



Exam : 156-815

Title : Check Point Certified Managed Security  
Expert NGX

Ver : 11-24-2008

---

**QUESTION 1:**

Two CMAs can be created for a single Customer, for High availability (HA). Which of these statements is NOT correct for this type of CMA configuration?

- A. The HA scheme requires one Primary CMA and one Secondary CMS, housed on different MDS computers
- B. Should a CMA fail for any reason, the Standby CMA can continue operation without service interruption
- C. Administrators make Security Policy changes through the Active CMA only
- D. The CMAs must be synchronized to maintain the same information
- E. If the Active CMA's data has not recently been synchronized with the standby CMA, it can no longer be used to replace the Active CMA if fail over occurs

Answer: E

---

**QUESTION 2:**

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. EVRSetup
- B. Cpconfig
- C. Sysconfig
- D. Setuptutil
- E. SVRSetup

Answer: E

---

**QUESTION 3:**

Which of the following statement is TRUE about Global Objects?

- A. A Global Object must have a different IP address than of the remote module on which it is installed
- B. Global Objects can share names if both the Provider-1 configuration and the remote Security Gateway are at version VPN-1 NGX
- C. A Global Object can't share the IP address of the remote module on which the Global Policy is installed
- D. Global Objects shared object names included in the Security Policy to which they are assigned
- E. Global Objects can only be edited in the Global SmartDashboard

Answer: E

**QUESTION 4:**

In Provider-1 NGX, which servers are predefined as global services for use in the Global SmartDashboard?

- A. Only Firewall-1 control connections are predefined
- B. All services are predefined in VPN-1 NGX, except VOIP related services
- C. All services are predefined in VPN-1 NGX, except the required user-defined CPMI service
- D. All services are predefined in VPN-1 NGX
- E. None of the services are predefined

Answer: D

---

**QUESTION 5:**

For which of the following components in a Provider-1 NGX deployment can a SmartCenter Server be configured as a backup?

- A. MLM
- B. Secondary MDS
- C. Primary MDS and a Secondary CMA
- D. Primary CMA not backed up by a Secondary CMA
- E. Primary MDS

Answer: D

---

**QUESTION 6:**

Which of the following Administrator types can migrate a SmartCenter Management Server into the Provider-1 system as a CMA?

- A. Provider-1 Superuser
- B. Both the Provider-1 and Customer Superusers
- C. Both the Provider-1 and Customer Managers
- D. Provider-1 Manager
- E. Customer Manager

Answer: B

---

**QUESTION 7:**

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. 256-bit SSL encryption
  - C. 128-bit SSL encryption
  - D. IKE with pre-shared secret
  - E. RSA encryption

Answer: C

---

**QUESTION 8:**

A Global VPN Community can be used in which of the following:

- A. In the implied rules of the customer-defined security policy
- B. At any point in the Customer-defined security policy
- C. In the Global security Policy, only above the customer-defined rules
- D. In the global Security Policy, only below the customer-defined rules
- E. In the Stealth rules associated with the Administrator Security Policy

Answer: B

---

**QUESTION 9:**

Which of the following services must be allowed through the NOC firewall to give a remote MDG access to the MDS?

- A. CP\_GUI
- B. CPMI
- C. FW1\_CPMI
- D. TCP\_GUI
- E. FW1\_MGMT

Answer: B

---

**QUESTION 10:**

Global SmartDefense settings may be modified within specific customer security policies.

- A. True, all aspects of a Global Policy may be modified within Individual Customer Security Policies, if the Administrator has Superuser privileges
- B. True, but only if the Global Policy is "merged" with the customer's existing Security Policy
- C. True, unlike globally defined rules, global SmartDefense settings are not read-only and may be modified
- D. True, but only if the Global Policy is applied to the customer but not installed. Once installed, the policy can't be modified

E. False, all aspects of a Global Policy are read-only and can't be modified within individual customer policies

Answer: C

---

**QUESTION 11:**

Which of the following views allows Administrators to create and configure a new CMA?

