

G-MAC

Document ID: 05102009



Table of contents

Cisco Certified Security Professional..... 3

Cisco Certified Security Professional

No. of Course(s): 4

Duration per Course: 60 Hours

Total Duration: 240 Hours

Course: Securing Networks with Cisco Routers and Switches (SNRS)

Implement Cisco Layer 2 security

- Utilize Cisco IOS commands to mitigate Layer 2 attacks
- Implement Cisco Identity-Based Networking Services on Cisco Catalyst Switches
- Implement Identity Management using ACS as the Authentication Server

Configure Cisco IOS Firewalls to mitigate network threats

- Identify and describe the advanced capabilities of the IOS firewall feature set
- Configure Classic IOS Firewall (CBAC) and NAT to dynamically mitigate identified threats to the network
- Verify Classic IOS Firewall (CBAC) configuration and operation
- Configure IOS Zone-Based Firewalls including advanced application inspections and URL filtering
- Verify Zone-Based Firewall operations

Configure Cisco IOS-IPS to identify and mitigate threats to network resources

- Identify and describe the advanced capabilities of the Cisco IOS-IPS feature set including Signature Event Action Processing
- Configure Cisco IOS-IPS features to identify threats and dynamically block them from entering the network
- Verify Cisco IOS-IPS operations
- Maintain, update and tune Cisco IOS-IPS signatures

Configure Cisco VPNs to provide secure connectivity for site-to-site and remote access communications

- Describe IPsec features and functionality
- Describe GRE/IPsec features and functionality
- Configure secure connectivity for site-to-site VPN using certificate authorities
- Describe DMVPN features and functionality
- Configure secure connectivity for site-to-site VPN using DMVPN
- Verify secure site-to-site VPN operations
- Implement IOS SSL VPN
- Configure Cisco IOS Easy VPN Server with Dynamic Virtual Tunnel Interface (DVTI)
- Configure Cisco IOS Easy VPN remote using both router and VPN software clients
- Verify Cisco IOS Easy VPN implementations
- Implement IOS GET VPN operations
- Describe High Availability IPsec VPNs

Implement Network Foundation Protection using the CLI

- Describe NFP features and functionality
- Secure the management plane using Cisco IOS security features
- Secure the data plane using Cisco IOS security features

- Secure the control plane using Cisco IOS security features

Course: Securing Networks with ASA Foundation (SNAF)

Configure Security Appliances for secured network connectivity

- Configure and verify network and interface settings using ASDM and CLI
- Configure and verify NAT globals, statics, NAT exemption, and Identity NAT using ASDM
- Configure and verify access-lists with or without object groups using ASDM

Configure and verify routing and switching on Security Appliances

- Describe the routing capabilities of the Security Appliance
- Use ASDM to configure VLANs on a Security Appliance interface
- Use ASDM to configure the passive RIP routing functionality of the Security Appliance

Configure and verify Authentication, Authorization, & Accounting services for Security Appliances

- Configure ACS for Security Appliance support
- Use ASDM to configure the Security Appliance AAA features
- Configure and verify Auth-Proxy (cut-through proxy) using ASDM

Configure and verify Layer 3 & 4 protocol inspection, Modular Policy Framework, and threat detection for Security Appliances

- Configure and verify Layer 3 and Layer 4 protocol inspection using ASDM
- Configure and verify Modular Policy Framework using ASDM
- Use ASDM to configure and verify threat detection

Configure and verify secure connectivity using VPNs

- Configure and verify remote access VPNs using ASDM
- Configure and verify IPsec VPN clients with preshared keys using ASDM
- Configure and verify site-to-site VPNs with preshared keys using ASDM
- Verify IKE and IPsec using ASDM and CLI
- Configure and verify clientless SSL VPN using ASDM

Configure and verify active/standby and active/active failover features on Security Appliances

- Configure and verify active/standby failover using ASDM
- Configure and verify active/active failover using ASDM
- Configure and verify redundant Interface using ASDM

Configure transparent firewall and virtual firewall features on a Security Appliance

- Explain the purpose of virtual & transparent firewalls
- Configure and verify the transparent firewall feature of the Security Appliance using CLI
- Configure and verify the virtual firewall feature of the Security Appliance using ASDM

Monitor and manage installed Security Appliances

- Update, backup, and restore configurations and software images using ASDM and CLI
- Install and verify Licensing using ASDM
- Configure and verify Console and SSH/Telnet access
- Configure and utilize Logging using ASDM

Course: Implementing Cisco Intrusion Prevention System (IPS)

Describe how Cisco IPS sensors are used to mitigate network security threats

- List sensor requirements for inline operations
- Explain the difference between inline and promiscuous mode sensor operations
- Explain how Cisco IPS protects network devices from attacks (Describe signatures, alerts, and actions)
- Explain the evasive techniques used by hackers and how Cisco IPS defeats those techniques
- Describe the considerations necessary for selection, placement, and deployment of a network intrusion prevention system
- Explain the Cisco IPS signature features

Install Cisco IPS sensors/modules and configure essential system parameters

- Explain AIP-SSM functionalities
- Use the CLI to initialize the sensor
- Configure user accounts and explain the different user roles
- Configure management access to the sensor appliance
- Explain how allowed hosts are used and how they are configured
- Describe sensor interfaces, interface pairs, VLAN-pairs, and VLAN-groups
- Use the Cisco IDM to configure sensor interfaces (enable, create pairs, assign to virtual sensors)
- Describe and configure software bypass
- Describe sensor communications with external management and monitoring systems
- Launch, navigate, and use the Cisco IDM to manage and monitor the sensor
- Describe the various CLI configuration modes and sub modes and navigate between them
- List the tasks for installing and configuring the IDSM-2 and AIP-SSM

