

ITNW 1049 [formerly CPMT 2034]

Course Syllabus/Outline Development Form

1. NAME OF COURSE:

CISCO Fundamentals of Network Security:

2. NUMBER OF CLOCK HOURS:

140 hrs

3. COURSE DESCRIPTION:

Fundamentals of Network Security is designed to prepare students for certification in this field. This 140-hour, two-part course is an introduction to **network security** and overall **security** processes. The first component of the course, **Network Security 1 (NS1)**, focuses on the overall **security** processes in a **network** with an emphasis on hands-on skills in the following areas: **Security** policy design and management, **Security** technologies, products, and solutions, Firewall and secure router design, installation, configuration, and maintenance, AAA implementation using routers and firewalls, Securing the **network** at Layers 2 and 3 of the OSI model. **Network Security 2 (NS2)** builds on the topics introduced in NS1 with additional emphasis on the following areas: Intrusion prevention implementation using routers and firewalls, VPN implementation using routers and firewalls. After completing this course, students will be prepared to take the Securing Networks with Cisco Routers and Switches (SNRS) and Securing Networks with PIX and ASA (SNPA) Security Certification exams.

4. COURSE LEARNING OBJECTIVES:

1. Explain security policy design and management.
2. Implement security technologies, products and solutions
3. Implement firewall and secure router design, installation, configuration and maintenance
4. Perform AAA implementation using routers and firewalls
5. Implement VPN using routers and firewalls

5. RATIONALE:

Over 80% of worldwide internet traffic is controlled by CISCO routers and hubs, and those certified by CISCO in the computer networking field are in high demand.

6. REQUIRED MATERIALS:

Students will be provided with official CICSO study materials.

7. EVALUATION:

Those who participate in class discussions, score 70% or higher on the final exam, and miss no more than three class meetings will be awarded seven continuing education units.

8. COURSE OUTLINE:

Network Security I

Lab Activity: Lab Activity: Lab Activity:

Module 1 – 10 Outline

Module 1: Vulnerabilities, Threats, and Attacks

1.1 Introduction to Network Security

1.1.1 The need for network security

Lab 1.1.1 Student Lab Orientation

1.1.2 Identifying potential risks to network security

1.1.3 Open versus closed security models

1.1.4 Trends driving network security

1.1.5 Information security organizations

1.2 Introduction to Vulnerabilities, Threats, and Attacks

1.2.1 Vulnerabilities

1.2.2 Threats

1.2.3 Attacks

1.3 Attack Examples

1.3.1 Reconnaissance attacks

1.3.2 Access attacks

1.3.3 Denial of service attacks

1.3.4 Distributed denial of service attacks

Lab 1.3.4 Vulnerabilities and Exploits

1.3.5 Malicious code

1.4 Vulnerability Analysis

1.4.1 Policy review

1.4.2 Network analysis

1.4.3 Host analysis

1.4.4 Analysis tools

Module 2: Security Planning and Policy

2.1 Discussing Network Security and Cisco

2.1.1 The security wheel

2.1.2 Network security policy

Lab 2.1.2 Designing a Security Plan

Lab Activity: Lab Activity: Lab Activity:

2.2 Endpoint Protection and Management

2.2.1 Host and server based security components and technologies

2.2.2 PC management

2.3 Network Protection and Management

2.3.1 Network based security components and technologies

2.3.2 Network security management

2.4 Security Architecture

2.4.1 Security architecture (SAFE)

2.4.2 The Cisco Self-Defending Network

2.4.3 Cisco integrated security

2.4.4 Plan, Design, Implement, Operate, Optimize (PDIOO)

2.5 Basic Router Security

2.5.1 Control access to network devices

2.5.2 Remote configuration using SSH

Lab 2.5.2a Configure SSH

Lab 2.5.2b Controlling TCP/IP Services

2.5.3 Router passwords

2.5.4 Router privileges and accounts

2.5.5 IOS network services

2.5.6 Routing, proxy ARP and ICMP

2.5.7 Routing protocol authentication and update filtering

Lab 2.5.7 Configure Routing Authentication and Filtering

2.5.8 NTP, SNMP, router name, DNS

Module 3: Security Devices

3.1 Device Options

3.1.1 Appliance-based, server-based, and integrated firewalls

3.1.2 Cisco IOS Firewall feature set

3.1.3 PIX Security Appliance

3.1.4 Adaptive Security Appliance

3.1.5 Finesse Operating System

3.1.6 Firewall Services Module

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:

3.2 Using Security Device Manager

3.2.1 Security Device Manager (SDM) overview

3.2.2 SDM software

3.2.3 Using the SDM startup wizard

Lab 3.2.3 Configure Basic Security using SDM

3.2.4 SDM user interface

3.2.5 SDM wizards

3.2.6 Using SDM to configure a WAN

3.2.7 Using the factory reset wizard

3.2.8 Monitor mode

3.3 Introduction to the Cisco Security Appliance Family

3.3.1 PIX Security Appliance models

3.3.2 Adaptive Security Appliance models

3.3.3 Security appliance licensing

3.3.4 Expanding the features of the security appliance

3.4 Getting Started with the PIX Security Appliance

3.4.1 User interface

3.4.2 Configuring the PIX Security Appliance

3.4.3 Security levels

3.4.4 Basic PIX Security Appliance configuration commands

3.4.5 Additional PIX Security Appliance configuration commands

E-Lab 3.4.5 Basic PIX Security Appliance Commands

3.4.6 Examining the PIX Security Appliance status

E-Lab 3.4.6 PIX Security Appliance show Commands

Lab 3.4.6a Configure the PIX Security Appliance using Setup Mode and ASDM Startup Wizard

Lab 3.4.6b Configure the PIX Security Appliance using CLI

3.4.7 Time setting and NTP support

3.4.8 Syslog configuration

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:

3.5 PIX Security Appliance Translations and Connections

3.5.1 Transport protocols

3.5.2 Network address translation (NAT)

E-Lab 3.5.2 Configure Internet Access on a PIX Security Appliance

3.5.3 Port address translation (PAT)

E-Lab 3.5.3 PIX Security Appliance PAT Configuration

3.5.4 The static command

3.5.5 The identity nat command

E-Lab 3.5.5 PIX Security Appliance NAT 0 Configuration

3.5.6 Connections and translations

3.5.7 Configuring multiple interfaces

E-Lab 3.5.7 Configure a PIX Security Appliance with Three Interfaces

E-Lab 3.5.7 Configure a PIX Security Appliance with Four Interfaces

3.6 Manage a PIX Security Appliance with Adaptive Security Device Manager (ASDM)

3.6.1 ASDM overview

3.6.2 ASDM operating requirements

3.6.3 Prepare for ASDM

Lab 3.6.3 Configuring the PIX Security Appliance with ASDM

3.6.4 Using ASDM to configure the PIX Security Appliance

3.7 PIX Security Appliance Routing Capabilities

3.7.1 Virtual LANs

3.7.2 Static and RIP routing

3.7.3 OSPF

3.7.4 Multicast routing

3.8 Firewall Services Module (FWSM) Operation

3.8.1 Firewall Services Module overview

3.8.2 Getting started with the FWSM

3.8.3 Using PDM with the FWSM

Module 4: Trust and Identity Technology

4.1 Authentication, Authorization, and Accounting (AAA)

4.1.1 TACACS+

4.1.2 RADIUS

4.1.3 Comparing TACACS+ and RADIUS

4.2 Authentication Technologies

4.2.1 Static passwords

4.2.2 One-time passwords and token cards

4.2.3 Digital certificates

4.2.4 Biometrics

4.3 Identity Based Networking Services (IBNS)

4.3.1 Introduction to IBNS

4.3.2 802.1x

4.3.3 Wired and wireless implementations

4.4 Network Admission Control (NAC)

4.4.1 NAC components

4.4.2 NAC phases

4.4.3 NAC operation

4.4.4 NAC vendor participation

Module 5: Cisco Secure Access Control Server

5.1 Cisco Secure Access Control Server (CSACS) for Windows

5.1.1 Cisco Secure Access Control Server product overview

5.1.2 Authentication and user databases

5.1.3 The Cisco Secure ACS user database

5.1.4 Keeping databases current

5.1.5 Cisco Secure ACS for Windows architecture

5.1.6 How Cisco Secure ACS authenticates users

5.1.7 User changeable passwords

5.2 Configuring RADIUS and TACACS+ with CSACS

5.2.1 Installation steps

Lab 5.2.1 Install and Configure CSACS 3.3 for Windows

5.2.2 Administering Cisco Secure ACS for Windows

5.2.3 Troubleshooting

5.2.4 Enabling TACACS+

5.2.5 Verifying TACACS+

5.2.6 Configuring RADIUS

Module 6: Configure Trust and Identity at Layer 3

6.1 Cisco IOS Firewall Authentication Proxy

6.1.1 Cisco IOS Firewall authentication proxy

6.1.2 AAA server configuration

6.1.3 AAA configuration

Lab 6.1.3 Configure Local AAA on Cisco Router

6.1.4 Allow AAA traffic to the router

Lab 6.1.4 Configure Authentication Proxy

6.1.5 Authentication proxy configuration

E-Lab 6.1.5 Configure AAA

E-Lab 6.1.5 Configure Authentication

E-Lab 6.1.5 Configure Authentication Proxy on Cisco Router

6.1.6 Test and verify authentication proxy

E-Lab 6.1.6 Test and Verify AAA

6.2 Introduction to PIX Security Appliance AAA Features

6.2.1 PIX Security Appliance authentication

6.2.2 PIX Security Appliance authorization

6.2.3 PIX Security Appliance accounting

6.2.4 AAA server support

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:

6.3 Configure AAA on the PIX Security Appliance

6.3.1 PIX Security Appliance access authentication

6.3.2 Interactive user authentication

6.3.3 The local user database

6.3.4 Authentication prompts and timeout

6.3.5 Cut-through proxy authentication

E-Lab 6.3.5 Configure PIX Security Appliance
Authentication

6.3.6 Authentication of Non-Telnet, FTP, or HTTP traffic

E-Lab 6.3.6 Authentication of Non-Telnet, FTP or HTTP
Traffic with the PIX Security Appliance

6.3.7 Authorization configuration

E-Lab 6.3.7a PIX Security Appliance Authorization
Configuration

E-Lab 6.3.7b PIX Security Appliance AAA Configuration
Lab

6.3.8 Downloadable ACLs

6.3.9 Accounting configuration

Lab 6.3.9 Configure Local AAA on the PIX Security
Appliance

6.3.10 Troubleshooting the AAA configuration

Lab 6.3.10 Configure AAA on the PIX Security Appliance
Using Cisco Secure ACS for Windows 2000

Module 7: Configure Trust and Identity at Layer 2

7.1 Identity-Based Networking Services (IBNS)

7.1.1 IBNS overview

7.1.2 IEEE 802.1x

7.1.3 802.1x components

7.1.4 802.1x applications with Cisco IOS Software

7.1.5 How 802.1x works

7.1.6 Selecting the correct Extensible Authentication Protocol (EAP)

7.1.7 IBNS and Cisco Secure ACS

7.1.8 ACS deployment considerations

7.1.9 Cisco Secure ACS RADIUS profile configuration

Lab 7.1.9 Configure EAP on Cisco ACS for Windows

7.2 Configuring 802.1x Port-Based Authentication

7.2.1 802.1x port-based authentication configuration tasks

7.2.2 Enabling 802.1x authentication

7.2.3 Configuring the switch-to-RADIUS-server communication

7.2.4 Enabling periodic re-authentication

7.2.5 Manually re-authenticating a client connected to a port

7.2.6 Enabling multiple hosts

7.2.7 Resetting the 802.1x configuration to the default values

7.2.8 Displaying 802.1x statistics and status

Lab 7.2.8 Configure 802.1x Port-Based Authentication

Module 8: Configure Filtering on a Router

8.1 Filtering Technologies

8.1.1 Packet filtering

8.1.2 Stateful filtering

8.1.3 URL filtering

8.2 Cisco IOS Firewall Context-Based Access Control

8.2.1 Context-based Access Control (CBAC)

8.2.2 Cisco IOS Access Control Lists (ACL)

8.2.3 How CBAC works

8.2.4 CBAC supported protocols

8.3 8.3 Configure Cisco IOS Firewall Context-Based Access Control

8.3.1 CBAC configuration tasks

8.3.2 Prepare for CBAC

8.3.3 Set audit trails and alerts

E-Lab 8.3.3 Configure CBAC Audit Trails and Alerts

8.3.4 Set global timeouts

8.3.5 Set global thresholds

8.3.6 Half-open connection limits by host

E-Lab 8.3.6 Half-Open Connection Limits

8.3.7 System-defined port-to-application mapping

8.3.8 User-defined port-to-application mapping

E-Lab 8.3.8 Port-to-Application Mapping

8.3.9 Define inspection rules for applications

8.3.10 Define inspection rules for IP fragmentation

8.3.11 Define inspection rules for ICMP

E-Lab 8.3.11 Define Inspection Rules

8.3.12 Apply inspection rules and ACLs to interfaces

E-Lab 8.3.12: Inspection Rules and ACLs Applied to Router Interfaces

8.3.13 Test and verify CBAC

E-Lab 8.3.13 Configure CBAC on a Cisco Router

Lab 8.3.13 Configure Cisco IOS Firewall CBAC

8.3.14 Configure an IOS firewall using SDM

Module 9: Configure Filtering on a PIX Security Appliance

9.1 Configure ACLs and Content Filters

9.1.1 PIX Security Appliance ACLs

9.1.2 Configuring ACLs

9.1.3 ACL line numbers

9.1.4 The icmp command

9.1.5 nat 0 ACLs

9.1.6 Turbo ACLs

9.1.7 Using ACLs

Lab 9.1.7a Configure Access Through the PIX Security Appliance using ASDM

Lab 9.1.7b Configure Access Through the PIX Security Appliance using CLI

Lab 9.1.7c Configure Multiple Interfaces using CLI – Challenge Lab

9.1.8 Malicious code filtering

9.1.9 URL filtering

E-Lab 9.1.9a Filter Java, ActiveX, and URLs with the PIX Security Appliance

E-Lab 9.1.9b URL Filtering with the PIX Security Appliance

Lab 9.1.9 Configure ACLs in the PIX Security Appliance using CLI

9.2 Object Grouping

9.2.1 Overview of object grouping

9.2.2 Getting started with object groups

9.2.3 Configure object groups

Lab 9.2.3 Configure Service Object Groups using ASDM

9.2.4 Nested object groups

9.2.5 Manage object groups

Lab 9.2.5 Configure Object Groups and Nested Object Groups using CLI

Lab Activity: Lab Activity:

9.3 Configure a Security Appliance Modular Policy

9.3.1 Modular policy overview

9.3.2 Configure a class map

9.3.3 Configure a policy map

9.3.4 Configure a service policy

9.4 Configure Advanced Protocol Inspection

9.4.1 Introduction to advanced protocol inspection

9.4.2 Default traffic inspection and port numbers

9.4.3 FTP inspection

9.4.4 FTP deep packet inspection

9.4.5 HTTP inspection

9.4.6 Protocol application inspection

9.4.7 Multimedia support

9.4.8 Real-Time Streaming Protocol (RTSP)

9.4.9 Protocols required to support IP telephony

9.4.10 DNS inspection

Lab 9.4.10 Configure and Test Advanced Protocol
Handling on the Cisco PIX Security
Appliance

Module 10: Configure Filtering on a Switch

10.1 Introduction to Layer 2 Attacks

10.1.1 Types of attacks

10.2 MAC Address, ARP, and DHCP Vulnerabilities

10.2.1 CAM table overflow attack

10.2.2 Mitigating the Content Addressable Memory (CAM) table
overflow attack

10.2.3 MAC spoofing – man in the middle attacks

10.2.4 Mitigating MAC spoofing attacks

Lab 10.2.4 Mitigate Layer 2 Attacks

10.2.5 Using dynamic ARP inspection to mitigate MAC spoofing
attacks

10.2.6 DHCP starvation attacks

10.2.7 Mitigating DHCP starvation attacks

10.3 VLAN Vulnerabilities

10.3.1 VLAN hopping attacks

10.3.2 Mitigating VLAN hopping attacks

10.3.3 Private VLAN vulnerabilities

10.3.4 Defending private VLANs

10.4 Spanning-Tree Protocol Vulnerabilities

10.4.1 Spanning-Tree Protocol vulnerabilities

10.4.2 Preventing Spanning-Tree Protocol manipulation

Network Security 2

Lab Activity:

Module 1 – 8 Outline

Module 1: Intrusion Detection and Prevention Technology

1.1 Overview of Intrusion Detection and Prevention

1.1.1 Introduction to intrusion detection and prevention

1.1.2 Network-based versus host-based

1.1.3 Types of alarms

1.2 Inspection Engine

1.2.1 Signature-based detection

1.2.2 Types of signatures

1.2.3 Anomaly-based detection

1.3 Cisco IDS and IPS Devices

1.3.1 Cisco integrated solutions

1.3.2 Cisco IPS 4200 Series sensors

Module 2: Configure Network Intrusion Detection and Prevention

2.1 Cisco IOS Intrusion Prevention System

2.1.1 Cisco IOS Intrusion Prevention System (IPS)

2.1.2 Cisco IOS IPS signatures

2.1.3 Cisco IOS IPS configuration tasks

2.1.4 Install the Cisco IOS IPS

2.1.5 Configure logging using Syslog or SDEE

2.1.6 Verify the IPS configuration

Lab 2.1.6 Configure a Router with the IOS Intrusion Prevention System

Lab Activity: Lab Activity:

2.2 Configure Attack Guards on the PIX Security Appliance

2.2.1 Mail Guard

2.2.2 DNS Guard

2.2.3 FragGuard and Virtual Reassembly

2.2.4 AAA Flood Guard

2.2.5 SYN Flood Guard

2.2.6 Connection limits

2.3 Configure Intrusion Prevention on the PIX Security Appliance

2.3.1 Intrusion detection and the PIX Security Appliance

2.3.2 Configure intrusion detection

2.3.3 Configure IDS policies

E-Lab 2.3.3 Configure PIX Security Appliance Message
Output to a Syslog Server

Lab 2.3.3 Configure Intrusion Prevention on the PIX
Security Appliance

2.4 Configure Shunning on the PIX Security Appliance

2.4.1 Overview of shunning

2.4.2 Example of shunning an attacker

Module 3: Encryption and VPN Technology

3.1 Encryption Basics

3.1.1 Symmetrical encryption

3.1.2 Asymmetrical encryption

3.1.3 Diffie-Hellman

3.2 Integrity Basics

3.2.1 Hashing

3.2.2 Hashed Method Authentication Code (HMAC)

3.2.3 Digital signatures and certificates

Lab Activity:

3.3 Implementing Digital Certificates

3.3.1 Certificate authority support

3.3.2 Simple Certificate Enrollment Protocol (SCEP)

3.3.3 Microsoft CA server

3.3.4 Enroll a device with a CA

3.4 VPN Topologies

3.4.1 Site-to-site VPNs

3.4.2 Remote access VPNs

3.5 VPN technologies

3.5.1 VPN technology options

3.5.2 WebVPN

3.5.3 Tunneling protocols

3.5.4 Tunnel interfaces

3.6 IPSec

3.6.1 Overview

3.6.2 Authentication Header (AH)

3.6.3 Encapsulating Security Payload (ESP)

3.6.4 Tunnel and transport modes

3.6.5 Security Associations

3.6.6 Five Steps of IPSec

3.6.7 Internet Key Exchange (IKE)

3.6.8 IKE and IPSec

3.6.9 Cisco VPN solutions

Module 4: Configure Site-to-Site VPN using Pre-Shared Keys

4.1 Prepare a Router for Site-to-Site VPN using Pre-shared Keys

4.1.1 IPSec Encryption with pre-shared keys

4.1.2 Planning the IKE and IPSec Policy

4.1.3 Step 1 – Determine ISAKMP (IKE Phase 1) policy

4.1.4 Step 2 – Determine IPSec (IKE Phase 2) Policy

4.1.5 Step 3 – Check the current configuration

4.1.6 Step 4 – Ensure the network works without encryption

4.1.7 Step 5 – Ensure ACLs are compatible with IPSec

E-Lab 4.1.7 Prepare for IPSec

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:

