects

Source Object Groups

Destination Object Groups

File Filtering Profiles

Web Reputation Profiles

NG IPS Profiles

## **Enabling User Identity Services**

Configuring Directory Servers

Connecting to AD Agent or CDA

Tuning Authentication Settings

Defining User Identity Discovery Policy

## **Enabling TLS Decryption**

Configuring Decryption Settings

Defining a Decryption Policy

## **Enabling NG IPS**

## **Defining Context-Aware Access Policies**

## **Configuring ASA for CX Traffic Redirection**

## **Monitoring ASA CX**

Dashboard Reports

Connection and System Events

Packet Captures

## **Chapter 10 Network Address Translation**

# **Table of Contents**

## Types of Address Translation

- Network Address Translation

- Port Address Translation

## Address Translation Methods

- Static NAT/PAT

- Dynamic NAT/PAT

- Policy NAT/PAT

- Identity NAT

## Security Protection Mechanisms Within Address Translation

- Randomization of Sequence Numbers

- TCP Intercept

## Understanding Address Translation Behavior

- Address Translation Behavior Prior to Version 8.3

- Packet Flow Sequence in Pre-8.3 Version

- NAT Order of Operation for Pre-8.3 Versions

- Redesigning Address Translation (Version 8.3 and Later)

- NAT Modes in Version 8.3 and Later

- NAT Order of Operation for Version 8.3 and Later

## Configuring Address Translation

- Auto NAT Configuration

- Available Auto NAT Settings

- Auto NAT Configuration Example

- Manual NAT Configuration

- Available Manual NAT Settings

- Manual NAT Configuration Example

- Integrating ACLs and NAT

- Pre-8.3 Behavior for NAT and ACL Integration

- Behavior of NAT and ACL Integration in Version 8.3 and Later

- Configuration Use Cases

- Use Case 1: Dynamic PAT for Inside Network with Static NAT for a DMZ

# **Table of Contents**

## Web Server

Use Case 2: Static PAT for a Web Server Located on the DMZ Network

Use Case 3: Static NAT for Overlapping Subnets Using Twice NAT

Use Case 4: Identity NAT for Site-to-Site VPN Tunnel

Use Case 5: Dynamic PAT for Remote-Access VPN Clients

## DNS Doctoring

## Monitoring Address Translations

## Chapter 11 IPv6 Support

### IP Version 6 Introduction

IPv6 Header

Supported IPv6 Address Types

Global Unicast Address

Site-Local Address

Link-Local Address

### Configuring IPv6

IP Address Assignment

IPv6 DHCP Relay

Optional IPv6 Parameters

Neighbor Solicitation Messages

Neighbor Reachable Time

Router Advertisement Transmission Interval

Setting Up an IPv6 ACL

IPv6 Address Translation

## Chapter 12 IP Routing

### Configuring Static Routes

Static Route Monitoring

Displaying the Routing Table

### RIP

Configuring RIP

# **Table of Contents**

RIP Authentication

RIP Route Filtering

Configuring RIP Redistribution

Troubleshooting RIP

Scenario 1: RIP Version Mismatch

Scenario 2: RIP Authentication Mismatch

Scenario 3: Multicast or Broadcast Packets Blocked

## **OSPF**

Configuring OSPF

Enabling OSPF

OSPF Virtual Links

Configuring OSPF Authentication

Configuring OSPF Redistribution

Stub Areas and NSSAs

OSPF Type 3 LSA Filtering

OSPF neighbor Command and Dynamic Routing over a VPN Tunnel

OSPFv3

Troubleshooting OSPF

Useful Troubleshooting Commands

Mismatched Areas

OSPF Authentication Mismatch

Troubleshooting Virtual Link Problems

## **EIGRP**

Configuring EIGRP

Enabling EIGRP

Configuring Route Filtering for EIGRP

EIGRP Authentication

Defining Static EIGRP Neighbors

Route Summarization in EIGRP

Split Horizon

# **Table of Contents**

Route Redistribution in EIGRP

Controlling Default Information

Troubleshooting EIGRP

Useful Troubleshooting Commands

Scenario 1: Link Failures

Scenario 2: Misconfigured Hello and Hold Intervals

Scenario 3: Misconfigured Authentication Parameters

## **Chapter 13 Application Inspection**

Enabling Application Inspection

Selective Inspection

CTIQBE Inspection

DCERPC Inspection

DNS Inspection

ESMTP Inspection

File Transfer Protocol

General Packet Radio Service Tunneling Protocol

GTPv0

GTPv1

Configuring GTP Inspection

### **H.323**

H.323 Protocol Suite

H.323 Version Compatibility

Enabling H.323 Inspection

Direct Call Signaling and Gatekeeper Routed Control Signaling T.38

T.38

Cisco Unified Communications Advanced Support

Phone Proxy

TLS Proxy

Mobility Proxy

# **Table of Contents**

Presence Federation Proxy

## **HTTP**

Enabling HTTP Inspection

strict-http Command

content-length Command

content-type-verification Command

max-header-length Command

max-uri-length Command

port-misuse Command

request-method Command

transfer-encoding type Command

## **ICMP**

## **ILS**

Instant Messenger (IM)

