Vendor: Cisco

Exam Code: 640-554

Exam Name: Implementing Cisco IOS Network Security (IINS v2.0)

Version: DEMO

QUESTION 1
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor

Answer: D
Explanation:
"Report Manager - Collects, displays and exports network usage and security information for ASA and IPS devices, and for remote-access IPsec and SSL VPNs. These reports aggregate security data such as top sources, destinations, attackers, victims, as well as security information such as top bandwidth, duration, and throughput users. Data is also aggregated for hourly, daily, and monthly periods." and
"Health and Performance Monitor (HPM) ?Monitors and displays key health, performance and VPN data for ASA and IPS devices in your network. This information includes critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. You also can categorize devices for normal or priority monitoring, and set different alert rules for the priority devices."

QUESTION 2
Which statements about smart tunnels on a Cisco firewall are true? (Choose two.)

A. Smart tunnels can be used by clients that do not have administrator privileges
B. Smart tunnels support all operating systems
C. Smart tunnels offer better performance than port forwarding
D. Smart tunnels require the client to have the application installed locally

Answer: AD
Explanation:
Smart Tunnel is also used to provide remote access to web applications that are difficult to rewrite, such as proprietary, non-standards-based Java, Java Script, or Flash animations.
Smart Tunnel also supports Single Sign-On to web applications that require either form-based POST parameters, http basic, FTP, or NTLM authentication
Smart Tunnel can also co-exist with a Full-Tunnel VPN Client. For example, an employee can connect to the company network by using Full-Tunnel VPN Client, while simultaneously connecting to a vendor network by using Smart Tunnel.
Smart Tunnel Advantages over Port-Forwarding, Plug-ins
Smart Tunnel offers better performance than browser plug-ins.
Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
Smart Tunnel does not require users to have administrator privileges.
Smart Tunnel does not require the administrator to know application port numbers in advance.

QUESTION 3
Which of the following are features of IPsec transport mode? (Choose three.)

A. IPsec transport mode is used between end stations
B. IPsec transport mode is used between gateways

C. IPsec transport mode supports multicast
D. IPsec transport mode supports unicast
E. IPsec transport mode encrypts only the payload
F. IPsec transport mode encrypts the entire packet

Answer: ADE
Explanation:
IPSec Transport Mode
IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.
Transport mode provides the protection of our data, also known as IP Payload, and consists of TCP/UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPSec headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.
IPSec transport mode is usually used when another tunneling protocol (like GRE) is used to first encapsulate the IP data packet, then IPSec is used to protect the GRE tunnel packets. IPSec protects the GRE tunnel traffic in transport mode.

QUESTION 4
Which command verifies phase 1 of an IPsec VPN on a Cisco router?

A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active

Answer: C
Explanation:
show crypto ipsec sa verifies Phase 2 of the tunnel.

QUESTION 5
Which syslog severity level is level number 7?

A. Warning
B. Informational
C. Notification
D. Debugging

Answer: D
Explanation:
The list of severity Levels:
0 Emergency: system is unusable
1 Alert: action must be taken immediately
2 Critical: critical conditions
3 Error: error conditions
4 Warning: warning conditions
5 Notice: normal but significant condition
6 Informational: informational messages
7 Debug: debug-level messages

QUESTION 6
Which tasks is the session management path responsible for? (Choose three.)

A. Verifying IP checksums
B. Performing route lookup
C. Performing session lookup
D. Allocating NAT translations
E. Checking TCP sequence numbers
F. Checking packets against the access list

Answer: BDF

QUESTION 7
Which option is the most effective placement of an IPS device within the infrastructure?

A. Inline, behind the internet router and firewall
B. Inline, before the internet router and firewall
C. Promiscuously, after the Internet router and before the firewall
D. Promiscuously, before the Internet router and the firewall

Answer: A

QUESTION 8
Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

A. SDEE
B. Syslog
C. SNMP
D. CSM

Answer: A

QUESTION 9
If a router configuration includes the line aaa authentication login default group tacacs+ enable, which events will occur when the TACACS+ server returns an error? (Choose two.)

A. The user will be prompted to authenticate using the enable password
B. Authentication attempts to the router will be denied
C. Authentication will use the router`s local database
D. Authentication attempts will be sent to the TACACS+ server

Answer: AD

QUESTION 10
Which three statements about TACACS+ are true? (Choose three.)

A. TACACS+ uses TCP port 49.

B. TACACS+ uses UDP ports 1645 and 1812.
C. TACACS+ encrypts the entire packet.
D. TACACS+ encrypts only the password in the Access-Request packet.
E. TACACS+ is a Cisco proprietary technology.
F. TACACS+ is an open standard.

Answer: ACE

QUESTION 11
What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds

Answer: A
Explanation:
Router(config)#tacacs-server timeout ?
<1-1000> Wait time (default 5 seconds)

QUESTION 12
Which three protocols are supported by management plane protection? (Choose three.)

A. SNMP
B. SMTP
C. SSH
D. OSPF
E. HTTPS
F. EIGRP

Answer: ACE

QUESTION 13
Which statement about rule-based policies in Cisco Security Manager is true?

A. Rule-based policies contain one or more rules that are related to a device's security and operations parameters.
B. Rule-based policies contain one or more rules that control how traffic is filtered and inspected on a device.
C. Rule-based policies contain one or more user roles that are related to a device's security and operations parameters.
D. Rule-based policies contain one or more user roles that control how user traffic is filtered and inspected on a device.

Answer: B

QUESTION 14

Which command initializes a lawful intercept view?

A. username cisco1 view lawful-intercept password cisco
B. parser view cisco li-view
C. li-view cisco user cisco1 password cisco
D. parser view li-view inclusive

Answer: C
Explanation:
Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the privilege command.
SUMMARY STEPS
1. enable view
2. configure terminal
3. li-view li-password user username password password
4. username lawful-intercept [name] [privilege privilege-level| view view-name] password password
5. parser view view-name
6. secret 5 encrypted-password
7. name new-name

QUESTION 15
Which statement about IPv6 address allocation is true?

A. IPv6-enabled devices can be assigned only one IPv6 IP address.
B. A DHCP server is required to allocate IPv6 IP addresses.
C. IPv6-enabled devices can be assigned multiple IPv6 IP addresses.
D. ULA addressing is required for Internet connectivity.

Answer: C

QUESTION 16
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL

Answer: D