



# Fundamentals of Network Security v1.1

## Scope and Sequence

The screenshot shows the Cisco Networking Academy website interface. At the top left is the Cisco Systems logo. To the right is the text 'CISCO NETWORKING ACADEMY PROGRAM'. Below this is a navigation bar with a dropdown menu labeled 'Modules'. The main content area is divided into three sections: 1. A blue box on the left containing an image of a blue network device and the text 'Take the Fundamentals of Network Security Curriculum Tour'. 2. A central image of a person working at a computer. 3. A grey box on the right titled 'Fundamentals of Network Security' with a detailed description of the course content, including topics like security policy design, router configuration, and VPN implementation.

Last Updated: September 9, 2003

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the Fundamentals of Network Security course as part of an official Cisco Networking Academy Program.

## TABLE OF CONTENTS

<b>FUNDAMENTALS OF NETWORK SECURITY V1.1 .....</b>	<b>1</b>
<b>SCOPE AND SEQUENCE .....</b>	<b>1</b>
<i>Target Audience .....</i>	<i>3</i>
<i>Prerequisites .....</i>	<i>3</i>
<i>Target Certifications .....</i>	<i>3</i>
<i>Course Description .....</i>	<i>3</i>
<i>Course Objectives .....</i>	<i>3</i>
<i>FNS Equipment Bundles .....</i>	<i>4</i>
<i>Minimum System Requirements .....</i>	<i>12</i>
<i>Course Overview .....</i>	<i>14</i>
<i>Course Outline .....</i>	<i>15</i>
<i>Module 1: Overview of Network Security .....</i>	<i>15</i>
<i>Module 2: Basic Router and Switch Security .....</i>	<i>16</i>
<i>Module 3: Router ACLs and CBAC .....</i>	<i>18</i>
<i>Module 4: Router AAA Security .....</i>	<i>20</i>
<i>Module 5: Router Intrusion Detection, Monitoring, and Management .....</i>	<i>22</i>
<i>Module 6: Router Site-to-site VPN .....</i>	<i>23</i>
<i>Module 7: Router Remote Access VPN .....</i>	<i>26</i>
<i>Module 8: PIX Security Appliance .....</i>	<i>27</i>
<i>Module 9: PIX Security Appliance Translations and Connections .....</i>	<i>28</i>
<i>Module 10: PIX Security Appliance ACLs .....</i>	<i>30</i>
<i>Module 11: PIX Security Appliance AAA .....</i>	<i>31</i>
<i>Module 12: PIX Advanced Protocols and Intrusion Detection .....</i>	<i>33</i>
<i>Module 13: PIX Failover and System Maintenance .....</i>	<i>34</i>
<i>Module 14: PIX VPN .....</i>	<i>36</i>
<i>Module 15: PIX Security Appliance Management .....</i>	<i>38</i>

## Target Audience

Advanced High School, Community College, Military and University students as well as transitional workers enrolled in the Cisco Networking Academy Program.

## Prerequisites

Students should have completed Semester 4 CNAP or hold current CCNA certification.

## Target Certifications

Students should be prepared to take the SECUR and CSPFA exams in preparation for the Cisco Firewall Specialist. These exams will also count towards the CCSP certification. Students will also be prepared to take the CompTIA Security+ exam.

## Course Description

Introduction to Network Security course focusing on the overall security processes with particular emphasis on hands on skills in the following areas:

- Security policy design & management
- Security technologies, products & solutions
- Firewall and secure router design, installation, configuration, & maintenance
- AAA implementation using routers and firewalls
- Intrusion Detection (IDS) implementation using routers and firewalls
- VPN implementation using routers and firewalls

## Course Objectives

Upon completion of this course, students will have an understanding of:

- Security terminology & acronyms
- Basic and advance security vulnerabilities
- Security Policy design & management
- Security technologies, products, solutions & design
- Advanced Firewall installation, configuration, monitoring & maintenance
- AAA and IDS implementation using Cisco routers and PIX Firewalls

- VPN implementation using Cisco routers and PIX Firewalls
- Secure Network Design

**The course does not cover essential information about:**

- Unix/Linux operation & configuration.
- Web server installation & configuration.
- Advanced routing & switching technologies
- Advanced remote access technologies (ISDN, dial, xDSL, Broadband Cable)
- Programming techniques.
- E-commerce
- Large-scale web site development and deployment.
- Business management.

## FNS Equipment Bundles

### FNS 1.1 - Standard Bundle

**Standard bundle primary purpose:**

The price/performance ratio of the FNS 1.1 - Standard Bundle is likely to be the most appropriate for Academies.

**Advantages of Standard bundle**

- 1) The Cisco 2950T-24 switch provides a single point of connection for all lab equipment.
- 2) Modular topology which allows for quick and cost effective expansion of student pods using new or existing gear.
- 3) Access to security technologies like modular routers, 802.1q VLAN trunking, and wider variety of hardware and IOS features.
- 4) Cisco 2600XM VPN security router bundle—The virtual private network (VPN) bundle allow academies to use a single part number when ordering a Cisco router with all the necessary VPN and security components at a reduced price compared to ordering each component separately. The bundles include the selected router platform, a VPN hardware card, additional memory, and the Cisco IOS® Software to run IP Security (IPSec) Triple Digital Encryption Standard (3DES) encryption, and Cisco IOS firewall with an intrusion detection system (IDS).
- 5) Recent pricing improvements make the upgrade even more attractive. Academies can also leverage the FNS equipment to add additional router and switch stations to CCNA/CCNP.

### Standard Bundle:

The Standard Lab Equipment Bundle is a value cost bundle allowing Academies to teach configuration of SOHO to enterprise level firewall security implementations using the IOS Firewall and PIX Firewall.

This lab bundle will allow students to gain configuration experience on two 2611XM VPN bundle routers with the IOS Firewall image which supports all features of IOS Firewall such as intrusion detection, stateful inspection, proxy authentication, etc. In addition, standard IOS features such as IP, IP Plus, enterprise and VPN capabilities are supported. The two 2611XM VPN student pod routers will be used in 40% of the labs and will help students prepare for the SECUR exam. The routers can also be used within the firewall labs for additional network integration practice and can be leveraged for CCNA/CCNP labs.

With this bundle, students will configure the enterprise level PIX 515E-R. All of the features except failover and multiple DMZs are configurable using the 515E-R (restricted) model, which is half the cost of the 515E-UR (unrestricted). The PIX Firewall will be used approximately in 60% of the labs and will help students prepare for the CSPFA exam.

The 2950T-24 series switch provides a common connection point for all equipment. A standard configuration with connection descriptions will be made available in the instructor manual. This will minimize the need for crossover cables, hubs, and additional servers by utilizing VLANs. The backbone router will provide routing between the VLANs of both the router and firewall pods without requiring frequent re-cabling. Optional labs can be done to help student understand switch security. The switch and backbone router will be utilized in 100% of the labs.

