COURSE SYLLABUS

Cisco Certified Security Professional (CCSP)

50 Cragwood Rd, Suite 350
South Plainfield, NJ 07080

Victoria Commons, 613 Hope Rd Building #5,
Eatontown, NJ 07724

130 Clinton Rd,
Fairfield, NJ 07004

Avtech Institute of Technology Course

Instructor:
Course Duration: 150 hours
Date/Time:
Training Location:

Course: CCSP

Text / Lab Books:

CCSP: Course Description

CCSP certification validates skills and knowledge in key areas of network security including firewalls, intrusion detection systems, and virtual private networks. With a CCSP, a network professional demonstrates the skills required to secure and manage network infrastructures to protect productivity and reduce costs. The CCSP curriculum emphasizes secure VPN management, Cisco Adaptive Security Device Manager (ASDM), PIX firewall, VPN Concentrator, Adaptive Security Appliance (ASA), Intrusion Prevention Systems (IPS), Cisco Security Agent (CSA), and techniques to combine these technologies in a single, integrated network security solution.

Five recommended training courses and five required exams comprise the CCSP certification curriculum. This course covers all of these five Cisco security courses - SND, SNPA, CSVPN, IPS, and SNRS After the class you will understand major networking protocols, procedures, and how to integrate security devices with the underlying network, you will be uniquely positioned to design secure network solutions.

Associated Certifications: CCSP
Associated Exam: Cisco 642-551 SND, 642-522 SNPA, 642-511 CSVPN, 642-532 IPS, and 642-502 SNRS

CCSP: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

CCSP: Who Needs To Attend

This course is designed for networking professionals tasked with ensuring the effective use of Cisco network security technologies within their networks; This course is valuable for network

and system engineers who support, implement and maintain Cisco network security technologies; Cisco channel partners who sell, implement, and maintain Cisco network security technologies; Individuals who seek Cisco Certified Security Professional (CCSP) certification or CCIE Security certification.

Securing Cisco Network Devices (SND)

Instructor:
Course Duration: 25 hours / 5 weeks
Date/Time:
Training Location:

Course: SND

Associated Certifications: CCSP, Cisco Firewall Specialist, Cisco IPS Specialist, and Cisco VPN Specialist
Associated Exam: Cisco 642-551 SND

SND: Description

SND is a 30 hours (over duration of 6 weeks), leader-led, lab-intensive course course. This course is an entry level network security course offered as a pre-requisite to the Cisco Qualified Specialist curriculum. It provides an opportunity to learn about a broad range of the components embedded in Cisco SAFE. Learners will recognize threats and vulnerabilities to networks and learn how to implement basic mitigation measures. The course provides an introduction to the Cisco products and solutions that form the basis of the Cisco security portfolio. Learners will be able to perform basic task to secure network devices at Layers 2 and 3 using command line interface and web-based GUIs. Devices include routers, switches, access control servers, IPS sensors and VPN Concentrators.

SND: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

SND: Learning Objectives

After completing this course, students will be able to:

- Describe Cisco SAFE, Cisco's security portfolio, and Cisco's VPN Management suite
- Configure Layer 2 and 3 devices on the network perimeter with CatOS and Cisco IOS security features

- Secure a network with the Cisco PIX Security Appliance
- Provide security connectivity to a network with IPSec VPN technology
- Secure networks with host- and network-based intrusion prevention systems (IPS)
- Complete basic network security configuration and administrative tasks using Cisco Secure Access Control Server (ACS) for Windows Server
- Manage network security with CiscoWorks VPN/Security Management Solution (VMS)

Course Outline

Module 1 Securing a Network with Cisco SAFE

Module 2 Securing the Perimeter

Module 3 Cisco Security Appliances

Module 4 Building IPSec VPNs

Module 5 Securing Networks with Host- and Network-based IPS

Module 6 Securing Access with Cisco Secure ACS

Module 7 Managing Network Security

Hands-on Training

Throughout this course, you will gain hands-on experience in implementing and evaluating security configurations on various Cisco devices which include router, switch, access control server, IPS sensor and VPN Concentrator.

SND: Who Needs To Attend

This course is designed for networking professionals tasked with ensuring the effective use of Cisco network security technologies within their networks; This course is valuable for network and system engineers who support, implement and maintain Cisco network security technologies; Cisco channel partners who sell, implement, and maintain Cisco network security technologies; Individuals who seek Cisco Certified Security Professional (CCSP) or Cisco Firewall Specialist, Cisco IPS Specialist, and Cisco VPN Specialist certifications.

