Checkpoint

Exam 156-315.71

Check Point Security Expert R71

Version: 8.0

[Total Questions: 480]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	280

Topic 1, Volume A

Question No : 1 - (Topic 1)

The following is cphaprob state command output from one New Mode High Availability ClusterXL cluster member:

```
Cluster Mode: New High Availability (Active Up)

Number          Unique IP Address      Assigned Load      State
1 (local)       192.168.1.1            0%                 standby
2               192.168.1.2            100%               active
```

Which member will be active after member 192.168.12 fails over and is rebooted?

A. 92.168.12
B. Both members' state will be active.
C. 192168.1.1
D. Both members' state will be in collision

Answer: C

Question No : 2 - (Topic 1)

Which of the following statements about the Port Scanning feature of IPS is TRUE?

A. The default scan detection is when more than 500 open inactive ports are open for a period of 120 seconds.
B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. Port Scanning does not block scanning; it detects port scans with one of three levels of detection sensitivity.
D. When a port scan is detected, only a log is issued, never an alert.

Answer: C

Question No : 3 - (Topic 1)

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps. and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic is passing through the QoS Module matches both rules, which of the following statements is TRUE?

A. Each H.323 connection will receive at least 512 Kbps of bandwidth.
B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
C. 50% of available bandwidth will be allocated to the Default Rule.
D. Neither rule will be allocated more than 10% of available bandwidth.

Answer: B

Question No : 4 - (Topic 1)

How can you verify that SecureXL is running?

A. cpstat os
B. fw ver
C. secureXL stat
D. fwaccel stat

Answer: D

Question No : 5 - (Topic 1)

How is change approved for implementation in SmartWorkflow?

A. The change is submitted for approval and is automatically installed by the approver once Approve is clicked
B. The change is submitted for approval and is automatically installed by the original submitter the next time he logs in after approval of the 3nge
C. The change is submitted for approval and is manually installed by the original submitter the next time he logs in after approval of the change.
D. The change is submitted for approval and is manually installed by the approver once Approve is clicked

Answer: C

Question No : 6 - (Topic 1)