Overall, the investment in the Standard Lab Equipment Bundle will provide students with a quality, hands-on lab environment to help them prepare for the SECUR and CSPFA exams.

### FNS 1.1 - STANDARD BUNDLE - Version 1.1 (Pricing is Subject to Change)

Firewall/Router Products	Description	Qty	US List	Ext List	Net Price
CISCO2611XM-ADSL	Cisco 2611XM ADSL Bundle	1	\$3,495.00	\$3,495.00	\$1747.50
CISCO2611XM-2FE/VPN/KP	Cisco 2611XM VPN Bundle	2	\$4,995.00	\$9990.00	\$4,995.00
PIX-515E-R-DMZ-BUN	PIX-515E-R-DMZ-BUN (Chassis, 3 FE ports)	2	\$3,695.00	\$7,390.00	\$3,695.00
<b>Subtotal</b>			<b>\$12,185.00</b>	<b>\$20,875.00</b>	<b>\$10,437.50</b>

					<b>Discount</b>	<b>50.0%</b>
<b>Switching Protocols</b>	<b>Description</b>	<b>Qty</b>	<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>	
WS-C2950T-24	24 10/100 ports w/ 2 10/100/1000BASE-T ports, Enhanced Image	1	\$1,295.00	\$1,295.00	\$ 647.50	
<b>SUB-TOTAL</b>			<b>\$1,295.00</b>	<b>\$1,295.00</b>	<b>\$ 647.50</b>	
					<b>DISCOUNT</b>	<b>50.0%</b>
<b>Support Products</b>	<b>Description</b>	<b>Qty</b>	<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>	
CON-SNT-26XX	SMARTnet 8x5xNBD for Cisco26XX	1	\$ 392.00	\$392.00	\$ 274.40	
CON-SNT-26XVPN	SMARTnet 8x5xNBD for Cisco26XX VPN Bundle	2	\$ 400.00	800.00	\$ 560.00	
CON-SNT-C2950T24	SMARTnet 8x5xNBD for Cisco2950T Catalyst Switch	1	\$ 192.00	\$ 192.00	\$ 134.40	
CON-SNT-PIX		2	\$ 419.00	\$ 838.00	\$ 586.60	
<b>SUB-TOTAL</b>			<b>\$ 1,403.00</b>	<b>\$2,222.00</b>	<b>\$ 1555.40</b>	
					<b>DISCOUNT</b>	<b>30.0%</b>
<b>GRAND TOTAL</b>			<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>	
			<b>\$ 1,4883.0</b>	<b>\$24,392.00</b>	<b>\$12,640.40</b>	
<b>Other Products</b>	<b>Description</b>	<b>Qty</b>	<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>	
PILA8470C3	Intel PRO/100 Server Adapter (802.1q support)	1	\$ 100.00	\$ 100.00	\$ 60.00	

## **FNS 1.1 - PIX Pod Bundle**

### **PIX POD bundle primary purpose:**

Academies can:

- 1) Purchase additional PIX pods to reduce the student-to-equipment ratio
- 2) Enable Academies to leverage their existing CCNA/CCNP Routers and switches for primary or additional student pods.\*\*

\*\*Some of the main issues are below. Instructor guides will be developed to help Academies leverage existing equipment. However, support issues which arise may not be readily solved by the Academy help desk and may ultimately rest with the Academies. Instructors will be encouraged to upload any additional materials, instructions, labs, worksheets and study guides to the Academy Connection.

**NOTE:** Academies are also encouraged to purchase additional PIX models through regular discounted channels. Other PIX models which could be leveraged in the course include the 501s, 506s, 525s, and 535s, however, the 501s and 506s do not support failover and DMZ interfaces.

### **Academies with 2500 routers and 1900 switches:**

Primary Issues and modifications:

- 1) A flash and DRAM upgrade is required to load the IOS Firewall image. Also, this image is very slow to boot on a 2500.
- 1) There is no common connection point for the equipment and ISL trunking cannot be achieved with the 2500s and 1900 switch. However, Academies can purchase an Intel Pro server card which supports VLAN trunking. This could provide a central connection point for all Ethernet connections.
- 2) Academies with 2500 series routers must use serial connections between two 2501 student router pods in order to complete the IOS Firewall Labs.
- 3) The lab topology will have to be slightly modified to achieve "WAN" connectivity between routers.
- 4) To avoid addressing and routing issues, an additional 2501 or 2514 will be needed as a backbone router. Otherwise, the WAN addressing must be modified to achieve connectivity and proper routing.
- 5) Not all features of the IOS Firewall feature set are supported by the 2500 series, including IDS and Easy VPN.
- 6) Academies must be prepared to make IOS Flash, RAM and image upgrades as needed to their existing routers.
- 7) Additional web/ftp servers will be required to complete some steps within certain labs. However some testing steps can be completed using simulated traffic or can be skipped.

8) A web server can be connected to an Ethernet port on the backbone router to provide an Internet web/ftp server.

9) With the use of the Intel Pro server card, labs which require DMZ and additional internal servers can be provided from one central server connected to a trunk port on the 1900, provided VLANs and trunking on the 1900 switch is configured correctly.

#### **Academies with 1700 series routers:**

Primary Issues and modifications:

1) A flash and DRAM upgrade is required to load the IOS Firewall image. Also, this image can be slow on a 1700 depending on the model.

1) There is no common connection point for the equipment and ISL trunking may not be possible with the 1700s and 1900 switch, however, academies can purchase an Intel Pro server card which supports VLAN trunking. This could provide a central connection point for all Ethernet connections.

2) Academies with 1700 series routers with only one Ethernet interface must use serial connections between two 1700 student router pods in order to complete the IOS Firewall Labs. The lab topology will have to be slightly modified to achieve "WAN" connectivity between routers.

4) To avoid addressing and routing issue, an additional 1700 with 2 Ethernet interfaces will be needed as a backbone router. Otherwise, the WAN addressing must be modified to achieve connectivity and proper routing.

5) Some features of the IOS Firewall feature set may not be supported by the 1700 series.

6) Academies must be prepared to make IOS flash, ram and image upgrades as needed to their existing routers.

7) Additional web/ftp servers will be required to complete some steps within certain labs.

However some testing steps can be completed using simulated traffic or can be skipped.

8) A web server can be connected a Ethernet port on the backbone router to provide a Internet web/ftp server.

9) With the use of the Intel Pro server card, labs which require DMZ and additional internal servers can be provided from one central server connected to a trunk port on the 1900, provided VLANs and trunking on the 1900 switch is configured correctly.

#### **Academies with 2600 routers and 2900 switches:**

Primary Issues and modifications:

1) The backbone switch, which is the 2900, will have to have use ISL for the VLAN trunking. The pre-configuration for the backbone router will have to be changed from dot1q to ISL encapsulation.