IPsec Pass-Through

## **MGCP**

## **NetBIOS**

## **PPTP**

Sun RPC

## **RSH**

## **RTSP**

## **SIP**

Skinny (SCCP)

## **SNMP**

SQL\*Net

## **TFTP**

## **WAAS**

## **XDMCP**



# **Table of Contents**

## **Chapter 14 Virtualization**

### **Architectural Overview**

- System Execution Space
- Admin Context
- User Context
- Packet Classification
- Packet Classification Criteria
- Destination IP Address
- Unique MAC Address
- Packet Flow in Multiple Mode
- Forwarding Without a Shared Interface
- Forwarding with a Shared Interface

### **Configuration of Security Contexts**

- Step 1: Enable Multiple Security Contexts Globally
- Step 2: Set Up the System Execution Space
- Step 3: Configure Interfaces
- Step 4: Specify a Configuration URL
- Step 5: Configure an Admin Context
- Step 6: Configure a User Context
- Step 7: Manage the Security Contexts (Optional)
- Step 8: Resource Management (Optional)
  - Step 1: Define a Resource Class
  - Step 2: Map the Resource Class to a Context

### **Deployment Scenarios**

- Virtual Firewall with Non-Shared Interfaces
- Configuration Steps with ASDM
- Configuration Steps with CLI
- Virtual Firewall with a Shared Interface
- Configuration Steps with ASDM
- Configuration Steps Using CLI

# **Table of Contents**

## Monitoring and Troubleshooting the Security Contexts

- Monitoring

- Troubleshooting

- Security Contexts Are Not Added

- Security Contexts Are Not Saved on the Local Disk

- Security Contexts Are Not Saved on the FTP Server

- User Having Connectivity Issues When Shared Security Contexts Are Used

## Chapter 15 Transparent Firewalls

### Architectural Overview

- Single-Mode Transparent Firewalls

- Packet Flow in an SMTF

- Multimode Transparent Firewalls

- Packet Flow in an MMTF

### Restrictions When Using Transparent Firewalls

- Transparent Firewalls and VPNs

- Transparent Firewalls and NAT

### Configuration of Transparent Firewalls

- Configuration Guidelines

- Configuration Steps

- Step 1: Enable Transparent Firewalls

- Step 2: Set Up Interfaces

- Step 3: Configure an IP Address

- Step 4: Set Up Routes

- Step 5: Configure Interface ACLs

- Step 6: Configure NAT (Optional)

- Step 7: Add Static L2F Table Entries (Optional)

- Step 8: Enable ARP Inspection (Optional)

- Step 9: Modify L2F Table Parameters (Optional)