4.2 Configure a Router for IKE Using Pre-shared Keys

4.2.1 Step 1 – Enable or disable IKE

4.2.2 Step 2 – Create IKE policies

4.2.3 Step 3 – Configure pre-shared keys

4.2.4 Step 4 – Verify the IKE configuration

E-Lab 4.2.4 Configure IKE

4.3 Configure a Router with IPSec Using Pre-shared Keys

4.3.1 Steps to configure IPSec

4.3.2 Step 1 – Configure transform set suites

4.3.3 Step 2 – Configure global IPSec SA lifetimes

4.3.4 Step 3 – Create crypto ACLs

4.3.5 Step 4 – Create crypto maps

4.3.6 Step 5 – Apply crypto maps to interfaces

4.4 Testing and Verifying IPSec Configuration

4.4.1 Test and Verify the IPSec Configuration of the Router

4.4.2 Display the configured ISAKMP policies

4.4.3 Display the configured transform sets

4.4.4 Display the current state of IPSec SAs

4.4.5 Display the configured crypto maps

4.4.6 Enable debug output for IPSec events

4.4.7 Enable debug output for ISAKMP events

E-Lab 4.4.7 Configure Cisco IOS IPSec for Pre-Shared Keys

E-Lab 4.4.7 IPSec Transforms Supported in the Cisco IOS Software

Lab 4.4.7 Configure Cisco IOS IPSec using Pre-Shared Keys

4.4.8 Configure a VPN using SDM

Lab 4.4.8a Configure a Cisco GRE over IPSec Tunnel using SDM

Lab 4.4.8b Configure Cisco IOS IPSec with Pre-Shared Keys using SDM

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:
Lab Activity:

4.5 Configure a PIX Security Appliance Site-to-Site VPN using Pre-shared Keys

4.5.1 IPSec configuration tasks

4.5.2 Task 1 – Prepare to Configure VPN Support

4.5.3 Task 2 – Configure IKE Parameters

E-Lab 4.5.3a Enable/Disable IKE on a PIX Security Appliance Interface

E-Lab 4.5.3b Configure an ISAKMP Policy on a PIX Security Appliance

E-Lab 4.5.3c Define a Tunnel Group on a PIX Security Appliance

4.5.4 Task 3 – Configure IPSec parameters

E-Lab 4.5.4a Configure a Crypto ACL on a PIX Security Appliance

E-Lab 4.5.4b Configure a Transform Set and ISAKMP Policy on a PIX Security Appliance

E-Lab 4.5.4c Create a Crypto Map and apply it to a PIX Security Appliance Interface

4.5.5 Task 4 – Test and verify the IPSec configuration

Lab 4.5.5a Configure a PIX Security Appliance Site-to-Site IPSec VPN Tunnel Using CLI

Lab 4.5.5b Configure a PIX Security Appliance Site-to-Site IPSec VPN Tunnel Using ASDM

Module 5: Configure Site to Site VPN using Digital Certificates

5.1 Configuring Certificate Authority (CA) Support on a Cisco Router

5.1.1 Steps to configure CA support

5.1.2 Step 1 – manage the non-volatile RAM (NVRAM)

5.1.3 Step 2 – set the router time and date

5.1.4 Step 3 – add a CA server entry to the router host table

5.1.5 Step 4 – generate an RSA key pair

5.1.6 Step 5 – declare a CA

5.1.7 Step 6 – authenticate the CA

5.1.8 Step 7 – request a certificate for the router

5.1.9 Step 8 – save the configuration

5.1.10 step 9 – monitor and maintain CA interoperability

5.1.11 step 10 – verify the CA support configuration

5.2 Configure an IOS Router Site-to-Site VPN Using Digital Certificates

5.2.1 Configuration Tasks

5.2.2 Task 1 – prepare for IKE and IPSec

5.2.3 Task 2 – configure CA support

E-Lab 5.2.3 Configure CA Support

5.2.4 Task 3 – configure IKE

E-Lab 5.2.4 Configure IKE

5.2.5 Task 4 – configure IPSec

E-Lab 5.2.5 Configure IPSec

5.2.6 Task 5 – test and verify IPSec

E-Lab 5.2.6 Configure Cisco IOS CA Support (RSA Signatures)

