FIREFLY

Managing Enterprise Security with Cisco Security Manager

DURATION: 5 DAYS   COURSE CODE: SSECMGT   FORMAT: LECTURE/LAB

COURSE DESCRIPTION

The Managing Enterprise Security with Cisco Security Manager (SSECMGT) 4.0 course is a five-day instructor-led course aimed at providing network security engineers with the knowledge and skills needed to configure and deploy Cisco Security Manager.

This course will help you:
- Configure and deploy Cisco Security Manager

WHO SHOULD ATTEND

Network Security Engineers that are working in the enterprise sector.

PREREQUISITES

Securing Networks with Cisco Routers and Switches (SECURE)

Deploying Cisco ASA Firewall Features (FIREWALL)

Deploying Cisco ASA VPN Solutions (VPN)

Implementing Cisco Intrusion Prevention System (IPS)

Understanding of networking and routing (on the CCNP level, but no certification is required).

Working knowledge of the Microsoft Windows operating system

LEARNING OBJECTIVES

Present an overview of the Cisco Security Manager product, describe the main product features, and introduce the basic deployment tasks

Manage configuration of Cisco ASA adaptive security appliances and Cisco FWSM firewall devices, and explain firewall event management and device configuration correlation

Describe the most commonly used VPN topologies and their deployment

Examine the configuration of intrusion prevention mechanisms on the Cisco IOS platform, modules, and standalone appliances, as well as explain the Cisco IPS event and configuration correlation

Explain how Cisco Security Manager works with Cisco IOS devices, including the new Cisco ISR G2 routers

Describe the FlexConfig functionality of Cisco Security Manager, the workflow mode of operation, and administrative tasks and integration with Cisco Secure ACS

COURSE OUTLINE

1. Cisco Security Manager Overview

Introducing Cisco Security Manager

Managing Devices

Managing Policies

Managing Objects

Using Map View

2. Firewall Policy Management

Managing Firewall Services

Managing Firewall Devices

Event Monitoring and Rule Correlation for Firewalls

3. VPN Policy Configuration

Managing VPNs

Managing Remote Access IPsec VPNs

Configuring Client-Based SSL VPNs

Configuring Clientless SSL VPNs

Configuring Advanced VPN Configurations

Deploying Advanced VPN Technologies

4. Cisco IPS Solutions Management

Managing Cisco IPS Services

Managing Cisco IPS Devices

Managing Cisco IPS Events

5. Cisco IOS Device Provisioning

Managing Routers

Using the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router Device Manager

6. Management, Deployment, and Administration of FlexConfigs in Cisco Security Manager

Managing FlexConfigs

Managing Activities and Workflow Deployments

Implementing Integration Between Cisco Security Manager and Cisco Secure ACS

Backing Up and Restoring Cisco Security Manager Databases

Using Monitoring, Troubleshooting, and Diagnostic Tools

DISCOVERY LABS

1: Importing Devices

2: Defining Interface Roles and Usage

3: Creating Policy Objects

4: Managing Firewall Policy—Policy Sharing

5: Managing Firewall Policy—Policy Inheritance

6: Configuring NAT and Inspecting Configuration Commands Prior to Deployment

7: Configuring Event Monitoring and Configuration Correlation for Firewalls

8: Managing SSL VPN Deployment Using Cisco AnyConnect

9: Managing Clientless SSL VPN Deployment

10: Managing DMVPN Deployment

11: Managing GET VPN Deployment

12: Configuring the Cisco IOS IPS

13: Configuring the Cisco IPS Module

14: Configuring Event Monitoring and Configuration Correlation for IPSs

15: Configuring the Cisco IOS Software Router

16: Managing DHCP Devices with the CiscoWorks Auto Update Server

17: Configuring FlexConfigs

18: Configuring Cisco Secure ACS and Cisco Security Manager Integration