156-215.81$^{\text{Q\&As}}$

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

QUESTION 1

The default shell of the Gaia CLI is cli.sh. How do you change from the cli.sh shell to the advanced shell to run Linux commands?

A. Execute the command \\'enable\\' in the cli.sh shell

B. Execute the \\'conf t\\' command in the cli.sh shell

C. Execute the command \\'expert\\' in the cli.sh shell

D. Execute the \\'exit\\' command in the cli.sh shell

Correct Answer: C

The default shell of the Gaia CLI is cli.sh, which provides a limited set of commands for basic configuration and troubleshooting. To change from the cli.sh shell to the advanced shell (also known as expert mode) to run Linux commands, the administrator needs to execute the command `expert\\' in the cli.sh shell

QUESTION 2

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

A. During the primary Security Management Server installation process.

B. Upon creation of a certificate

C. When an administrator decides to create one

D. When an administrator initially logs into SmartConsole.

Correct Answer: A

The Internal Certificate Authority (ICA) is created during the primary Security Management Server installation process. The ICA is a component that issues and manages certificates for Check Point products. The ICA is automatically installed and initialized when installing the Security Management Server. References: Check Point R81 Security Management Administration Guide, page 26.

QUESTION 3

How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

A. Involved traffic logs will be forwarded to a log server.

B. Provides log details view email to the Administrator.

C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.

D. Provides additional information to the connected user.

Correct Answer: C

The Accounting tracking option is used to monitor the amount of data that passes through a connection. When this option is enabled on a traffic rule, the involved traffic logs are updated every 10 minutes to show how much data has passed on the connection. This information can be used for billing or auditing purposes. References: Check Point R81 Logging and Monitoring Administration Guide

QUESTION 4

In SmartEvent, a correlation unit (CU) is used to do what?

A. Collect security gateway logs, Index the logs and then compress the logs.

B. Receive firewall and other software blade logs in a region and forward them to the primary log server.

C. Analyze log entries and identify events.

D. Send SAM block rules to the firewalls during a DOS attack.

Correct Answer: C

A correlation unit (CU) is a component of SmartEvent that analyzes log entries on log servers and identifies events based on predefined or custom rules. A CU receives logs from one or more log servers and forwards them to the SmartEvent server, where they are stored in the events database

QUESTION 5

Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

A. Application Control

B. Threat Emulation

C. Logging and Status

D. Monitoring

Correct Answer: D

The Check Point software blade that monitors Check Point devices and provides a picture of network and security performance is Monitoring. The Monitoring Software Blade presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events. It centrally monitors Check Point devices and alerts security administrators to changes to gateways, endpoints, tunnels, remote users and security activities. References: Monitoring Software Blade, Check Point Integrated Security Architecture, Support, Support Requests, Training, Documentation, and Knowledge base for Check Point products and services

QUESTION 6

Identity Awareness lets an administrator easily configure network access and auditing based on three items Choose the correct statement.

A. Network location, the identity of a user and the active directory membership.

B. Network location, the identity of a user and the identity of a machine.

C. Network location, the telephone number of a user and the UID of a machine D. Geographical location, the identity of a user and the identity of a machine

Correct Answer: B

Identity Awareness is a software blade that lets an administrator easily configure network access and auditing based on three items: network location, the identity of a user, and the identity of a machine. These items are used to identify and authenticate users and machines, and to enforce identity-based policies. Network location refers to the IP address or subnet of the source or destination of the traffic. The identity of a user can be obtained from various sources, such as Active Directory, LDAP, or Captive Portal. The identity of a machine can be verified by using Secure Domain Logon or Identity Agent.

QUESTION 7

Which of the following is NOT a component of a Distinguished Name?

A. Common Name

B. Country

C. User container

D. Organizational Unit

Correct Answer: C

A Distinguished Name (DN) is a unique identifier for an entry in an LDAP directory. A DN consists of a sequence of relative distinguished names (RDNs) separated by commas. Each RDN is composed of an attribute type and an attribute value, such as cn=John Smith or ou=Sales. A DN can have different components depending on the structure and schema of the LDAP directory, but some common components are: Common Name (cn), Country? Organizational Unit (ou), Organization (o), State or Province (st), and Locality (l). User container is not a component of a DN. References: Check Point R81 Identity Awareness Administration Guide

QUESTION 8

What is the SOLR database for?

A. Used for full text search and enables powerful matching capabilities

B. Writes data to the database and full text search C. Serves GUI responsible to transfer request to the DLE server

D. Enables powerful matching capabilities and writes data to the database

Correct Answer: A

The SOLR database is used for full text search and enables powerful matching capabilities . SOLR is an open source enterprise search platform that provides fast and scalable indexing and searching of data. It supports advanced features such as faceting, highlighting, spell checking, synonyms, etc. The SOLR database is used by Check Point products such as SmartLog and SmartEvent to store and query logs and events . The other options are incorrect. Option B is false, as SOLR does not write data to the database, but only reads data from it. Option C is false, as SOLR does not serve GUI, but only provides a RESTful API for queries. Option D is false, as SOLR does not enable powerful matching capabilities and write data to the database, but only enables powerful matching capabilities. References: SOLR - Check Point Software, [Apache Solr]

QUESTION 9

What is User Check?