E-Lab 5.2.6 Testing & Verifying IPSec

Lab 5.2.6 Configure a Cisco Router for IPSec using Digital Certificates

Lab Activity: Lab Activity: Lab Activity: Lab Activity:

5.3 Configure a PIX Security Appliance Site-to-Site VPN Using Digital Certificates

5.3.1 Scaling PIX Security Appliance VPNs

5.3.2 Enroll the PIX Security Appliance with a CA

E-Lab 5.3.2 Configure Cisco PIX Security Appliance for CA Support (RSA Signatures)

Lab 5.3.2 Configure a PIX Security Appliance Site-to-Site IPSec VPN Tunnel with CA support

Module 6: Configure Remote Access VPN

6.1 Introduction to Cisco Easy VPN

6.1.1 Introduction to Cisco Easy VPN

6.1.2 Overview of the Easy VPN Server

6.1.3 Overview of the Easy VPN Remote

6.1.4 How the Cisco Easy VPN Works

6.1.5 Easy VPN Remote client connection in detail

6.2 Configure the Easy VPN Server

6.2.1 Cisco Easy VPN Server configuration tasks

6.2.2 Task 1 – create an IP address pool

6.2.3 Task 2 – configure group policy lookup

6.2.4 Task 3 – create ISAKMP policy for remote VPN access

6.2.5 Task 4 – define a group policy for a mode configuration push

6.2.6 Task 5 – create a transform set

6.2.7 Task 6 – create a dynamic crypto map with RRI

6.2.8 Task 7 – apply mode configuration to the dynamic crypto map

6.2.9 Task 8 – apply a dynamic crypto map to the router interface

6.2.10 Task 9 – enable IKE dead peer detection

6.2.11 Task 10 – (optional) configure XAUTH

6.2.12 Task 11 – (optional) enable XAUTH save password feature

Lab 6.2.12a Configure Remote Access Using Cisco Easy VPN

Lab 6.2.12b Configure Cisco Easy VPN Server with NAT

Lab Activity:

6.3 Configure Easy VPN Remote for the Cisco VPN Client 4.x

6.3.1 Cisco Easy VPN Client 4.x configuration tasks

6.3.2 Task 1 – install the Cisco VPN Client 4.x on the remote PC

6.3.3 Task 2 – create a new client connection entry

6.3.4 Task 3 – choose an authentication method

6.3.5 Task 4 – configure transparent tunneling

6.3.6 Task 5 – enable and add backup servers

6.3.7 Task 6 – configure connection to the Internet through dial-up networking

E-Lab 6.3.7 Configure the Adaptive Security Appliance for WebVPN

6.4 Configure Cisco Easy VPN Remote for Access Routers

6.4.1 Easy VPN Remote modes of operation

6.4.2 Configuration tasks for Cisco Easy VPN Remote for access routers

6.4.3 Task 1 – configure the DHCP server pool

6.4.4 Task 2 – configure and assign the Cisco Easy VPN Client profile

6.4.5 Task 3 – (optional) configure XAUTH save password feature

6.4.6 Task 4 – (optional) initiate the VPN tunnel

6.4.7 Task 5 – verify the Cisco Easy VPN configuration

Lab Activity: Lab Activity:

- 6.5 Configure the PIX Security Appliance as an Easy VPN Server
 - 6.5.1 Easy VPN Server general configuration tasks
 - 6.5.2 Task 1 – create ISAKMP policy for remote VPN Client access
 - 6.5.3 Task 2 – create an IP address pool
 - 6.5.4 Task 3 – define a group policy for mode configuration push
 - 6.5.5 Task 4 – create a transform set
 - 6.5.6 Tasks 5 through 7– dynamic crypto map
 - 6.5.7 Task 8 – configure XAUTH
 - 6.5.8 Task 9 – configure NAT and NAT 0
 - 6.5.9 Task 10 – enable IKE dead peer detection
 - Lab 6.5.9a Configure a Secure VPN Using IPsec between a PIX and a VPN Client using ASDM
 - Lab 6.5.9b Configure a Secure VPN Using IPsec between a PIX and a VPN Client using CLI
- 6.6 Configure a PIX 501 or 506 as an easy VPN client
 - 6.6.1 Firewall appliance Easy VPN Remote feature overview
 - 6.6.2 Easy VPN Remote configuration
 - 6.6.3 Easy VPN Client device mode and enabling Easy VPN Remote clients
 - 6.6.4 Easy VPN Remote authentication
- 6.7 Configure the Adaptive Security Appliance to Support WebVPN
 - 6.7.1 WebVPN end-user interface
 - 6.7.2 Configure WebVPN general parameters
 - 6.7.3 Configure WebVPN servers and URLs
 - 6.7.4 Configure WebVPN port forwarding
 - 6.7.5 Configure WebVPN e-mail proxy
 - 6.7.6 Configure WebVPN content filters and ACLs

