

CCSE R70 Exam Objectives

Chapter 1: Management Portal

- Configure Administrative access to the Security Management server from an offsite machine to facilitate remote management of corporate Security Gateways.

Key Points to Remember:

- Define how the Management Portal aids in managing and troubleshooting security configurations.
- Describe how to extend access to network policy settings to outside auditors.

Chapter 2: SmartWorkflow

- Process a change request based on an organization's existing management infrastructure.

Key Points to Remember:

- Identify the advantages of SmartWorkflow in tracking, approving, and auditing security policy changes.
- Assess the benefits of policy life-cycle management and change management.
- Determine typical SmartWorkflow administrative and use processes.

Chapter 3: Provisioning

- Determine and implement the appropriate Provisioning deployment scenario based on corporate requirements.
- Modify different properties on remote Gateways (i.e., DNS, Networking) per corporate requirements.

Key Points to Remember:

- Identify the advantages of SmartProvisioning as a centralized management tool.
- Determine typical SmartProvisioning deployment scenarios.
- Describe profile based management as it applies to SmartProvisioning.

Chapter 4: SSL VPN

- Configure applications for SSL VPN remote access based on corporate and user requirements.

Key Points to Remember:

- Describe the security features of SSL VPN.
- Identify the role of the SSL VPN in common deployment scenarios.

Chapter 5: Acceleration

- Configure and verify that traffic throughput is enhanced using SecureXL on a SecurePlatform Pro Security Gateway.

Key Points to Remember:

- Identify the advantages of SecureXL security acceleration with intense security processing requirements.
- Assess the benefits of multi-core CPU combined with SecureXL security acceleration.

Chapter 6: High Availability

- Deploy New Mode HA on a new cluster member.

Key Points to Remember:

- Identify the features and limitations of Management High Availability.

Chapter 7: Clustering

- Configure ClusterXL in a corporate network.

Key Points to Remember:

- Determine typical multiple Security Gateway cluster configurations using ClusterXL.
- List the advantages of implementing the Sticky Decision Function in a clustered environment, and determine the circumstances that it would be most beneficial.

Chapter 8: Advanced Networking - Routing

- Configure VPN in a clustered environment, and demonstrate VPN failover.
- Configure and test VPN Tunnel Interfaces (VTIs) for a clustered environment.

Key Points to Remember:

- Identify the advantages of Advanced Routing protocols for scalability, fault-tolerance, and security.

Chapter 9: Advanced Networking – Load Balancing

- Configure Load Sharing Unicast (Pivot) and Multicast Mode on a cluster member.

Key Points to Remember:

- Determine typical Load Balancing configurations using Advanced Networking.

Chapter 10: Advanced Networking – QoS

- Configure and verify the best QoS configuration using the Advanced Networking Software Blade for your corporate environment, and verify the Policy.

Key Points to Remember:

- Learn QoS architecture and typical configurations.

Chapter 11: Reporting

- Given logged data, produce reports by viewing the consolidation policy, creating a consolidation session, and changing a predefined report that provides an audit of network traffic.
- Install and configure the Eventia Suite to chart events and correlate logs into meaningful data.

Key Points to Remember:

- Define the purpose for Reporting.
- Given logged data, produce reports that provide an audit of network traffic.

Chapter 12: IPS Event Analysis

- Monitor and analyze alerts to track and identify network intrusions.
- Based on reports, modify the IPS Policy to improve system bandwidth and protections.

Key Points to Remember:

- Define the need for intrusion event analysis.
- Monitor and analyze alerts to track and identify network intrusions.