### Deployment Scenarios

# **Table of Contents**

SMTF Deployment

Configuration Steps Using ASDM

Configuration Steps Using CLI

MMTF Deployment with Security Contexts

Configuration Steps Using ASDM

Configuration Steps Using CLI

## **Monitoring and Troubleshooting Transparent Firewalls**

Monitoring

Troubleshooting

Hosts Are Not Able to Communicate

Moved Host Is Not Able to Communicate

General Syslogging

## **Chapter 16 High Availability**

### **Redundant Interfaces**

Using Redundant Interfaces

Deployment Scenarios

Configuration and Monitoring

### **Static Route Tracking**

Configuring Static Routes with an SLA Monitor

Floating Connection Timeout

Sample Backup ISP Deployment

### **Failover**

Unit Roles and Functions in Failover

Stateful Failover

Active/Standby and Active/Active Failover

Failover Hardware and Software Requirements

Zero Downtime Upgrade in Failover

Failover Licensing

Failover Interfaces

# **Table of Contents**

Stateful Link

Failover Link Security

Data Interface Addressing

Asymmetric Routing Groups

Failover Health Monitoring

State and Role Transition

Configuring Failover

Basic Failover Settings

Data Interface Configuration

Failover Policies and Timers

Active/Active Failover

Monitoring and Troubleshooting Failover

Active/Standby Failover Deployment Scenario

## **Clustering**

Unit Roles and Functions in Clustering

Master and Slave Units

Flow Owner

Flow Director

Flow Forwarder

Clustering Hardware and Software Requirements

Zero Downtime Upgrade in Clustering

Unsupported Features

Cluster Licensing

Control and Data Interfaces

Spanned EtherChannel Mode

Individual Mode

Cluster Management

Cluster Health Monitoring

Network Address Translation

Performance

# **Table of Contents**

Centralized Features

Scaling Factors

Packet Flow

TCP Connection Processing

UDP Connection Processing

Centralized Connection Processing

State Transition

Configuring Clustering

Setting Interface Mode

Management Access for ASDM Deployment

Building a Cluster

Data Interface Configuration

Monitoring and Troubleshooting Clustering

Spanned EtherChannel Cluster Deployment Scenario

## **Chapter 17 Implementing Cisco ASA Intrusion Prevention System (IPS)**

### **IPS Integration Overview**

IPS Logical Architecture

IPS Hardware Modules

IPS Software Modules

Inline and Promiscuous Modes

IPS High Availability

### **Cisco IPS Software Architecture**

MainApp

AuthenticationApp

Attack Response Controller

cipsWebserver

Logger

CtlTransSource

NotificationApp

# **Table of Contents**

SensorApp

CollaborationApp

EventStore

## **Preparing ASA IPS for Configuration**

Installing CIPS System Software

Accessing CIPS from the ASA CLI

Configuring Basic Management Settings

Setting Up ASDM for IPS Management

Installing the CIPS License Key

## **Configuring CIPS Software on ASA IPS**

Custom Signatures

Remote Blocking

Anomaly Detection

Global Correlation

## **Maintaining ASA IPS**

User Account Administration

Administrator Account

Operator Account

Viewer Account

Service Account

Adding, Changing, and Deleting Users

Displaying CIPS Software and Process Information

Upgrading CIPS Software and Signatures

One-Time Upgrades

Scheduled Upgrades

Backing Up ASA IPS Configuration

Displaying and Clearing Events

## **Configuring ASA for IPS Traffic Redirection**

### **Botnet Traffic Filter**

Dynamic and Local Blacklist Data

# **Table of Contents**

DNS Snooping

Traffic Selection

## **Chapter 18 Tuning and Monitoring IPS**

IPS Tuning Process

Risk Ratings

ASR

TVR

SFR

ARR

PD

WLR

Disabling IPS Signatures

Retiring IPS Signatures

Tools to Help with Monitoring and Tuning

ASDM and IME

CSM Event Manager

Removing False Positive IPS Events from the Event Table

Splunk

RSA Security Analytics

Displaying and Clearing Statistics in the Cisco ASA IPS

## **Chapter 19 Site-to-Site IPsec VPNs**

Preconfiguration Checklist

Configuration Steps

Step 1: Enable ISAKMP

Step 2: Create the ISAKMP Policy

Step 3: Set Up the Tunnel Groups

Step 4: Define the IPsec Policy

Step 5: Create a Crypto Map

Step 6: Configure Traffic Filtering (Optional)

# **Table of Contents**

Step 7: Bypass NAT (Optional)

Step 8: Enable Perfect Forward Secrecy (Optional)

