

# CheckPoint

## Exam Questions 156-315.81

Check Point Certified Security Expert R81



#### NEW QUESTION 1

- (Exam Topic 1)

Which statement is NOT TRUE about Delta synchronization?

- A. Using UDP Multicast or Broadcast on port 8161
- B. Using UDP Multicast or Broadcast on port 8116
- C. Quicker than Full sync
- D. Transfers changes in the Kernel tables between cluster members.

**Answer:** A

#### NEW QUESTION 2

- (Exam Topic 1)

In R81 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

**Answer:** D

#### Explanation:

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

#### NEW QUESTION 3

- (Exam Topic 2)

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode.
- B. Install appliance TE250X in standalone mode and setup MTA.
- C. You can utilize only Check Point Cloud Services for this scenario.
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance.

**Answer:** C

#### NEW QUESTION 4

- (Exam Topic 2)

What is the command to see cluster status in cli expert mode?

- A. fw ctl stat
- B. clusterXL stat
- C. clusterXL status
- D. cphaprob stat

**Answer:** D

#### NEW QUESTION 5

- (Exam Topic 2)

What is the benefit of "fw monitor" over "tcpdump"?

- A. "fw monitor" reveals Layer 2 information, while "tcpdump" acts at Layer 3.
- B. "fw monitor" is also available for 64-Bit operating systems.
- C. With "fw monitor", you can see the inspection points, which cannot be seen in "tcpdump"
- D. "fw monitor" can be used from the CLI of the Management Server to collect information from multiple gateways.

**Answer:** C

#### NEW QUESTION 6

- (Exam Topic 2)

SandBlast appliances can be deployed in the following modes:

- A. using a SPAN port to receive a copy of the traffic only
- B. detect only
- C. inline/prevent or detect
- D. as a Mail Transfer Agent and as part of the traffic flow only

**Answer:** C

#### NEW QUESTION 7

- (Exam Topic 3)

Check Point security components are divided into the following components:

- A. GUI Client, Security Gateway, WebUI Interface
- B. GUI Client, Security Management, Security Gateway
- C. Security Gateway, WebUI Interface, Consolidated Security Logs
- D. Security Management, Security Gateway, Consolidate Security Logs

**Answer: B**

**NEW QUESTION 8**

- (Exam Topic 3)

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is \_\_\_\_\_ .

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

**Answer: D**

**NEW QUESTION 9**

- (Exam Topic 3)

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas\_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.

Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, username Password, Path, Comment, Member

**Answer: C**

**NEW QUESTION 10**

- (Exam Topic 4)

Which components allow you to reset a VPN tunnel?

- A. vpn tu command or SmartView monitor
- B. delete vpn ike sa or vpn she11 command
- C. vpn tunnelutil or delete vpn ike sa command
- D. SmartView monitor only

**Answer: D**

**NEW QUESTION 11**

- (Exam Topic 4)

Which of the following is NOT a type of Endpoint Identity Agent?

- A. Terminal
- B. Light
- C. Full
- D. Custom

**Answer: A**

**NEW QUESTION 12**

- (Exam Topic 4)

Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

- A. fw tab -t connections -s
- B. fw tab -t connections
- C. fw tab -t connections -c
- D. fw tab -t connections -f

**Answer: B**

**NEW QUESTION 13**

- (Exam Topic 4)

Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with \_\_\_\_\_ will not apply.

- A. ffffffff
- B. 00000001
- C. 00000002
- D. 00000003

**Answer: B**

**NEW QUESTION 14**

- (Exam Topic 4)

What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

- A. Specific VPN Communities
- B. Remote Access VPN Switch
- C. Mobile Access VPN Domain
- D. Network Access VPN Domain

**Answer: B**

**NEW QUESTION 15**

- (Exam Topic 4)

The WebUI offers several methods for downloading hotfixes via CPUSE except:

- A. Automatic
- B. Force override
- C. Manually
- D. Scheduled

**Answer: B**

**NEW QUESTION 16**

- (Exam Topic 4)

What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

- A. CPUSE offline upgrade only
- B. Advanced upgrade or CPUSE offline upgrade
- C. Advanced Upgrade only
- D. SmartUpdate offline upgrade

**Answer: B**

**NEW QUESTION 17**

- (Exam Topic 4)

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate.
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

**Answer: B**

**NEW QUESTION 18**

- (Exam Topic 4)

SmartEvent uses its event policy to identify events. How can this be customized?

- A. By modifying the firewall rulebase
- B. By creating event candidates
- C. By matching logs against exclusions
- D. By matching logs against event rules

**Answer: D**

**NEW QUESTION 19**

- (Exam Topic 4)

Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

- A. Security Gateway Clusters in Load Sharing mode
- B. Dedicated Log Server
- C. Dedicated SmartEvent Server
- D. Security Gateways/Clusters in ClusterXL HA new mode

**Answer: D**

**NEW QUESTION 20**

- (Exam Topic 4)

What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

- A. set config-lock on override
- B. Click the Lock icon in the WebUI
- C. "set rbac rw = 1"
- D. lock database override

**Answer:**

C

**NEW QUESTION 21**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **156-315.81 Practice Exam Features:**

- \* 156-315.81 Questions and Answers Updated Frequently
- \* 156-315.81 Practice Questions Verified by Expert Senior Certified Staff
- \* 156-315.81 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 156-315.81 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 156-315.81 Practice Test Here](#)**