CheckPoint 156-315.81 CCSE Practice Questions

Shared by Keith on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The Check Point installation history feature in provides the following:

Options:

A- View install changes and install specific version
B- Policy Installation Date only
C- Policy Installation Date, view install changes and install specific version
D- View install changes

Answer:

C

Explanation:

The Check Point installation history feature provides the following:

Policy Installation Date: The date and time when the policy was installed on the Security Gateway.

View install changes: The ability to view the differences between two policy versions that were installed on the Security Gateway.

Install specific version: The ability to install a specific policy version from the installation history on the Security Gateway3. Reference:Check Point R81 SmartConsole Guide

Question 2

Question Type: MultipleChoice

What is the benefit of ''tw monitor'' over ''tcpdump''?

Options:

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

Explanation:

The benefit of fw monitor over tcpdump is that with fw monitor, you can see the inspection points, which cannot be seen in tcpdump. Inspection points are the locations in the firewall kernel where packets are inspected by the security policy and other software blades. Fw monitor allows you to capture packets at different inspection points and see how they are processed by the firewall. Tcpdump, on the other hand, is a generic packet capture tool that only shows the packets as they enter or leave the network interface. Reference:Check Point Security Expert R81 Course,fw monitor, tcpdump

Question 3

Question Type: MultipleChoice

Alice was asked by Bob to implement the Check Point Mobile Access VPN blade - therefore are some basic configuration steps required - which statement about the configuration steps is true?

Options:

A- 1. Add a rule in the Access Control Policy and install policy
2. Configure Mobile Access parameters in Security Gateway object
3. Enable Mobile Access blade on the Security Gateway object and complete the wizard
4. Connect to the Mobile Access Portal
B- 1. Connect to the Mobile Access Portal
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Configure Mobile Access parameters in Security Gateway object
4. Add a rule in the Access Control Policy and install policy
C- 1. Configure Mobile Access parameters in Security Gateway object
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal
D- 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard
2. Configure Mobile Access parameters in Security Gateway object
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal

Answer:

D

Explanation:

The verified answer is D) 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard 2. Configure Mobile Access parameters in Security Gateway object 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal

The basic configuration steps for the Check Point Mobile Access VPN blade are as follows1:

Enable Mobile Access blade on the Security Gateway object and complete the wizard: This step activates the Mobile Access blade on the selected gateway and guides you through the initial configuration, such as defining the portal name, the certificate, and the authentication methods.

Configure Mobile Access parameters in Security Gateway object: This step allows you to customize the Mobile Access settings, such as defining the supported applications, the access roles, the client settings, and the advanced options.

Add a rule in the Access Control Policy and install policy: This step creates a rule that allows the traffic from the Mobile Access portal to the protected resources and installs the policy on the gateway.

Connect to the Mobile Access Portal: This step verifies that the Mobile Access portal is accessible and functional from a web browser or a mobile device.

The other options are incorrect because they do not follow the correct order or include the necessary steps.

Mobile Access Administration Guide R81 - Check Point Software1

Question 4

Question Type: MultipleChoice

Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n)_____ Server.

Options:

A- SecurID

B- NT domain
C- LDAP
D- SMTP

Answer:

C

Explanation:

The User Directory Software Blade allows you to create user definitions on an LDAP server, such as Active Directory, and use them in your security policy. You can also integrate with other user authentication methods, such as SecurID, RADIUS, or TACACS+, but you cannot create user definitions on those servers.

The references are:

Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 13

Check Point R81 Quantum Security Gateway Guide, page 139

Check Point R81 Identity Awareness Administration Guide, page 9

Question 5

Question Type: MultipleChoice

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

Options:

A- Go to clash-Run cpstop | Run cpstart
B- Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
C- Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
D- Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer:

B

Explanation:

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, the administrator needs to perform some additional tasks for it to function properly.

The tasks that the administrator needs to perform are:

Go to Clish-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway

Go to SmartConsole | Install Security Policy

The first task is to enable and configure CoreXL, which is a performance enhancement feature that allows running multiple instances of the firewall kernel on multiple CPU cores. CoreXL can be enabled and configured via cpconfig, which is a utility that provides a menu-based interface for various system settings. After enabling CoreXL, the administrator needs to reboot the Security Gateway for the changes to take effect.

The second task is to install the security policy on the Security Gateway via SmartConsole, which is a unified graphical user interface for managing Check Point products. Installing the security policy will activate the CoreXL instances and distribute the traffic among them. Reference:R81 Performance Tuning Administration Guide, page 15;R81 Security Management Administration Guide, page 83.

Question 6

Question Type: MultipleChoice

What object type would you use to grant network access to an LDAP user group?

Options:

A- Access Role
B- Group Template
C- SmartDirectory Group
D- User Group

Answer:

A

Question 7

Question Type: MultipleChoice

You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

Options:

A- sim erdos --e 1
B- sim erdos -- m 1
C- sim erdos --v 1
D- sim erdos --x 1

Answer:

A

Explanation:

The command that would be used to enable the Penalty Box feature issim erdos -e 1. Penalty Box is a feature that protects the Security Gateway from DDoS attacks by dropping packets from sources that send excessive traffic. Sim erdos is a command that allows administrators to configure and manage the Penalty Box feature. Sim erdos -e 1 enables the Penalty Box feature on the Security Gateway. The other options are either invalid or perform different functions.

Question 8

Question Type: MultipleChoice

What is required for a site-to-site VPN tunnel that does not use certificates?

Options:

A- Pre-Shared Secret
B- RSA Token
C- Unique Passwords
D- SecurelD

Answer:

A

Explanation:

A pre-shared secret is a secret key that is shared between the two VPN peers before establishing a secure connection. It is used to authenticate the VPN peers and encrypt the VPN traffic. A pre-shared secret is required for a site-to-site VPN tunnel that does not use certificates, because certificates are another way of authenticating the VPN peers using public key cryptography. Without certificates, the VPN peers need to have a common secret key that only they know. Reference:Check Point R81 VPN Administration Guide, page 13

Question 9

Question Type: MultipleChoice

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

Options:

A- show interface eth0 mq
B- ethtool A eth0
C- ifconfig -i eth0 verbose
D- ip show Int eth0

Answer:

B

Explanation:

The command to identify the NIC driver before considering about the employment of the Multi-Queue feature isethtool -i eth0, whereeth0is the name of the network interface.This command displays the information about the driver and firmware version of the NIC, as well as other details such as bus-info and supported features1.The Multi-Queue feature requires a NIC driver that supports multiple transmit and receive queues2.

Question 10

Question Type: MultipleChoice

Which one of the following is true about Threat Extraction?

Options:

A- Always delivers a file to user
B- Works on all MS Office, Executables, and PDF files
C- Can take up to 3 minutes to complete
D- Delivers file only if no threats found

Answer:

A

Explanation:

Threat Extraction is a software blade that always delivers a file to user. Threat Extraction removes or sanitizes the active content from the files and converts them to PDF format, which is safer and more compatible. Threat Extraction can also work together with Threat Emulation to provide both clean and original files to the users. Threat Extraction works on MS Office, PDF, and archive files, but not on executables. Threat Extraction can take up to 3 minutes to complete, depending on the file size and complexity. Reference:Check Point Security Expert R81 Course,Threat Extraction Administration Guide