- 1) Two 2611s and one 2621 is required. The 2611s must have 16 MB flash and 64 MB DRAM. The 2621, serving as the backbone router, needs to be capable of IP routing using EIGRP and VLAN trunking.
- 2) Academies which only have 2600 series routers with only 1 Ethernet interface can use serial connections between two 2600 student router pods in order to complete the IOS Firewall Labs. Academies can also add network module (NM) to provide this additional interface.
- 3) The lab topology will have to be slightly modified to achieve "WAN" connectivity between 2610 or 2620 student routers.
- 4) To avoid addressing and routing issues, an additional 2600 will be needed as a backbone router. Otherwise, the WAN addressing must be modified to achieve connectivity and proper routing between 2 directly connected student pods.
- 6) Academies must be prepared to make IOS Flash, RAM and image upgrades as needed to their existing routers.
- 7) Additional web/ftp servers will be required to complete some steps within certain labs, depending on the 2600 models utilized. However some testing steps can be completed using simulated traffic or can be skipped.
- 9) With the use of the Intel Pro server card, labs which require Internet, DMZ and additional internal servers can be provided from one central server, connected to a trunk port on the 2900, provided VLANs and trunking on the 2900 switch is configured correctly.

#### **Academies with the CCNA/CCNP 3.0 Premium bundles**

Primary Issues and modifications

- 1) Instructors will only have to load the appropriate IOS Firewall image on the two student routers.
- 2) Instructors must load the standard FNS pre-configurations on the backbone router and backbone switch.
- 3) Academies who leverage their existing equipment will also need to purchase an Intel PRO/100 Server Adapter with 802.1q support.

#### **Academies with 806 routers**

Primary Issues and modifications

- 1) An 806 router can be used for the IOS Firewall configuration labs either in addition to the standard bundle or standalone.
- 2) The standard FNS pre-configurations on the backbone router may have to be modified if port speed and duplex options have been set.
- 3) The 806 routers require a DRAM upgrade to 32MB to support the IOS Firewall image.

<b>Firewall/Router Products</b>	<b>Description</b>	<b>Qty</b>	<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>
PIX-515E-R-DMZ-BUN	PIX-515E-R-DMZ-BUN (Chassis, 3 FE ports)	2	\$ 3,695.00	\$ 7,390.00	\$ 3,695.00
CON-SNT-PIX515ER	SMARTnet 8x5xNBD for Cisco PIX 515ER	2	\$ 419.00	\$ 838.00	\$ 586.60
<b>SUB-TOTAL</b>			<b>\$ 4,114.00</b>	<b>\$ 8,228.00</b>	<b>\$ 4,281.60</b>
<b>GRAND TOTAL</b>			<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>
			<b>\$ 4,114.00</b>	<b>\$ 8,228.00</b>	<b>\$ 4,281.60</b>

## FNS 1.1 - Remote Bundle

During the time an Academy is actively involved in the Academy Program, it may purchase up to four Bundles at the special Academy discount. This discount is offered only to Cisco Networking Academy Program.

**NOTE:** Academies must configure appropriate WAN services to provide connectivity to the backbone router (RBB) which will serve also as a Remote Terminal Server (RTS) router. Instructor guides will be provided for common scenarios using dialup, DSL, Cable and LAN connectivity

Remote bundle primary purpose:

This hardware addition will allow Academies to offer remote access to any lab equipment for additional hands on remote practice.

With two additions to the backbone router (16 port Asynchronous Module and Octal cable) for Terminal services, students could have remote access to the lab pods outside of the standard class time. Connection options could include dialup, isdn, dsl, cable or LAN connectivity. Academies who currently have any AS router can utilize this for remote access as well.

Academies can also setup remote access to the backbone router, enabling student telnet/SSH access to the devices. However, this requires the lab to be fully functional to gain access to all the devices. Some additional configurations may be required on all of the student devices to enable telnet or SSH access. This type of remote access can be unreliable though, during pod device configurations.

### CCNA OPTIONAL ISDN LAB BUNDLE (Pricing is Subject to Change)

Routing Products	Description	Qty	US List	Ext List	Net Price
NM-16A	16 port Asynchronous module	1	\$ 2,300.00	\$ 2,300.00	\$ 1,150.00
CAB-OCTAL-ASYNC=	CABLE ASYNC 8PORT RJ45	1	\$ 200.00	\$ 200.00	\$ 100.00
<b>SUB-TOTAL</b>			<b>\$ 2,500.00</b>	<b>\$ 2,500.00</b>	<b>\$1,250.00</b>
<b>DISCOUNT</b>					<b>50.0%</b>
<b>GRAND TOTAL</b>			<b>US List</b>	<b>Ext List</b>	<b>Net Price</b>
			<b>\$ 2,500.00</b>	<b>\$ 2,500.00</b>	<b>\$ 1,250.00</b>

## Minimum System Requirements

Curriculum Requirements: 10 Student PC's and 1 curriculum server  
Lab Requirements: 2 Lab PC's or laptops (Win 2000 server)  
1 Lab PC's Win 2000 server  
(SuperServer)

### Curriculum Requirements:

#### PC

Windows 98/98SE, NT 4.0 (SP6), or Windows 2000 (SP2)\*  
400 MHz processor or higher  
Minimum 128 MB, 256MB RAM recommended  
5 GB of available hard-disk space for all applications  
Color Monitor with 256-color (8-bit) or greater video card  
800x600 or greater monitor resolution  
CD-ROM drive  
IE 5.0 or NN 4.7 (or later versions)

#### or Mac:

PowerPC®-based Macintosh® computer  
Mac OS software version 9.0.4  
Minimum 128 MB, 256MB RAM recommended  
5 GB of available hard-disk space  
Color monitor with 256-color (8-bit) or greater video card  
Monitor resolution of 800x600 or greater  
CD-ROM drive  
IE 5.0 or NN 4.7 (or later versions)

#### Server

NT 4.0 (SP6), or Windows 2000 Server (SP2)\*  
800 MHz processor or higher  
Minimum 128 MB, 256MB RAM recommended  
5GB of available hard-disk space  
Color Monitor with 256-color (8-bit) or greater video card  
800x600 or greater monitor resolution

CD-ROM drive  
IE 5.0 or NN 4.7 (or later versions)

### **Lab Requirements:**

#### **PC or Laptops (2 student)**

Win 2000 server, SP 2  
600Mhz processor or higher  
Minimum 256MB of RAM  
10GB of available hard-disk space for all applications  
Color Monitor with 256-color (8-bit) or greater video card  
800x600 or greater monitor resolution  
CD-ROM drive  
IE 5.0 or NN 4.7 (or later versions)

#### **SuperServer (1)**

Win 2000 server, SP 2  
1000MHz processor or higher  
Minimum 256MB of RAM, 512 Recommended  
10GB of available hard-disk space for all applications  
Color Monitor with 256-color (8-bit) or greater video card  
800x600 or greater monitor resolution  
CD-ROM drive  
IE 5.0 or NN 4.7 (or later versions)

It is highly recommended that the SuperServer should not have built in Ethernet port since the Intel Pro Server VLAN card will be installed. However, some server platforms ship with the Intel Pro S card or the port built into the server.

