Checkpoint

Exam 156-915.71

Check Point Certified Security Expert R71 Update

Version: 6.3

[Total Questions: 313]

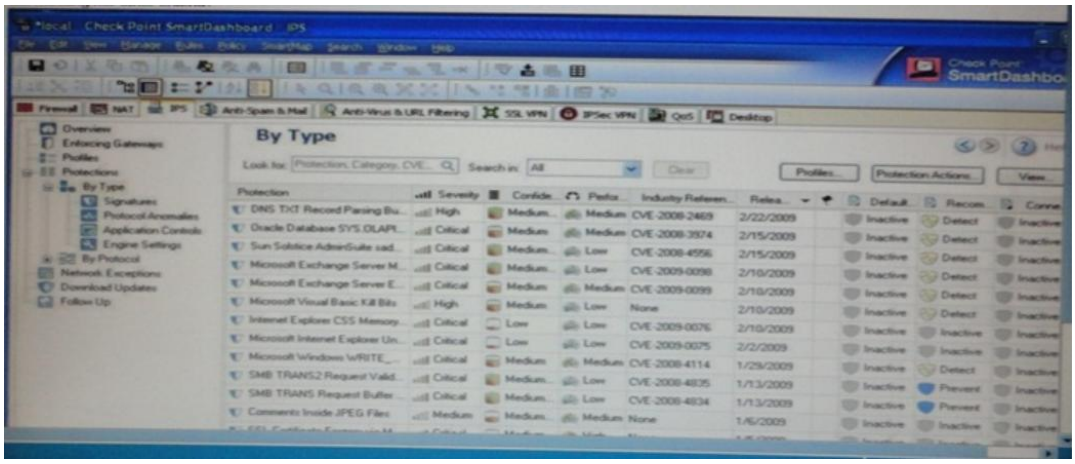
Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	113

Topic 1, Volume A

Question No : 1 - (Topic 1)

Laura notices the Microsoft Visual Basic Kill Bits Protection is set to inactive. She wants to set the Microsoft Visual Basic Kill Bits Protection and all other Performance Impact Protections to Prevent. She asks her manager for approval and he started she can turn these on. But he wants Laura to make sure High Performance Impacted Protections are turned on while changing this setting. Using the output below, how would Laura Change the Default_Protection on Performance Impact Protections classified as Low from inactive to Prevent still meeting her other criteria?



A. Go to Profiles / Default_Protection and uncheck Do not activate protections with performance impact to Medium or Above
B. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to Low or Above
C. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to Medium or Above
D. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to High or Above

Answer: C

Question No : 2 - (Topic 1)

Which of the following services will cause the secure XL templates to be disabled?

A. TELNET

B. FTP
C. LDAP
D. HTTPS

Answer: D

Question No : 3 - (Topic 1)

What command will allow you to disable sync on a cluster firewall member?

A. fw ctl setaync 0
B. fw ctl syncsatat stop
C. fw ctl syncstat off
D. fw ctl setsync off

Answer: D

Question No : 4 - (Topic 1)

Your customer complaints of the weak performance of his systems. He has heard that connection templates accelerate traffic. How do you explain to the customer about template restrictions and how to verify that they are enabled?

A. To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the destination port. to test if the connection templates are enabled, use the command “fw ct1’ templates
B. To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the secure port. to test if the connection templates are enabled, use the command “fw ct1
C. To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the secure port. to test if the connection templates are enabled, use the command “fw ct1 templates
D. To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the destination port. To test if the connection templates are enabled, use the command “fwaccel templates”

Answer: D

Question No : 5 - (Topic 1)

A VPN Tunnel Interface (VTI) is defined on SecurelPlatform Pro as:

Vpn ahell interface add numbered 10.10.0.1 10.10.0.2 madrid.cp

What do you know about this VTI?

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

Answer: A

Question No : 6 - (Topic 1)

In R71, My Organization e-mail addresses or domains are used for:

A. Scanning e-mails only if its sender e-mail address is part of this definition, by default
B. Defining the e-mail address of the SMTP relay server
C. FTP traffic sent from a user where his e-mail is part of this definition scanned by DLP, by default.
D. HTTP traffic sent from a user where his e-mail is part of this definition scanned by DLP, by default.

Answer: D

Question No : 7 - (Topic 1)

You are using tracelogger to debug SSL VPN's server side and obtain a textual traffic dump which type of traffic wills you NOT see in the output?

A. Traffic outbound from the internal networks

B. Traffic to the portal
C. Traffic outbound to the external networks
D. Traffic inbound from the external networks

Answer: B

Question No : 8 - (Topic 1)

From the following rule base, for which rules will the connection templates be generated in secureXL?

A. Rule nos 2 to 5
B. Rule nos 2 and 5
C. Rule no 2 only
D. All rules except rule no 3

Answer: C

Question No : 9 - (Topic 1)

Which procedure creates a new administrator in smartworkflow?