Securing Networks with PIX and ASA (SNPA)

Instructor:
Course Duration: 35 hours / 7 weeks
Date/Time:
Training Location:

Course: SNPA

Associated Certifications: CCSP, Cisco Firewall Specialist
Associated Exam: Cisco 642-522 SNPA

SNPA: Description

The SNPA course is a 35 hours (over duration of 7 weeks), leader-led, lab-intensive course. It is one of the exams associated with the Cisco Certified Security Professional (CCSP) and the Cisco Firewall Specialist certifications. The course takes a task-oriented approach to teaching the skills to configure, operate, and manage Cisco PIX 500 Series Security Appliances and Cisco ASA 5500 Series Adaptive Security Appliances.

SNPA: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

SNPA: Learning Objectives

After completing this course, students will be able to:

- Describe the Security Appliance features, models, components, and benefits
- Discuss Adaptive Security Algorithm (ASA) and ASA security levels
- Configure a Security Appliance for basic network connectivity
- Configure the Security Appliance to send syslog messages to a syslog server
- Describe how the TCP and UDP protocols function within the Security Appliance
- Describe how static and dynamic translations function
- Explain the Security Appliance PAT feature
- Configure and explain the function of ACLs and NAT 0 ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the Security Appliance for URL filtering
- Describe the object grouping feature of the Security Appliance and its advantages
- Name the AAA protocols supported by the Security Appliance
- Define and configure cut-through proxy authentication and tunnel access authentication
- Define and configure AAA accounting
- Install and configure basic Cisco Secure ACS function
- Describe how the Security Appliance implements FTP and HTTP protocol inspection
- Describe how the Security Appliance implements remote shell (rsh), SQL, SMTP, ICMP, and SNMP protocol inspection
- Identify the tasks and commands to configure Security Appliance IPSec support
- Describe and configure the Easy VPN Server and Remote using the Cisco VPN Client
- Configure WebVPN general parameters, servers, URLs, and port forwarding
- Monitor and maintain transparent firewall mode
- Configure and manager a security context
- Define the Security Appliance hardware failover requirements
- Install ASDM and use it to configure the Security Appliance
- Configure the AIP-SSM setup parameters
- Configure a security policy on an ASA Security Appliance using ASDM
- Configure Telnet and SSH access to the Security Appliance console
- Recover the Security Appliance passwords using general password recovery procedures

Use TFTP to install and upgrade the software image on the Security Appliance

SNPA: Course Outline

1. Course Introduction
2. Cisco Security Appliance Technology and Features
3. Cisco PIX Security Appliance and ASA (Adaptive Security Appliance) Families
4. Getting Started with Cisco Security Appliances
5. Translations and Connections
6. Access Control Lists and Content Filtering
7. Object Grouping
8. Authentication, Authorization, and Accounting
9. Switching and Routing
10. Modular Policy Framework **(new section)**
11. Protocol Handling
12. Virtual Private Network Configuration
13. Configuring Security Appliance Remote Access Using Cisco Easy VPN
14. Configuring ASA for WebVPN **(new section)**
15. Configuring Transparent Firewall **(new section)**
16. Configuring Security Contexts **(new section)**
17. Failover
18. Cisco Security Appliance Device Manager
19. AIP-Security Services Module-Getting Started **(new section)**
20. Managing Security Appliances **(new section)**
21. Configuring PIX Security Appliance Remote Access Using Cisco Easy VPN
22. Firewall Services Module

Hands-on Training
Throughout this course, you will gain extensive experience in implementing and evaluating various Firewall configurations on Cisco PIX 500 Series Security Appliances.

SNPA: Who Needs To Attend

This course is designed for networking professionals tasked with ensuring the effective use of Cisco PIX security appliance and ASA Security Appliances technologies within their networks; Network and system engineers who support, implement and maintain PIX security appliance and ASA Security Appliances; Cisco channel partners who sell, implement, and maintain PIX security appliance and ASA Security Appliances; Individuals who seek Cisco Certified Security Professional (CCSP) or Cisco Firewall Specialist certifications.

