156-315.81 Q&As

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

When performing a minimal effort upgrade, what will happen to the network traffic?

A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.

B. All connections that were initiated before the upgrade will be handled by the active gateway

C. All connections that were initiated before the upgrade will be handled normally

D. All connections that were initiated before the upgrade will be handled by the standby gateway

Correct Answer: B

All connections that were initiated before the upgrade will be handled by the active gateway. According to the Check Point documentation1, a minimal effort upgrade is a procedure that allows you to upgrade each Security Gateway individually, without affecting the cluster operation. The active gateway continues to handle the traffic while the standby gateway is upgraded, and then they switch roles. This way, there is no network downtime and no need to synchronize the cluster members before or after the upgrade1. However, some connections may be dropped during the switch-over, so it is recommended to use a connectivity upgrade or a zero downtime upgrade for mission- critical environments2. References: : Best Practices - Security Gateway Performance - Check Point Software : Checkpoint Cluster Firmware Upgrade - Check Point CheckMates

QUESTION 2

There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

A. Using Web Services

B. Using Mgmt_cli tool

C. Using CLISH

D. Using SmartConsole GUI console

E. Events are collected with SmartWorkflow from Trouble Ticket systems

Correct Answer: E

There are four ways to use the Management API for creating host object with R81 Management API: Using Web Services, Using mgmt_cli tool, Using CLISH, and Using SmartConsole GUI console. Events are collected with SmartWorkflow from Trouble Ticket systems is not a correct option. References: Check Point Management APIs

QUESTION 3

What a valid SecureXL paths in R81.20?

A. F2F (Slow path). Templated Path. PQX and F2V

B. F2F (Slow path). PXL, QXL and F2V

C. F2F (Slow path), Accelerated Path, PQX and F2V

D. F2F (Slow path), Accelerated Path, Medium Path and F2V

Correct Answer: D

The valid SecureXL paths in R81.20 are F2F (Slow path), Accelerated Path, Medium Path and F2V1. SecureXL is a technology that accelerates the performance of the Security Gateway by offloading CPU-intensive operations to the

SecureXL device2. SecureXL uses different paths to process packets, depending on the type and state of the connection3. The SecureXL paths are3:

F2F (Slow path): This path handles packets that require a full inspection by the Firewall kernel. It is the slowest path, but it supports all features and blades. Examples of packets that use this path are packets that belong to a new connection,

packets that match a rule with UTM blades, or packets that require address translation.

Accelerated Path: This path handles packets that belong to an established connection that does not require any further inspection by the Firewall kernel. It is the fastest path, but it supports only a limited set of features and blades. Examples

of packets that use this path are packets that match an accept rule with no UTM blades, or packets that match a rule with SecureXL acceleration enabled. Medium Path: This path handles packets that belong to an established connection that

requires some inspection by the Firewall kernel, but not a full inspection. It is faster than the F2F path, but slower than the Accelerated path. It supports more features and blades than the Accelerated path, but less than the F2F path.

Examples of packets that use this path are packets that match a rule with IPS or Anti-Bot blades, or packets that require NAT templates. F2V: This path handles packets that are encapsulated or decapsulated by the VPN kernel. It is faster

than the F2F path, but slower than the Accelerated path. It supports VPN features such as encryption, decryption, encapsulation, and decapsulation. References: R81.x Security Gateway Architecture (Logical Packet Flow) - Check Point CheckMates, SecureXL Mechanism in R80.10 and above - Check Point Software, SecureXL - Check Point Software

QUESTION 4

In R81, how do you manage your Mobile Access Policy?

A. Through the Unified Policy

B. Through the Mobile Console

C. From SmartDashboard

D. From the Dedicated Mobility Tab

Correct Answer: A

In R81, you can manage your Mobile Access Policy through the Unified Policy. The Unified Policy is a single policy that combines access control, threat prevention, data protection, and identity awareness. You can create rules for mobile access in the Unified Policy rulebase and apply them to mobile devices, users, and applications. You can also use the Mobile Access blade to configure additional settings for mobile access, such as authentication methods, VPN settings, and application portal.