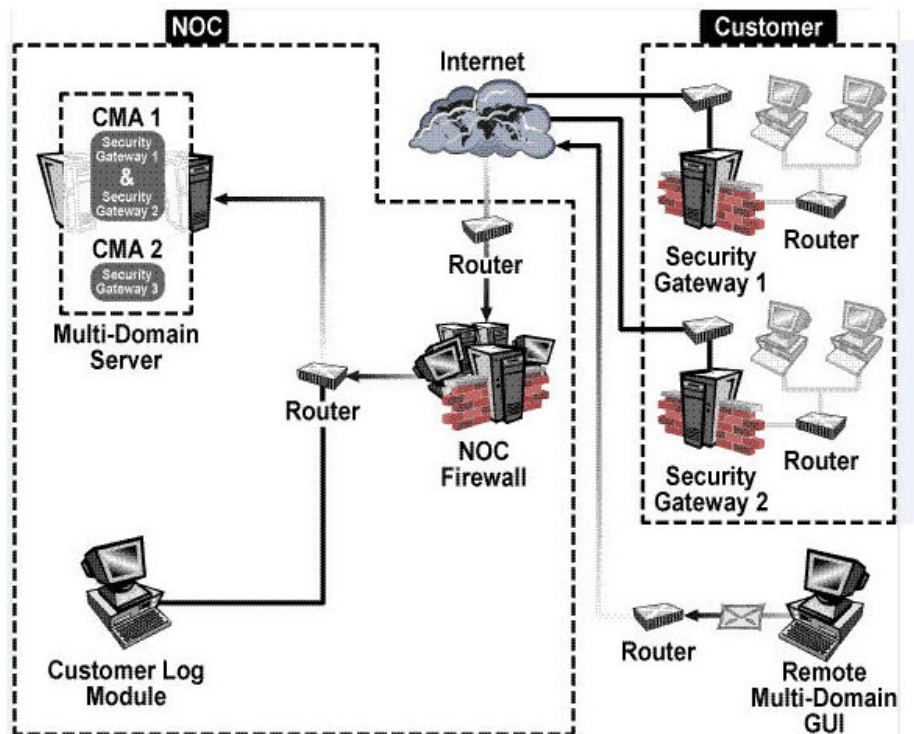
- A. System status view
- B. General view, Network Objects mode
- C. Global Policies view, Security Policies mode
- D. General view, customer contents mode
- E. General view, MDS Contents mode

Answer: D

---

**QUESTION 12:**

Exhibit:



If a NOC firewall separates the Provider-1 MDS machine and the MDG ( as shown below), what would you need to do, to allow the MDG to connect to the MDS?

- A. Create a specific RPC service and rule on the NOC firewall for MDG traffic
- B. Create a rule the NOC firewall that allows CPD and CPD\_amon traffic to pass from the MDG to the MDS object

- C. Create a UDP service and rule on the NOC firewall for MDG traffic
- D. Create a rule on the NOC firewall that allows CPMI traffic to pass from the MDG to the MDS object

Answer: D

---

**QUESTION 13:**

Before the CLM can act as a log repository, which of the following tasks must be performed?

- A. The CMA Security Policy must be installed on the CLM
- B. The administrator must log directly in to the CLM with the SmartDashboard. The Administrator must then create a Rule base with a rule allowing logs from the remote gateway access to the CLM and a rule allowing the GUI client access to the CLM
- C. The Administrator must log directly in to the CLM with the SmartView Tracker and switch Mode To Active
- D. The user database of the CMA must be installed on the CLM
- E. A Global Policy must be installed, which includes a rule at the bottom of the Rule Base that sends all logs from any Gateways to the MDS MLM

Answer: D

---

**QUESTION 14:**

Two CMAs can be for a single customer, for High Availability (HA). Which of these statements is NOT correct for this type of CMA configuration?

- A. The HA scheme requires one primary CMA and one secondary CMS, housed on different MDS computers
- B. If the Active CMAs data has not recently been synchronized with the Standby CMA, it can no longer be used to replace the Active CMA if failover occurs.
- C. Should a CMA fail for any reason, the standby CMA can continue operation without service interruption
- D. Administrators make Security Policy changes through the Active CMA only

Answer:

---

**QUESTION 15:**

Once integrated into a Provider-1 environment, Eventia Reporter maintains a connection to which of the following components?

- A. MDS MLM
- B. CMA

- C. Primary DNS
- D. Secondary MDS
- E. CLM

Answer: C

---

**QUESTION 16:**

How many CMAs can be configured for each customer on a single MDS?

- A. Two different Primary CMAs
- B. Depends on configuration: either one primary CMA and one secondary CMA or one primary CMA and one customer Log Module
- C. Unlimited
- D. Two, one primary CMA and one secondary CMA
- E. One

Answer: E

---

**QUESTION 17:**

All Security Gateway participating in a Global VPN Community must share the same \_\_\_\_\_.

- A. VPN Configuration
- B. Log Server
- C. Legal Entity
- D. User Database
- E. Management Server (CMA)

Answer: A

---

**QUESTION 18:**

Exhibit:

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Stealth Rule	★ Any	NOC_Firewall	★ Any Traffic	★ Any	drop	Log
2	MDG-to-MDS Rule	MDG	MDS	★ Any Traffic	CPMI	accept	Log
3	CMAs-to-Security Gateways Rule	CMAs	Security Gateways	★ Any Traffic	FireWall-1	accept	Log
4	Cleanup Rule	★ Any	★ Any	★ Any Traffic	★ Any	drop	Log

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?



- A. Create a Rule allowing the Primary and Secondary MDS Machine located at the NOC to connect to each other
- B. Create a Rule allowing the remote Gateways access to the MDS
- C. Create a Rule allowing the remote Gateways access to the NOC Firewall
- D. Create a Rule that allows the remote Gateways access to the CMAs
- E. The MDS must be added to the Source column of the CMAs-to-Security Gateway Rule

Answer: E

---

**QUESTION 19:**

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 0
- B. ccprod\_SetPNPDisable 1
- C. SetPNPPDisable lic
- D. Cpprod\_util CPPROD\_SetPnPDDisable 1
- E. Ccprod\_util CPPROD\_SetPnPDDisable 0

Answer: D

---

**QUESTION 20:**

Which of the following examples are the BEST uses of a Global Policy?

- A. Allowing SecureClient access to a specific customer's VPN Domain
- B. Controlling connections with a global object to which all remote customer systems have access, such as an FTP server installed at the MSP
- C. Forcing a specific group of users to authenticate before entering a specific customer's VPN Domain
- D. Logging all traffic
- E. Logging all accepted traffic

Answer: B

---

**QUESTION 21:**

Which of the following NGX SmartConsole options can be opened from the MDG?

- A. SmartView Status
- B. User Monitor
- C. SecureClient Packing Tool



- D. SmartView Tracker
- E. SmartUpdate

Answer: E

---

**QUESTION 22:**

You are an administrator who has just hired an assistant administrator to help manage the NOC and all customer Security Policies. When creating a new user for your assistant in the Provider-1 configuration, which of the following would be the MOST appropriate permission settings to assign?

- A. None
- B. Customer Superuse
- C. Customer Manager
- D. Provider-1 Manager
- E. Provider-1 SuperUser

Answer: E

---

**QUESTION 23:**

Which of the following actions is NOT possible from the SmartUpdate View?

- A. Edit Provider-1 Properties
- B. Uninstall a package
- C. Launch CMA SmartDashboard
- D. Reboot remote workstation
- E. Get node license and product information from a remote Security Gateway

Answer: C

---

**QUESTION 24:**

How can a Provider-1 Administrator verify if a specific Administrator made changes to a specific Security Policy?

- A. From the SmartDashboard of the CMA, select the Manage option; select the Audit Mode from the menu that appears
- B. From the MDS contents mode of the General View, right-click the MDS icon on which the CMA resides and select the Launch SmartView Tracker (Audit Mode) option from the menu
- C. From the SmartDashboard of the CMA, select the View option: select the Audit Mode from the Menu that appears
- D. From the CMA contents mode of the General view, right-click the MDS icon on which the CMA resides and select the Launch SmartView Tracker (Audit Mode) option

from the menu

E. This action is not possible

Answer: B

---

**QUESTION 25:**

Which of the following commands will mirror the complete functionality of MDS1 to MDS2?

A. Mdscmd mirrormds MDS2 MDS1

B. Mirror MDS1 MDS2

C. Mdscmd mirrorcma < IP Address of MDS1> < IP Address of MDS2>

D. Mdscmd mirrormds < IP Address of MDS1> < IP Address of MDS2>

E. Mdscmd mirrorcma MDS1 MDS2

Answer: E

---

**QUESTION 26:**

By NOT checking the install Policy on assigned customers option at the bottom of the Assign/Install Global Policy screen, the Global Policy will:

A. Not be installed, but will require the Administrator to install policy from the SmartDashboard on the MDS

B. Not to be installed, but will require the Administrator to rename the Global Policy so that it will be available for future assignment

C. Not be installed, but will require the Administrator to back up Global Policy information on a Secondary MDS, if one is configured

D. Be installed on the remote Security Gateways, but not enforced

E. Be installed either when installed from the MDS or from the CMA SmartDashboard

Answer: A

---

**QUESTION 27:**

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

A. 5

B. 250

C. Unlimited

D. 1

E. 500

Answer: C

---

**QUESTION 28:**

Can Multiple MDGs connect to a provider-1 system in Read/Write Mode?

- A. Yes, if all connect through MDS Manager Machines
- B. No, Provider-1 can't have more than one MDS Manager
- C. No, only one MDG at a time can have Read/Write Permissions in the Provider-1 system
- D. Yes, only if Administrators connecting through the MDGs have different permission levels
- E. Yes, if one MDG is connected to the MDS Manager and the other MDG is connected to a MDG container

Answer: A

---

**QUESTION 29:**

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) can maintain multiple customer databases managing one CMA per customer database
- 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) does not maintain customer databases or CMAs
- D. The Multi Domain Server (MDS) maintains one customer database able to relate to multiple CMAs
- E. The Multi Domain Server (MDS) can maintain a single customer database able to relate to one CMA

Answer: A

---

**QUESTION 30:**

Which of the following statements is true about configuring Global VPNs?

- A. To configure a Global VPN for gateways from different legal entities, the Security Gateway's CMAs must be configured on different MDS machines
- B. Remote-access VPNs are only available for use in Global VPN for Security Gateways with VPN-1 Pro installed
- C. For Gateways to be included in a Global VPN configuration, each must exchange the same shared-secret key to all community member gateways
- D. Site-to-Site VPNs are only available for use in Global VPN for Security Gateways with VPN-1 installed
- E. It is possible to have a single customer participate in multiple Global VPN

communities

Answer: E

---

**QUESTION 31:**

After the trail period expires, a permanent license must be installed. To successfully install a bundle license before the trail 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\_SetPNPNDisabel 0
- B. Cpprod\_util CPPROD\_SetPnPDisable 0
- C. cpprod\_setPNPDisable 1
- D. Cpprod\_util CPPROD\_SetPnPDisable 1
- E. Cpprod\_util CPPROD\_SetPnPDisable 0
- F. Set PNPDisable Lic

Answer: A

---

**QUESTION 32:**

Which of the following views allows Administrators to create and configure a new CMA?

- A. System status view
- B. General view, customer contents mode
- C. General view, Network Objects mode
- D. General view, MDS Contents mode
- E. Global Policies view, Security Policies mode

Answer: B

---

**QUESTION 33:**

Provider-1 uses which protocol to communicate among MDS machines?

- A. P1\_mgmt
- B. CPM1
- C. P1\_omi
- D. CP\_mgmt
- E. FW1\_mgmt

Answer: B

---

**QUESTION 34:**

After configuring all licensing a backup CMA on a Secondary MDS, What must you do to ensure that the backup CMA can install Policy in the event of a failover?

- A. Using the Primary CMA's SmartDashboard place the system-created object representing the backup CMA into the list of Masters for the remote Gateway
- B. Using the NOC firewall's SmartDashboard, place the system-created object representing the backup CMA into the list of Masters for the Security Gateway
- C. No action is required. When a backup CMA is created for a customer, the system automatically adjusts the Security Policy of the CMA and the backup to include the backup CMA as a Secondary Management Server
- D. From the MDG of the Primary MDS, configure the customer for which CMA HA is desired. Select the High Availability tab in the Customer Configuring screen. On the High Availability tab , enter name IP address and server information for the primary and secondary CMA

Answer: A

---

**QUESTION 35:**

In Provider-1 NGX, which servers are predefined as global services for use in the Global SmartDashboard?

