Network Security 2

This document is the 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 Network Security 2 course as part of an official Cisco Networking Academy Program.

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 essential that students **MUST** have also completed the Network Security 1 course before being permitted to attempt Network Security 2.

Target Certifications

After completing this course AND the Network Security 1 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 2 course focuses on the overall security process 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
- Intrusion Prevention (IPS) implementation using routers and firewalls
- VPN implementation using routers and firewalls

Course Objectives

Upon completion of this Network Security 2 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
- Advanced firewall installation, configuration, monitoring and maintenance
- Secure Network Architecture and management

- Intrusion Detection and Prevention Technology
- The configuration of Network Intrusion Detection and Prevention systems
- Encryption and VPN Technology
- The configuration of Site-to-Site VPN using Pre-Shared Keys and Digital Certificates
- The configuration of remote access VPN
- PIX Security Appliance Contexts, Failover, and Management

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 – 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 casks

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 Activity: Lab 2.1.6 Configure a Router with the IOS Intrusion Prevention System

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

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

Lab Activity: 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

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

Lab Activity: E-Lab 4.1.7 Prepare for IPSec

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

Lab Activity: 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

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

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

Lab Activity: Lab 4.4.7 Configure Cisco IOS IPSec using Pre-Shared Keys

4.4.8 Configure a VPN using SDM

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

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

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

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

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

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

4.5.4 Task 3 – Configure IPSec parameters

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

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

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

Lab Activity: 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

Lab Activity: E-Lab 5.2.3 Configure CA Support

5.2.4 Task 3 – configure IKE

Lab Activity: E-Lab 5.2.4 Configure IKE

5.2.5 Task 4 – configure IPSec

Lab Activity: E-Lab 5.2.5 Configure IPSec

5.2.6 Task 5 – test and verify IPSec

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

Lab Activity: E-Lab 5.2.6 Testing & Verifying IPSec

Lab Activity: Lab 5.2.6 Configure a Cisco Router for IPSec using Digital Certificates

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

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

Lab Activity: 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 Activity: Lab 6.2.12a Configure Remote Access Using Cisco Easy VPN

Lab Activity: Lab 6.2.12b Configure Cisco Easy VPN Server with NAT

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

Lab Activity: 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

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 Activity: Lab 6.5.9a Configure a Secure VPN Using IPSec between a PIX and a VPN Client using ASDM

Lab Activity: 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 Activity: Lab 7.4.5 Configure SNMP Messages on a Cisco Router

7.4.6 Configure SNMP support on a PIX Security Appliance

Lab Activity: 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

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

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

8.2.5 Active/active failover

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 Activity: 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

Lab Activity: E-Lab 8.4.1 The PIX Security Appliance telnet Command

8.4.2 Managing SSH access

8.4.3 Command authorization

Lab Activity: Lab 8.4.3a Configure User Authentication and Command Authorization using ASDM

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

8.4.4 PIX Security Appliance password recovery

Lab Activity: 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

Lab Activity: E-Lab 8.4.7 Upgrade the PIX Security Appliance Software Image