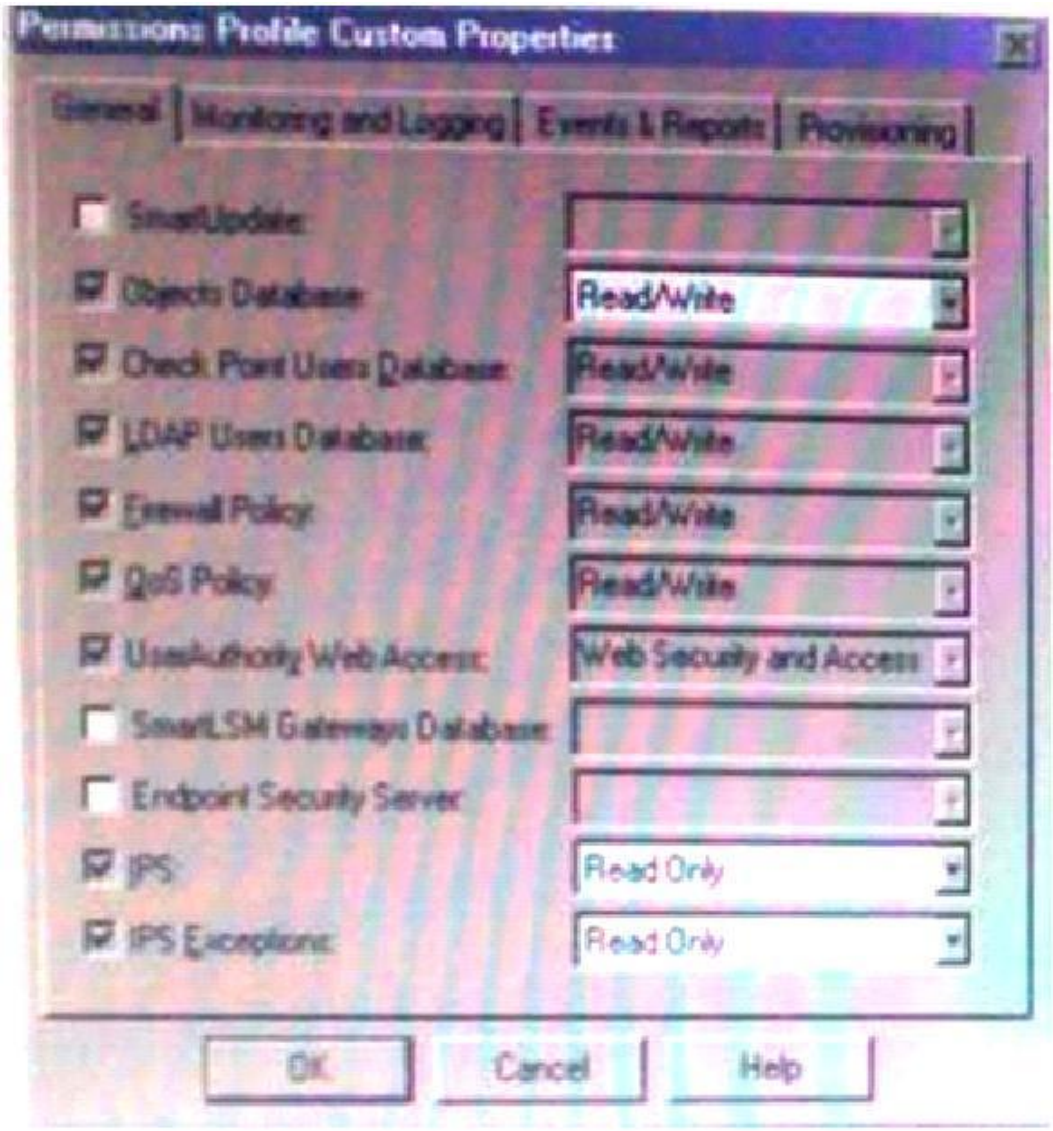
You need to publish SecurePlatform routes using the ospf routing protocol. What is the correct command structure, once entering the route command, to implement ospf successfully?

A. Run cpconfig utility to enable ospf routing
B. ip route ospf
ospf network1
ospf network2
C. Enable
Configure terminal
Router ospf [id]
Network [network] [wildmask] area [id]
D. Use DBedit utility to either the objects_5_0.c file

Answer: C

Question No : 7 - (Topic 1)

Exhibit :



UserA is able to create a SmartLSM Security Cluster Profile , you must select the correct justification.

A. False. The user must have at least Read permissions for the SmartLSM Gateways Database
B. True Only Object Database Read/Write permissions are required to create SmartLSM Profiles
C. False The user must have Read/Write permissions for the SmartLSM Gateways Database.
D. Not enough information to determine. You must know the user's Provisioning permissions to determine whether they are able to create a SmartLSM Security Cluster Profile

Answer: D

Question No : 8 - (Topic 1)

You are running R71 and using the new IPS Software Blade. To maintain the highest level of security, you are doing IPS updates regularly. What kind of problems can be caused by the automatic updates?

A. None; updates will not add any new security checks causing problematic behaviour on the systems.
B. None, all new updates will be implemented in Detect only mode to avoid unwanted trafficinterruptions. They have to be activated manually later.
C. None, all the checks will be activated from the beginning, but will only detect attacks and not disturb any non-malicious traffic in the network.
D. All checks will be activated from the beginning and might cause unwanted traffic outage due to false positives of the new checks and non-RFC compliant self-written applications.

Answer: B

Question No : 9 - (Topic 1)

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting All IP Addresses behind Gateway based on Topology information.