- A. All services are predefined in VPN-1 NGX, except VOIP related services
- B. None of the services are predefined
- C. All services are predefined in VPN-1 NGX, except the required user-defined CPMI service
- D. Only Firewall-1 control connections are predefined
- E. All services are predefined in VPN-1 NGX

Answer: E

---

**QUESTION 36:**

SmartDefense can be modified on an individual CMA in which of the following ways?

- A. Directly changing a setting on the SmartDefense or web intelligence tabs and performing an online update
- B. Activating one of the settings in Central configuration
- C. Performing an online update and updating the Global SmartDefense settings in the provider-1 properties window
- D. Directly changing a setting on the SmartDefense or Web intelligence tabs
- E. Updating the Global Smartdefense settings in the Provider-1 Properties Window

Answer: A

---

**QUESTION 37:**

Once integrated into a Provider-1 environment, Eventia Reporter maintains a connection to which of the following components?

Answer: A

---

**QUESTION 38:**

How many CMAs can be configured for each customer?

- A. No more than five
- B. Only One
- C. Two Primary and two secondary
- D. One primary and one secondary
- E. Unlimited

Answer: D

---

**QUESTION 39:**

How many CMAs can each MDS Manage?

- A. 500
- B. 50
- C. Unlimited
- D. 250
- E. 200

Answer: A

---

**QUESTION 40:**

Which of the following types of Communities can be configured as a Global VPN?

- A. Site-to-Site star
- B. Dual
- C. Remote access meshed
- D. Site-to-Site ring
- E. Remote-Access star

Answer: A

---

**QUESTION 41:**

To configure cross-customer VPNs, what CMA information must be imported into the Global Security Policy?

- A. User Group objects
- B. Network objects
- C. Administrators objects
- D. Gateway objects
- E. Customer objects

Answer: D

---

**QUESTION 42:**

Logging in to the MDS requires your username or certificate and password. Which of the following is also required?

- A. Resolvable name of Primary MDS
- B. IP Address of CMA
- C. Resolvable name of CMA
- D. Virtual IP Address (VIP) of CMA
- E. Default IP Address of CMA

Answer: A

---

**QUESTION 43:**

If a CLM is hosted on a non-MLM type of MDS, which of the following is TRUE?

- A. There is a limit to the number of modules (20) that can log to the CLM
- B. The CLM can only function as a backup log server if the CMA is unreachable
- C. The CLM must be licensed
- D. The CLM can function as both a log and management server
- E. This scenario is impossible. The CLMs can't be loaded on any other type of MDS

Answer: C

---

**QUESTION 44:**

To configure cross-customer VPNs, what CMA information must be imported into the Global Security Policy?

- A. User Group objects
- B. Certificate Authority Objects and Certificates
- C. Customer objects
- D. Administrator Objects
- E. Network Objects



Answer: B

---

**QUESTION 45:**

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 number of CMAs to be configured
- C. Type of MDS and one-time password
- D. Type of MDS and IP Address of range for virtual IP Addresses
- E. Type of MDS and name of leading virtual IP interface

Answer: E

---

**QUESTION 46:**

Can Global objects be edited in the CMA SmartDashboard?

- A. Yes, except objects defined as internally Managed to the CMA specific Policy
- B. Yes, except objects defined as Externally Managed to the CMA specific Policy
- C. Yes, without restriction
- D. Yes, except objects with the VPN-1 Pro or VPN-1 Net options selected in the Check Point Products installed list
- E. No, Global Objects can't be edited in the CMA SmartDashboard

Answer: E

---

**QUESTION 47:**

When creating a CMA, is it necessary to license the CMA and the MDS?

