



CTREC HILTON
IT ACADEMY

5051 Westheimer
Suite 500
Houston, Texas 77056
(713) 871-8411
866-88-C-TREC
Fax (713) 622-1915

Class Code: SNAA
Number of Days: 5
Format: Instructor-Led

Securing Networks with ASA Advance (SNAA) Version 1.0

Course Description: Securing Networks with ASA Advanced (SNAA) v1.0 is a new five-day course to replace the Cisco Secure Virtual Private networks (CSVPN) & Securing Networks with PIX and ASA (SNPA) courses. Recommended training for the Cisco Certified Security Professional (CCSP) certification, SNAA takes over where SNAF leaves off, covering advanced topics of Adaptive Security. In order to cover new features in ASA software version 8.0 and to fully cover the VPN features of the ASA, the content of SNPA was split into two courses, one that covers the fundamentals and one that covers more advanced topics.

The SNAA 1.0 course takes a task-oriented approach to teaching the skills to deploy, configure and administer the Cisco ASA using a fictional company's deployment of an ASA which is based on real world scenarios. We have added depth to the existing Cisco-developed hands-on labs for SNAA. 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. Our 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.

Prerequisites: To fully benefit from this course, learners should have the following prerequisite skills and knowledge:

- SNAF - Securing Networks with ASA Fundamentals (SNAF) Version 1.0.
- Cisco CCNA or equivalent knowledge.
- Basic knowledge of the Microsoft Windows operating system.
- Familiarity with networking and security terms and concept .

Delivery Method: Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

Course Objectives

- Use advanced NAT features such as policy-based NAT.
- Use advanced modular policy framework for deep packet inspection of application protocols such as HTTP and FTP.
- How the multimedia protocols are handled and configured by the modular policy framework of the security appliance at Layer 3, 4, and 7.
- Configure the security appliance to segment traffic with VLANs.
- Configure dynamic routing capabilities of the appliance.
- Configure the security appliance to route multicast traffic.

Course Objectives - Continued

- Use advanced IPSec VPN technologies such as peer authentication using digital certificates.
- Steps necessary to configure the ASA as a CA Server.
- Configure the IPSec VPN Client using digital certificates.
- Configure the advanced Easy VPN Server features of the ASA.
- Necessary configuration for the ASA 5505 to be a VPN hardware client.
- Steps to configure QoS for VPN traffic.
- Enable clientless SSL VPNs with the security appliance.
- Enable AnyConnect SSL VPN Client with the security appliance.
- Enable the Cisco Secure Desktop with the security appliance to increase the security posture of SSL VPN connections.
- Enable Dynamic Access Policy with the Cisco Secure Desktop.
- Understand characteristics of the services modules for the ASA.

Course Outline

Advanced ASA NAT Configuration

- ACLs, NAT 0, Policy NA.

Advanced Protocol Handling

- Modular Policy Framework.
- Protocol Application Inspection.
- Multimedia Protocol Handling.

Dynamic Routing and Switching

- VLANs.
- Dynamic Routing.
- Multicast.

VPNs with IPSec

- IPSec and Digital Certificates.
- ASA CA Server.
- LAN-to-LAN with Digital Certificates.
- IPSec VPN Client.
- Remote Access with Digital Certificates.
- Advanced Remote Access Features.
- ASA 5505 as a Hardware Client.
- VPN QoS.