I. Description of Course:

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

12. Catalog Description:
   The Cisco 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.

13. Class Schedule Description:
   Learn secure perimeter and connectivity, security management, identity services, and intrusion detection. (Part 1)

14. Counselor Information:
   After completing this course and the CNet 172B 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 identify acronyms.
2. Analyze both basic and advanced security vulnerabilities in a network.
3. Develop a security policy design, a secure network design, and management plan.
4. Evaluate security technologies, products, solutions, and design.
5. Apply and evaluate trust and identity technology at layer 2 and 3.
6. Configure and use the Cisco Secure Access Server and a AAA implementation using Cisco routers and PIX Security Appliances.
7. Complete an advanced installation, configuration, monitoring, and maintenance of a Firewall.
8. Apply layer 2 security features including Identity Based Network Services (IBNS) and
Apply, analyze and evaluate filtering network traffic on switches, routers and PIX devices.

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: Vulnerabilities, Threats, and Attacks

1. Introduction to Network Security
   a. The need for network security
   b. Identifying potential risks to network security
   c. Open versus closed security models
   d. Trends driving network security
   e. Information security organizations

2. Introduction to Vulnerabilities, Threats, and Attacks
   a. Vulnerabilities
   b. Threats
   c. Attacks

3. Attack Examples
   a. Reconnaissance attacks
   b. Access attacks
   c. Denial of service attacks
   d. Distributed denial of service attacks
   e. Malicious code

4. Vulnerability Analysis
   a. Policy review
b. Network analysis

c. Host analysis

d. Analysis tools

B. Module 2: Security Planning and Policy

1. Discussing Network Security and Cisco
   a. The security wheel
   b. Network security policy

2. Endpoint Protection and Management
   a. Host and server based security components and technologies
   b. PC management

3. Network Protection and Management
   a. Network based security components and technologies
   b. Network security management

4. Security Architecture
   a. Security architecture (SAFE)
   b. The Cisco Self-Defending Network
   c. Cisco integrated security
   d. Plan, Design, Implement, Operate, Optimize (PDIOO)

5. Basic Router Security
   a. Control access to network devices
   b. Remote configuration using SSH
   c. Router passwords
d. Router privileges and accounts

e. IOS network services

f. Routing, proxy ARP and ICMP

g. Routing protocol authentication and update filtering

h. NTP, SNMP, router name, DNS

C. Module 3: Security Devices

1. Device Options

   a. Appliance-based, server-based, and integrated firewalls

   b. Cisco IOS Firewall feature set

   c. PIX Security Appliance

   d. Adaptive Security Appliance

   e. Finesse Operating System

   f. Firewall Services Module

2. Using Security Device Manager

   a. Security Device Manager (SDM) overview

   b. SDM software

   c. Using the SDM startup wizard

   d. SDM user interface

   e. SDM wizards

   f. Using SDM to configure a WAN

   g. Using the factory reset wizard

   h. Monitor mode
3. Introduction to the Cisco Security Appliance Family
   a. PIX Security Appliance models
   b. Adaptive Security Appliance models
   c. Security appliance licensing
   d. Expanding the features of the security appliance

4. Getting Started with the PIX Security Appliance
   a. User interface
   b. Configuring the PIX Security Appliance
   c. Security levels
   d. Basic PIX Security Appliance configuration commands
   e. Additional PIX Security Appliance configuration commands
   f. Examining the PIX Security Appliance status ASDM Startup Wizard
   g. Time setting and NTP support
   h. Syslog configuration

5. PIX Security Appliance Translations and Connections
   a. Transport protocols
   b. Network address translation (NAT)
   c. Port address translation (PAT)
   d. The static command
   e. The identity nat command
   f. Connections and translations
g. Configuring multiple interfaces

   a. ADSM overview
   b. ADSM operating requirements
   c. Prepare for ADSM
   d. Using ASDM to configure the PIX Security Appliance

7. PIX Security Appliance Routing Capabilities
   a. Virtual LANs
   b. Static and RIP routing
   c. OSPF
   d. Multicast routing

8. Firewall Services Module (FWSM) Operation
   a. Firewall Services Module overview
   b. Getting started with the FWSM
   c. Using PDM with the FWSM

D. Module 4 : Trust and Identity Technology

   1. Authentication, Authorization, and Accounting (AAA)
      a. TACACS+
      b. RADIUS
      c. Comparing TACACS+ and RADIUS