- A. Yes, but only if you configuring CMA-level High Availability
- B. No, the MDS license includes the CMA licenses
- C. Yes, but only if the CMA is installed on an MDS Manager machine without an MDS container
- D. Yes, but only if the MDS is not licensed
- E. Yes, each CMA requires its own license, in addition to the MDS license

Answer: E

---

**QUESTION 48:**

Which of the following statements is TRUE concerning Provider-1?

- A. The MDS Manager functions as a firewall for the Provider-1 system, protecting the

MDS Containers

- B. The provider-1 environment should be protected by its own CMA
- C. The added security of a firewall to protect the Provider-1 system provides a greater level of security, but is not recommended, due to the complicated security policies that would be necessary
- D. All traffic between Provider-1 modules is encrypted, no firewall is necessary to protect the Provider-1 system
- E. The Provider-1 environment should be protected by a separately managed firewall

Answer: E

---

**QUESTION 49:**

To configure for CMA redundancy, which of the following would be necessary?

- A. Multiple MDS Manager Machines
- B. Multiple MDS container machines
- C. The CMA High Availability option selected in the customer properties window
- D. The CMA high Availability option selected in the CMA properties window
- E. Multiple CMAs configured on a single MDS

Answer: B

---

**QUESTION 50:**

Which of the following directories are required to migrate an existing VPN-1 NG Management Server into Provider-1 NGX?

- A. Conf and database directories
- B. Conf state and database directories
- C. Conf, bin and lib directories
- D. Conf, state and PCshared conf directories
- E. Conf, CPshared conf and CPshared database directories

Answer: A

---

**QUESTION 51:**

Which command, run from the MDS Manager, will stop a specific CMA?

- A. mdscmd fwstop <CMA Name>
- B. mdsstop\_customer <CMA Name>
- C. mdscmd stopcustomer <CMA Name>
- D. mdsstop <CMA Name>
- E. customer\_stop <CMA Name>

Answer: B

### QUESTION 52:

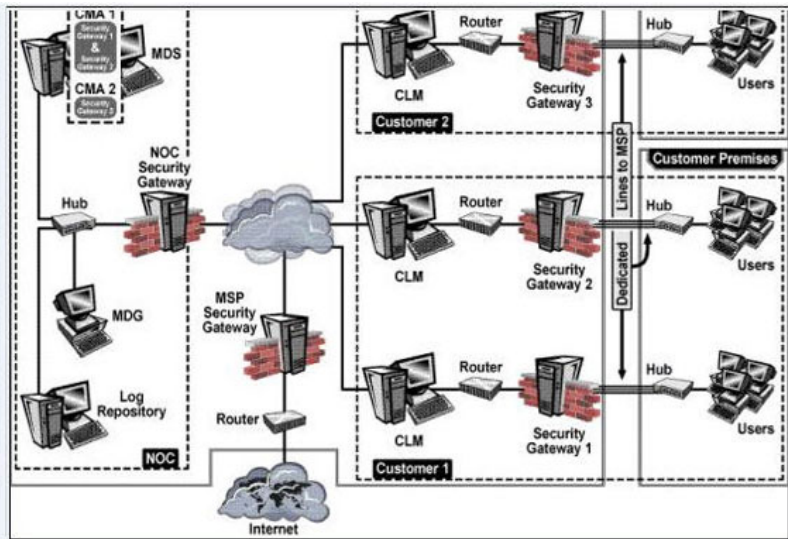
When you set up administrator permissions during the initial installation and configuration process, which of the following options is NOT available?

- A. Provider Superuser
- B. Regular Administrator (None)
- C. Provider Manager
- D. Customer Manager
- E. Customer Superuser

Answer: C

### QUESTION 53:

Exhibit



Identify the following provider-1 configuration:

- A. MSP
- B. Standard
- C. ISP
- D. NOC
- E. Point-of-Preference

Answer:

### QUESTION 54:

Which of the following action is NOT possible from the SmartUpdate view?

- A. Reboot Firewall
- B. Edit Provider-1 properties
- C. Uninstall a package
- D. Get node license and product information from a remote security gateway
- E. Execute custom commands

Answer: E

---

**QUESTION 55:**

When creating a CMA, is it necessary to license the CMA and the MDS?

