ASAE 3.0 - ASA Essentials 3.0 (5 Days)

Course Overview
Gain the essential skills required to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security Appliances based on ASA Software v9.x. If you need to get up to speed quickly with Cisco's Adaptive Security Appliance (ASA), this is the course for you.

SLI has combined the most important content from Cisco's Authorized FIREWALL v2.0 and VPN v2.0 courses and added additional information on the new features in v9.x software to hone in on the most crucial aspects of the ASA. In just one week, students will cover: Firewall Basics, Network Address Translation (NAT), Access Control Lists (ACLs), Object Groups, Stateful Inspection, Modular Policy Framework, PKI Integration, Site-to-site and Remote Access VPN (both IPsec and SSL), Active/Standby Failover, Server-based Authentication, Authorization, and Accounting (AAA) using ACS 5.2 and Cisco Identity Services Engine (ISE).

Students will complete their training with high availability failover coverage, including an exclusive demonstration of what happens to firewall connections and VPN sessions during a device failure.

Target Audience

- Network administrators, managers, and coordinators
- Anyone who requires fundamental training on the ASA
- Security technicians, administrators, and engineers

Prerequisites
It is recommended that prior to taking this course, students have successfully completed the following: IINS v2.0 - Implementing Cisco IOS Network Security

Course Objectives

- Technology and features of the Cisco ASA
- Cisco ASA product family
- How ASAs protect network devices from attacks
- Bootstrap the security appliance
- Prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM)
- Launch and navigate ASDM
- Essential security appliance configuration using ASDM and the command-line interface (CLI)
- Configure dynamic and static address translations
- Configure access policy based on ACLs
- Use object groups to simplify ACL complexity and maintenance
- Use the Modular Policy Framework to provide unique policies to specific data flows
- Handle advanced protocols with application inspection
- Troubleshoot with syslog and tcp ping

Course Objectives (continued)

- Configure the ASA to work with Cisco Secure ACS 5.2 for RADIUS-based AAA of VPNs
- Basics of Identity Services Engine (ISE) integration
- Implement site-to-site IPsec VPN
- Implement remote access IPsec and SSL VPNs using the Cisco AnyConnect 3.0 Secure Mobility Client
- Work with the 5.x Legacy Cisco IPsec VPN client
- Deploy clientless SSL VPN access, including smart tunnels, plug-ins, and web-type ACLs
- Configure access control policies to implement your security policy across all classes of VPN
- Configure Active/Standby failover for both firewall and VPN high availability

Course Outline

- Module 1: Cisco ASA Essentials
- Module 2: Basic Connectivity and Device Management
- Module 3: Network Integration
- Module 4: Cisco ASA Policy Control
- Module 5: Cisco ASA VPN Architecture and Common Components
- Module 6: Cisco ASA Clientless Remote Access SSL VPN Solutions