

**OHLONE COLLEGE**  
**Ohlone Community College District**  
**OFFICIAL COURSE OUTLINE**

**I. Description of Course:**

- |   |   |
|---|---|
| 1. <b>Department/Course:</b> <u>CNET - 172B</u>                                       | 7. <b>Degree/Applicability:</b><br>Credit, Degree Applicable, Transferable -<br>CSU (T) |
| 2. <b>Title:</b> <u>Cisco Network Security 2 (CCSP)</u>                               | 8. <b>General Education:</b>  |
| 3. <b>Cross Reference:</b>  | 9. <b>Field Trips:</b> <u>Not Required</u>  |
| 4. <b>Units:</b> <u>2</u><br><b>Lec Hrs:</b> <u>1.5</u><br><b>Lab Hrs:</b> <u>1.5</u> | 10. <b>Requisites:</b>  |
| 5. <b>Repeatability:</b> <u>Yes Times:3</u>   |   |
| 6. <b>Grade Options:</b> Letter Grade, May<br>Petition Credit/No Credit (GC)          |   |

**12. Catalog Description:**

The Cisco 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;

**13. Class Schedule Description:**

Learn secure perimeter and connectivity, security management, identity services, and intrusion detection. (Part 2)

**14. Counselor Information:**

After completing this course and the CNET 172A 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.

**II. Student Learning Outcomes**

The student will:

1. Define and explain security terminology and to identify acronyms.
2. Analyze both basic and advanced security vulnerabilities in a network.
3. Improve their skills on developing a security policy design, a secure network design, and management plan.
4. Configure, apply, and evaluate intrusion detection and prevention technology.
5. Describe and compare encryption and VPN technology.
6. Configure site-to-site VPN using pre-shared keys and digital certificates.
7. Configure remote access VPN
8. Configure and apply PIX Security Appliance contexts, failover, and management.

### **III. Course Outline:**

Each of the topical areas includes integrated hands-on labs that are completed in the open lab or remotely.

#### **A. Module 1: Intrusion Detection and Prevention Technology**

##### **1. Overview of Intrusion Detection and Prevention**

- a. Introduction to intrusion detection and prevention**
- b. Network-based versus host-based**
- c. Types of alarms**

##### **2. Inspection Engine**

- a. Signature-based detection**
- b. Types of signatures**
- c. Anomaly-based detection**

##### **3. Cisco IDS and IPS Devices**

- a. Cisco integrated solutions**
- b. Cisco IPS 4200 Series sensors**

#### **B. Module 2: Configure Network Intrusion Detection and Prevention**

##### **1. Cisco IOS Intrusion Prevention System**

- a. Cisco IOS Intrusion Prevention System (IPS)**
- b. Cisco IOS IPS signatures**
- c. Cisco IOS IPS configuration tasks**
- d. Install the cisco IOS IPS**
- e. Configure logging using Syslog or SDEE**
- f. Verify the IPS configuration**

## **2. Configure Attack Guards on the PIX Security Appliance**

- a. Mail Guard**
- b. DNS Guard**
- c. FragGuard and Virtual Reassembly**
- d. AAA Flood Guard**
- e. SYN Flood Guard**
- f. Connection limits**

## **3. Configure Intrusion Prevention on the PIX Security Appliance**

- a. Intrusion detection and the PIX Security Appliance**
- b. Configure intrusion detection**
- c. Configure IDS policies**

## **4. Configure Shunning on the PIX Security Appliance**

- a. Overview of shunning**
- b. Example of shunning an attacker**

## **C. Module 3: Encryption and VPN Technology**

### **1. Encryption Basics**

- a. Symmetrical encryption**
- b. Asymmetrical encryption**
- c. Diffie-Hellman**

