Checkpoint

Exam 156-915-65

Accelerated CCSE NGX R65

Version: 4.1

[Total Questions: 204]

Question No : 1

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when

(1)The Security Policy is installed.

(2)The Security Policy is saved.

(3)The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active.

(4)A scheduled event occurs.

(5)The user database is installed.

Select the BEST response for the synchronization sequence. Choose One:

A. 1,2,3,4
B. 1,2,5
C. 1,2,4
D. 1,3,4

Answer: C

Question No : 2

When configuring site-to-site VPN High Availability (HA) with MEP, which of the following is correct?

A. MEP Gateways cannot be geographically separated machines.
B. MEP Gateways must be managed by the same SmartCenter Server.
C. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.
D. If one MEP Security Gateway fails, the connection is lost and the backup Gateway picks up the next connection.

Answer: D

Question No : 3

How do you verify a VPN Tunnel Interface (VTI) is configured properly?

A. vpn shell display interface detailed <VTI name>
B. vpn shell show interface detailed <VTI name*
C. vpn shell display <VTI name> detailed
D. vpn shell show<VTI name> detailed

Answer: B

Question No : 4

A VPN Tunnel Interface (VTI) is defined on SecurePlatform Pro as: vpn shell interface add numbered 10.10.0.1 10.10.0.2 madrid.cp What do you know about this VTI?

A. The VTI name is "madrid.cp".
B. The peer Security Gateway's name is "madrid.cp"
C. 10.10.0.1 is the local Gateway's internal interface, and 10.10.0.2 is the internal interface of the remote Gateway
D. The local Gateway's object name is "madrid.cp".

Answer: B

Question No : 5

What physical machine must have access to the User Center public IP when checking for new packages with SmartUpdate?

A. SmartUpdate installed SmartCenter Server PC
B. SmartUpdate GUI PC
C. VPN.1 Security Gateway getting the new upgrade package
D. SmartUpdate Repository SQL database Server

Answer: B

Question No : 6

Which of the following would NOT be a reason for beginning with a fresh installation of VPN.1 NGX R65, instead of upgrading a previous version to VPN.1 NGX R65?

A. You see a more logical way to organize your rules and objects.
B. YOU want to keep your Check Point configuration.
C. Your Security Policy includes rules and objects whose purpose you do not know.
D. Objects and rules' naming conventions have changed overtime.

Answer: B

Question No : 7

When configuring VPN High Availability (HA) with MEP, which of the following is correct?

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the same SmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

Question No : 8

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

A. Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. Use Eventia Reporter to merge the two log server records into the same database for HIPPA log audits.
B. Install the "View Implicit Rules" package using SmartUpdate.
C. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
D. Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

Question No : 9

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartViewTracker
B. SmartView Status
C. SmartView Monitor
D. SmartDashboard

Answer: B

Question No : 10

Which of the following statements about file-type recognition in Content Inspection is TRUE?

A. A scan failure will only occur if the antivirus engine fails to initialize.
B. Antivirus status is monitored using SmartView Tracker.
C. The antivirus engine acts as a proxy, caching the scanned file before delivering it to the client.
D. All file types are considered "at risk", and are not subject to the whims of the Administrator or the Security Policy

Answer: C

Question No : 11

The Web Filtering Policy can be configured to monitor URLs in order to:

A. Log sites that are currently being blocked.
B. Log sites from blocked categories.
C. Alert the Administrator to block a suspicious site.
D. Block sites only once.

Answer: B

Question No : 12

When configuring VPN High Availability (HA) with MEP, which of the following is correct?

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the same SmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

Question No : 13

A marketing firm's networking team is trying to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks you to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should you use to check these objects and rules?

A. SmartViewTracker
B. SmartView Status
C. SmartView Monitor
D. SmartDashboard

Answer: B

Question No : 14

Which of the following is the most critical step in a SmartCenter Server NGX R65 backup strategy?

