Free Questions for 156-215.81 by dumpssheet

Shared by Vance on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Fill in the blank: An identity server uses a_____to trust a Terminal Server Identity Agent.

Options:

A- One-time password

B- Shared secret

C- Certificate

D- Token

Answer:

B

Question 2

Question Type: MultipleChoice

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

Options:

A- Since they both are logged in on different interfaces, they will both be able to make changes.

B- When Joe logs in. Bob will be logged out automatically.

C- The database will be locked by Bob and Joe will not be able to make any changes.

D- Bob will receive a prompt that Joe has logged in.

Answer:

A

Explanation:

Since Bob and Joe both have Administrator Roles on their Gaia Platform and they both are logged in on different interfaces, they will both be able to make changes. Gaia allows multiple administrators to log in simultaneously and perform different tasks without locking the database or logging out each other.Reference:Gaia R81.20 Administration Guide, page 18.

Question 3

Question Type: MultipleChoice

Which option in tracking allows you to see the amount of data passed in the connection?

Options:

A- Data

B- Accounting

C- Logs

D- Advanced

Answer:

B

Explanation:

Accounting is the option in tracking that allows you to see the amount of data passed in the connection. Accounting tracks the number of bytes and packets for each connection and generates reports based on the collected data.Reference:Certified Security Administrator (CCSA) R81.20 Course Overview, page 14.

Question 4

Question Type: MultipleChoice

Which of the following is true about Stateful Inspection?

Options:

A- Stateful Inspection tracks state using two tables, one for incoming traffic and one for outgoing traffic

B- Stateful Inspection looks at both the headers of packets, as well as deeply examining their content.

C- Stateful Inspection requires that a server reply to a request, in order to track a connection's state

D- Stateful Inspection requires two rules, one for outgoing traffic and one for incoming traffic.

Answer:

B

Explanation:

Stateful Inspection is true about looking at both the headers of packets, as well as deeply examining their content. Stateful Inspection inspects packets at all layers of the OSI model and maintains information about the state and context of each connection in a state table.Reference:Certified Security Administrator (CCSA) R81.20 Course Overview, page 6.

Question 5

Question Type: MultipleChoice

Which Check Point supported authentication scheme typically requires a user to possess a token?

Options:

A- RADIUS

B- Check Point password

C- TACACS

D- SecurID

Answer:

D

Explanation:

SecurID is a Check Point supported authentication scheme that typically requires a user to possess a token. A token is a physical device that generates a one-time password that changes periodically. The user must enter the password along with their username to authenticate.Reference:Remote Access VPN R81.20 Administration Guide, page 30.

Question 6

Question Type: MultipleChoice

Fill in the blank: A(n)_____rule is created by an administrator and configured to allow or block traffic based on specified criteria.

Options:

A- Inline

B- Explicit

C- Implicit drop

D- Implicit accept

Answer:

B

Explanation:

An explicit rule is created by an administrator and configured to allow or block traffic based on specified criteria. Explicit rules are displayed in the Rule Base and can be modified by the administrator.Reference:Certified Security Administrator (CCSA) R81.20 Course Overview, page 12.

Question 7

Question Type: MultipleChoice

Which Security Blade needs to be enabled in order to sanitize and remove potentially malicious content from files, before those files enter the network?

Options:

A- Threat Emulation

B- Anti-Malware

C- Anti-Virus

D- Threat Extraction

Answer:

D

Explanation:

Threat Extraction is the Security Blade that needs to be enabled in order to sanitize and remove potentially malicious content from files, before those files enter the network. It can strip out active content, embedded objects, and other risky elements from documents and deliver a safe version of the file to the user.Reference:Remote Access VPN R81.20 Administration Guide, page 18.

Question 8

Question Type: MultipleChoice

Fill in the blank: The_____is used to obtain identification and security information about network users.

Options:

A- User index

B- UserCheck

C- User Directory

D- User server

Answer:

C

Explanation:

The User Directory is used to obtain identification and security information about network users. It can be integrated with external user databases such as LDAP, RADIUS, or TACACS+.Reference:Certified Security Administrator (CCSA) R81.20 Course Overview, page 9.

Question 9

Question Type: MultipleChoice

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server?

Options:

A- Display policies and logs on the administrator's workstation.

B- Processing and sending alerts such as SNMP traps and email notifications.

C- Verify and compile Security Policies.

D- Store firewall logs to hard drive storage.

Answer:

A

Explanation:

The Security Management Server does not display policies and logs on the administrator's workstation. That is the function of the SmartConsole, which is a separate component that connects to the Security Management Server.Reference:Certified Security Administrator (CCSA) R81.20 Course Overview, page 4.

Question 10

Question Type: MultipleChoice

You want to set up a VPN tunnel to a external gateway. You had to make sure that the IKE P2 SA will only be established between two subnets and not all subnets defined in the default VPN domain of your gateway.

Options:

A- In the SmartConsole create a dedicated VPN Community for both Gateways. On the Management add the following line to the $FWDIR/conf/user.def.FWI file subnet_for_range_and_peer = {);

B- In the SmartConsole create a dedicated VPN Community for both Gateways. Selecting the local gateway in the Community you can set the VPN Domain to 'User defined' and put in the local network.

C- In the SmartConsole create a dedicated VPN Community for both Gateways. On the Gateway add the following line to the $FWDlR/cont/user.def.FW1 file subnet_for_range_and_peer = { };

D- In the SmartConsole create a dedicated VPN Community for both Gateways. Go to Security Policies / Access Control and create an in-line layer rule with source and destination containing the two networks used for the IKE P2 SA. Put the name of the Community in the VPN column.

Answer:

B

Explanation:

This answer is correct because this is the recommended way to configure a VPN tunnel between two subnets and not all subnets defined in the default VPN domain of your gateway1.By creating a dedicated VPN Community, you can specify the VPN peers and the encryption settings for the VPN tunnel2.By selecting the local gateway in the Community, you can set the VPN Domain to 'User defined' and put in the local network that you want to include in the VPN tunnel1. This way, you can limit the VPN traffic to the subnets that you want and avoid unnecessary encryption and decryption of other traffic.

The other answers are not correct because they are either outdated or incorrect ways to configure a VPN tunnel between two subnets.Answer A and C are outdated methods that involve editing the user.def file, which is not recommended and can cause problems with the VPN configuration3.Answer D is incorrect because creating an in-line layer rule with source and destination containing the two networks used for the IKE P2 SA will not affect the VPN tunnel establishment, but only the access control policy4.The VPN column in the rule is used to specify the VPN direction, not the VPN Community name4.

How to configure a Site-to-Site VPN with a universal tunnel

Site to Site VPN R81 Administration Guide - Check Point Software

How to configure a Site-to-Site VPN with a 3rd-party remote gateway

Access Control Policy R81 Administration Guide - Check Point Software