An existing server with a built in NIC can be used. However, if it has a PCI card, remove the card before installing the Intel Pro S card. If the NIC is integrated into the motherboard, the NIC should be disabled before installing the Intel Pro S card. Some support issues may arise that are beyond the academy help desk or support.

## Course Overview

- 1 [Overview of Network Security](#)
  - 2 [Securing the Perimeter Router](#)
  - 3 [ACLs and CABC](#)
  - 4 [Router AAA Security](#)
  - 5 [Intrusion Detection](#)
  - 6 [IP Security](#)
  - 7 [Easy VPN](#)
- Mid-Term Exam (online and hands-on)
- 8 [PIX Firewall](#)
  - 9 [Translations and Connections](#)
  - 10 [Access Control Lists for the PIX Firewall](#)
  - 11 [AAA on PIX Firewalls](#)
  - 12 [PIX IDS](#)
  - 13 [PIX Failover and System Maintenance](#)
  - 14 [PIX VPN](#)
  - 15 [PIX Device Manager](#)
- Final Exam (online and hands-on)

## Course Outline

### Module 1 - 15 Outline

#### Module 1: Overview of Network Security

##### Module Overview

##### 1.1 Overview of Network Security

- 1.1.1 The need for network security
- 1.1.2 Trends that affect network security
- 1.1.3 The goals of network security
- 1.1.4 Key elements of network security
- 1.1.5 Security awareness

Lab: Student Lab Orientation

##### 1.2 Vulnerabilities and Threats

- 1.2.1 Network security weaknesses
- 1.2.2 Primary network threats
- 1.2.3 Reconnaissance
- 1.2.4 Eavesdropping
- 1.2.5 Access
- 1.2.6 Other access attacks
- 1.2.7 Denial of service
- 1.2.8 Distributed denial of service attacks

Lab: Vulnerabilities and Exploits

- 1.2.9 Vulnerabilities - the OSI model layers

##### 1.3 Security Framework and Policy

- 1.3.1 The security wheel
  - 1.3.2 The security wheel in detail
  - 1.3.3 Security policy basics
- Lab: Designing a Security Plan
- 1.3.4 The nature and levels of security policies
  - 1.3.5 Network security case studies

## **1.4 Security Products and Solutions**

- 1.4.1 Overview
- 1.4.2 Identity
- 1.4.3 Firewalls
- 1.4.4 Virtual Private Networks
- 1.4.5 Intrusion detection
- 1.4.6 Monitor, manage, and audit
- 1.4.7 SAFE

### **Module Summary**

### **Module Quiz**

## **Module 2: Basic Router and Switch Security**

### **Module Overview**

### **2.1 General Router and Switch Security**

- 2.1.1 Router topologies
  - PhotoZoom: Cisco 806 Router
  - PhotoZoom: Cisco 2501 Router
  - PhotoZoom: Cisco 2514 Router
  - PhotoZoom: Cisco 2621 Router
  - PhotoZoom: Cisco1721 Router
  - PhotoZoom: Cisco 1751Router
- 2.1.2 Installation
- 2.1.3 Controlling access
- 2.1.4 Passwords
- 2.1.5 Privileges and accounts
- 2.1.6 Login banner
  - Lab: Configure General Router Security

### **2.2 Disable Unneeded Services**

- 2.2.1 IOS network services
  - Lab: Controlling TCP/IP Services
- 2.2.2 Routing, proxy arp, ICMP
- 2.2.3 NTP, SNMP, router name, DNS

## **2.3 Securing the Perimeter Router**

2.3.1 Inbound and outbound traffic

2.3.2 Network Address Translation (NAT)

Lab: Configuring NAT/PAT

2.3.3 Routing protocol authentication and update filtering

Lab: Configure Routing Authentication and Filtering

2.3.4 Traffic filtering

2.3.5 Filter ICMP

2.3.6 Cisco IOS firewall

Demonstration Activity: Cisco IOS Firewall versus PIX Security Appliance

## **2.4 Router Management**

2.4.1 Router administration

2.4.2 Logging

Lab: Configure Logging

2.4.3 Time

Lab: Setting Time and NTP

Demonstration Activity: Configuring and verifying NTP

2.4.4 Software and configuration maintenance

2.4.5 Remote management using SSH

Lab: Configure SSH

Demonstration Activity: Configuring SSH Access

Demonstration Activity: Setting up an IOS Router as an SSH Client and Adding Terminal Line Access

Demonstration Activity: Troubleshoot and Debug SSH

## **2.5 Securing Switches and LAN Access**

2.5.1 Overview

PhotoZoom: Cisco 2924 Switch

PhotoZoom: Cisco 2950 Switch

PhotoZoom: Cisco 4006 Switch

PhotoZoom: Cisco AP1100 Access Point

PhotoZoom: Cisco Aironet 1200 Series

2.5.2 Layer 2 attacks and mitigation

2.5.3 Port security

2.5.4 VLANs

## **Module Summary**

## **Module Quiz**

# **Module 3: Router ACLs and CBAC**

## **Module Overview**

### **3.1 Access Control Lists**

3.1.1 ACL basics

3.1.2 Understanding ACL concepts

3.1.3 Summarizing ACLs

3.1.4 Processing ACLs

3.1.5 Applying ACLs

3.1.6 Editing ACLs

3.1.7 Troubleshooting

### **3.2 Types of IP ACLs**

3.2.1 Standard ACLs

3.2.2 Extended ACLs

3.2.3 IP named ACLs

3.2.4 Commented IP ACL entries

Lab: Standard, Extended, Named and Context ACLs

3.2.5 Lock-and-key, dynamic ACLs

Lab: Lock and Key ACLs

3.2.6 Reflexive ACLs

3.2.7 Time-based ACLs using time ranges

Lab: Time Based ACLs

Demonstration Activity: Time-Based ACLs

3.2.8 Authentication proxy

3.2.9 Turbo ACLs

3.2.10 Context-based Access Control

### **3.3 Context-based Access Control (CBAC)**

3.3.1 ACL limitations

3.3.2 How CBAC works

3.3.3 CBAC supported protocols

### **3.4 Configure CBAC (Task 1 and 2)**

3.4.1 Configure alerts and audit trails

e-Lab: CBAC Audit Trail and Alert

3.4.2 Global timeouts and thresholds

3.4.3 Global half-open connections limit

e-Lab: Half-open Connections Limit

### **3.5 Task 3: Port to Application Mapping (PAM)**

3.5.1 PAM overview

3.5.2 System-defined port mapping

3.5.3 User-defined port mapping

e-Lab: Port-to-Application Mapping

### **3.6 Task 4: Define Inspection Rules**

3.6.1 Overview of inspection rules

3.6.2 Inspection rules for applications

e-Lab: Configure AAA

3.6.3 Inspection rules for IP packet fragmentation

e-Lab: Define Inspection Rules

3.6.4 Inspection rules for URL Filtering

3.6.5 Inspection rules for ICMP

### **3.7 Task 5: Inspection Rules and ACLs Applied to Router Interfaces**

3.7.1 Applying inspection rules and ACLs

3.7.2 Two interface firewall

Demonstration Activity: Outbound and Inbound Traffic Filters for 2 Interface Firewall

### 3.7.3 Three interface firewall

Demonstration Activity: Outbound Traffic 3 Interface Firewall

## **3.8 Task 6: Test and Verify CBAC**

3.8.1 Show and debug commands

3.8.2 Remove CBAC configuration

3.8.3 Configuring a null interface

Lab: Configure Cisco IOS Firewall CBAC on a Cisco Router

e-Lab: Configure CBAC on a Cisco Router

## **Module Summary**

## **Module Quiz**

# **Module 4: Router AAA Security**

## **Module Overview**

### **4.1 AAA Secure Network Access**

4.1.1 Introduction to AAA

4.1.2 AAA secures network architecture

4.1.3 Authentication methods

4.1.4 Authentication - remote PC username and password

4.1.5 Authentication - one time passwords - S/Key

4.1.6 Authentication - token cards and servers

### **4.2 Network Access Server (NAS) AAA Authentication Process**

4.2.1 Overview of NAS

4.2.2 AAA security server options

4.2.3 NAS configuration

Lab: Configure AAA on a Cisco Router

Demonstration Activity: Configuring AAA For Cisco Perimeter Routers

### **4.3 Cisco Secure ACS**

#### 4.3.1 Overview of Cisco Secure ACS 3.0 Windows NT or 2000

Lab: Install and Configure CSACS 3.0 for Windows

Demonstration Activity: Cisco Secure ACS for Windows NT or Windows 2000

#### 4.3.2 Troubleshooting techniques for Cisco Secure ACS 3.0 for Windows

Demonstration Activity: Troubleshooting Techniques for Cisco Secure ACS 3.0 for Windows

#### 4.3.3 Overview of Cisco Secure ACS for UNIX

#### 4.3.4 Cisco Secure ACS Solutions Engine

### 4.4 AAA Servers Overview and Configuration

#### 4.4.1 Introduction to TACACS+

Demonstration Activity: TACACS+ Overview and Configuration

#### 4.4.2 Introductions to RADIUS

Demonstration Activity: Radius Configuration Overview

#### 4.4.3 RADIUS versus TACACS+

#### 4.4.4 Kerberos overview

### 4.5 The Cisco IOS Firewall Authentication Proxy

#### 4.5.1 Introduction to the IOS firewall authentication proxy

#### 4.5.2 Authentication proxy operation

Lab: Configuring Authentication Proxy

e-Lab: Configure Authentication Proxy on A Cisco Router

e-Lab: Test and Verify AAA

e-Lab: Configure Authentication

e-Lab: Configure AAA

#### 4.5.3 Authentication proxy configuration tasks

Demonstration Activity: Task 1 - AAA Server Configuration for Auth-proxy

Demonstration Activity: Task 2 - AAA Configuration for Auth-proxy

Demonstration Activity: Task 3 - Authentication Proxy Configuration

Demonstration Activity: Task 4 - Test and Verify the Auth-proxy Configuration

4.5.4 HTTPS authentication proxy

**Module Summary**

**Module Quiz**

**Module 5: Router Intrusion Detection, Monitoring, and Management**

**Module Overview**

**5.1 IOS Firewall IDS**

5.1.1 Introduction

5.1.2 Signature implementations

5.1.3 Response options

**5.2 Setting Up the Cisco Firewall IDS**

5.2.1 Configuring tasks

5.2.2 Initialize IOS firewall IDS

5.2.3 Configuring, disabling, and excluding signatures

5.2.4 Creating and applying audit rules

5.2.5 Verifying the configuration

Lab: Configure IOS Firewall IDS

**5.3 Monitoring with Logging and Syslog**

5.3.1 The value of logging

5.3.2 Configure logging

5.3.3 Configure synchronization of logging messages

5.3.4 Limiting the error message severity level

5.3.5 Syslog

5.3.6 Syslog message parts and codes

5.3.7 Logging to a server

5.3.8 Syslog platforms and applications

Lab: Configuring Syslog

## **5.4 SNMP**

- 5.4.1 SNMP introduction
  - 5.4.2 SNMP security
  - 5.4.3 SNMP version 3 (SNMPv3)
  - 5.4.4 Configure SNMP
  - 5.4.5 SNMP management applications
- Lab: Configure SNMP

## **5.5 Managing the Router**

- 5.5.1 Concepts
- 5.5.2 Access mechanisms for administrators
- 5.5.3 Updating the router
- 5.5.4 Testing and security validation
- 5.5.5 Enterprise monitoring

## **5.6 Security Device Manager (SDM)**

- 5.6.1 Overview
- 5.6.2 Accessing SDM
- 5.6.3 Downloading and installing the SDM

## **Module Summary**

## **Module Quiz**

# **Module 6: Router Site-to-site VPN**

## **Module Overview**

### **6.1 Virtual Private Networks**

- 6.1.1 Introduction
- 6.1.2 Site-to-site VPN
- 6.1.3 VPN technology options
  - e-Lab: Selecting VPN Technologies
- 6.1.4 Tunneling protocols
- 6.1.5 Tunnel interfaces