Cisco Secure Virtual Private Networks (CSVPN)

Instructor:
Course Duration: 30 hours / 6 weeks

Date/Time:
Training Location:

Course: CSVPN

Associated Certifications: CCSP, Cisco VPN Specialist
Associated Exam: Cisco 642-511 CSVPN

CSVPN: Description

CSVPN is a 30 hours (over duration of 6 weeks), leader-led, lab-intensive course. This task-oriented course teaches the knowledge and skills needed to describe, configure, verify, and manage the Cisco VPN 3000 Concentrator, Cisco VPN Software Client, and Cisco VPN 3002 Hardware Client feature set.

CSVPN: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

In addition, it is highly recommended that students have at least basic knowledge of and experience with the Cisco PIX Firewall when attending this course.

CSVPN: Learning Objectives

After completing this course, students will be able to:

- Describe the features, functions, and benefits of Cisco VPN products.
- Explain the IPSec and IKE component technologies that are implemented in Cisco Secure VPN products.
- Install and configure the Cisco IPSec VPN Software client.
- Configure Cisco VPN 3000 for remote access using pre-shared keys
- Configure Cisco VPN 3000 for remote access using digital certificates
- Configure Cisco VPN 3000 firewall feature.
- Configure Cisco VPN Windows Client auto-initiate feature

CSVPN: Course Outline

Chapter 1: Introduction
Chapter 2: Network Security and the Cisco Virtual Private Network
Chapter 3: Overview of VPN and IPSec Technologies
Chapter 4: Cisco Virtual Private Network 3000 Concentrator Series Hardware Overview
Chapter 5: Configure Cisco VPN 3000 for Remote Access Using Pre-shared Keys

Chapter 6: Configure Cisco VPN 3000 for Remote Access Using Digital Certificates
Chapter 7: Configure Cisco VPN Firewall Feature for IPSec Software Client
Chapter 8: Configure Cisco VPN Client Auto-initiation
Chapter 9: Monitor and Administer Cisco Virtual Private Network 3000 Remote Access Networks
Chapter 10: Configure Cisco Virtual Private Network 3002 Hardware Client Remote Access
Chapter 11: Configuring Cisco 3002 Hardware Client for user and unit authentication
Chapter 12: Configuring Cisco 3002 Hardware Client for backup server, load balancing and reverse route
Chapter 13: Configuring Cisco 3002 Hardware Client for software auto-update
Chapter 14: Configuring Cisco 3002 Hardware Client for IPSec over TCP and UDP
Chapter 15: Cisco VPN 3000 LAN-to-LAN with Pre-Shared Keys
Chapter 16: Configure Cisco VPN Concentrator for LAN-toLAN Using NAT
Chapter 17: Configure Cisco Virtual Private Network 3000 LAN-to-LAN Using Digital Certificates

Hands-on Training
Throughout this course, you will gain extensive experience in implementing and evaluating various VPN configurations on Cisco VPN Concentrator, Cisco Software VPN Client, and Cisco Hardware VPN Client.

CSVPN: Who Needs To Attend

This course is designed for networking professionals tasked with ensuring the effective use of Cisco VPN technologies within their networks; This course is valuable for network and system engineers who support, implement and maintain Cisco Virtual Private Networks (VPNs); Cisco channel partners who sell, implement, and maintain Cisco VPNs; Individuals who seek Cisco Certified Security Professional (CCSP) or Cisco VPN Specialist certifications.

Implementing Cisco Intrusion Prevention System (IPS)

Instructor:
Course Duration: 30 hours / 6 weeks
Date/Time:
Training Location:

Course: IPS

Associated Certifications: CCSP, Cisco IPS Specialist
Associated Exam: Cisco 642-532 IPS

IPS: Description

IPS is a 30 hours (over duration of 6 weeks), leader-led, task-oriented course. This course teaches the knowledge and skills needed to design, install, and configure a Cisco Intrusion Prevention solution for small, medium, and enterprise networks. The course covers Cisco IPS sensor platforms, including the 4200 series sensors and the Catalyst 6000 series Intrusion Detection Module 2 (IDSM-2). The IPS Device Manager is used to configure and manage Cisco IPS Sensors. The Security Monitor is used to view and respond to IPS alarms.

