156-215.81 Q&As

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

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

https://www.certbus.com/156-215-81.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which type of attack can a firewall NOT prevent?

A. Network Bandwidth Saturation

B. Buffer Overflow

C. SYN Flood

D. SQL Injection

Correct Answer: A

A firewall can NOT prevent a network bandwidth saturation attack, which is a type of denial-of-service (DoS) attack that aims to consume all the available bandwidth of a target network or device, p. 9. A firewall can prevent other types of attacks, such as buffer overflow, SYN flood, and SQL injection, by inspecting packets and applying security rules, p. 11-12.

, 156-315.81 Checkpoint Exam Info and Free Practice Test

QUESTION 2

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

A. Limit

B. Resource

C. Custom Application / Site

D. Network Object

Correct Answer: B

Resource is NOT an objects category in SmartConsole, p. 18. The objects categories in SmartConsole are Network Object, Host, Network, Group, Gateway, Cluster, VPN Community, Service, Time Object, Access Role, Custom Application / Site, Data Center Object, Limit. , [Check Point SmartConsole R81 Help]

QUESTION 3

When configuring LDAP with User Directory integration, changes applied to a User Directory template are:

A. Not reflected for any users unless the local user template is changed.

B. Not reflected for any users who are using that template.

C. Reflected for ail users who are using that template and if the local user template is changed as well.

D. Reflected immediately for all users who are using that template.

Correct Answer: D

LDAP (Lightweight Directory Access Protocol) is a protocol that allows accessing and maintaining distributed directory information services over a network. User Directory integration is a feature of Identity Awareness that allows Check Point products to use LDAP servers as identity sources. When configuring LDAP with User Directory integration, changes applied to a User Directory template are reflected immediately for all users who are using that template. A User Directory template defines the settings for connecting to an LDAP server and retrieving user information3. References: Check Point R81 Identity Awareness Administration Guide

QUESTION 4

When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

A. The URL and server certificate are sent to the Check Point Online Web Service

B. The full URL, including page data, is sent to the Check Point Online Web Service

C. The host part of the URL is sent to the Check Point Online Web Service

D. The URL and IP address are sent to the Check Point Online Web Service

Correct Answer: C

When URL Filtering is set, only the host part of the URL is sent to the Check Point Online Web Service for analysis. The host part is the part of the URL that identifies the web server, such as www.example.com. The Check Point Online Web Service uses this information to categorize the URL and return the appropriate action to the Security Gateway. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data. References:

1: Policy Layers

2: Adding a New Log Server

3: Suspicious Activity Monitoring : [URL Filtering]

QUESTION 5

Fill in the blank RADIUS protocol uses_____to communicate with the gateway

A. UDP

B. CCP

C. TDP

D. HTTP

Correct Answer: A

RADIUS protocol uses UDP (User Datagram Protocol) to communicate with the gateway. UDP is a connectionless protocol that does not require a handshake or acknowledgment before sending or receiving data2. References: [Check Point R81 Identity Awareness Administration Guide], page 14.

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

Identify the ports to which the Client Authentication daemon listens on by default?

A. 259, 900

B. 256, 257

C. 8080, 529

D. 80, 256

Correct Answer: A

The ports to which the Client Authentication daemon listens on by default are 259 and 900. Client Authentication is a method that allows users to authenticate with the Security Gateway before they are allowed access to protected resources. The Client Authentication daemon (fwauthd) runs on the Security Gateway and listens for authentication requests on TCP ports 259 and 900 . References: [Check Point R81 Remote Access VPN Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

QUESTION 8

What are the advantages of a "shared policy" in R80?

A. Allows the administrator to share a policy between all the users identified by the Security Gateway

B. Allows the administrator to share a policy between all the administrators managing the Security Management Server

C. Allows the administrator to share a policy so that it is available to use in another Policy Package

D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Correct Answer: C

A shared policy is a set of rules that can be used in multiple policy packages. It allows the administrator to create a common security policy for different gateways or domains, and avoid duplication and inconsistency. The other options are not advantages of a shared policy. References: [Shared Policies Overview], [Shared Policies Best Practices]

QUESTION 9

Name the authentication method that requires token authenticator.

A. SecureID

B. Radius

C. DynamicID

D. TACACS

Correct Answer: A

SecureID is the authentication method that requires token authenticator. SecureID is a two-factor authentication method that uses a hardware or software token to generate a one-time password. The user must enter the token code along with their username and password to authenticate. References: Check Point R81 Identity Awareness Administration Guide

QUESTION 10

What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync

B. Use 1 dedicated sync interface

C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

D. Use 2 clusters + 1st sync + 2nd sync

Correct Answer: B

The best sync method in the ClusterXL deployment is to use one dedicated sync interface. This method provides optimal performance and reliability for synchronization traffic. Using multiple sync interfaces is not recommended as it increases CPU load and does not provide 100% sync redundancy. Using multiple clusters is not a sync method, but a cluster topology. References: Sync Redundancy in ClusterXL, Best Practice for HA sync interface

QUESTION 11

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 12

One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.

B. AdminA and AdminB are editing the same rule at the same time.

C. AdminB sees a pencil icon next the rule that AdminB is currently editing.

D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Correct Answer: B

One of the major features in R80.x SmartConsole is concurrent administration, which allows multiple administrators to work on the same Security Policy at the same time. However, only one administrator can edit a rule at a time. If AdminA and AdminB are editing the same rule at the same time, it will cause a conflict and prevent them from saving their changes. Therefore, the correct answer is B. AdminA and AdminB are editing the same rule at the same time.

QUESTION 13

What is the purpose of the Stealth Rule?

A. To prevent users from directly connecting to a Security Gateway.

B. To reduce the number of rules in the database.

C. To reduce the amount of logs for performance issues.

D. To hide the gateway from the Internet.

Correct Answer: A

The Stealth Rule is used to prevent users from directly connecting to a Security Gateway. It is usually placed at the top of the rule base, before any other rule that allows traffic to the Security Gateway, p. 32

QUESTION 14

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don\\'t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw ctl multik dynamic_dispatching on

B. fw ctl multik dynamic_dispatching set_mode 9

C. fw ctl multik set_mode 9

D. fw ctl miltik pq enable

Correct Answer: C

To optimize drops, you can use Priority Queues and fully enable Dynamic Dispatcher on the Security Gateway. Priority Queues are a mechanism that prioritizes part of the traffic when the Security Gateway is stressed and needs to drop packets. Dynamic Dispatcher is a feature that dynamically assigns new connections to a CoreXL FW instance based on the utilization of CPU cores. To enable both features, you need to run the command fw ctl multik set_mode 9 on the Security Gateway. Therefore, the correct answer is C. fw ctl multik set_mode 9. References: CoreXL Dynamic Dispatcher - Check Point Software, Firewall Priority Queues in R80.x / R81.x - Check Point Software, Separate Config for Dynamic Dispatcher and Priority Queues

QUESTION 15

Check Point licenses come in two forms. What are those forms?

A. Central and Local.

B. Access Control and Threat Prevention.

C. On-premise and Public Cloud.

D. Security Gateway and Security Management.

Correct Answer: A

Check Point licenses come in two forms: central and local. Central licenses are attached to the Security Management Server and are distributed to managed Security Gateways. Local licenses are attached directly to a specific Security Gateway.