Implementing Security Manager for Cisco Networks v1.1

SMN

Delivery Type: Classroom
Duration: 3 days

Overview

The Cisco Security Manager is part of the Cisco Security Management Suite, which delivers comprehensive policy administration and enforcement for the Cisco Self-Defending Network. Cisco Security Manager centrally provisions all aspects of device configurations and security policies for Cisco firewalls, virtual private networks (VPNs), and Cisco Intrusion Prevention System (IPS). It also supports advanced settings that are not strictly related to security, such as quality of service (QoS) routing and Simple Network Management Protocol (SNMP). The solution is effective for managing even small networks consisting of fewer than 10 devices, but also scales to efficiently manage large-scale networks composed of thousands of devices. Scalability is achieved through intelligent policy-based management techniques that can simplify administration.

Target Audience

Engineers who support sales of Cisco security product solution, Cisco channel partners who sell, implement, and maintain secure networks and Cisco customers who implement and maintain secure networks.

Pre-Requisites

Delegates are required to meet the following prerequisites:
Cisco CCSP® certification or the equivalent knowledge
Passage of the Securing Cisco Network Devices (SND) exam (642-551), the Securing Networks with Cisco Routers and Switches (SNRS) exam (642-502), or both
At least six months of practical experience configuring Cisco routers and security products
Familiarity with implementing network security policies and these networking components and concepts:
Security technologies: Network Address Translation (NAT), Port Address Translation (PAT), firewall appliances, VPN, IPS, Cisco Security Agent, Cisco Secure Access Control Server (ACS), integrated router and switch security, and security management software
Security protocols: authentication, authorization, and accounting (AAA), IP Security (IPsec), Internet Key Exchange (IKE), and various tunneling protocols
Application protocols: HTTP, HTTPS, Internet Control Message Protocol (ICMP), Secure Shell (SSH), Secure Sockets Layer (SSL), Network Time Protocol (NTP), FTP, TFTP, Domain Name System (DNS), and so on

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

Objectives

After completing this program, you will be able to:

- ✓ Describe the Cisco Security Manager solution, features, and functions
- ✓ Describe how to manage devices in Cisco Security Manager
- ✓ Describe the concept of policies in Cisco Security Manager and how to use and manage them
- ✓ Describe the concept of objects in Cisco Security Manager and how to use and manage them
- ✓ Describe how to use the Map view
- ✓ Describe various services and platform policies that are used to manage site-to-site VPN, remote-access VPN, and SSL VPN
- ✓ Describe various firewall services that are used to manage firewall-related policies
- ✓ Describe how to configure platform policies on firewall devices
- ✓ Describe how to configure platform-specific services and policies on Cisco IPS sensors and Cisco IOS IPS devices
- ✓ Describe how to configure platform policies and interface policies on Cisco IOS routers
- ✓ Describe how to configure platform-specific services and policies on Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- ✓ Describe the FlexConfig feature and how to use it
- ✓ Describe the process of working with activities and managing deployment in Cisco Security Manager
- ✓ Describe monitoring, troubleshooting, and diagnostic tools that are available in Cisco Security Manager

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