IPS: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system

Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

IPS: Learning Objectives

After completing this course the student should be able to:

- Explain how Cisco IPS protects network devices from attacks
- Install an IPS sensor appliance in the network and initialize it
- Configure basic sensor settings using IDM
- Configure built-in signatures to meet the requirements of a given security policy using IDM
- Describe the functions of signature engines and their parameters
- Tune and create signatures to meet the requirements of a given security policy using IDM
- Tune a sensor to work optimally in the network using IDM
- Maximize alarm management efficiency by using the Monitoring Center for Security and Cisco Threat Response
- Explain blocking concepts and use IDM to configure blocking
- Install the NM-CIDS in a router and initialize it
- Install the module in a Cisco Catalyst 6500 Switch and initialize it
- Use a Cisco Catalyst 6500 Switch to capture network traffic for intrusion prevention analysis
- Install and recover the sensor software image and perform service pack and signature updates
- Use the CLI and IDM to verify system configuration

IPS: Course Outline

Lesson 1: Course Introduction

Lesson 2: Security Fundamentals

Lesson 3: Intrusion Prevention Overview

Lesson 4: Getting Started with the IDS Command Line Interface

Lesson 5: Using IDM

Lesson 6: Basic Sensor Configuration
Lesson 7: Cisco Intrusion Detection System Alarms and Signatures
Lesson 8: Signature Engines
Lesson 9: Signature Configuration
Lesson 10: Sensor Tuning
Lesson 11: Alarm Monitoring and Management
Lesson 12: Blocking Configuration
Lesson 13: Cisco Intrusion Detection System Network Module
Lesson 14: Intrusion Detection System Module Configuration
Lesson 15: Capturing Network Traffic for Intrusion Detection Systems
Lesson 16: Sensor Maintenance
Lesson 17: Verifying System Configuration

Hands-on Training

Throughout this course, you will gain extensive experience in implementing and evaluating various configurations on Cisco IPS devices.

IPS: Who Needs To Attend

This course is designed for networking professionals tasked to ensure security on their network using Cisco IPS technologies; This course is valuable for network and system engineers who support, implement and maintain Cisco IPS devices; Cisco channel partners who sell, implement, and maintain IPS devices; Individuals who seek Cisco Certified Security Professional (CCSP) or Cisco IPS Specialist certifications.

Securing Networks with Cisco Routers and Switches (SNRS)

Instructor:
Course Duration: 30 hours / 6 weeks
Date/Time:
Training Location:

Course: SNRS

Associated Certifications: CCSP
Associated Exam: Cisco 642-502 SNRS

SNRS: Description

SNRS is a 30 hours (over duration of 6 weeks), leader-led, lab-intensive course. This course is aimed at providing network specialists with the knowledge and skills needed to secure Cisco IOS router and switch networks. Successful graduates will be able to secure the network environment using existing Cisco IOS and CatOS security features, configure the three primary components of the Cisco IOS Firewall Feature set (context-based access control (CBAC), intrusion prevention, and authentication proxy), implement secure tunnels (VPNs) using IPSec

technology, and implement basic access switch security. In addition, they will complete a security audit using functions embedded in Cisco Security Device Manager.

SNRS: Prerequisite

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge.
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

SNRS: Learning Objectives

After completing this course the student should be able to:

- Identify network security threats.
- Secure remote access using Cisco Secure ACS for Windows 2000 and Cisco IOS AAA software features.
- Protect Internet access by configuring a Cisco perimeter router.
- Configure the Cisco IOS Firewall Feature Set Context-Based Access Control.
- Configure Cisco IOS Firewall Authentication Proxy
- Configure Cisco IOS Firewall Intrusion Detection System
- Use IPSec features in Cisco IOS software to create a secure site-to-site VPN using pre-shared keys and digital certificates.
- Use Cisco Easy VPN features to create a secure remote access VPN solution.
- Use Cisco Security Device Manager to secure Cisco routers

Use Cisco Router Management Center to manage Cisco Router VPN implementations

SNRS: Course Outline

Module 1 - Cisco Secure ACS for Windows configuration

Module 2 - Configuring Cisco IOS Security Feature Set including IOS Firewall CBAC (Context-Based Access Control), Authentication Proxy and IPS(Intrusion Prevention System)

Module 3 - Layer 2 Security, including Cisco IBNS (Identity Based Network Services), and 802.1x Port-Based Authentication

Module 4 - Building Cisco IOS-based VPNs Using Cisco Routers and Pre-Shared Keys

Module 5 - Building Cisco IOS-based VPNs Using Cisco Routers and Certificate Authorities

Module 6 - Cisco IOS Remote Access Using Cisco Easy VPN

Module 7 - Cisco Security Device Manager (SDM)

Hands-on Training

Throughout this course, you will gain extensive experience in implementing and evaluating various Cisco IOS security configurations on Cisco routers and switches.

