Free Questions for 156-215.81 by certsdeals

Shared by Jones on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

DLP and Geo Policy are examples of what type of Policy?

Options:

A- Inspection Policies

B- Shared Policies

C- Unified Policies

D- Standard Policies

Answer:

B

Explanation:

DLP and Geo Policy are examples ofShared Policies. Shared Policies are policies that can be shared with other policy packages to save time and effort when managing multiple gateways with similar security requirements. Shared Policies can be applied to Access Control, Threat Prevention, and HTTPS Inspection layers. Other types of policies include Inspection Policies, Unified Policies, and Standard

Policies. Reference: [Check Point R81 Security Management Administration Guide], [Check Point R81 SmartConsole R81 Resolved Issues]

Question 2

Question Type: **MultipleChoice**

Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

Options:

A- IPS blade

B- IPSEC VPN Blade

C- Identity Awareness Blade

D- Firewall Blade

Answer:

A

Explanation:

The following is considered a "Subscription Blade", requiring renewal every 1-3 years:IPS blade4. The IPS blade is a software blade that provides protection against network attacks and exploits by inspecting traffic and blocking malicious packets. The IPS blade requires a subscription license that includes updates for the IPS signatures and Geo Protection database. Other subscription blades include Anti-Bot, Anti-Virus, URL Filtering, Application Control, Threat Emulation, and Threat Extraction. Reference:Check Point Licensing and Contract Operations User Guide

Question 3

Question Type: MultipleChoice

Which default Gaia user has full read/write access?

Options:

A- admin

B- superuser

C- monitor

D- altuser

Answer:

A

Explanation:

The default Gaia user that has full read/write access isadmin3. The admin user is the superuser that can perform any administrative task on the Gaia system, such as configuring network settings, installing software updates, managing licenses, creating snapshots, and more. The admin user can also access the Gaia Portal, which is a web-based interface for managing Gaia settings and features.
Reference:Check Point R81 Gaia Administration Guide

Question 4

Question Type: MultipleChoice

Which is a main component of the Check Point security management architecture?

Options:

A- Identity Collector

B- Endpoint VPN client

C- SmartConsole

D- Proxy Server

Answer:

C

Explanation:

A main component of the Check Point security management architecture isSmartConsole2. SmartConsole is a unified graphical user interface that allows administrators to manage multiple security functions such as firewall, VPN, IPS, application control, URL filtering, identity awareness, and more. SmartConsole connects to the Security Management Server and interacts with other Check Point components such as Security Gateways and Endpoint Security Servers. Reference:Check Point R81 Security Management Administration Guide

Question 5

Question Type: MultipleChoice

When using Automatic Hide NAT, what is enabled by default?

Options:

A- Source Port Address Translation (PAT)

B- Static NAT

C- Static Route

D- HTTPS Inspection

Answer:

A

Explanation:

When using Automatic Hide NAT,Source Port Address Translation (PAT)is enabled by default1. This means that the source IP address and port number are translated to a different IP address and port number. This allows multiple hosts to share a single IP address for outbound connections. Reference:Check Point R81 Firewall Administration Guide

Question 6

Question Type: MultipleChoice

Which of the following cannot be configured in an Access Role Object?

Options:

A- Networks

B- Users

C- Time

D- Machines

Answer:

C

Explanation:

The following cannot be configured in an Access Role Object:Time4.An Access Role Object is a way to define a group of users based on four criteria: Networks, Users, Machines, and Locations5. Networks are IP addresses or network objects that represent the source or destination of the traffic. Users are user accounts or user groups from an identity source such as LDAP or RADIUS. Machines are endpoints that are identified by MAC addresses or certificates. Locations are geographical regions based on IP addresses.

Reference:Check Point R81 Firewall Administration Guide,Check Point R81 Identity Awareness Administration Guide

Question 7

Question Type: MultipleChoice

What is the default tracking option of a rule?

Options:

A- Tracking

B- Log

C- None

D- Alert

Answer:

B

Explanation:

The default tracking option of a rule isLog3. This means that the Security Gateway will generate a log entry for every connection that matches the rule. The log entry will contain information such as source, destination, service, action, and time. Other tracking options include None, Alert, Mail, SNMP Trap, User Alert, and Accounting. Reference:Check Point R81 Firewall Administration Guide

Question 8

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- LDAP

C- NT domain

D- SMTP

Answer:

B

Explanation:

With the User Directory Software Blade, you can create user definitions on a(n)LDAPServer2. LDAP stands for Lightweight Directory Access Protocol and is a protocol for accessing and managing user information stored in a directory service. The User Directory Software Blade enables integration with LDAP servers such as Microsoft Active Directory, Novell eDirectory, and OpenLDAP.
Reference:Check Point R81 Identity Awareness Administration Guide