Module 7: Secure Network Architecture and Management

7.1 Layer 2 Security Best Practices

7.1.1 Factors affecting layer 2 mitigation techniques

7.1.2 Single security zone, one user group, single physical switch

7.1.3 Single security zone, one user group, multiple physical switches

7.1.4 Single security zone, multiple user groups, single physical switch

7.1.5 Single security zone, multiple user groups, multiple physical switches

7.1.6 Multiple security zones, one user group, single physical switch

7.1.7 Multiple security zones, one user group, multiple physical switches

7.1.8 Multiple security zones, multiple user groups, single physical switch

7.1.9 Multiple security zones, multiple user groups, multiple physical switches

7.1.10 Layer 2 security best practices

7.2 SDM Security Audit

7.2.1 Using SDM to perform security audits

7.2.2 Using SDM monitor mode

7.3 Router Management Center (MC)

7.3.1 Introduction to the Router MC

7.3.2 Key concepts in the Router MC

7.3.3 Supported tunneling technologies

7.3.4 Router MC installation

7.3.5 Installation process

7.3.6 Getting started with the Router MC

7.3.7 Router MC interface

7.3.8 Installation process

7.3.9 Basic work flow and tasks

7.4 Simple Network Management Protocol (SNMP)

7.4.1 SNMP introduction

7.4.2 SNMP security

7.4.3 SNMP Version 3 (SNMPv3)

7.4.4 SNMP management applications

7.4.5 Configure SNMP support on an IOS router

Lab 7.4.5 Configure SNMP Messages on a Cisco Router

7.4.6 Configure SNMP support on a PIX Security Appliance

Lab 7.4.6 Configure SNMP Monitoring of the PIX Security Appliance Using ASDM

Module 8: PIX Security Appliance Contexts, Failover, and Management

8.1 Configure a PIX Security Appliance to Perform in Multiple Context Mode

8.1.1 Security context overview

8.1.2 Enable multiple context mode

8.1.3 Configure a security context

8.1.4 Managing security contexts

8.2 Configure PIX Security Appliance Failover

8.2.1 Understanding failover

8.2.2 Failover requirements

8.2.3 Serial cable-based failover configuration

8.2.4 Active/standby LAN-based failover configuration

E-Lab 8.2.4 Configure a PIX Security Appliance for Active/Standby Failover

Lab 8.2.4 Configure LAN-Based Failover Between Two PIX Security Appliances (OPTIONAL)

8.2.5 Active/active failover

Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity: Lab Activity:

8.3 Configure Transparent Firewall Mode

8.3.1 Transparent firewall mode overview

8.3.2 Enable transparent firewall mode

8.3.3 Monitor and maintain a transparent firewall

Lab 8.3.3 Configure a PIX Security Appliance as a Transparent Firewall

8.4 PIX Security Appliance Management

8.4.1 Managing Telnet access

E-Lab 8.4.1 The PIX Security Appliance telnet Command

8.4.2 Managing SSH access

8.4.3 Command authorization

Lab 8.4.3a Configure User Authentication and Command Authorization using ASDM

Lab 8.4.3b Configure SSH, Command Authorization, and Local User Authentication using CLI

8.4.4 PIX Security Appliance password recovery

Lab 8.4.4 Perform Password Recovery on the PIX Security Appliance

8.4.5 Adaptive Security Appliance password recovery

8.4.6 File management

8.4.7 Image upgrade and activation keys

E-Lab 8.4.7 Upgrade the PIX Security Appliance Software Image