Describe Cisco IPS sensor advanced system parameters

- Plan the mitigation of specific network vulnerabilities and exploits
- Describe sensor tuning
- Explain IP fragment and TCP stream reassembly options
- Explain how IP logging should be used and how it is configured
- Explain the use of Event Variables
- Describe signature engines and their functionality
- Determine which response actions need to be configured for a given scenario
- Describe the purpose of the Meta Event Generator
- Explain Target Value Ratings and how they are used
- Determine the need for Event Action Rules in a given scenario
- Explain event Risk Ratings and how they are used

Tune Cisco IPS sensor advanced system parameters to optimize attack mitigation performance

- Use the IDM to tune the sensor to work optimally in the network
- Use the IDM to tune signatures to provide maximum protection for a network
- Given a scenario, use the IDM to create custom signature to meet the requirements
- Configure response actions for a signature
- Configure the sensor to take response actions based on a risk rating
- Use the Cisco IDM to create a Meta signature and disable alert production for the component signatures
- Configure Event Action Filters

- Configure Target Value Ratings
- Configure general settings for Event Action Rules
- Configure Event Variables
- Use the sensor application policy enforcement feature
- Configure passive OS fingerprinting (POSFP)
- Explain the External Product Interface, its benefits, and specifications
- Configure a virtual sensor
- Configure anomaly detection
- Use IDM/CLI to monitor advanced features such as POSFP and AD

Analyze Cisco IPS sensor events to determine the appropriate response to network attacks

- Use the CLI and the Cisco IDM and IEV to monitor events

Upgrade and maintain Cisco IPS sensors

- Move software images/upgrades and configuration files via HTTP, HTTPS, SCP, and FTP
- Apply the appropriate system image to the sensor
- Perform sensor password recovery
- Explain sensor licensing and how to install a license
- Describe service pack and signature update file names and how to install them

Course: Implementing Cisco NAC Appliance (CANAC)

Implement Cisco NAC Appliance

- Identify the components and features used for Cisco NAC Appliance
- Configure and verify NAM and NAS to support the Cisco NAC Appliance In-Band server solutions
- Configure and verify NAM and NAS to support the Cisco NAC appliance Out-of-Band server solutions
- Configure Single Sign on
- Configure and verify Cisco Switches as network access devices
- Configure and verify user roles
- Implement and verify rule based policies
- Configure Cisco NAC Appliance network scanning
- Configure NAM to implement NAA on user devices
- Implement and verify an HA solution
- Administer and monitor a Cisco NAC Appliance solution

Course: Implementing Cisco Security Monitoring, Analysis and Response System (MARS)

Install and configure the Cisco Security MARS product

- Describe, configure and verify features and functions of the Cisco Security MARS appliance
- Describe, configure and verify the installation of the Cisco Security MARS appliance
- Add supported Cisco reporting devices to the Cisco Security MARS appliance and verify the operations
- Add supported third-party reporting devices to the Cisco Security MARS appliance and verify the operations
- Perform incident investigation and mitigation from the Cisco Security MARS appliance
- Configure the Cisco Security MARS appliance to send alerts and notifications

- Generate queries and reports on the Cisco Security MARS appliance
- Describe, configure and verify rules to detect interesting patterns of network activity and other anomalous network behavior
- Use the Management options in the Cisco Security MARS appliance user interface to configure and verify Event, IP, Service, and User information
- Describe and perform Cisco Security MARS appliance maintenance activities
- Describe Cisco Security MARS Global Controller functionalities

Course: Securing Networks with ASA Advanced (SNAA)

Configure and verify NAT, dynamic routing, and switching on Security Appliances

- Configure and verify VLANs using ASDM
- Configure and verify dynamic routing protocols and route redistribution using ASDM
- Configure and verify policy NAT using ASDM

Configure and verify application layer protocol inspection and Modular Policy Framework for Security Appliances

- Describe the Layer 7 advanced protocol handling capabilities of the Security Appliance
- Configure and verify Layer 7 application layer protocol inspection using ASDM
- Configure and verify Modular Policy Framework using ASDM

Configure and verify secure connectivity using IPsec VPNs

- Describe the features and capabilities of digital certificates
- Describe how to use digital certificate enrollment with the Security Appliance and Cisco VPN client
- Configure and verify remote access VPNs with digital certificates using ASDM
- Configure and verify IPsec VPN clients with digital certificates using ASDM
- Configure and verify site-to-site VPNs with digital certificates using ASDM
- Configure and verify advanced remote access features using ASDM
- Configure and verify the ASA 5505 as a remote access client using ASDM
- Configure and verify QoS for tunnel traffic using ASDM

Configure and verify secure connectivity using SSL VPNs

- Describe the features and capabilities of SSL VPNs
- Configure and verify the local certificate authority using ASDM
- Configure and verify clientless access including smart tunnels, plug-ins and bookmarks using ASDM
- Configure and verify port forwarding using ASDM
- Configure the Security Appliance for SSL VPN client access using ASDM
- Configure and verify the AnyConnect VPN client
- Configure and verify CSD using ASDM
- Configure and verify DAP using ASDM

Configure and verify AIP-SSM and CSC-SSM modules

- Explain the function that AIP-SSM and CSC-SSM perform within a network
- Configure and verify AIP-SSM
- Configure and verify CSC-SSM

Exam(s):

642-504: Securing Networks with Cisco Routers and Switches (SNRS)
642-524: Securing Networks with ASA Foundation (SNAF)
642-533: Implementing Cisco Intrusion Prevention System (IPS)

Elective(s):

642-591: Implementing Cisco NAC Appliance (CANAC) (or)
642-545: Implementing Cisco Security Monitoring, Analysis and Response System (MARS)
(or)
642-515: Securing Networks with ASA Advanced (SNAA)