SNRS: Who Needs To Attend

This course is designed for networking professionals tasked with ensuring the effective use of Cisco IOS and CatOS security features within their networks; This course is valuable for network and system engineers who support, implement and maintain Cisco IOS and CatOS security features; Cisco channel partners who sell, implement, and maintain Cisco IOS and CatOS security features; Individuals who seek Cisco Certified Security Professional (CCSP) certification.

Contact Hours

_____ Contact Hours (Lecture ___ Hours / Lab ___ Hours)

Semester Credit Hours

_____ semester credit hours

Teaching Strategies

A variety of teaching strategies may be utilized in this course, including but not limited to, lecture, discussion, written classroom exercises, written lab exercises, performance based lab exercises, demonstrations, quizzes and examinations. Some quizzes may be entirely or contain lab based components. A mid-course and end course examination will be given.

Method of Evaluating Students

Grade Distribution

Class Attendance	10
Mid Term	30
Finals	50
Special Projects Makeup projects	10
Total	**100%**

Grading Policy

At the end of each course, each student is assigned a final grade as follows:

Point Range	Interpretation	Grade	Quality Points
90 – 100	Excellent	A	4.0
80 – 89	Very Good	B	3.0 – 3.9
70 – 79	Average	C	2.0 – 2.9
60 – 69	Poor	D	1.0 – 1.9
Below 60	Failure	F	0

N/A	Withdrawal	W	0
N/A	Pass	P	0
N/A	Incomplete	I	0

A student earning a grade of D or above is considered to have passed the course and is eligible to pursue further studies. A student receiving a grade of F has failed the course. A failed course must be repeated and passed to meet Avtech Institute's graduation requirements, in addition to an overall program GPA of 2.0.

Requirements for Successful Completion of the Course

At a minimum, students must achieve the following:

- A passing grade of **D** or above
- Completion of all required examinations
- Submission of all required lab exercises and projects and;
- Adherence to the school attendance policy.

Equipment Needed

Industry standard desktop computer for lab exercises.

Equipment Breakdown Lab room

Videos and Projector

Library Assignments

To be determined by the instructor.

Portfolio Assignment

Student program outcome portfolios are required to demonstrate student competencies. In conjunction with your course structure, please select a project/paper that best demonstrates what you have learned in this course and add it to your program portfolio.

Course Policies

Disruptive Behavior

Disruptive behavior is an activity that interferes with learning and teaching. Inappropriate talking during class, surfing inappropriate website, tardiness, cheating, alcohol or drug use, use of cell phone, playing lout music during class, etc. all disrupt the learning process.

Copyright Infringement

Specific exemptions to copyright infringement are made for student use in the context of learning activities. Graphic design students often download images from the Internet, or scan images from publications. As long as this work is for educational purpose, and subject to faculty permission, this is not a problem.

Plagiarism

Faculty cannot tolerate the ***misrepresentation of work as the student's own***. This often involves the use by one student or another student's design, whether voluntarily or involuntarily. In the event that plagiarism is evident and documented, all students involved in the conscious decision to misrepresent work must receive an F as the grade for the project. A second occurrence may result in suspension for the rest of the quarter, and return to the school only after a review by the Academic Standards Committee.

Attendance

Attendance and Lateness

In education and the workplace, regular attendance is necessary if individuals are to excel. There is a direct correlation between attendance and academic success. Attendance is mandatory. All students must arrive on time and prepared to learn at each class session. At the faculty member's discretion, students may be marked absent if they arrive more than 15 minutes late to any class. More that five absences in a class that meets twice per week or more that two absences in a class that meets once per week may result in a failure.

Make-Up Work

Late Projects and Homework

All projects and homework must be handed in on time. Homework should be emailed to your instructor if you are going to miss a class. Work that is submitted one week late will result in the loss of one full grade; and work that is submitted two weeks late will result in the loss of two full grades; more than two weeks late you will receive a failing grade on the project.