ASAE v2.0 - ASA Essentials v2.0

GK5807

Delivery Type: Classroom
Duration: 5 days

Overview

Gain the essential skills required to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security Appliances. During this 5-day virtual course you will have 24-hour access to labs to practice course objectives. You'll receive ten extra ASAE e-lab credits (good for 30 days) to review a topic after class, refine your skills, or get in extra practice-whatever lab activities complete your training.

Audio for this virtual course will be delivered by toll-free integrated telephone conference bridge, rather than VoIP through your computer. To prepare for your class, the following hardware options are recommended:

- ✓ Wired speakerphone
- ✓ Wired telephone with headset or handset
- ✓ Wireless phone/speakerphone handset with headset adapter
- ✓ Wireless speakerphone

Pre-Requisites

- ✓ IINS 2.0 - Implementing Cisco IOS Network Security

Target Audience

Network administrators, managers, and coordinators plus anyone who requires fundamental training on the ASA Security technicians, administrators, and engineers.

Follow on Courses

- FIREWALL 2.0 - Deploying Cisco ASA Firewall Solutions
- VPN 2.0 - Deploying Cisco ASA VPN Solutions

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

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg

- ✓ 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
- ✓ Configure the ASA to work with Cisco Secure ACS 5.2 for RADIUS-based AAA of VPNs
- ✓ 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

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg