

Fundamentals of Network Security
Cisco Secur and Pix Firewall Certification Prep
Spring 2005 (2/5-5/26)

Instructor: Wallace Wong

E-mail: wallacew@rocketmail.com

Course: CS-214G-01 (4.0 units)

Classroom: Bldg 6, room 6106

Lecture: Saturdays, 9:00am – 12:20pm

Textbook: CCSP SECUR Exam Certification Guide (CCSP Self-Study, 642-501) (Cisp Self-Study)

Publisher: Cisco Press (December 22, 2003), ISBN: 1587200724

CCSP Self-Study : Cisco Secure PIX Firewall Advanced (CSPFA) (2nd Edition)

Publisher: Cisco Press; 2 edition (January 14, 2004), ISBN: 1587051494

Course Objectives:

This course prepares students for the Cisco Systems SECUR and CSPFA (Pix Firewall) certification exams in preparation for Firewall Specialist. This course is divided into 2 sections. The first half of the course will be devoted towards Cisco IOS Network Security. We will focus on the installation, configuration, and operation of IP network security on perimeter routers: AAA security, access control, intrusion detection, network address translation, and virtual private networks (Cisco SECUR Certification Exam# 642-501 SECUR).

The second half of the course will be devoted towards Cisco PIX Firewalls. We will focus on the installation, configuration, and operation of IP network security on PIX firewalls: AAA security, access control, intrusion detection, network address translation, virtual private networks, and content filtering. (Cisco Advanced PIX Certification Exam Number# 642-521).

These exams also count toward security-professional-level CCSP certification. Successful completion of the course also helps prepare students for the CompTIA Security+ exam.

E-Mail

All students are requested to obtain an e-mail account. If you have any questions about the course or need assistance, please contact me in person or by telephone during office hours; or by e-mail at any time. Also, you may submit the end of chapter case project assignments in class on the due date or by e-mail with a date stamp of 5:00 P.M. on the due date. E-mail submissions should be as an attachment in Microsoft Word format.

Grading and Evaluation Criteria

Grading:

Class participation	10%
Labs	25%
Midterm (2)	30%
Final examination	<u>35%</u>
	100%

Grading Scale:

90 - 100 = A
80 - 89 = B
70 - 79 = C
60 - 69 = D
< 59 = F

Course Outline

Project Due Dates and Exam Dates

Dates	Topics	Chapter Readings	Hands-On Projects Notebook	Exams
2/5/05	Module 1 - Overview of Network Security	Module 1	1.1 - Student Lab Orientation 1.2 - Vulnerabilities and Exploits	
2/12/05	Module 2 - Basic Router and Switch Security Module 3 – Router ACLs and CBAC	Module 2 Module 3	2.1 – Configure SSH 2.2 – Controlling TCP/IP Services 2.3 – Configure Routing Authen. and Filtering 2.4 – Configure General Router Security 2.5 – Configure Basic Security using SDM 3.1 – Lock & Key ACLs 3.2 – Time-Based ACLs 3.3 – CBAC: Audit Trail & Alert (e-lab) 3.4 – Half-Open Connection Limits (e-lab) 3.5 – Port-to-Application Mapping (e-lab) 3.6 – Inspection Rules & ACLs applied to router interfaces (e-lab) 3.7 – Define Inspection Rules (e-lab) 3.8 – Configure CBAC on a Cisco Router (e-lab) 3.9 – Configure Cisco IOS FW CBAC	Module 1
2/19/05	President's Day	No Class		
2/26/05	Module 4 – Router AAA Security	Module 4	4.1 – Configure Local AAA on Cisco Router 4.2 – Install and Configure CSACS 3.2 for Windows 4.3 – Configure Authentication Proxy 4.4 – Configure Authentication Proxy on Cisco Router (e-lab) 4.5 – Test and Verify AAA (e-lab) 4.6 – Configure Authentication (e-lab) 4.7 – Configure AAA (e-lab)	Module 2 (2 exams) Module 3 (3 exams)
3/5/05	Module 5 – Router IDS, Monitoring, & Mngmnt	Module 5	5.1 – Configure IOS Firewall IDS 5.2 – Configure Logging 5.3 – Configure SNMP 5.4 – Setting Time	Module 4
3/12/05	Module 6 – Router Site-to-site VPN	Module 6	6.1.0 – Tunneling Protocols (e-lab) 6.1.1 – Prepare for IPsec (e-lab) 6.2 – Configure IKE (e-lab) 6.3 – IPsec Transforms Supported in Cisco IOS (e-lab) 6.4 – Configure Cisco IOS IPsec for PreShared Keys (e-lab) 6.5.1 – Configure IOS IPsec using Preshared Keys 6.5.2 – Configuring Cisco IOS IPsec w/ Preshared Keys using SDM 6.6 – Configuring Cisco GRE IPsec Tunnel using SDM 6.7.1 – Configure CA Support (e-lab) 6.7.2 – Configure IKE (e-lab) 6.7.3 – Configure IPsec (e-lab) 6.7.4 – Configure IPsec using Digital Certificates 6.8 – Testing & Verifying IPsec (e-lab) 6.9 – Configure Cisco IOS CA Support (RSA Signatures)	Module 5 (2 exams)
3/19/05	Module 7 – Router Remote Access VPN	Module 7	7.1 - Configure Remote Access Using Cisco Easy VPN	Module 6 (2 exams)
3/26/05	Module 8 – PIX Security Appliance Basics	Module 8	8.1 - Using Help (e-lab) 8.2 - nameif, interface, ip address, and route Commands (e-lab) 8.3 - Configuring the PIX Security Appliance using Setup Mode and PDM Startup Wizard 8.4 - Configuring the PIX Security Appliance with PDM 8.5 - Configuring the PIX Security Appliance as a DHCP Server	Module 7
4/2/05	Module 9 – Pix Security Appliance Translations and Connections	Module 9	9.1 - Internet Access Configuration (e-lab) 9.2 - nat 0 Configuration (e-lab) 9.3 - Configure Access Through the PIX Security Appliance using PDM 9.4 - static and conduit Commands (e-lab)	Module 8 (3 exams)

			<p>9.5 - PAT Configuration (e-lab)</p> <p>9.6 - Configure the PIX Security Appliance (e-lab)</p> <p>9.7 - Configure Access Through the PIX Security Appliance using CLI</p> <p>9.8 - Configure Multiple Interfaces using CLI – Challenge Lab</p> <p>9.9 - Configuring Four Interfaces (e-lab)</p>	
4/9/05	Module 10 – PIX Security Appliance ACLs	Module 10	<p>10.1 - Configure ACLs in the PIX Security Appliance using CLI</p> <p>10.2 - Filtering Java, ActiveX, and URLs (e-lab)</p> <p>10.3 - URL Filtering (e-lab)</p> <p>10.4 - Configure Service Object Groups using PDM</p> <p>10.5 - Configure Object Groups and Nested Object Groups using CLI</p>	Module 9 (2 exams)
4/16/05	Module 11 – PIX Security Appliance AAA	Module 11	<p>11.1 - Authentication Configuration (e-lab)</p> <p>11.2 - Authentication of Non-Telnet, FTP or HTTP Traffic (e-lab)</p> <p>11.3 - Authorization Configuration (e-lab)</p> <p>11.4 - AAA Configuration Lab (e-lab)</p> <p>11.5 - Configure Local AAA on the PIX Security Appliance</p>	Module 10
4/23/05	Module 12 – PIX Advanced Protocols and Intrusion Detection	Module 12	<p>12.1 - fixup Command (e-lab)</p> <p>12.2 - Flood Defender (e-lab)</p> <p>12.3 - Configure and Test Advanced Protocol Handling on the Cisco PIX Security Appliance</p> <p>12.4 - Configuring Message output to the Cisco Syslog Server (e-lab)</p> <p>12.5 - Configure Intrusion Detection</p>	Module 11 (2 exams)
4/30/05	Module 13 – PIX Failover and System Maintenance	Module 13	<p>13.1 - failover Commands (e-lab)</p> <p>13.2 - telnet Command (e-lab)</p> <p>13.3 - Configure User Authentication and Command Authorization using PDM</p> <p>13.4 - Configure SSH, Command Authorization, and Local User Authentication using CLI</p>	Module 12 (2 exams)
5/7/05	Module 14 - PIX Security Appliance VPN	Module 14	<p>14.1.1 - Enable/Disable IKE (e-lab)</p> <p>14.1.2 - Configure Pre-Shared Keys (e-lab)</p> <p>14.1.3 - Configure IKE Parameters (e-lab)</p> <p>14.1.4 - Configure and Verify IKE Phase 1 Policy (e-lab)</p> <p>14.1.5 - Configure Crypto Map (e-lab)</p> <p>14.1.6 - Configure IPSec (e-lab)</p> <p>14.2 - Configure a Site-to-Site IPSec VPN Tunnel Using PDM</p> <p>14.3 - Configure a Site-to-Site IPSec VPN Tunnel Using CLI</p> <p>14.4 - Configure PIX Security Appliance IPSec for Pre-Shared Keys (e-lab)</p> <p>14.5 - IKE Mode Configuration-PIX</p> <p>14.6 - Configure a Secure VPN Using IPSec between a PIX and a VPN Client using PDM</p> <p>14.7 - Configure a Secure VPN Using IPSec between a PIX and a VPN Client using CLI</p> <p>14.8 - Configure Cisco PIX Security Appliance for CA Support (RSA Signatures) (e-lab)</p> <p>14.9 - Configure a Site-to-Site IPSec VPN Tunnel with CA support</p>	Module 13
5/14/05	Module 15 - PIX Security Appliance Management and System Maintenance	Module 15	<p>15.1 - Configure SNMP using PDM</p> <p>15.2 - Perform Password Recovery</p> <p>15.3 - Upgrade PIX Image (e-lab)</p>	Module 14 Module 15
5/21/05	Final			