   2. Authentication Technologies
      a. Static passwords
b. One-time passwords and token cards

c. Digital certificates

d. Biometrics

3. Identity Based Networking Services (IBNS)

4. Introduction to IBNS

   a. 802.1x

   b. Wired and wireless implementations

5. Network Admission Control (NAC)

   a. NAC components

   b. NAC phases

   c. NAC operation

   d. NAC vendor participation

E. Module 5: Cisco Secure Access Control Server

   1. Cisco Secure Access Control Server (CSACS) for Windows

      a. Cisco Secure Access Control Server product overview

      b. Authentication and user databases

      c. The Cisco Secure ACS user database

      d. Keeping databases current

      e. Cisco Secure ACS for Windows architecture

      f. How Cisco Secure ACS authenticates users

      g. User changeable passwords

   2. Configuring RADIUS and TACACS+ with CSACS

      a. Installation steps
b. Administering Cisco Secure ACS for Windows

c. Troubleshooting

d. Enabling TACACS+

e. Verifying TACACS+

f. Configuring RADIUS

F. Module 6: Configure Trust and Identity at Layer 3

1. Cisco IOS Firewall Authentication Proxy

   a. Cisco IOS Firewall authentication proxy

   b. AAA server configuration

   c. AAA configuration

   d. Allow AAA traffic to the router

   e. Authentication proxy configuration

   f. Test and verify authentication proxy

2. Introduction to PIX Security Appliance AAA Features

   a. PIX Security Appliance authentication

   b. PIX Security Appliance authorization

   c. PIX Security Appliance accounting

      a. AAA server support

3. Configure AAA on the PIX Security Appliance

   a. PIX Security Appliance access authentication

   b. Interactive user authentication

   c. The local user database

   d. Authentication prompts and timeout

   e. Cut-through proxy authentication
f. Authentication of Non-Telnet, FTP, or HTTP traffic

g. Authorization configuration

h. Downloadable ACLs

i. Accounting configuration

j. Troubleshooting the AAA configuration

G. Module 7: Configure Trust and Identity at Layer 2

1. Identity-Based Networking Services (IBNS)

   a. IBNS overview

   b. IEEE 802.1x

   c. 802.1x components

   d. 802.1x applications with Cisco IOS Software

   e. How 802.1x works

   f. Selecting the correct Extensible Authentication Protocol (EAP)

   g. IBNS and Cisco Secure ACS

   h. ACS deployment considerations

      i. Cisco Secure ACS RADIUS profile configuration

2. Configuring 802.1x Port-Based Authentication

   a. 802.1x port-based authentication configuration tasks

   b. Enabling 802.1x authentication

   c. Configuring the switch-to-RADIUS-server communication

   d. Enabling periodic re-authentication

   e. Manually re-authenticating a client connected to a port

   f. Enabling multiple hosts

   g. Resetting the 802.1x configuration to the default values

   h. Displaying 802.1x statistics and status
H. Module 8: Configure Filtering on a Router

1. Filtering Technologies
   a. Packet filtering
   b. Stateful filtering
      a. URL filtering

2. Cisco IOS Firewall Context-Based Access Control
   a. Context-based Access Control (CBAC)
   b. Cisco IOS Access Control Lists (ACL)
   c. How CBAC works
      a. CBAC supported protocols

3. Configure Cisco IOS Firewall Context-Based Access Control
   a. CBAC configuration tasks
   b. Prepare for CBAC
   c. Set audit trails and alerts
   d. Set global timeouts
   e. Set global thresholds
   f. Half-open connection limits by host
   g. System-defined port-to-application mapping
   h. User-defined port-to-application mapping
   i. Define inspection rules for applications
   j. Define inspection rules for IP fragmentation
   k. Define inspection rules for ICMP
   l. Apply inspection rules and ACLs to interfaces
m. Test and verify CBAC
n. Configure an IOS firewall using SDM

I. Module 9: Configure Filtering on a PIX Security Appliance

1. Configure ACLs and Content Filters
   a. PIX Security Appliance ACLs
   b. Configuring ACLs
   c. ACL line numbers
   d. The icmp command
   e. nat 0 ACLs
   f. Turbo ACLs
   g. Using ACLs
   h. Malicious code filtering
      i. URL filtering

2. Object Grouping
   a. Overview of object grouping
   b. Getting started with object groups
   c. Configure object groups
   d. Nested object groups
   e. Manage object groups

3. Configure a Security Appliance Modular Policy
   a. Modular policy overview
   b. Configure a class map
   c. Configure a policy map
   d. Configure a service policy

4. Configure Advanced Protocol Inspection
   a. Introduction to advanced protocol inspection
b. Default traffic inspection and port numbers

c. FTP inspection

d. FTP deep packet inspection

e. HTTP inspection

f. Protocol application inspection

g. Multimedia support

h. Real-Time Streaming Protocol (RTSP)

i. Protocols required to support IP telephony
j. DNS inspection

J. Module 10: Configure Filtering on a Switch

1. Introduction to Layer 2 Attacks

   a. Types of attacks

2. MAC Address, ARP, and DHCP Vulnerabilities

   a. CAM table overflow attack

   b. Mitigating the Content Addressable Memory (CAM) table overflow attack

   c. MAC spoofing – man in the middle attacks

   d. Mitigating MAC spoofing attacks

   e. Using dynamic ARP inspection to mitigate MAC spoofing attacks

   f. DHCP starvation attacks

      a. Mitigating DHCP starvation attacks

3. VLAN Vulnerabilities

   a. VLAN hopping attacks

   b. Mitigating VLAN hopping attacks

   c. Private VLAN vulnerabilities
d. Defending private VLANs
4. Spanning-Tree Protocol Vulnerabilities
   a. Spanning-Tree Protocol vulnerabilities
   b. Preventing Spanning-Tree Protocol manipulation

IV. Course Assignments:
   A. Reading Assignments
      1. Web-based textbook reading assignments.
   B. Projects, Activities, and other Assignments
      1. Hands-on laboratory assignments
   C. Writing Assignments

V. Methods of Evaluation/Assessment:
   A. Objective exams
   B. Hands-on Labs
   C. Performance skills-based assessments

VI. Methods of Instruction:
   A. Lecture
   B. Laboratory
   C. Discussion
   D. Demonstration

VII. Textbooks:
   Required
   Optional

VIII. Supplies:

CID 1972