



Course Title: **Securing Networks with ASA Advanced**
Duration: **5 days**

Certification

This course forms a part of the CCSP and completes course material for exam **642-515 (SNA)**

Pre-requisites

SNAF - Securing Networks with ASA Fundamentals

Objectives

This Cisco course develops knowledge and skills on configuring, maintaining, and operating Cisco ASA 5500 Series Adaptive Security. SNA progress's from the SNAF covering advanced topics of Adaptive Security. We have added depth to the existing Cisco-developed hands-on labs for SNA. Our advanced hands-on labs, delivered in an enhanced topology designed to simulate a typical production network, guide you through exercises such as managing digital certificates for IPsec and SSL VPNs, deep packet inspection, and using the 5505 in the SOHO environment.

Labs utilize ASA 5520 security appliances, though this course and lab content is applicable across the ASA and PIX families of security appliances, since the command syntax is generally the same. This course covers the features and syntax of Cisco Security Appliance Software v8.0.

Content

1. Advanced ASA NAT

- Applying NAT 0 and Policy NAT

2. Advanced Protocol Handling

- Applying the Cisco Modular Policy Framework
- Handling Advanced Protocol

3. Dynamic Routing and Switching

- Switching with VLANs
- Routing with Dynamic Protocols

4. IPsec VPNs

- Understanding IPsec and Digital Certificates
- Implementing Site-to-Site VPNs with Digital Certificates
- Configuring the Cisco VPN Client
- Implementing Remote Access VPNs with Digital Certificates
- Configuring Advanced Remote Access Features and Policy
- Configuring the ASA 5505 as an Easy VPN Hardware Client
- IPsec VPNs and QoS

5. SSL VPNs

- SSL VPN Technology Overview
- Configuring Clientless SSL VPNs
- Configuring Full Network Access SSL VPNs
- Cisco Secure Desktop
- Securing the Desktop with CSD and DAP

6. Security Services Modules

- Examining the SSMs
- CSC-SSM: Getting Started
- AIP-SSM: Getting Started