CISCO NETWORKING ACADEMY PROGRAM

Network Security 1

TABLE OF CONTENTS

Target Audience

The Network Security course is targeted at 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. It is also recommended that students have a basic understanding of common network and IT security issues and terminology.

Target Certifications

After completing this course AND the Network Security 2 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. These are two of the five exams that count towards the Cisco Certified Security Professional (CCSP) certification. In addition, Network Academy students who pass these two exams will be able to apply for Cisco Firewall/ASA Specialist status.

Course Description

The Network Security 1 course focuses on the overall security processes in a network with particular 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 both layer 2 and 3 of the OSI model

Course Objectives

Upon completion of the Network Security 1 course, students will have developed an understanding of:

- Security terminology and acronyms
- Basic and advanced security vulnerabilities
- Security policy design and management
- Security technologies, products, solutions and design
- Trust and identity technology at layer 2 and 3
- Configuring and using the Cisco Secure Access Server

- Advanced Firewall installation, configuration, monitoring and maintenance
- AAA implementation using Cisco routers and PIX Security Appliances
- Layer 2 security features including Identity Based Network Services (IBNS) and 802.1x
- Filtering network traffic on switches, routers and PIX devices
- Secure Network Design

Minimum System Requirements

Curriculum Requirements:	1 Student PC per student and 1 curriculum server
Lab Requirements:	2 Lab PCs or laptops (Win 2000 server preferred)
	1 Lab PC with Windows 2000 server (“SuperServer”)
	Network Security Lab bundle

Curriculum Requirements

Student PC

The curriculum may be viewed on a wide range of computers that use various operating systems – Windows; MAC OS; Linux; Unix etc. The machine and associated OS must host a browser such as Netscape 7.0x or 7.1 (only); Internet Explorer 5.5 (SP2); or Firefox 1.x. Other browsers may work but are not supported.

Java, Javascript and StyleSheets must be enabled in the browser preference setting.

The Macromedia Flash 7 plugin should be downloaded and enabled. The computer should also have the free Adobe Acrobat Reader software loaded.

The monitor should support, as a minimum, 800 x 600 resolution with a video card supporting a color depth of 256 colors. The minimum size monitor recommended for a desktop machine is 15 inch (38 cm). If available, a 17 inch (43 cm) monitor with a 16 bit color depth video card is preferred.

The computer will require a sound card, speakers or headphones (preferred) and a mouse. In addition, it should be fitted with a network interface card (NIC) that supports a minimum of 10MB/s Ethernet.

Curriculum Server

As with the curriculum viewing computers, a wide range of computers and operating systems are available to host the curriculum locally. However, consideration needs to be given to the number of students that may be accessing the machine when considering suitability.

The recommended operating system is Microsoft Windows 2000 Server (SP2) or later.

The server computer will require 5 to 10GB of hard disk space for the curriculum. The minimum recommended memory requirements is 256MB.

Lab Requirements

PC or Laptops (2 student)

Recommended OS - Windows2000 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 Netscape Navigator 4.7 (or later versions)

SuperServer (1)

Win 2000 server, SP 2

1GHz 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 Netscape Navigator 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, it is recommended that you 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. If this is not done, then some support issues may arise that are beyond the academy help desk or support.

Course Outline

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 Activity: 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 Activity: 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 Activity: Lab 2.1.2 Designing a Security Plan

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 Activity: Lab 2.5.2a Configure SSH

Lab Activity: 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 Activity: 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

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 Activity: 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

Lab Activity: E-Lab 3.4.5 Basic PIX Security Appliance Commands

3.4.6 Examining the PIX Security Appliance status

Lab Activity: E-Lab 3.4.6 PIX Security Appliance show Commands

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

Lab Activity: Lab 3.4.6b Configure the PIX Security Appliance using CLI

3.4.7 Time setting and NTP support

3.4.8 Syslog configuration

3.5 PIX Security Appliance Translations and Connections

3.5.1 Transport protocols

3.5.2 Network address translation (NAT)

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

3.5.3 Port address translation (PAT)

Lab Activity: E-Lab 3.5.3 PIX Security Appliance PAT Configuration

3.5.4 The static command

3.5.5 The identity nat command

Lab Activity: E-Lab 3.5.5 PIX Security Appliance NAT 0 Configuration

3.5.6 Connections and translations

3.5.7 Configuring multiple interfaces

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

Lab Activity: 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 ADSM overview

3.6.2 ADSM operating requirements

3.6.3 Prepare for ADSM

Lab Activity: 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 Activity: 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 Activity: Lab 6.1.3 Configure Local AAA on Cisco Router

6.1.4 Allow AAA traffic to the router

Lab Activity: Lab 6.1.4 Configure Authentication Proxy

6.1.5 Authentication proxy configuration

Lab Activity: E-Lab 6.1.5 Configure AAA

Lab Activity: E-Lab 6.1.5 Configure Authentication

Lab Activity: E-Lab 6.1.5 Configure Authentication Proxy on Cisco Router

6.1.6 Test and verify authentication proxy

Lab Activity: 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

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

Lab Activity: E-Lab 6.3.5 Configure PIX Security Appliance Authentication

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

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

6.3.7 Authorization configuration

Lab Activity: E-Lab 6.3.7a PIX Security Appliance Authorization Configuration

Lab Activity: E-Lab 6.3.7b PIX Security Appliance AAA Configuration Lab

6.3.8 Downloadable ACLs

6.3.9 Accounting configuration

Lab Activity: Lab 6.3.9 Configure Local AAA on the PIX Security Appliance

6.3.10 Troubleshooting the AAA configuration

Lab Activity: 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 Activity: 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 Activity: 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 8.3Configure 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

Lab Activity: 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

Lab Activity: 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

Lab Activity: 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

Lab Activity: E-Lab 8.3.11 Define Inspection Rules

8.3.12 Apply inspection rules and ACLs to interfaces

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

8.3.13 Test and verify CBAC

Lab Activity: E-Lab 8.3.13 Configure CBAC on a Cisco Router

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

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

Lab Activity: Lab 9.1.7c Configure Multiple Interfaces using CLI – Challenge Lab

9.1.8 Malicious code filtering

9.1.9 URL filtering

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

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

Lab Activity: 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 Activity: Lab 9.2.3 Configure Service Object Groups using ASDM

9.2.4 Nested object groups

9.2.5 Manage object groups

Lab Activity: Lab 9.2.5 Configure Object Groups and Nested Object Groups using CLI

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 Activity: 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 Contenet Addressable Memeory (CAM) table overflow attack

10.2.3 MAC spoofing – man in the middle attacks

10.2.4 Mitigating MAC spoofing attacks

Lab Activity: 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 10.4 Spanning-Tree Protocol Vulnerabilities

10.4.1 Spanning-Tree Protocol vulnerabilities

10.4.2 Preventing Spanning-Tree Protocol manipulation