You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPSec tunnels instead of the routed VTI tunnels. What is the problem and how do you make the VPN use the VTI tunnels?

A. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.
B. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, use an empty group object as each Gateway's VPN Domain
C. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community
D. Route-based VTI takes precedence over the Domain VPN. To make the VPN go through VTI,use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes

Answer: B

Question No : 10 - (Topic 1)

Based on the following information, which of the statements below is TRUE?

A DLP Rule Base has the following conditions:

Data Type = Large file (> 500KB)

Source = My Organization

Destination = Free Web Mails

Protocol = Any

Action = Ask User

All other rules are set to Detect. UserCheck is enabled and installed on all client machines.

A. When a user uploads a 600 KB file to his Yahoo account via Web Mail (via his browser), he will be prompted by UserCheck
B. When a user sends an e-mail with a small body and 5 attachments, each of 200 KB to, he will be prompted by UserCheck.
C. When a user sends an e-mail with an attachment larger than 500 KB to, he will be prompted by UserCheck.
D. When a user sends an e-mail with an attachment larger than 500KB to, he will be prompted by UserCheck.

Answer: A

Question No : 11 - (Topic 1)

What is the advantage for deploying SSL VPN in a DMZ, versus a LAN?

A. SSL VPN adds another layer of access security to internal resources, when it resides in a DMZ.
B. SSL Network Extender is ineffective in a LAN deployment.
C. Traffic is in clear text when forwarded to internal servers, but the back connection is encrypted for remote users
D. Traffic is authenticated without hiding behind Connectra's IP address

Answer: A

Question No : 12 - (Topic 1)

What cluster mode is represented in this case?

1 (local) 172.168.1.1 100$ active

2 172.14*.1.2 0$ standby

A. Load Sharing (multicast mode)
B. HA (New mode).
C. 3rd party cluster
D. Load Sharing Unicast (Pivot) mode

Answer: B

Question No : 13 - (Topic 1)

Which of the following actions is most likely to improve the performance of Check Point QoS?

A. Put the most frequently used rules at the bottom of the QoS Rule Base.
B. Define Check Point QoS only on the external interfaces of the QoS Module.
C. Turn per rule limits into per connection limits
D. Turn per rule guarantees into per connection guarantees.

Answer: B

Question No : 14 - (Topic 1)

John is the MegaCorp Security Administrator, and is using Check Point R71. Malcolm is the Security Administrator of a partner company and is using a different vendor's product and both have to build a VPN tunnel between their companies. Both are using clusters with Load Sharing for their firewalls and John is using ClusterXL as a Check Point clustering solution. While trying to establish the VPN, they are constantly noticing problems and the tunnel is not stable and then Malcolm notices that there seems to be 2 SPIs with the same IP from the Check Point site. How can they solve this problem and stabilize the tunnel?

A. This can be solved by running the command Sticky VPN on the Check Point CLI. This keeps the VPN Sticky to one member and the problem is resolved.
B. This is surely a problem in the ISPs network and not related to the VPN configuration.

C. This can be solved when using clusters; they have to use single firewalls.
D. This can easily be solved by using the Sticky decision function in ClusterXL.

Answer: D

Question No : 15 - (Topic 1)

Which of the following deployment scenarios CANNOT be managed by Check Point QoS?

A. Two lines connected to a single router, and the router is connected directly to the Gateway
B. Two lines connected to separate routers, and each router is connected to separate interfaces on the Gateway
C. One LAN line and one DMZ line connected to separate Gateway interfaces
D. Two lines connected directly to the Gateway through a hub

Answer: A

Question No : 16 - (Topic 1)

How does a cluster member take over the VIP after a failover event?

A. Ping the sync interface
B. if list -renew
C. Broadcast storm
D. Gratuitous ARP

Answer: D

Question No : 17 - (Topic 1)

Which SmartReporter report type is generated from the SmartView Monitor history file?

A. Express
B. Standard
C. Custom
D. Traditional