QUESTION 5

Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine

B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine

C. Size of the $FWDIR/log folder of the target machine must be at least 30% of the size of the $FWDIR/log directory on the source machine

D. Size of the /var/log folder of the target machine must be at least 25GB or more

Correct Answer: B

One of the requirements for a successful upgrade using the Advanced Upgrade with Database Migration is that the size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine. This is to ensure that there is enough space to copy the log files from the source machine to the target machine during the upgrade process. References: Advanced Upgrade with Database Migration

QUESTION 6

What is the difference between an event and a log?

A. Events are generated at gateway according to Event Policy

B. A log entry becomes an event when it matches any rule defined in Event Policy

C. Events are collected with SmartWorkflow form Trouble Ticket systems

D. Log and Events are synonyms

Correct Answer: B

The difference between an event and a log is that a log entry becomes an event when it matches any rule defined in Event Policy. A log entry is a record of a network activity that is generated by a Security Gateway or a Management Server. An event is a log entry that meets certain criteria and triggers an action or a notification. The other options are either not true or not accurate definitions of events and logs. References: Check Point R81 Logging and Monitoring Administration Guide

QUESTION 7

Which of the following process pulls application monitoring status?

A. fwd

B. fwm

C. cpwd

D. cpd

Correct Answer: D

The process that pulls application monitoring status is cpd. cpd is a daemon that runs on Check Point products and performs various tasks related to management communication, policy installation, license verification, logging, etc. cpd also monitors the status of other processes and applications on the system and reports it to the management server. cpd uses SNMP to collect information from various sources, such as blades, gateways, servers, etc. You can view the application monitoring status in SmartConsole by using the Gateways and Servers tab in the Logs and Monitor view. References: Check Point Processes and Daemons

QUESTION 8

Which is not a blade option when configuring SmartEvent?

A. Correlation Unit

B. SmartEvent Unit

C. SmartEvent Server

D. Log Server

Correct Answer: B

SmartEvent Unit is not a blade option when configuring SmartEvent. SmartEvent is a unified security event management solution that provides visibility, analysis, and reporting of security events across multiple Check Point products. SmartEvent consists of three main components: SmartEvent Server, Correlation Unit, and Log Server. SmartEvent Server is responsible for storing and displaying security events in SmartConsole and SmartEventWeb. Correlation Unit is responsible for collecting and correlating logs from various sources and generating security events based on predefined or custom scenarios. Log Server is responsible for receiving and indexing logs from Security Gateways and other Check Point modules. SmartEvent Unit is not a valid component or blade of SmartEvent.

QUESTION 9

IF the first packet of an UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), what message is sent back through the kernel?

A. Nothing

B. TCP FIN

C. TCP RST

D. ICMP unreachable

Correct Answer: A

If the first packet of a UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), nothing is sent back through the kernel. This is because UDP is a connectionless protocol that does not require an acknowledgement from the receiver. Therefore, if a UDP packet is dropped by the Firewall, the sender will not receive

any feedback or notification. References: UDP Protocol

QUESTION 10

What is the purpose of Priority Delta in VRRP?

A. When a box up, Effective Priority = Priority + Priority Delta

B. When an Interface is up, Effective Priority = Priority + Priority Delta

C. When an Interface fail, Effective Priority = Priority ?Priority Delta

D. When a box fail, Effective Priority = Priority ?Priority Delta

Correct Answer: C

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will begin to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP.

References:

QUESTION 11

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.

B. Fill Layer4 VPN SL VPN that gives users network access to all mobile applications.

C. Full Layer3 VPN PSec VPN that gives users network access to all mobile applications.

D. You can make sure that documents are sent to the intended recipients only.

Correct Answer: C

The feature that provides Full Layer3 VPN PSec VPN, giving users network access to all mobile applications, is the correct answer.

Capsule Connect/VPN is used to establish secure VPN connections for mobile devices, and the Full Layer3 VPN (IPSec VPN) option provides comprehensive network access.

