Free Questions for 156-315.81 by certscare

Shared by Shaffer on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You pushed a policy to your gateway and you cannot access the gateway remotely any more. What command should you use to remove the policy from the gateway by logging in through console access?

Options:

A- 'fw cpstop'

B- 'fw unloadlocal'

C- 'fwundo'

D- 'fw unloadpolicy''

Answer:

B

Explanation:

The command that should be used to remove the policy from the gateway by logging in through console access is ''fw unloadlocal''. This command will unload all security policies from a gateway or cluster member and allow all traffic to pass through it. This command can be

useful for troubleshooting purposes or for emergency access to a gateway. Reference: [Check Point R81 CLI Reference Guide]

Question 2

Question Type: MultipleChoice

What are the main stages of a policy installation?

Options:

A- Initiation, Conversion and FWD REXEC

B- Verification, Commit, Installation

C- Initiation, Conversion and Save

D- Verification Compilation, Transfer and Commit

Answer:

D

Explanation:

The main stages of a policy installation are Verification, Compilation, Transfer, and Commit. Verification is the stage where the policy is checked for syntax errors and conflicts. Compilation is the stage where the policy is translated into a binary format that can be executed by the Security Gateway. Transfer is the stage where the policy is sent from the Security Management Server to the Security Gateway.Commit is the stage where the policy is activated on the Security Gateway3. Reference:Check Point R81 Security Management Guide

Question 3

Question Type: MultipleChoice

Using fw monitor you see the following inspection point notion E and i what does that mean?

Options:

A- E shows the packet before the VPN encryption, i after the inbound firewall VM

B- E shows the packet reaching the external interface, i leaving the internal interface

C- E shows the packet after the VPN encryption, i before the inbound firewall VM

D- E shows the packet leaving the external interface, i reaching the internal interface

Answer:

C

Explanation:

Using fw monitor, the inspection point notation E and i means that E shows the packet after the VPN encryption, and i shows the packet before the inbound firewall VM. E (for example, eth4:E) is the Post-Outbound inspection point, which captures packets after they are encrypted by VPN Outbound.i (for example, eth4:i) is the Pre-Inbound inspection point, which captures packets before they are inspected by the in-bound FireWall VM2. Reference:Check Point R81 CLI Reference Guide

Question 4

Question Type: MultipleChoice

From SecureXL perspective, what are the three paths of traffic flow:

Options:

A- Initial Path; Medium Path; Accelerated Path

B- Layer Path; Blade Path; Rule Path

C- Firewall Path; Accelerated Path; Medium Path

D- Firewall Path; Accept Path; Drop Path

Answer:

C

Explanation:

From SecureXL perspective, the three paths of traffic flow are Firewall Path, Accelerated Path, and Medium Path. Firewall Path is the path that handles packets that are not processed by SecureXL and are sent to the Firewall kernel for inspection. Accelerated Path is the path that handles packets that are processed by SecureXL and bypass the Firewall kernel.Medium Path is the path that handles packets that are partially processed by SecureXL and partially by the Firewall kernel1. Reference:Check Point R81 Performance Tuning Administration Guide

Question 5

Question Type: MultipleChoice

Using Web Services to access the API, which Header Name-Value had to be in the HTTP Post request after the login?

Options:

A- X-chkp-sid Session Unique Identifier

B- API-Key

C- user-uid

D- uuid Universally Unique Identifier

Answer:

A

Explanation:

The header name-value that has to be in the HTTP Post request after the login when using Web Services to access the API is X-chkp-sid Session Unique Identifier. This header contains the session ID that is returned by the login command and identifies the session for subsequent API commands. The session ID is valid for a limited time and can be extended by using keepalive or logout commands.
Reference: [Check Point R81 Management API Reference Guide]

Question 6

Question Type: MultipleChoice

What are valid authentication methods for mutual authenticating the VPN gateways?

Options:

A- PKI Certificates and Kerberos Tickets

B- PKI Certificates and DynamicID OTP

C- Pre-Shared Secrets and Kerberos Ticket

D- Pre-shared Secret and PKI Certificates

Answer:

D

Explanation:

The valid authentication methods for mutual authenticating the VPN gateways are Pre-shared Secret and PKI Certificates. Pre-shared Secret is a method that uses a secret key that is known only to the two VPN gateways. PKI Certificates is a method that uses digital certificates that are issued by a trusted Certificate Authority (CA) and contain the public key of each VPN gateway. Both methods ensure

that the VPN gateways can verify each other's identity before establishing a secure VPN tunnel. Reference: [Check Point R81 VPN Administration Guide]

Question 7

Question Type: MultipleChoice

Bob is going to prepare the import of the exported R81.20 management database. Now he wants to verify that the installed tools on the new target security management machine are able to handle the R81.20 release. Which of the following Check Point command is true?

Options:

A- $FWDIR/scripts/migrate_server print_installed_tools -v R77.30

B- $CPDIR/scripts/migrate_server print_installed_tools -v R81.20

C- $FWDIR/scripts/migrate_server print_installed_tools -v R81.20

D- $FWDIR/scripts/migrate_server print_uninstalled_tools -v R81.20

Answer:

C

Explanation:

The correct Check Point command to verify that the installed tools on the new target security management machine are able to handle the R81.20 release is$FWDIR/scripts/migrate_server print_installed_tools -v R81.20. This command will print the list of installed migration tools and their versions, and check if they match the specified version (R81.20 in this case).If the tools are not installed or do not match, the command will print an error message3. Reference:Check Point R81 Installation and Upgrade Guide

Question 8

Question Type: MultipleChoice

Which SmartEvent component is responsible to collect the logs from different Log Servers?

Options:

A- SmartEvent Server

B- SmartEvent Database

C- SmartEvent Collector

D- SmartEvent Correlation Unit

Answer:

D

Explanation:

The SmartEvent component that is responsible to collect the logs from different Log Servers is the SmartEvent Correlation Unit. The SmartEvent Correlation Unit is a daemon that runs on the SmartEvent Server and receives logs from one or more Log Servers.The SmartEvent Correlation Unit analyzes the logs and generates correlated events according to the SmartEvent policy2. Reference:Check Point R81 SmartEvent Administration Guide