

Securing Networks with ASA Advanced (SNAA)

(5 Days)

1. Introduction
2. Initial Configuration
 - a. Interface
 - i. Security Levels
 - ii. Speed
 - b. Access Lists
 - c. Address Translation
3. Advanced ASA NAT
 - a. Applying NAT 0 and Policy NAT
 - i. ACLs
 - ii. NAT
 - iii. Translation Behavior
 - iv. NAT Exemption
 - v. Policy NAT
 - vi. Verify and Troubleshoot
4. Advanced Protocol Handling
 - a. Applying the Cisco Modular Policy Framework
 - i. Modular Policy Framework Overview
 - ii. Configuring the Modular Policy Framework
 - iii. Configuring a Layer 7 Class Map
 - iv. Configuring a REGEX Class Map
 - v. Configuring a Layer 7 Policy Map
 - vi. Verifying the Modular Policy Framework Configuration
 - b. Handling Advanced Protocol
 - i. Protocol Inspection Overview
 - ii. FTP Inspection
 - iii. HTTP Inspection
 - iv. Instant Messaging Inspection
 - v. ESMTP Inspection
 - vi. DNS Inspection
 - vii. ICMP Inspection
 - viii. Verifying Protocol Inspection
5. Dynamic Routing and Switching
 - a. Switching with VLANs
 - i. ASA VLAN Operations
 - ii. VLAN Configuration
 - iii. Configuring VLANs on the ASA 5505
 - iv. Verify VLANs
 - b. Routing with Dynamic Protocols

- i. Dynamic vs. Static Routing
 - ii. RIP
 - iii. OSPF
 - iv. EIGRP
 - v. Redistribution
 - vi. Verification and Troubleshooting
- 6. IPsec VPNs
 - a. Understanding IPsec and Digital Certificates
 - i. What IPsec Is
 - ii. IPsec Operation
 - iii. Digital Certificates and Public Key Cryptography
 - iv. Certificates and Scalability
 - v. Certificate Enrollment Process
 - vi. Validating the Certificate
 - vii. Certificate Revocation Lists
 - viii. Security Appliance Certificate Enrollment Support
 - ix. Key Pairs and Trustpoints
 - b. Implementing Site-to-Site VPNs with Digital Certificates
 - i. Site-to-Site VPNs
 - ii. Configuring CA Certificates
 - iii. Site-to-Site IPsec Connection Profiles
 - iv. Modifying Certificate to Connection Mapping
 - v. Hub and Spoke
 - vi. Site-to-Site Redundancy
 - vii. Verifying Site-to-Site VPNs
 - viii. Troubleshooting Site-to-Site VPNs
 - c. Configuring the Cisco VPN Client
 - i. Cisco VPN Client
 - ii. Client Installation
 - iii. Digital Certificates with Cisco VPN Client
 - iv. Connection Entry
 - v. Advanced Options
 - vi. Verify and Troubleshoot Client Configuration
 - d. Implementing Remote Access VPNs with Digital Certificates
 - i. Remote Access VPNs
 - ii. Configuring an ASA for Remote Access
 - iii. Installing ASA Certificates
 - iv. Defining a Remote Access Address Pool
 - v. User Policy Attribute Inheritance
 - vi. Configuring an IPSec Connection Profile
 - vii. Configuring the Certificate to Connection Profile Policy
 - viii. Verifying Remote Access VPNs
 - ix. Troubleshooting Remote Access VPNs
 - e. Configuring Advanced Remote Access Features and Policy
 - i. Load Balancing
 - ii. Reverse Route Injection

- iii. Backup Servers
 - iv. Intra-Interface VPN Traffic
 - v. NAT Transparency
 - vi. Client Update
 - vii. Split Tunneling
 - viii. Personal Firewalls
 - f. Configuring the ASA 5505 as an Easy VPN Hardware Client
 - i. Introduction to Cisco Easy VPN
 - ii. Cisco Easy VPN Server Policy
 - iii. Easy VPN Hardware Client
- 7. SSL VPNs
 - a. SSL VPN Technology Overview
 - i. SSL Overview
 - ii. Clientless SSL VPN
 - b. Configuring Clientless SSL VPNs
 - i. Configuring Clientless SSL VPN
 - ii. Verifying Clientless SSL VPN Operation
 - c. Configuring Full Network Access SSL VPNs
 - i. Cisco Full Network Access SSL VPN Overview
 - ii. Configuring Cisco AnyConnect SSL VPN
 - iii. Verifying Cisco AnyConnect SSL VPN Operation
 - iv. Configuring Advanced Features for the Cisco AnyConnect SSL VPN Client
 - v. Configuring Certificate-Based Authentication for AnyConnect SSL VPN
 - vi. Troubleshooting Cisco AnyConnect SSL VPN Client Operation
- 8. Security Services Modules
 - a. Examining the SSMs
 - i. Business Challenges
 - ii. SSMs
 - iii. CSC-SSM
 - iv. AIP-SSM
 - v. AIP-SSM or CSC-SSM
 - vi. Configure an IPS Security Policy
 - b. AIP-SSM configuration
 - i. IPS theories
 - ii. Where to deploy IPS
 - iii. Manage IPS module
 - iv. Configure IPS module
 - v. Tune IPS signatures
- 9. Security Contexts
 - a. Need for Multiple Security Contexts
 - b. Configuration
- 10. ASA Failover
 - a. Configuring Failover