## **6.2 IOS Cryptosystem**

6.2.1 Overview

6.2.2 Symmetrical encryption

6.2.3 Asymmetric encryption

6.2.4 Diffie-Hellman

6.2.5 Data integrity

6.2.6 HMAC

6.2.7 Digital certificates

e-Lab: VPN and IPSec terms

## **6.3 IPSec**

6.3.1 Overview

6.3.2 Authentication Header

6.3.3 Encapsulating security payload

6.3.4 Modes

6.3.5 Security associations

6.3.6 Five steps of IPSec

e-Lab: Five Steps of IPSec

6.3.7 IKE

6.3.8 Logical flow of IPSec and IKE

e-Lab: IKE and IPSec Flowchart

## **6.4 Site-to-Site IPSec VPN Using Pre-shared Keys**

6.4.1 Tasks to configure IPSec

e-Lab: Tasks to Configure IPSec

6.4.2 Task 1 - prepare for IKE and IPSec

e-Lab: Prepare for IPSec

e-Lab: Prepare for IPSec

6.4.3 Task 2 - configure IKE

e-Lab: Configure IKE

e-Lab: Configure IKE

Demonstration Activity: Configuring IKE

6.4.4 Task 3 - configure IPSec

e-Lab: Configure IPSec

e-Lab: Configure IPSec

Demonstration Activity: Configuring IPSec

#### 6.4.5 Task 4 - test and verify IPSec

Lab: Configuring Cisco IOS IPSec using Pre-Shared Keys

e-Lab: IP Sec Transforms Supported in the Cisco IOS Software

e-Lab: Configure Cisco IOS IPSec for Pre-Shared Keys

Demonstration Activity: Displaying IKE Policy

### 6.5 Digital Certificates

6.5.1 Overview

6.5.2 Simple Certificate Enrollment Protocol (SCEP)

6.5.3 CA servers

6.5.4 Enroll a device with a CA

### 6.6 Configure Site-to-Site IPSec VPN Using Digital Certificates

6.6.1 Configure CA support tasks

6.6.2 Prepare for IKE and IPSec

Demonstration Activity: Configuring CA Support

6.6.3 Task 2 - configure CA support

e-Lab: Configure CA Support

Demonstration Activity: CA Support with Microsoft Certificate Server

6.6.4 Task 3 - configure IKE

e-Lab: Configure IKE

6.6.5 Task 4 - configure IPSec

e-Lab: Configure IPSec

6.6.6 Task 5 - test and verify IPSec

Lab: Configure IPSec using Digital Certificates

e-Lab: Testing & Verifying IPSec

e-Lab: Configure Cisco IOS CA Support (RSA Signatures)

### Module Summary

## Module Quiz

### Module 7: Router Remote Access VPN

#### Module Overview

##### 7.1 Remote Access VPN

7.1.1 Introduction

7.1.2 Remote Access VPN

7.1.3 Tunneling protocols for remote access

Demonstration Activity: Cisco VPN Devices

##### 7.2 Cisco Easy VPN

7.2.1 Easy VPN Server and Remote

7.2.2 Overview of the Easy VPN Server

7.2.3 Configuring the Easy VPN Server

Demonstration Activity: Configuring the Easy VPN Server

##### 7.3 Cisco VPN 3.5 Client

7.3.1 Overview

7.3.2 How Easy VPN works

Demonstration Activity: How Easy VPN Works

7.3.3 Working with the Cisco VPN 3.5 Client

7.3.4 VPN Client log

7.3.5 Setting MTU size

7.3.6 Status

Lab: Configure Remote Access Using Cisco Easy VPN

Demonstration Activity: Cisco VPN Client 3.5 Manual  
Configuration Tasks

##### 7.4 VPN Enterprise Management

7.4.1 Introduction

7.4.2 Key concepts in the router MC

7.4.3 Supported tunneling technologies

- 7.4.4 Router MC installation
- 7.4.5 Installation process
- 7.4.6 Getting started
- 7.4.7 Router MC interface

## **Module Summary**

## **Module Quiz**

# **Module 8: PIX Security Appliance**

## **Module Overview**

### **8.1 Introduction to Firewalls**

- 8.1.1 Firewalls and firewall technologies
- 8.1.2 Firewall technologies
- 8.1.3 The firewall marketplace
- 8.1.4 Security and VPN certifications

### **8.2 The Cisco PIX Security Appliance**

- 8.2.1 Introduction to the PIX Security Appliance
- 8.2.2 The Finesse operating system
- 8.2.3 Adaptive Security Algorithm (ASA)
- 8.2.4 Cut-through proxy operation
- 8.2.5 Failover
- 8.2.6 Network Address Translation (NAT)
- 8.2.7 The PIX Security Appliance family
  - PhotoZoom: PIX 506 Security Appliance
  - PhotoZoom: PIX 506E Security Appliance
  - PhotoZoom: PIX 515 Security Appliance
  - PhotoZoom: PIX 515E Security Appliance
  - PhotoZoom: PIX 525 Security Appliance
  - PhotoZoom: PIX 535 Security Appliance
- 8.2.8 Firewall Services Module (FWSM)
- 8.2.9 License types and VPN capabilities

### **8.3 Getting Started**

#### 8.3.1 User interface

e-Lab: Using Help

#### 8.3.2 Basic PIX Security Appliance configurations commands

e-Lab: nameif, interface, ip address, and route Commands

#### 8.3.3 Examine PIX Security Appliance status

Lab: Configure the PIX Firewall

e-Lab: show Commands

### **8.4 Routing and Multicast Configuration**

#### 8.4.1 Static routes

#### 8.4.2 Dynamic routes

#### 8.4.3 Multicast routing

#### 8.4.4 Allowing hosts to receive multicast transmissions

#### 8.4.5 Forwarding multicasts from a transmission source

#### 8.4.6 View and debug SMR

### **8.5 PIX Dynamic Host Configuration Protocol (DHCP)**

#### 8.5.1 Sever and client

#### 8.5.2 DHCP server

#### 8.5.3 Configuring the PIX Security Appliance as a DHCP server

Lab: Configure the PIX Firewall as a DHCP Server

Demonstration Activity: Configuring the PIX as a DHCP Server

### **Module Summary**

### **Module Quiz**

## **Module 9: PIX Security Appliance Translations and Connections**

### **Module Overview**

#### **9.1 Transport Protocols**

##### 9.1.1 Sessions in an IP world

##### 9.1.2 TCP detailed review

### 9.1.3 TCP features and interaction with PIX

Demonstration Activity: TCP Initialization Inside to Outside

### 9.1.4 UDP features and interaction with PIX

Demonstration Activity: UDP Initialization Inside to Outside

## 9.2 Network Address Translations

### 9.2.1 Understanding NAT

### 9.2.2 Dynamic inside translations

e-Lab: Internet Access Configuration

### 9.2.3 Static inside translations

### 9.2.4 Dynamic outside translations

### 9.2.5 Static outside translations

Demonstration Activity: Enabling Static Outside Translations

### 9.2.6 Identify NAT

e-Lab: nat 0 Configuration

## 9.3 Configuring DNS Support

### 9.3.1 Overview of the alias command

### 9.3.2 DNS doctoring process

Demonstration Activity: Enabling DNS Doctoring Process

### 9.3.3 Destination NAT with the alias command

Demonstration Activity: Enabling dnat

### 9.3.4 DNS record translation

## 9.4 Connections

### 9.4.1 Two ways through the PIX Security Appliance

### 9.4.2 Statics and conduits

e-Lab: static and conduit Commands

## 9.5 Port Address Translation (PAT)

### 9.5.1 PAT for the PIX Security Appliance

### 9.5.2 PAT using outside interface addresses

e-Lab: PAT Configuration

- 9.5.3 Mapping subnets to PAT addresses
- 9.5.4 Backing up PAT addresses by using multiple PATs
- 9.5.5 Augmenting a global pool with PAT
- 9.5.6 Port redirection
  - Lab: Configure PAT

## **9.6 Multiple Interfaces on a PIX Security Appliance**

- 9.6.1 Additional interface support
- 9.6.2 Configuring three interfaces on a PIX Security Appliance
  - e-Lab: Configuring the PIX Security Appliance
- 9.6.3 Configuring four interfaces on a PIX Security Appliance
  - Lab: Configure Access Through the PIX Security Appliance
  - Lab: Configure Multiple Interfaces
  - e-Lab: Configuring Four Interfaces

### **Module Summary**

### **Module Quiz**

## **Module 10: PIX Security Appliance ACLs**

### **Module Overview**

#### **10.1 Access Control Lists and the PIX Security Appliance**

- 10.1.1 Access Control List (ACL)
- 10.1.2 Configuring ACLs
  - Lab: Configure ACLs in the PIX Security Appliance
- 10.1.3 Turbo ACLs
- 10.1.4 ACLs versus conduits
- 10.1.5 Case study - differences in the behavior of conduits and ACLs
- 10.1.6 Verifying and troubleshooting ACLs

#### **10.2 Using ACLs**

- 10.2.1 Denying web access to the Internet
- 10.2.2 Permitting web access to the DMZ

- 10.2.3 Two common uses of access lists
- 10.2.4 VPN solution: dual DMZ and VPN concentrator
- 10.2.5 Ping

### **10.3 Filtering**

- 10.3.1 Malicious applet filtering
  - e-Lab: Filtering Java, ActiveX and URLs
  - Demonstration Activity: Example of ActiveX Filtering
- 10.3.2 URL filtering
  - e-Lab: URL Filtering

### **10.4 Object Grouping**

- 10.4.1 Grouping objects of similar types
- 10.4.2 Using object groups in ACLs
  - Demonstration Activity: 7 Step Process to Configure ACLs with Object Groups
- 10.4.3 Configuring object groups
- 10.4.4 Applying ACLs to object groups
  - Lab: Configure Object Groups

### **10.5 Nested Object Groups**

- 10.5.1 Overview
  - Demonstration Activity: 5 Step Process to Creating Nested Object Groups
- 10.5.2 Configuring nested object groups
- 10.5.3 Nested object group example
- 10.5.4 Multiple object groups in ACLs example
- 10.5.5 Verifying and managing object groups

### **Module Summary**

### **Module Quiz**

## **Module 11: PIX Security Appliance AAA**

## **Module Overview**

### **11.1 AAA**

- 11.1.1 Overview of authentication, authorization, and accounting
- 11.1.2 What the user sees
- 11.1.3 Cut-through proxy operation
- 11.1.4 TACACS+ and RADIUS
- 11.1.5 Cisco secure ACS and the PIX Security Appliance

### **11.2 Authentication Configuration**

- 11.2.1 Configuring the PIX Security Appliance to support authentication
- 11.2.2 AAA authentication example
  - e-Lab: Authentication Configuration
- 11.2.3 Authentication of non-Telnet, FTP, or HTTP traffic
- 11.2.4 Virtual Telnet
- 11.2.5 Virtual HTTP
- 11.2.6 Authentication of console access
- 11.2.7 Changing authentication timeouts and authentication prompts
  - e-Lab: Authentication of Non-Telnet, FTP or HTTP Traffic

### **11.3 Authorization and Accounting Configuration**

- 11.3.1 Configuring the PIX Security Appliance to support AAA authorization
- 11.3.2 Providing authorization using downloadable ACLs
- 11.3.3 Configuring the PIX Security Appliance to support AAA accounting
  - e-Lab: Authorization Configuration
- 11.3.4 Defining traffic to utilize AAA services
  - e-Lab: AAA Configuration Lab
- 11.3.5 Monitoring the AAA configuration
  - Lab: Configure AAA on the PIX Security Appliance Using Cisco Secure ACS for Windows 2000

### **11.4 PPPoE and the PIX Security Appliance**

- 11.4.1 Overview of PPPoE
- 11.4.2 The PIX Security Appliance and PPPoE
- 11.4.3 Configuring the PIX Security Appliance to support PPPoE
- 11.4.4 Monitoring and troubleshooting the PPPoE client

### **Module Summary**

### **Module Quiz**

## **Module 12: PIX Advanced Protocols and Intrusion Detection**

### **Module Overview**

#### **12.1 Advanced Protocols**

- 12.1.1 Need for advanced protocol handling
- 12.1.2 fixup command
- 12.1.3 FTP fixup configuration
- 12.1.4 Remote shell (rsh) fixup configuration
- 12.1.5 SQL\*Net fixup configuration
- 12.1.6 SIP fixup configuration
- 12.1.7 Skinny fixup configuration

e-Lab: fixup Command

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

#### **12.2 Multimedia Support**

- 12.2.1 Why multimedia is an issue
- 12.2.2 Real-time streaming protocol
- 12.2.3 H.323
- 12.2.4 IP phones and the PIX Security Appliance DHCP server

#### **12.3 Attack Guards**

- 12.3.1 Mail guard
- 12.3.2 DNS guard
- 12.3.3 FragGuard and virtual re-assembly
- 12.3.4 AAA flood guard
- 12.3.5 SYN flood attack

e-Lab: Flood Defender

#### 12.3.6 TCP intercept

### 12.4 Intrusion Detection

12.4.1 Overview of intrusion detection and the PIX Security Appliance

12.4.2 Information and attack intrusion detection signatures

12.4.3 Intrusion detection in the PIX Security Appliance

Lab: Configure Intrusion Detection

Demonstration Activity: Intrusion Detection Process in the PIX Security Appliance

### 12.5 Shunning

12.5.1 Overview of shunning

12.5.2 Example of shunning an attacker

### 12.6 Syslog Configuration on the PIX

12.6.1 Configure Syslog output to a Syslog server

12.6.2 Syslog messages

e-Lab: Configuring Message output to the Cisco Syslog Server

### 12.7 SNMP

12.7.1 SNMP overview

12.7.2 MIB support

Demonstration Activity: Configuring SNMP to the PIX Security Appliance

12.7.3 Example of an SNMP through the PIX Security Appliance

### Module Summary

### Module Quiz

## Module 13: PIX Failover and System Maintenance

### Module Overview

### 13.1 Understanding Failover

- 13.1.1 PIX Security Appliance failover overview
- 13.1.2 IP addresses for failover
- 13.1.3 Configuration replication
- 13.1.4 Failover and stateful failover
- 13.1.5 Failover interface tests

## **13.2 Serial Cable Failover Configuration**

- 13.2.1 Overview of configuring serial cable failover
- 13.2.2 Steps 1-4 configuring serial cable failover
  - e-Lab: failover Commands
  - Demonstration Activity: Configuring the Primary PIX Security Appliance for Serial Cable Failover
- 13.2.3 Additional failover commands
- 13.2.4 Verifying failover configuration

