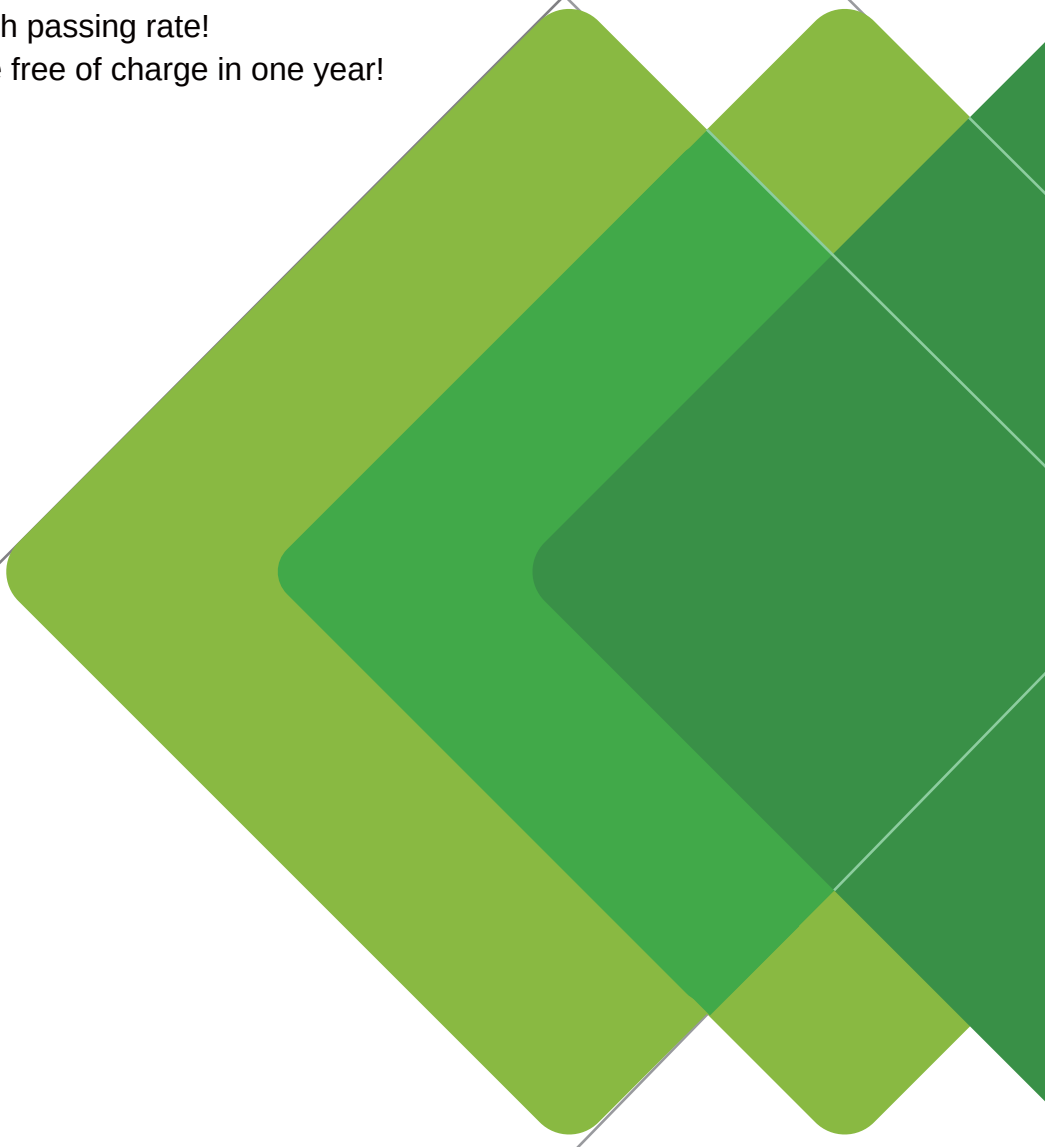
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



Exam : **156-815**

Title : Check Point Certified Managed Security Expert NGX

Version : DEMO

1. To configure for CMA redundancy, which of the following would be necessary?
A. Multiple MDS Container machines
B. The CMA High Availability option selected in the CMA properties window
C. Multiple CMAs configured on a single MDS
D. Multiple MDS Manager machines
E. The CMA High Availability option selected in the Customer properties window
Answer: A

2. The MDS will initiate status collection from the CMAs when which of the following occurs?
A. MDS-level High Availability is configured.
B. CMA-level High Availability is configured.
C. CMAs have established SIC with remote Security Gateways.
D. Get Node Data action is requested for a specific object displayed in the SmartUpdate View.
E. The MDG connects to the MDS Manager.
Answer: E

3. Which of the following actions occurs after the configuration of a CLM on an MDS MLM for a specific Customer?
A. The CLM object appears in the MDG. The Administrator needs to launch a SmartDashboard for that CLM, and configure it to retrieve the logs from the CMA's Gateway.
B. A default CLM object is created in the CMA Security Policy and is added to the list of log servers for each configured
Security Gateway.
C. No changes appear in the CMA Security Policy, but none are required. Once the CLM of a specific Customer is created, all logs are sent to that CLM by default. This is after the Policy is installed on the Gateway and the master's file is edited by the system.
D. The system creates a default CLM object in the CMA Security Policy. The Administrator must then log in to the CMA and configure the Gateway to send all logs to the CLM, by including the CLM object in its list of log servers.
E. The system performs no default configuration tasks. The Administrator must log into the CMA, create the CLM object,and add it to the Gateway's list of log servers.
Answer: D

4. The Rule Base shown below is installed on the NOC firewall at the MSP:If the Administrator intended to install licenses on remote Security Gateways by using SmartUpdate, this Rule Base is incomplete. Which of the following additions would complete the Rule Base configuration?
<e ip="4-1.gif"></e>
A. The MDS must be added to the Source column of the CMAs-to-Security Gateways Rule.
B. Create a rule allowing the remote Gateways access to the MDS.
C. Create a rule that allows the remote Gateways access to the CMAs.
D. Create a rule allowing the Primary and Secondary MDS machines located at the NOC to connect to each other.
E. Create a rule allowing the remote Gateways access to the NOC firewall.
Answer: A

5. What is the function of a CLM?
A. Performs system backups of the Primary and Secondary MDS machines.
B. Regulates ConnectControl traffic from the NOC to remote Gateways.
C. Serves as a backup CMA for CMA-level High Availability.
D. Protects the Provider-1 system from a network attack.
E. Collects log data for managed Security Gateways.
Answer: E

6. A Managed Service Provider (MSP) is using Provider-1 to manage their customer's security policies. What is the recommended method of securing the Provider-1 system in a NOC environment?
A. The Provider-1 software does not include an integrated firewall to protect the Provider-1 system. It is recommended to use a separate firewall to secure the Provider-1 environment, managed by the NOC Security Administrator and the
Provider-1 / MSP Administrator.
B. The Provider-1 software includes an integrated firewall to protect the Provider-1 system. It is recommended to use the included firewall to secure the Provider-1 environment, managed by the NOC Security Administrator.
C. The Provider-1 software includes an integrated firewall to protect the Provider-1 system. It is recommended to use the included firewall to secure the Provider-1 environment, managed by the Provider-1 / MSP Administrator.
D. The Provider-1 software does not include an integrated firewall to protect the Provider-1 system. It is recommended to use a separate firewall to secure the Provider-1 environment, managed by the NOC Security Administrator.
E. The Provider-1 software does not include an integrated firewall to protect the Provider-1 system. It is recommended to use a separate firewall to secure the Provider-1 environment, managed by the Provider-1 / MSP Administrator.
Answer: D

7. The Eventia Reporter Add-on for Provider-1 does not have its own package. It is installed, removed, enabled, and disabled using which of the following scripts?
A. SVRSetup
B. sysconfig
C. cpconfig
D. SetupUtil
E. EVRSetup
Answer: A

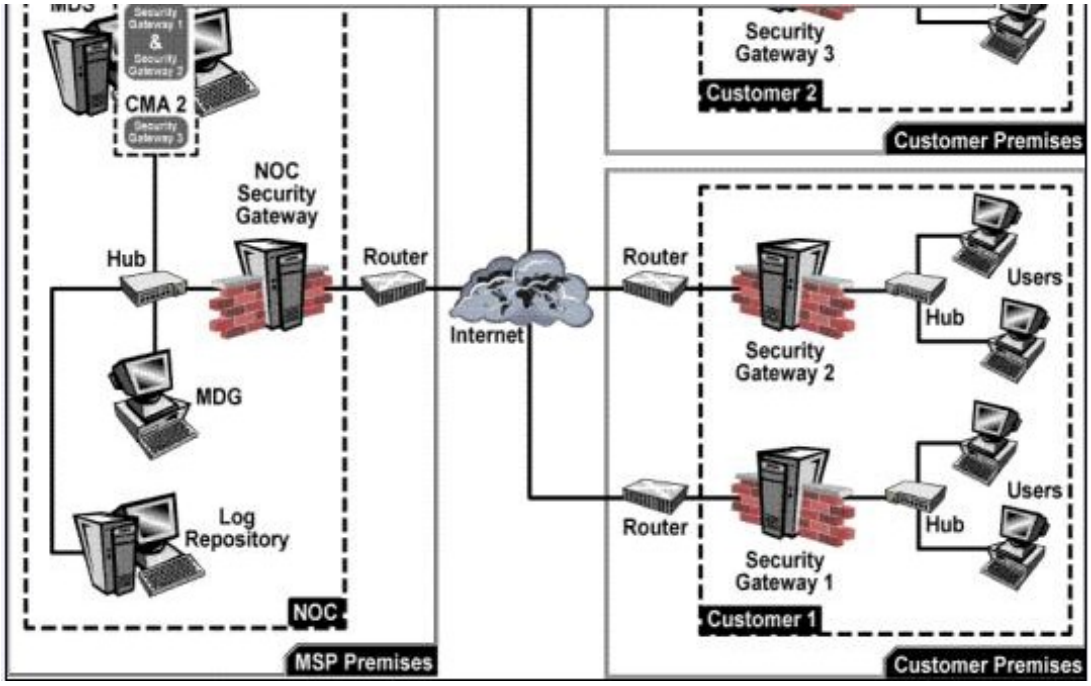
8. After the trial period expires, a permanent license must be installed. To successfully install a bundle license before the trial license expires, you must disable the trial license. Which of the following commands will disable the trial-period license on a CMA before the license expires?
A. cpprod_SetPNPDisable 1
B. SetPNPDisable lic
C. cpprod_util CPPROD_SetPnPDisable 0
D. cpprod_SetPNPDisable 0

E. cpprod_util CPPROD_SetPnPDisable 1
Answer: E

9. Secure communication from CMAs to the Security Gateways uses which type of encryption?
A. Traffic between CMAs and Security Gateways is not encrypted. Therefore, no encryption is used.
B. IKE with pre-shared secret
C. 256-bit SSL encryption
D. 128-bit SSL encryption
E. RSA encryption
Answer: D

10. All Check Point Products come with a 15-day trial-period license. How many CMAs can be managed by an MDS
Manager running with only the trial license?
A. 500
B. 1
C. 200
D. 5
E. 100
Answer: C

11. As a Provider-1 Administrator, you are concerned about the security of your NOC. You decide to install a NOC firewall and hire a firewall expert to administer it. Your firewall expert wants to institute some security measures to increase the firewall's ability to protect the NOC. One of his ideas is to hide all of the invalid IP addresses of the CMAs, by installing a Hide NAT Policy on the firewall. Will this plan work?



A. Yes, because the CMAs use virtual IP addresses, and they require a single valid IP address to manage remote Security Gateways.

B. No, because Hide NAT does not allow remote Gateways to connect directly to the CMAs.
C. Yes, but only if Hide NAT is configured with the Hide address of 0.0.0.0.
D. No, because VPN-1 NGX does not allow Administrators to configure Hide NAT on objects with assigned virtual IP addresses.
E. Yes, but only if Hide NAT is configured with the Hide address of the leading MDS interface.
Answer: B

12. When installing the Primary MDS, what information must you have?
A. Type of MDS and IP address of Secondary MDS
B. Type of MDS and IP address range for virtual IP addresses
C. Type of MDS and name of leading virtual IP interface
D. Type of MDS and one-time password
E. Type of MDS and number of CMAs to be configured
Answer: C

13. How many CLMs can each MDS MLM hold?
A. 225
B. unlimited
C. 50
D. 500
E. 250
Answer: E

14. Does the Multi Domain Server (MDS) maintain multiple customer data bases, with each customer data base relating to a single CMA?
A. The Multi Domain Server (MDS) does not maintain customer databases or CMAs.
B. The Multi Domain Server (MDS) can maintain multiple customer databases with each customer database relating to multiple CMAs.
C. The Multi Domain Server (MDS) can maintain multiple customer databases managing one CMA per customer database.
D. The Multi Domain Server (MDS) can maintain a single customer database able to relate to one CMA.
E. The Multi Domain Server (MDS) maintains one customer database able to relate to multiple CMAs.
Answer: C