- A. No, the MDS license includes the CMA licenses
- B. Yes, each CMA requires its own license, in addition to the MDS license
- C. Yes, but only if the CMA is installed on an MDS Manager machine without an MDS container
- D. Yes, but only if the MDS is not licensed
- E. Yes, but only if you are configuring CMA-level High Availability

Answer: B

---

**QUESTION 56:**

Which of the following Security Policy Components can be part of a Global Security Policy applied to Provider-1 Customer CMAs?

- A. Customer-defined objects
- B. Security Rules and Customer-defined objects
- C. Security Rules
- D. Web intelligence settings
- E. Security Rules and Web Intelligence settings

Answer: E

---

**QUESTION 57:**

You have created a new Administrator with the permissions set to NONE. What type of permissions does this grant the Administrator?

- A. The Administrator logged in to the MDG with Read/Write Permissions can access all aspects of the Provider-1 configuration, but can only access specifically assigned customers and CMAs with Read only Permissions
- B. The Administrator logged in to the MDG with Read Only permissions can access all aspects of the Provider-1 configuration and specifically assigned customers and CMAs

- C. The administrator can log in to the CMA directly using one of the NGX SmartConsoles, but can't access the MDG
- D. The Administrator logged in to the MDG with Read Only permissions can only access specifically assigned Customers and CMAs and can't access the MDS contents mode of any MDG view
- E. The Administrator is blocked from connecting to the MDG or CMAs. This action can be set for a specified duration of time or an expiration date

Answer: C

---

**QUESTION 58:**

Which of the following SmartConsoles CANNOT launch from a CLM?

- A. SmartView Status
- B. SmartUpdate
- C. SmartDashboard
- D. SmartView Monitor

Answer: B

---

**QUESTION 59:**

By default, remote security gateways deployed as part of a Provider-1 configuration send their logs to the:

- A. Local firewall and CMA
- B. Local CLM only
- C. CLM located on the secondary MDS, which is configured by default when a CMA is created
- D. CMA only
- E. CLM located on the Primary MDS, which is configured by default when a CMA is created

Answer: D

---

**QUESTION 60:**

Which of the following statements is TRUE about Global Policies?

- A. Global Policy information stored on the Primary MDS can be configured on the Secondary MDS for management failover in a High Availability configuration
- B. The Global Policy must be assigned and installed during initial MDS installation and configuration
- C. Before the MDG can create a global Policy, the Provider-1 Administrator must load the Global Policy SmartDashboard package on the MDS machine. This special Policy

Editor is available from the check point user center  
D. Every time the Global Policy is assigned, it is installed

Answer: A

---

**QUESTION 61:**

During the installation process of an MDS MLM, the MLM should be configured as a:

- A. VPN-1 NGX Management Server
- B. Comprehensive log server
- C. MDS Container
- D. Primary MDS
- E. Primary MLM

Answer: C

---

**QUESTION 62:**

What utility is a CPMD client that allows an Administrator to add or remove a customer or to use the mirror option to back up MDS information?

- A. mdsenv
- B. fwmds
- C. mdsconfig
- D. mdscmd
- E. mdsstat

Answer: D

---

**QUESTION 63:**

When is it necessary to configure an IP Address range on the Secondary MDS?

- A. When Selectively backing up a specific CMA from the Primary MDS
- B. When configuring the Secondary MDS for Management High Availability
- C. When mirroring the Primary MDS to the Secondary MDS
- D. When the Secondary MDS is located outside the NOC configuration
- E. When configuring the Secondary MDS as an MLM

Answer: C

---

**QUESTION 64:**

When you install a Global Policy on a remote Security Gateway, Where can you place the Global Rules within a CMA's existing Policy?

- A. In the middle of CMA-specific Rules
- B. Before CMA-specific rules
- C. In the Stealth Rules
- D. In the implied Rules
- E. At any Point in the CMA Rule Base as defined in the Global Policy SmartDashboard

Answer: B

---

**QUESTION 65:**

Two CMAs can be created for a single customer, for High Availability (HA). Which of these statements is NOT correct for this type of CMA configuration?