## **13.3 LAN-Based Failover**

- 13.3.1 LAN-based failover overview
- 13.3.2 Steps 1-4: preparing the primary PIX Security Appliance
  - Demonstration Activity: Configuring the Primary PIX Security Appliance to Support LAN-Based Failover
- 13.3.3 Steps 5-10: Preparing the secondary PIX Security Appliance
  - Lab: Configure LAN-Based Failover (OPTIONAL)
  - Demonstration Activity: Configuring the Secondary PIX Security Appliance to Support LAN-Based Failover

## **13.4 System Maintenance via Remote Access**

- 13.4.1 Configuring telnet access to the PIX Security Appliance console
  - e-Lab: telnet Command
- 13.4.2 SSH connections to the PIX Security Appliance
  - Demonstration Activity: Configuring SSH Access on the PIX Security Appliance
- 13.4.3 Connecting to the PIX Security Appliance with an SSH client

## **13.5 Command Authorization**

13.5.1 Command authorization overview

13.5.2 (Method 1) enable level command authorization

13.5.3 (Method 2) local command authorization

Lab: Configure SSH, Command Authorization, and Local User Authentication

13.5.4 (Method 3) ACS command authorization

## **13.6 PIX Security Appliance Password Recovery and Upgrades**

13.6.1 Password Recovery

13.6.2 Upgrading the image and the activation key

Lab: Perform Password Recovery

e-Lab: Upgrade PIX Image

### **Module Summary**

### **Module Quiz**

## **Module 14: PIX VPN**

### **Module Overview**

#### **14.1 The PIX Security Appliance Enables a Secure VPN**

14.1.1 PIX Security Appliance VPN capabilities

14.1.2 PIX Security Appliance VPN topologies

14.1.3 IPSec enables PIX Security Appliance VPN features

14.1.4 Overview of IPSec

14.1.5 IPSec standards supported by the PIX Security Appliance

#### **14.2 Tasks to Configure VPN**

14.2.1 IPSec configuration tasks overview

#### **14.3 Task 1 - Prepare to Configure VPN Support** **14.3.1 Step 1 - prepare for IKE**

14.3.2 Step 2 - determine the IKE phase one policy parameters

14.3.3 Step 3 - plan for IPSec

14.3.4 Step 4 - determine the IPSec policy

14.3.5 Step 5 - Ensure that the network works without encryption

e-Lab: Task One - Prepare for IPSec Steps 3, 4, & 5

14.3.6 Step 6 - Implicitly permit IPSec bypass

e-Lab: Configure IPSec

#### **14.4 Task 2 - Configure IKE Parameters**

14.4.1 Step 1 - enable or disable IKE

e-Lab: Enable/Disable IKE

Demonstration Activity: Enable or Disable IKE

14.4.2 Step 2 - configure an IKE phase one policy

14.4.3 Step 3 - configure the IKE pre-shared key

e-Lab: Configure Pre-Shared Keys

14.4.4 Step 4 - verify IKE phase one policies

e-Lab: Configure IKE Parameters

e-Lab: Configure and Verify IKE Phase 1 Policy

#### **14.5 Task 3 - Configure IPSec Parameters**

14.5.1 Step 1 - configure interesting traffic

Demonstration Activity: Configure Interesting Traffic

14.5.2 Example crypto ACLs

14.5.3 Step 2 - configure and IPSec transform set

e-Lab: IPSec Transform Set

14.5.4 Available IPSec transforms

14.5.5 Step 3 - configure the crypto map

14.5.6 Step 4 - Apply the crypto map to an interface

e-Lab: Configure Crypto Map

#### **14.6 Task 4 - Test and Verify VPN Configuration**

14.6.1 Verify ACLs and interesting traffic

14.6.2 Verify correct IKE phase one configuration

14.6.3 Verify correct IPSec algorithm configuration

14.6.4 Verify the correct crypto map configuration

e-Lab: Configure PIX Security Appliance IPSec

14.6.5 Show and clear the IPSec and IKE SAs

14.6.6 Debug IKE and IPSec traffic through the PIX Security Appliance

Lab: Configure a Secure VPN gateway Using IPSecs between Two PIX Security Appliances

e-Lab: Configure PIX Security Appliance IPSec

## **14.7 The Cisco VPN Client**

14.7.1 Cisco VPN client features

14.7.2 Topology overview

14.7.3 PIX Security Appliance assigns the IP address to the VPN client

e-Lab: IKE Mode Configuration-PIX

14.7.4 Configuring a PIX Security Appliance for a PIX-to-VPN client tunnel

14.7.5 Configuring a VPN client for a Plix-to-VPN client tunnel

Lab: Configure a Secure VPN Using IPSec Between a PIX and a VPN Client

## **14.8 Scaling PIX Security Appliance VPNs**

14.8.1 CA server fulfilling requests from IPSec peers

14.8.2 Enroll a PIX Security Appliance with a CA

Lab: Configure IPSec between Two PIX Security Appliances with CA support

Lab: IKE Mode Configuration-PIX Security Appliance

## **Module Summary**

### **Module Quiz**

## **Module 15: PIX Security Appliance Management**

### **Module Overview**

#### **15.1 PIX Security Appliance Management Tools**

15.1.1 Overview of PIX Security Appliance management tool options

15.1.2 PIX Device Manager

15.1.3 Cisco secure policy manager

15.1.4 PIX Management Center

## **15.2 The Cisco PIX Device Manager**

15.2.1 PDM overview

15.2.2 PDM operating requirements

15.2.3 PDM's browser requirements

## **15.3 Preparation for PDM**

15.3.1 Configure a new PIX Security Appliance to use PDM (CLI)

15.3.2 Configure a new PIX Security Appliance to use PDM (setup dialog)

15.3.3 Configure and existing PIX Security Appliance to use PDM

## **15.4 Using PDM to Configure the PIX Security Appliance**

15.4.1 Startup Wizard

15.4.2 Overall layout of the Cisco PDM

15.4.3 Access Rules tab

15.4.4 Translation Rules tab

15.4.5 VPN tab

15.4.6 Hosts/NetworkS tab

15.4.7 System Properties tab

15.4.8 Monitoring tab

15.4.9 Interface Graphics panel

15.4.10 Tools and options

## **15.5 Using PDM to Create Site-to-Site VPNs 15.5.1 Overview**

15.5.2 Setting system options

15.5.3 Configure IKE

15.5.4 Configuring certificate support

15.5.5 Configuring transform sets

15.5.6 Creating a crypto map

15.5.7 Creating an IPSec rule

## **15.6 Using PDM to Create Remote Access VPNs**

15.6.1 The PIX Security Appliance for Unity and Cisco VPN Clients

15.6.2 The PIX Security Appliance for Windows 2000 clients

15.6.3 VPN hardware client setting

Lab: Configuring the PIX Security Appliance with PDM

## **15.7 Enterprise PIX Firewall Management**

15.7.1 Management center for PIX Security Appliance

15.7.2 Key concepts

15.7.3 Auto update server (AUS)

### **Module Summary**

### **Module Quiz**