### **2. Integrity Basics**

- a. Hashing**

**b. Hashed Method Authentication Code (HMAC)**

**c. Digital signatures and certificates**

### **3. Implementing Digital Certificates**

**a. Certificate authority support**

**b. Simple Certificate Enrollment Protocol (SCEP)**

**c. Microsoft CA server**

**d. Enroll a device with a CA**

### **4. VPN Topologies**

**a. Site-to-site VPNs**

**b. Remote access VPNs**

### **5. VPN technologies**

**a. VPN technology options**

**b. WebVPN**

**c. Tunneling protocols**

**d. Tunnel interfaces**

### **6. 3.6 IPSec**

**a. Overview**

**b. Authentication Header (AH)**

**c. Encapsulating Security Payload (ESP)**

**d. Tunnel and transport modes**

**e. Security Associations**

**f. Five Steps of IPSec**

**g. Internet Key Exchange (IKE)**

**h. IKE and IPSec**

**i. Cisco VPN solutions**

#### **D. Module 4: Configure Site-to-Site VPN using Pre-Shared Keys**

##### **1. Prepare a Router for Site-to-Site VPN using Pre-shared Keys**

**a. IPSec Encryption with pre-shared keys**

**b. Planning the IKE and IPSec Policy**

**c. Step 1 – Determine ISAKMP (IKE Phase 1) policy**

**d. Step 2 – Determine IPSec (IKE Phase 2) Policy**

**e. Step 3 – Check the current configuration**

**f. Step 4 – Ensure the network works without encryption**

**g. Step 5 – Ensure ACLs are compatible with IPSec**

##### **2. Configure a Router for IKE Using Pre-shared Keys**

**a. Step 1 – Enable or disable IKE**

**b. Step 2 – Create IKE policies**

**c. Step 3 – Configure pre-shared keys**

**d. Step 4 – Verify the IKE configuration**

##### **3. Configure a Router with IPSec Using Pre-shared Keys**

##### **4. Steps to configure IPSec**

**a. Step 1 – Configure transform set suites**

**b. Step 2 – Configure global IPSec SA lifetimes**

**c. Step 3 – Create crypto ACLs**

- d. **Step 4 – Create crypto maps**
- e. **Step 5 – Apply crypto maps to interfaces**

## **5. Testing and Verifying IPsec Configuration**

- a. **Test and Verify the IPsec Configuration of the Router**
- b. **Display the configured ISAKMP policies**
- c. **Display the configured transform sets**
- d. **Display the current state of IPsec SAs**
- e. **Display the configured crypto maps**
- f. **Enable debug output for IPsec events**
- g. **Enable debug output for ISAKMP events**
- h. **Configure a VPN using SDM**

## **6. Configure a PIX Security Appliance Site-to-Site VPN using Pre-shared Keys**

- a. **IPsec configuration tasks**
- b. **Task 1 – Prepare to Configure VPN Support**
- c. **Task 2 – Configure IKE Parameters**
- d. **Task 3 – Configure IPsec parameters**
- e. **Task 4 – Test and verify the IPsec configuration**

## **E. Module 5: Configure Site to Site VPN using Digital Certificates**

### **1. Configuring Certificate Authority (CA) Support on a Cisco Router**

- a. **Steps to configure CA support**
- b. **Step 1 – manage the non-volatile RAM (NVRAM)**

- c. **Step 2 – set the router time and date**
- d. **Step 3 – add a CA server entry to the router host table**
- e. **Step 4 – generate an RSA key pair**
- f. **Step 5 – declare a CA**
- g. **Step 6 – authenticate the CA**
- h. **Step 7 – request a certificate for the router**
- i. **Step 8 – save the configuration**
- j. **Step 9 – monitor and maintain CA interoperability**
- k. **Step 10 – verify the CA support configuration**

## **2. Configure an IOS Router Site-to-Site VPN Using Digital Certificates**

- a. **Configuration Tasks**
- b. **Task 1 – prepare for IKE and IPsec**
- c. **Task 2 – configure CA support**
- d. **Task 3 – configure IKE**
- e. **Task 4 – configure IPsec**
- f. **Task 5 – test and verify IPsec**

## **3. Configure a PIX Security Appliance Site-to-Site VPN Using Digital Certificates**

- a. **Scaling PIX Security Appliance VPNs**
- b. **Enroll the PIX Security Appliance with a CA**

## **F. Module 6: Configure Remote Access VPN**

- a. **Introduction to Cisco Easy VPN**

- b. Introduction to Cisco Easy VPN**
- c. Overview of the Easy VPN Server**
- d. Overview of the Easy VPN Remote**
- e. How the Cisco Easy VPN Works**
- f. Easy VPN Remote client connection in detail**

## **1. Configure the Easy VPN Server**

- a. Cisco Easy VPN Server configuration tasks**
- b. Task 1 – create an IP address pool**
- c. Task 2 – configure group policy lookup**
- d. Task 3 – create ISAKMP policy for remote VPN access**
- e. Task 4 – define a group policy for a mode configuration push**
- f. Task 5 – create a transform set**
- g. Task 6 – create a dynamic crypto map with RRI**
- h. Task 7 – apply mode configuration to the dynamic crypto map**
- i. Task 8 – apply a dynamic crypto map to the router interface**
- j. Task 9 – enable IKE dead peer detection**
- k. Task 10 – (optional) configure XAUTH**
  - l. Task 11 – (optional) enable XAUTH save password feature**

## **2. Configure Easy VPN Remote for the Cisco VPN Client 4.x**

- a. Cisco Easy VPN Client 4.x configuration tasks**
- b. Task 1 – install the Cisco VPN Client 4.x on the remote PC**
- c. Task 2 – create a new client connection entry**