Alternative Configuration Methods Through ASDM

Defining Site-to-Site Tunnel Using the IPsec VPN Wizard

Defining a Site-to-Site Tunnel Through a Connection Profile

## **Optional Attributes and Features**

OSPF Updates over IPsec

Reverse Route Injection

NAT Traversal

Tunnel Default Gateway

Management Access

Fragmentation Policies

## **Deployment Scenarios**

Single Site-to-Site Tunnel Configuration Using NAT-T, RRI, and IKEv2

Configuration Steps Through ASDM

Configuration Steps Through CLI

Hub and Spoke Using Security Contexts

Configuration Steps Through ASDM

Configuration Steps Through CLI

## **Monitoring and Troubleshooting Site-to-Site IPsec VPNs**

Monitoring Site-to-Site VPNs

Troubleshooting Site-to-Site VPNs

ISAKMP Proposal Unacceptable

Mismatched Preshared Keys

Incompatible IPsec Transform Set

Mismatched Proxy Identities

ISAKMP Captures

## **Chapter 20 IPsec Remote-Access VPNs**

Cisco IPsec Remote Access VPN Solution



# **Table of Contents**

IPsec (IKEv1) Remote-Access Configuration Steps

Using the ASDM IPsec IKEv1 Remote Access VPN Wizard

Manually Configuring IPsec (IKEv1) VPN Using ASDM and CLI

Configuring Group Policies

Configuring a Tunnel Group

IPsec (IKEv2) Remote-Access Configuration Steps

Step 1: Introduction

Step 2: Connection Profile Identification

Step 3: VPN Protocols

Step 4: Client Images

Step 5: Specify User Authentication Method

Step 6: Specify an Address Pool

Step 7: Network Name Resolution Servers

Step 8: NAT Exemption

Step 9: AnyConnect Client Deployment

Hardware-Based VPN Clients

## **Advanced Cisco IPsec VPN Features**

Tunnel Default Gateway

Transparent Tunneling

NAT Traversal

IPsec over UDP

IPsec over TCP

IPsec Hairpinning

VPN Load Balancing

Client Firewalling

Personal Firewall Check

Central Protection Policy

Hardware-Based Easy VPN Client Features

Interactive Client Authentication

Individual User Authentication

# **Table of Contents**

LEAP Bypass

Cisco IP Phone Bypass

Hardware Client Network Extension Mode

## **L2TP over IPsec Remote-Access VPN (IKEv1)**

L2TP over IPsec Remote-Access Configuration Steps

Step 1: Select Tunnel Interface

Step 2: Select Remote Access Client

Step 3: Select VPN Client Authentication Method

Step 4: Specify User Authentication Method

Step 5: User Accounts

Step 6: Specify an Address Pool

Step 7: Specify Attributes Pushed to Clients

Step 8: Select the IPsec Settings (Optional)

Step 9: Verify the Configuration

Windows L2TP over IPsec Client Configuration

## **Deployment Scenarios**

Load Balancing of Cisco IPsec Clients and Site-to-Site Integration

Configuration Steps Through ASDM

Configuration Steps Using the CLI

## **Monitoring and Troubleshooting Cisco Remote-Access VPNs**

Monitoring Cisco Remote-Access IPsec VPNs

Troubleshooting Cisco IPsec VPN Clients

## **Chapter 21 Configuring and Troubleshooting PKI**

### **Introduction to PKI**

Certificates

Certificate Authority

Certificate Revocation List

Simple Certificate Enrollment Protocol

### **Installing Certificates**

# **Table of Contents**

Installing Certificates Through ASDM

Installing a CA Certificate from a File

Installing an Identity Certificate from a File

Installing a CA Certificate by the Copy-and-Paste Method

Installing a CA Certificate Using SCEP

Installing an Identity Certificate Using SCEP

Installing Certificates Using the CLI

Generating the RSA Key Pair in the CLI

Configuring a Trustpoint

Manual (Cut-and-Paste) Enrollment via the CLI

Configuring CRL Options via the CLI

## **The Local Certificate Authority**

Configuring the Local CA Through ASDM

Configuring the Local CA Using the CLI

Enrolling Local CA Users Through ASDM

Enrolling Local CA Users Through the CLI

## **Configuring IPsec Site-to-Site Tunnels Using Certificates**

## **Configuring the Cisco ASA to Accept Remote-Access IPsec VPN Clients Using Certificates**

## **Troubleshooting PKI**

Time and Date Mismatch

SCEP Enrollment Problems

CRL Retrieval Problems

## **Chapter 22 Clientless Remote-Access SSL VPNs**

### **SSL VPN Design Considerations**

User Connectivity

ASA Feature Set

Infrastructure Planning

Implementation Scope

### **SSL VPN Prerequisites**

# **Table of Contents**

SSL VPN Licenses

AnyConnect Premium

AnyConnect Essentials

AnyConnect Mobile

Shared Premium Licensing

VPN Flex Licenses

Client Operating System and Browser and Software Requirements

Infrastructure Requirements

## **Pre-SSL VPN Configuration Guide**

Enroll Digital Certificates (Recommended)

Step 1: Obtaining a CA Certificate

Step 2: Request a Certificate

Step 3: Apply Identity Certificate for SSL VPN Connections

Set Up Tunnel and Group Policies

Configure Group Policies

Configure a Tunnel Group

Set Up User Authentication

## **Clientless SSL VPN Configuration Guide**

Enable Clientless SSL VPN on an Interface

Configure SSL VPN Portal Customization

Logon Page

Portal Page

Logout Page

Portal Customization and User Group

Full Customization

Configure Bookmarks

Configure Websites

Configure File Servers

Apply a Bookmark List to a Group Policy

Single Sign-on

# **Table of Contents**

- Configure Web-Type ACLs
- Configure Application Access
- Configure Port Forwarding
- Configure Smart Tunnels
- Configure Client-Server Plug-ins

## **Cisco Secure Desktop**

- CSD Components
- Secure Desktop Manager
- Secure Desktop
- Cache Cleaner
- CSD Requirements
- Supported Operating Systems
- User Privileges
- Supported Internet Browsers
- Internet Browser Settings
- CSD Architecture
- Configuring CSD
- Step 1: Load the CSD Package
- Step 2: Define Prelogin Sequences

## **Host Scan**

- Host Scan Modules
- Basic Host Scan
- Endpoint Assessment
- Advanced Endpoint Assessment
- Configuring Host Scan
- Set Up Basic Host Scan
- Enable Endpoint Host Scan
- Set Up an Advanced Endpoint Host Scan

## **Dynamic Access Policies**

- DAP Architecture

# **Table of Contents**

DAP Sequence of Events

Configuring DAP

Choose AAA Attributes

Choose Endpoint Attributes

Define Access Policies

## **Deployment Scenario**

Step 1: Define Clientless Connections

Step 2: Configure DAP

## **Monitoring and Troubleshooting SSL VPN**

Monitoring SSL VPN

Troubleshooting SSL VPN

Troubleshooting SSL Negotiations

Troubleshooting Clientless Issues

Troubleshooting CSD

Troubleshooting DAP

## **Chapter 23 Client-Based Remote-Access SSL VPNs**

### **SSL VPN Deployment Considerations**

Cisco AnyConnect Secure Mobility Client Licenses

Cisco ASA Design Considerations

ASA Feature Set

Infrastructure Planning

Implementation Scope

### **SSL VPN Prerequisites**

Client Operating System and Browser and Software Requirements

Supported Operating Systems

Compatible Browsers

Infrastructure Requirements

ASA Placement and Requirements

User Account

Administrative Privileges

# **Table of Contents**

## **Pre-SSL VPN Configuration Guide**

Enrolling Digital Certificates (Recommended)

Setting Up Tunnel and Group Policies

Configuring Group Policies

Configuring a Tunnel Group

Setting Up User Authentication

## **Cisco AnyConnect Secure Mobility Client Configuration Guide**

Loading the Cisco AnyConnect Secure Mobility Client Package

Defining the Cisco AnyConnect Secure Mobility Client Attributes

Enabling Cisco AnyConnect Secure Mobility Client VPN Client  
Functionality

Defining a Pool of Addresses

Advanced Full Tunnel Features

Split Tunneling

DNS and WINS Assignment

Keeping the SSL VPN Client Installed

Configuring DTLS

Configuring Traffic Filters

AnyConnect Client Configuration

Creating AnyConnect Client Profile

Connecting from AnyConnect Client

## **Deployment Scenario of AnyConnect Client**

Step 1: Set Up CSD for Registry Check

Step 2: Set Up RADIUS for Authentication

Step 3: Configure AnyConnect SSL VPN

Step 4: Enable Address Translation for Internet Access

## **Monitoring and Troubleshooting AnyConnect SSL VPNs**

Troubleshooting SSL VPN

Troubleshooting SSL Negotiations

Troubleshooting AnyConnect Client Issues

# **Table of Contents**

## **Chapter 24 IP Multicast Routing**

- IGMP Support

- PIM Sparse Mode

- Configuring IP Multicast Routing

  - Enabling Multicast Routing

  - Statically Assigning an IGMP Group

  - Limiting IGMP States

  - IGMP Query Timeout

  - Defining the IGMP Version

  - Enabling PIM

  - Configuring Rendezvous Points

  - Filtering PIM Neighbors

  - Configuring a Static Multicast Route

- Troubleshooting IP Multicast Routing

  - Useful show Commands

  - Useful debug Commands

## **Chapter 25 Quality of Service**

- QoS Types

  - Traffic Prioritization

  - Traffic Policing

  - Traffic Shaping

- QoS Architecture

  - Packet Flow Sequence

  - Packet Classification

  - IP Precedence Field

  - IP DSCP Field

  - IP Access Control List

  - IP Flow

  - VPN Tunnel Group



# **Table of Contents**

QoS and VPN Tunnels

## **Configuring Quality of Service**

QoS Configuration via ASDM

Step 1: Tune Priority Queue

Step 2: Define a Service Policy

Step 3: Specify Traffic Classification Criteria

Step 4: Apply an Action Rule

QoS Configuration via CLI

Step 1: Tune the Priority Queue

Step 2: Set Up a Class Map

Step 3: Configure a Policy Map

Step 4: Apply the Policy Map on the Interface

## **QoS Deployment Scenario**

Configuration Steps Through ASDM

Configuration Steps Through the CLI

## **Monitoring QoS**

## **Index**