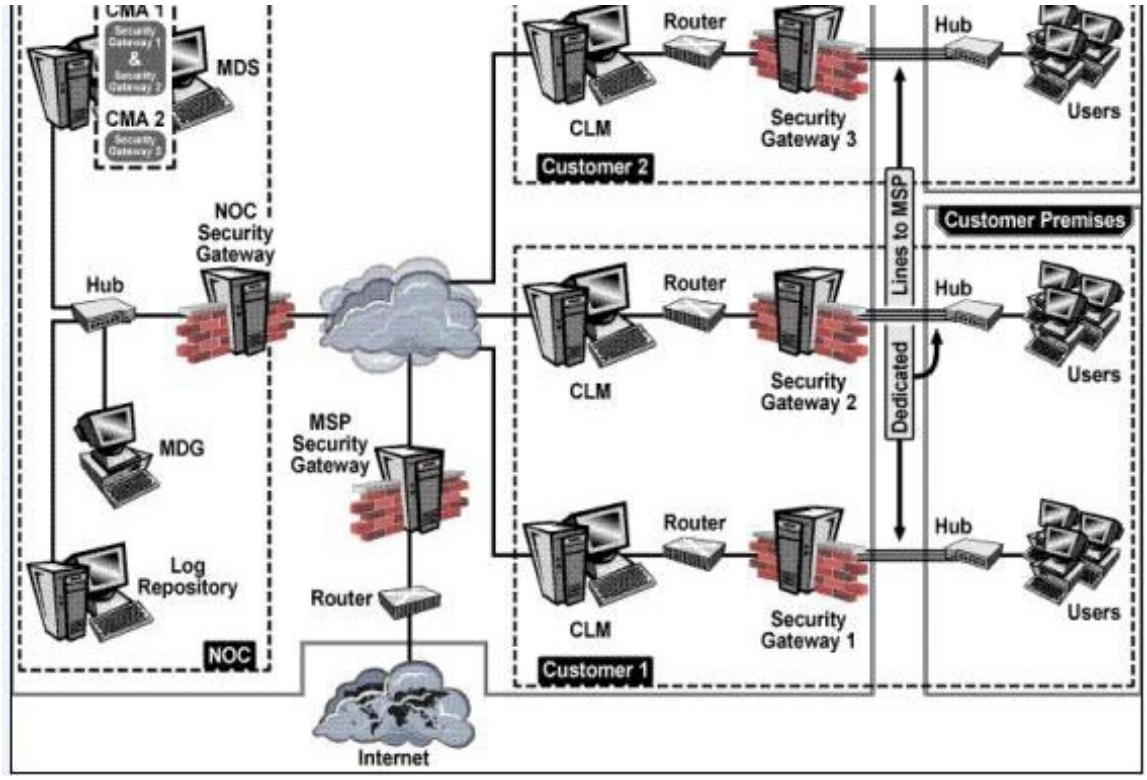
15. How many CMAs can each MDS manage?
A. Unlimited
B. 50
C. 500
D. 250
E. 200
Answer: C

16. When you set up Administrator permissions during the initial installation and configuration process, which of the

following options is NOT available?
A. Regular Administrator (None)
B. Customer Superuser
C. Provider Superuser
D. Provider Manager
E. Customer Manager
Answer: D

17. Which service does the MDG use to connect to the MDS?
A. SAM
B. CPD
C. CPMI
D. SWTP
E. SVC
Answer: C

18. Identify the following Provider-1 configuration:



A. NOC
B. ISP
C. Standard
D. Point-of-presence
E. MSP
Answer: D

19. How many Multi Domain GUIs (MDG) can connect a Multi Domain Server (MDS) at a time?

A. 250
B. 5
C. unlimited
D. 500
E. 1
Answer: C

20. When configuring an MDS MLM from the MDG, which of the following are required?
A. MDS IP address and MDS type
B. MDS Name and CMA IP address range
C. MDS Name and MDS type
D. MDS Name and MDS IP address
E. MDS IP address and CMA IP address range
Answer: D