- A. Administrators make Security Policy changes through the Active CMA only
- B. The CMAs must be synchronized to maintain the same information
- C. The HA scheme requires one primary CMA and one secondary CMS, housed on different MDS computers
- D. If the Active CMA's data has not recently been synchronized with the Standby CMA, it can no longer be used to replace the Active CMA if fail over occurs
- E. Should a CMA fail for any reason, the Standby CMA can continue operation without service interruption

Answer: D

---

**QUESTION 66:**

How many CLMs can each MDs MLM hold?

- A. 500
- B. 50
- C. 225
- D. 250
- E. unlimited

Answer: D

---

**QUESTION 67:**

Can Multiple MDGs connect to a provider-1 system in Read/Write Mode?

- A. Yes, only if Administrators connecting through the MDGs have different permission levels
- B. Yes, if all connect through MDS Manager Machines
- C. Yes, if one MDG is connected to the MDS Manager and the other MDG is connected to a MDG container



- D. No, only one MDG at a time can have Read/Write Permissions in the Provider-1 system
- E. No, Provider-1 can't have more than one MDS Manager

Answer: B

---

**QUESTION 68:**

For which of the following components in a Provider-1 NGX deployment can a SmartCenter server be configured as a backup?

- A. Primary MLM backed up by a Secondary CMA
- B. CLM
- C. Primary CMA backed up by a Secondary CMA
- D. MDG
- E. MLM

Answer: C

---

**QUESTION 69:**

If services other than the predefined global services are needed:

- A. No action can be taken. Administrators can't create services not predefined in the Global SmartDashboard
- B. They must be imported from a preconfigured Global Policy
- C. They can be created by editing a default service already included in the Global Policy database and saved under a new name
- D. They must be imported from a preconfigured CMA Security Policy
- E. They can be specifically defined in the Global SmartDashboard

Answer: E

---

**QUESTION 70:**

Which of the following actions is possible from the High Availability view of the MDG?

- A. Create new MDS machines from the MDS contents mode
- B. View status of High Availability configuration
- C. Create a new backup CMA for a customer with an existing CMA, from the customer contents mode
- D. Change the Active/Standby status of CMAs from the customer contents mode

Answer: B

---

**QUESTION 71:**

In Provider-1 NGX, which services are predefined as global services for use in the Global SmartDashboard?

- A. None of the services are predefined
- B. All Services are predefined in VPN-1 NGX
- C. All Services are predefined in VPN-1 NGX, except the required user-defined CPMI services
- D. All Services are predefined in VPN-1, except VOIP related services
- E. Only Firewall-1 control connections are predefined

Answer: B

---

**QUESTION 72:**

Evaluate the following statement: GUI clients and Administrators defined on the MDS are transferred to the SmartCenter Database during synchronization.

- A. False, only Administrators defined on the MDS are transferred during database synchronization. GUI clients must be manually defined
- B. True, all GUI clients and Administrators are applied to a backup SmartCenter Server automatically during database synchronization
- C. False, a SmartCenter Server cannot be used to back up a CMA in a Provider-1 NGX configuration
- D. False, GUI clients and Administrators must be manually defined on the SmartCenter Server. They are not transferred during database synchronization
- E. False, only GUI clients defined on the MDS are transferred during database synchronization. Administrators must be manually defined

Answer: D

---

**QUESTION 73:**

The MDS will initiate status collection from the CMAs when which of the following occurs?

- A. The MDG connects to the MDS Manager
- B. CMA-level High Availability is configured
- C. CMAs have established SIC with remote security Gateways
- D. MDS-level High Availability is configured
- E. Get Node data action is requested for a specific object displayed in the SmartUpdate View

Answer: A

---

**QUESTION 74:**

When configuring an MDS MLM from the MDG, which of the following are required?

- A. MDS Name and CMA IP Address range
- B. MDS Name and MDS IP Address
- C. MDS IP address and MDS type
- D. MDS IP Address and CMA IP Address range
- E. MDS Name and MDS Type

Answer: B

---

**QUESTION 75:**

The General View is the only view in which an administrator can:

- A. Execute custom commands
- B. Assign a Global Policy to a customer
- C. Edit the CMA and MDS objects
- D. Reboot a remote workstation
- E. View statistics on a remote Security Gateway's performance

Answer: C