A. Messaging tool user to verify a user\\'s credentials

B. Communication tool used to inform a user about a website or application they are trying to access

C. Administrator tool used to monitor users on their network

D. Communication tool used to notify an administrator when a new user is created

Correct Answer: B

UserCheck is a communication tool used to inform a user about a website or application they are trying to access. UserCheck allows administrators to define actions that require user interaction, such as asking for confirmation, informing about risks, or blocking access, p. 38. UserCheck is not a messaging tool, an administrator tool, or a notification tool. , [Check Point UserCheck Administration Guide R81]

QUESTION 10

In which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to a 2200 Appliance

B. From a 4400 Appliance to an HP Open Server

C. From an IBM Open Server to an HP Open Server

D. From an IBM Open Server to a 2200 Appliance

Correct Answer: A

The scenario where it is a valid option to transfer a license from one hardware device to another is from a 4400 Appliance to a 2200 Appliance. This is because both appliances are Check Point products and have the same license type (Central License). You can transfer a license from one hardware device to another if they have the same license type and vendor. Therefore, the correct answer is A. From a 4400 Appliance to a 2200 Appliance.

QUESTION 11

An administrator can use section titles to more easily navigate between large rule bases.

Which of these statements is FALSE?

A. Section titles are not sent to the gateway side.

B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.

C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.

D. Sectional Titles do not need to be created in the SmartConsole.

Correct Answer: C

The statement that a Sectional Title can be used to disable multiple rules by disabling only the sectional title is false. A Sectional Title is a visual divider that helps organize and navigate large rule bases. It does not affect the rule enforcement order or the rule functionality. Disabling a Sectional Title does not disable the rules under it. To disable multiple rules, you need to select them individually or use Shift+Click or Ctrl+Click to select them in bulk, and then right-click and choose Disable Rule(s). The other statements are true. Section titles are not sent to the gateway side, they are only displayed in SmartConsole. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement. Sectional Titles do not need to be created in SmartConsole, they can also be created using SmartConsole CLI or API commands.References: [Sectional Titles], [SmartConsole CLI Guide], [SmartConsole API Reference Guide]

QUESTION 12

Choose what BEST describes users on Gaia Platform.

A. There are two default users and neither can be deleted.

B. There are two default users and one cannot be deleted.

C. There is one default user that can be deleted.

D. There is one default user that cannot be deleted.

Correct Answer: A

There are two default users on Gaia Platform and neither can be deleted. The two default users are admin and monitor. The admin user has full access to the Gaia configuration and management tools, such as CLI and WebUI. The monitor user has read- only access to the Gaia configuration and management tools, and can only view the system status and settings. These two users cannot be deleted, but their passwords can be changed.References: [Gaia Administration Guide], [Gaia Overview]

QUESTION 13

Which method below is NOT one of the ways to communicate using the Management API\\'s?

A. Typing API commands using the "mgmt_cli" command

B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Typing API commands using Gaia\\'s secure shell (clash)19+

D. Sending API commands over an http connection using web-services

Correct Answer: D

The correct answer is D because sending API commands over an http connection using web-services is not one of the ways to communicate using the Management API\\'s. The Management API\\'s support HTTPS protocol only, not HTTP. The other methods are valid ways to communicate using the Management API\\'s. References: Check Point Learning and Training Frequently Asked Questions (FAQs)

QUESTION 14

What are the two elements of address translation rules?

A. Original packet and translated packet

B. Manipulated packet and original packet

C. Translated packet and untranslated packet

D. Untranslated packet and manipulated packet

Correct Answer: A

Address translation rules are used to map an IP address space into another by modifying network address information in the IP header of packets. Address translation rules have two elements: original packet and translated packet. The original packet is the packet before it undergoes address translation, and the translated packet is the packet after it undergoes address translation. The original packet and the translated packet may have different source and destination IP addresses, depending on the type and direction of address translation.

QUESTION 15

What are two basic rules Check Point recommending for building an effective security policy?

A. Accept Rule and Drop Rule

B. Cleanup Rule and Stealth Rule

C. Explicit Rule and Implied Rule

D. NAT Rule and Reject Rule

Correct Answer: B

Two basic rules that Check Point recommends for building an effective security policy are Cleanup Rule and Stealth Rule. A Cleanup Rule is a rule that is placed at the end of the rule base and drops or logs any traffic that does not match any of the previous rules. A Stealth Rule is a rule that is placed at the top of the rule base and protects the Security Gateway from direct access by unauthorized users. The other options are not basic rules for building a security policy, but rather types or categories of rules.

156-215.81 Study Guide   156-215.81 Exam Questions   156-215.81 Braindumps