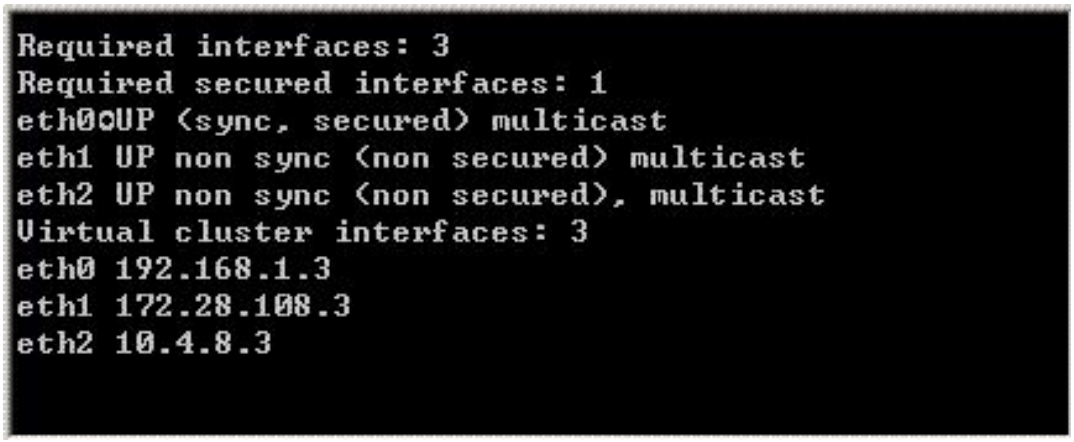
A. Perform a full system tape backup of both the SmartCenter and Security Gateway machines.
B. Run the cpstop command prior to running the upgrade_export command

C. Using the upgradejmport command, attempt to restore the SmartCenter Server to a non-production system
D. Move the *.tgz upgrade_export file to an off site location via ftp.

Answer: C

Question No : 15

An NGXR65 HA cluster contains two members with external interfaces 172.28.108.1 and 172.28.108.2. The internal interfaces are 10.4.8.1 and 10.4.8.2. The external cluster VIP address is 172.28.108.3 and the internal cluster VIP address is 10.4.8.3. The synchronization interfaces are 192.168.1.1 and 192.168.1.2. The Security Administrator discovers State Synchronization is not working properly. The cphaprob if command output displays shows:What is causing the State Synchronization problem?



A. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

Question No : 16

What is a Consolidation Policy?

A. A global Policy used to share a common enforcement policy for multiple similar Security Gateways
B. The collective name of the logs generated by Eventia Reporter
C. The collective name of the Security Policy, Address Translation, and SmartDefense Policies
D. The specific Policy written in SmartDashboard to configure which log data is stored in the Eventia Reporter database

Answer: D

Question No : 17

Which is the BEST configuration option to protect internal users from malicious Java code, without stripping Java scripts?

A. Use the URI resource to strip ActiveX tags
B. Use the URI resource to block Java code
C. Use CVP in the URI resource to block Java code
D. Use the URI resource to strip applet tags

Answer: B

Question No : 18

When configuring VPN High Availability (HA) with MEP, which of the following is correct?

A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
B. MEP Gateways must be managed by the same SmartCenter Server.
C. MEP VPN Gateways cannot be geographically separated machines.
D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

Question No : 19

Which SmartView Tracker mode allows you to read the SMTP email body sent from the Chief Executive Officer (CEO)?

A. Log Tab
B. Display Capture Action
C. This is not a SmartView Tracker feature
D. Account Query

Answer: B

Question No : 20

Match the remote-access VPN Connection mode features with their descriptions:

A. Office Mode	1. E-mail client tries to access an IMAP server behind the Security Gateway, SecureClient prompts the user to initiate a tunnel to that Gateway.
B. Visitor Mode	2. Resolves routing issues between the client and the Gateway
C. Hub Mode	3. Tunnels client-to-Gateway traffic via TCP on port 443
D. Auto Connect	4. All traffic routed through the Gateway