A. run the cpconfig, supply the login name, profile properties, name. access applications and permissions.
B. In smart dashboard, click smartworkflow / enable smartworkflow and the enable

smartworkflow wizard will start. Supply the login name, profile properties, name, access applications and prompted.
C. On the provider-1 primary MDS, run cpconfig, supply the lgin name, profile properties, name access applications and permissions.
D. In the smart dashboard, click user and administrators right click administrators / new administrator and supply the login name, profile properties, access applications and permissions

Answer: D

Question No : 10 - (Topic 1)

Which of the ft flowing is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?

A. VTTs cannot be assigned a proxy interface
B. Local IP addresses are not configured, remote IP addresses are configured
C. VTIs can only be physical, not loopback
D. VTIs are only supported on the IPSO Operating System

Answer: B

Question No : 11 - (Topic 1)

Which component functions as the Internal Certificate Authority for R71?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: B

Question No : 12 - (Topic 1)

Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?

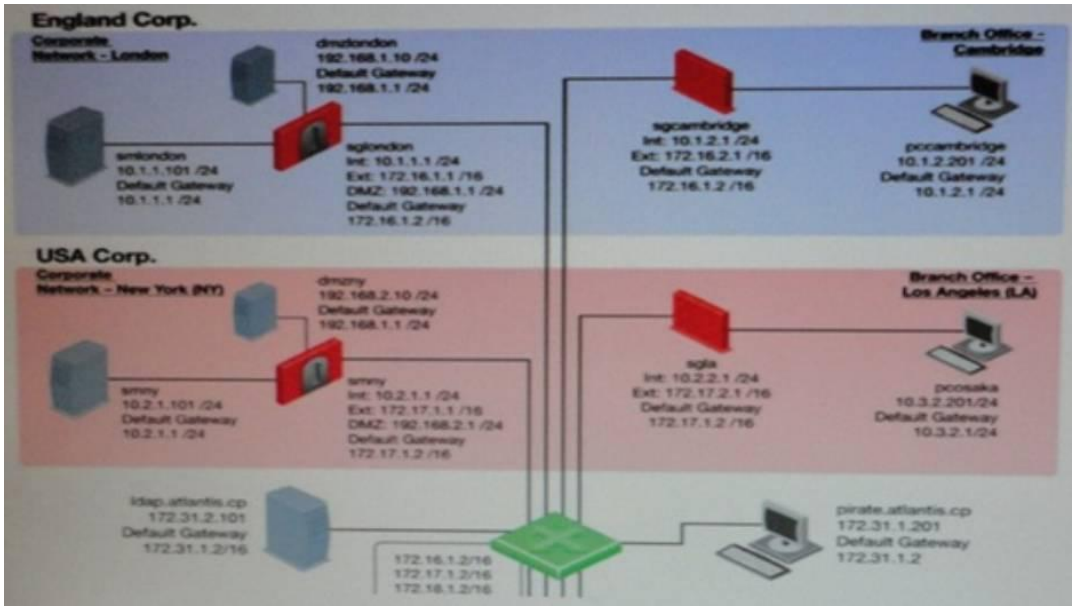
- Use same hard drive for database directory, log files and temporary directory
- Use Consolidation Rules
- Limit logging to blocked traffic only
- Using Multiple Database Tables

A. (i), (ii) and (iv)
B. (i), (iii), (iv)
C. (ii) and (iv)
D. (i) and (ii)

Answer: C

Question No : 13 - (Topic 1)

Refer to the network topology below. You have IPS Software Blades active on the Security Gateways sglondon, sgla, and sgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?



A. AH of these options are possible.
B. The attacker may have used a bunch of evasion techniques like using escape sequence instead of cleartext commands. It is also possible that there are entry points not shown in the network layout, like rogue access points.
C. Since other Gateways do not have IPS activated, attacks may originate from their network without anyone noticing.
D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-turned anomaly algorithms. Even if this is accomplished, no

technology can offer 100 % protection.

Answer: C

Question No : 14 - (Topic 1)

Among the authentication schemes SSI VPN employs for users, which scheme does Check Point recommended so all servers are replicated?

A. User certificates
B. LDAP
C. Username and password
D. RADIUS

Answer: B

Question No : 15 - (Topic 1)

The default port for browser access to the Management Portal is

A. 4433
B. 4343
C. 8080
D. 443

Answer: A

Question No : 16 - (Topic 1)

In the following command LSMcli [-d] <server> <pswd> <action> "server" should be replaced with

A. Hostname of ROBO gateway
B. Hostname DAP device
C. IP address of theSecurity Management server
D. GUclient

Answer: C

Question No : 17 - (Topic 1)

Which at the following commands shows full synchronization status?

A. cphaprob -i list.
B. fw ctl if list
C. Fw hastat
D. cphaprob –a if

Answer: A

Question No : 18 - (Topic 1)

Which of the following commands can be used to stop Management Portal services?

A. fw stopportal
B. cpportalstop
C. cpstop /portal
D. smartportalstop

Answer: D

Question No : 19 - (Topic 1)

You have a High Availability ClusterXL configuration. Machines are not synchronizer. What happens to connections on failover?

A. It is not possible to configure High Availability that is not synchronized.
B. B. Old connections are lost but can be reestablished.
C. Connection cannot be established until cluster members are fully synchronized.
D. Old connections are lost but are automatically recovered whenever the failed machine recovers.

Answer: B