- d. **Task 3 – choose an authentication method**
- e. **Task 4 – configure transparent tunneling**
- f. **Task 5 – enable and add backup servers**
- g. **Task 6 – configure connection to the Internet through dial-up networking**

### **3. Configure Cisco Easy VPN Remote for Access Routers**

- a. **Easy VPN Remote modes of operation**
- b. **Configuration tasks for Cisco Easy VPN Remote for access routers**
- c. **Task 1 – configure the DHCP server pool**
- d. **Task 2 – configure and assign the Cisco Easy VPN Client profile**
- e. **Task 3 – (optional) configure XAUTH save password feature**
- f. **Task 4 – (optional) initiate the VPN tunnel**
- g. **Task 5 – verify the Cisco Easy VPN configuration**

### **4. Configure the PIX Security Appliance as an Easy VPN Server**

- a. **Easy VPN Server general configuration tasks**
- b. **Task 1 – create ISAKMP policy for remote VPN Client access**
- c. **Task 2 – create an IP address pool**
- d. **Task 3 – define a group policy for mode configuration push**
- e. **Task 4 – create a transform set**
- f. **Tasks 5 through 7– dynamic crypto map**
- g. **Task 8 – configure XAUTH**
- h. **Task 9 – configure NAT and NAT 0**

**i. Task 10 – enable IKE dead peer detection**

**5. Configure a PIX 501 or 506 as an easy VPN client**

**a. Firewall appliance Easy VPN Remote feature overview**

**b. Easy VPN Remote configuration**

**c. Easy VPN Client device mode and enabling Easy VPN Remote clients**

**d. Easy VPN Remote authentication**

**e. Configure the Adaptive Security Appliance to Support WebVPN**

**f. WebVPN end-user interface**

**g. Configure WebVPN general parameters**

**h. Configure WebVPN servers and URLs**

**i. Configure WebVPN port forwarding**

**j. Configure WebVPN e-mail proxy**

**k. Configure WebVPN content filters and ACLs**

**G. Module 7: Secure Network Architecture and Management**

**1. Layer 2 Security Best Practices**

**a. Factors affecting layer 2 mitigation techniques**

**b. Single security zone, one user group, single physical switch**

**c. Single security zone, one user group, multiple physical switches**

**d. Single security zone, multiple user groups, single physical switch**

**e. Single security zone, multiple user groups, multiple physical switches**

**f. Multiple security zones, one user group, single physical switch**

**g. Multiple security zones, one user group, multiple physical switches**

- h. Multiple security zones, multiple user groups, single physical switch**
- i. Multiple security zones, multiple user groups, multiple physical switches**
- j. Layer 2 security best practices**

## **2. SDM Security Audit**

- a. Using SDM to perform security audits**
- b. Using SDM monitor mode**

## **3. Router Management Center (MC)**

- a. Introduction to the Router MC**
- b. Key concepts in the Router MC**
- c. Supported tunneling technologies**
- d. Router MC installation**
- e. Installation process**
- f. Getting started with the Router MC**
- g. Router MC interface**
- h. Installation process**
- i. Basic work flow and tasks**

## **4. Simple Network Management Protocol (SNMP)**

- a. SNMP introduction**
- b. SNMP security**
- c. SNMP Version 3 (SNMPv3)**
- d. SNMP management applications**
- e. Configure SNMP support on an IOS router**

**f. Configure SNMP support on a PIX Security Appliance**

**H. Module 8: PIX Security Appliance Contexts, Failover, and Management**

**1. Configure a PIX Security Appliance to Perform in Multiple Context Mode**

- a. Security context overview**
- b. Enable multiple context mode**
- c. Configure a security context**
- d. Managing security contexts**

**2. Configure PIX Security Appliance Failover**

- a. Understanding failover**
- b. Failover requirements**
- c. Serial cable-based failover configuration**
- d. Active/standby LAN-based failover configuration**
- e. Active/active failover**

**3. Configure Transparent Firewall Mode**

- a. Transparent firewall mode overview**
- b. Enable transparent firewall mode**
- c. Monitor and maintain a transparent firewall**

**4. PIX Security Appliance Management**

- a. Managing Telnet access**
- b. Managing SSH access**
- c. Command authorization**
- d. PIX Security Appliance password recovery**

e. Adaptive Security Appliance password recovery

f. File management

g. Image upgrade and activation keys

**IV. Course Assignments:**

A. Reading Assignments

1. Web-based textbook. Supplemental online reading.

B. Projects, Activities, and other Assignments

1. hands-on face-to-face and eLearning labs

C. Writing Assignments

**V. Methods of Evaluation/Assessment:**

A. Objective exams

B. Performance-based skills assessments

**VI. Methods of Instruction:**

A. Lecture

B. Laboratory

C. Discussion

D. Demonstration

**VII. Textbooks:**

Required

Optional

**VIII. Supplies:**