A. A 3,B 4,C 2,D 1
B. A 2,B 3,C 4,D 1
C. A 2,B 4,C 3,D 1
D. A 1. B 3,C 4,D 2

Answer: B

Question No : 21

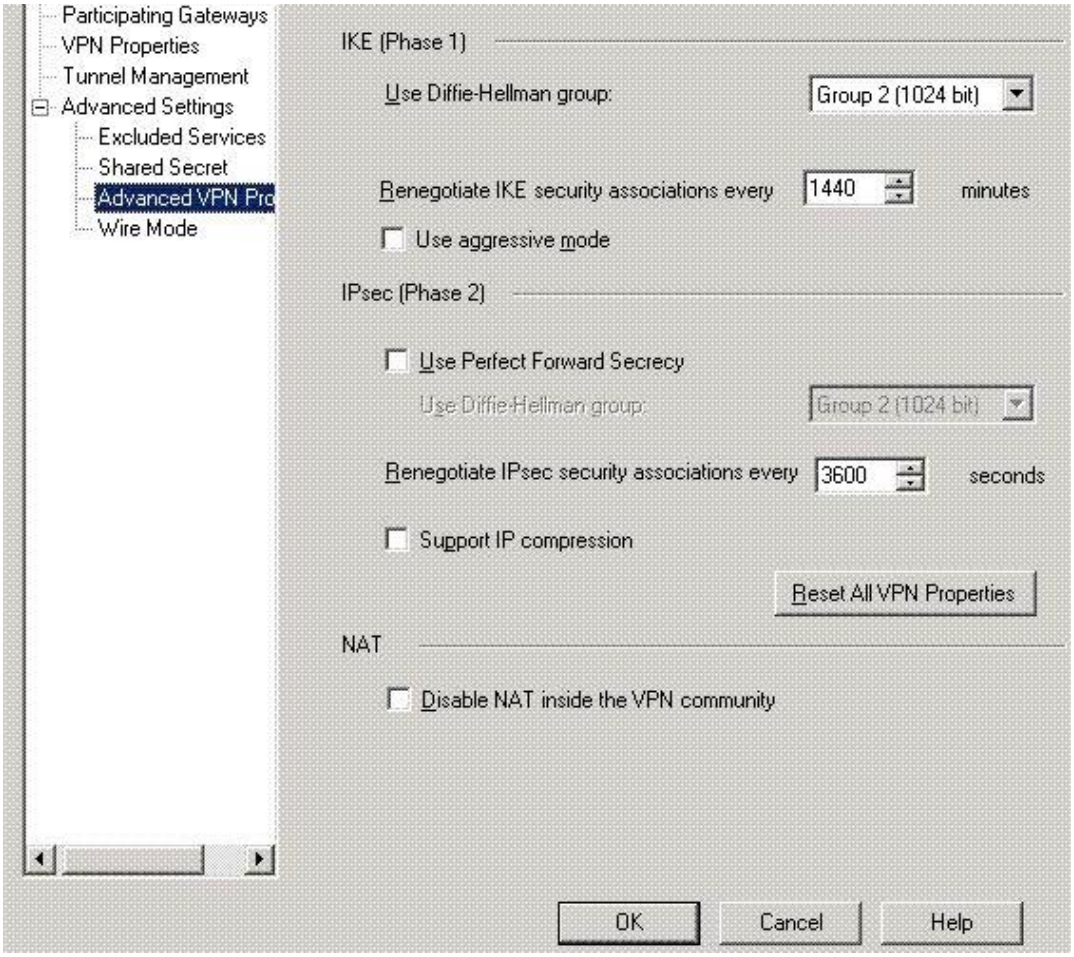
Your bank's distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. Smartupdate
B. SmartView Tracker
C. SmartDashboard
D. SmartPortal

Answer: D

Question No : 22

Look at the Advanced Properties screen exhibit. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?



A. Check the box "Use aggressive mode"
B. Change the "Renegotiate IPSec security associations every 3600 seconds" to 7200
C. Change the setting "Use Diffie-Hellman group:" to "Group 5 (1536 bit)"
D. Check the box "Use Perfect Forward Secrecy"

Answer: B

Question No : 23

Which of the following would NOT be a function of the Check Point license-upgrade tool?