References: Check Point documentation or training materials related to Mobile Access Methods and VPN configurations.

QUESTION 12

Identity Awareness allows the Security Administrator to configure network access based on which of the following?

A. Name of the application, identity of the user, and identity of the machine

B. Identity of the machine, username, and certificate

C. Browser-Based Authentication, identity of a user, and network location

D. Network location, identity of a user, and identity of a machine

Correct Answer: D

Implied rules are predefined rules that are automatically added to the Access Control rulebase by the Security Management Server. Implied rules allow the control connections that are essential for the functionality and security of the Check Point products, such as communication between the Security Gateway and the Security Management Server, synchronization between cluster members, logging, VPN, and ICMP. Implied rules are not visible in the SmartConsole, but they can be viewed and modified using the Global Properties window. The references are: Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 12 Check Point R81 Quantum Security Gateway Guide, page 141 Check Point R81 Firewall Administration Guide, page 21

QUESTION 13

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust.

B. The Security Gateway name cannot be changed in command line without re- establishing trust.

C. The Security Management Server name cannot be changed in SmartConsole without re- establishing trust.

D. The Security Management Server IP-address cannot be changed without re-establishing the trust.

Correct Answer: A

After trust has been established between the Check Point components, the Security Gateway IP address cannot be changed without re-establishing the trust. This is because the trust is based on the Secure Internal Communication (SIC) mechanism, which uses certificates to authenticate and encrypt the communication. The certificates are issued by the Internal Certificate Authority (ICA) of the Security Management Server / Domain Management Server, and contain the name and IP address of the component. Therefore, if the IP address of a component is changed, the certificate will become invalid and the trust will be lost. To restore the trust, the certificate must be renewed or reissued by the ICA12. However, there are some exceptions to this rule. The Security Gateway name can be changed in command line without re-establishing trust, as long as the IP address remains the same. This is because the SIC mechanism does not rely on the hostname, but on the IP address and the SIC name (which is usually derived from the hostname, but can be manually changed). The Security Management Server name can be changed in SmartConsole without re-establishing trust, as long as the IP address remains the same. This is because SmartConsole uses a different mechanism to connect to the Security Management Server, which does not depend on the SIC certificate. The Security Management Server IP address can be changed without re-establishing trust, as long as some steps are followed to update the Check Point Registry file on the managed Security Gateways / Cluster Members / VSX Virtual Devices. This is because the Registry file contains the IP address of the ICA, which is used for certificate renewal. If the Registry file is not updated, then the certificate renewal will fail and the trust will be lost3. References: 1: Check Point R81 Security Administration Guide - Check Point Software, page 162 2: Check Point R81 Security Engineering Guide - Check Point Software, page 162 3: How to renew SIC after changing IP Address of Security Management Server - Check Point Software, Solution ID: sk103356

QUESTION 14

You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

A. Check Point Capsule Cloud

B. Sandblast Mobile Protect

C. SecuRemote

D. SmartEvent Client Info

Correct Answer: B

SandBlast Mobile Protect is an application that provides comprehensive protection for mobile devices against cyber threats. SandBlast Mobile Protect is a lightweight app that does not affect the device performance or battery life. It monitors network traffic, device behavior, and installed apps to detect and prevent attacks such as phishing, malware, ransomware, botnets, and man-in-the-middle5. SandBlast Mobile Protect also integrates with Check Point\\'s ThreatCloud intelligence network to provide real- time threat information and updates6. Therefore, the correct answer is B. References: 5: [SandBlast Mobile Protect] 6: [SandBlast Mobile Administration Guide]

QUESTION 15

Connections to the Check Point R81 Web API use what protocol?

A. HTTPS

B. RPC

C. VPN

D. SIC

Correct Answer: A

Connections to the Check Point R81 Web API use the HTTPS protocol. The Web API is a RESTful web service that allows you to perform management tasks on the Security Management Server using HTTP requests. References: Check Point Management APIs