

Checkpoint.156-215.81.vJun-2024.by.Antony.203q

Number: 156-215.81
Passing Score: 800
Time Limit: 120
File Version: 12.0

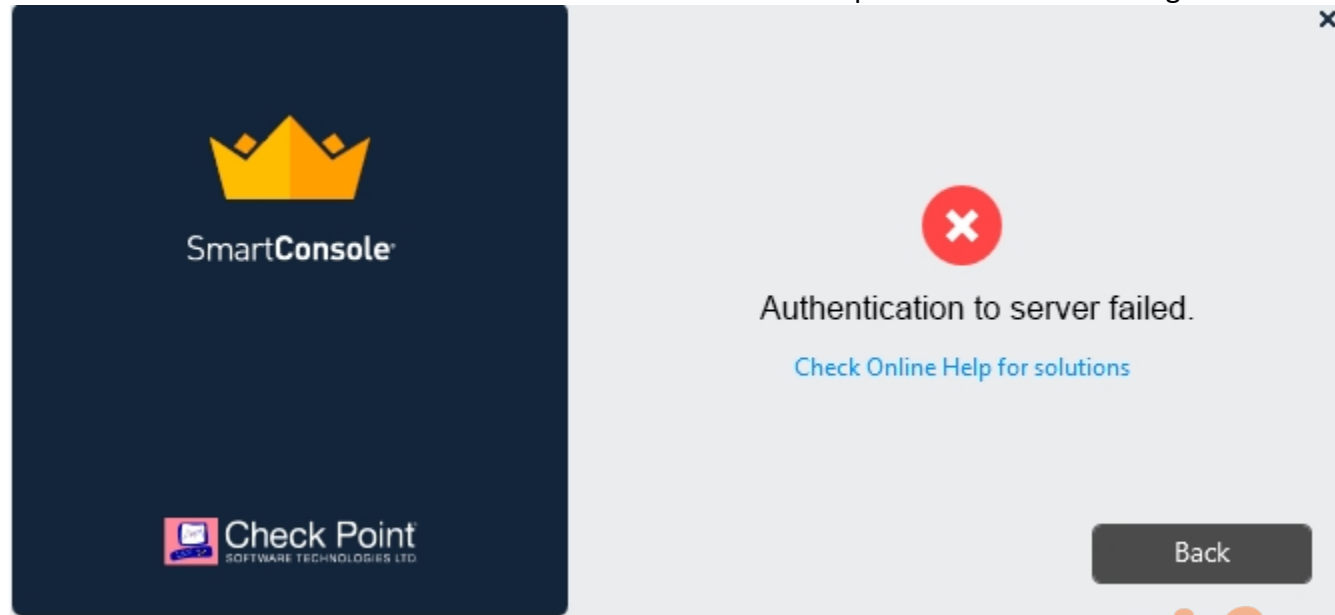
Exam Code: 156-215.81
Exam Name: Check Point Certified Security Administrator R81



Exam A

QUESTION 1

Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



What is the most likely reason?

- A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole. Check that the correct key details are used.
- B. Check Point Management software authentication details are not automatically the same as the Operating System authentication details. Check that she is using the correct details.
- C. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
- D. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Correct Answer: B

Section:

Explanation:

The most likely reason for Vanessa's authentication failure is that she is using the wrong details for SmartConsole. Check Point Management software authentication details are not automatically the same as the Operating System authentication details. She needs to use the credentials that were defined during the initial configuration of the Security Management Server, or the ones that were assigned to her by the administrator. The other options are not valid reasons for this error.

Reference: SmartConsole Login, Check Point CCSA - R81: Practice Test & Explanation

QUESTION 2

What is the most complete definition of the difference between the Install Policy button on the SmartConsole's tab, and the Install Policy within a specific policy?

- A. The Global one also saves and publishes the session before installation.
- B. The Global one can install multiple selected policies at the same time.
- C. The local one does not install the Anti-Malware policy along with the Network policy.
- D. The second one pre-selects the installation for only the current policy and for the applicable gateways.

Correct Answer: D

Section:

Explanation:

The difference between the Install Policy button on the SmartConsole's tab and the Install Policy within a specific policy is that the former installs all the policies that are selected in the Install Policy window, while the latter pre-selects the installation for only the current policy and for the applicable gateways. The other options are not accurate differences.

Reference: Installing Policies, [Check Point CCSA - R81: Practice Test & Explanation]

QUESTION 3

Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

- A. Both License (.lic) and Contract (.xml) files
- B. cp.macro
- C. Contract file (.xml)
- D. license File (.lie)

Correct Answer: B

Section:

Explanation:

The file that is an electronically signed file used by Check Point to translate the features in the license into a code is cp.macro. This file contains a list of macros that define the license features and their values. It is located in the \$FWDIR/conf directory on the Security Management Server or Security Gateway.

Reference: [Check Point R81 Licensing Guide], [Check Point R80.40 Licensing Guide]

QUESTION 4

Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____.

- A. User Center
- B. User Administration
- C. User Directory
- D. UserCheck



Correct Answer: C

Section:

Explanation:

When LDAP is integrated with Check Point Security Management, it is then referred to as User Directory. User Directory is a feature that allows you to import users and groups from an external LDAP server and use them in your security policies. User Center, User Administration, and UserCheck are different features that are not related to LDAP integration.

Reference: [User Directory], [LDAP Integration]

QUESTION 5

Can you use the same layer in multiple policies or rulebases?

- A. Yes - a layer can be shared with multiple policies and rules.
- B. No - each layer must be unique.
- C. No - layers cannot be shared or reused, but an identical one can be created.
- D. Yes - but it must be copied and pasted with a different name.

Correct Answer: A

Section:

Explanation:

You can use the same layer in multiple policies or rulebases. A layer is a set of rules that can be shared, reused, or inherited by different policies. This allows you to create modular and flexible security policies that can be applied to different scenarios.

Reference: [Layers], [Policy Layers and Sub-Policies]

QUESTION 6

Security Gateway software blades must be attached to what?

- A. Security Gateway
- B. Security Gateway container
- C. Management server
- D. Management container

Correct Answer: B

Section:

Explanation:

Security Gateway software blades must be attached to a Security Gateway container. A Security Gateway container is a logical object that represents a physical or virtual machine that runs the Security Gateway software. A software blade is a modular security feature that can be enabled or disabled away container. A software blade can provide functions such as firewall, VPN, IPS, anti-virus, anti-bot, application control, URL filtering, etc.

Reference: [Security Gateway Containers], [Software Blades]

QUESTION 7

Which tool allows you to monitor the top bandwidth on smart console?

- A. Logs & Monitoring
- B. Smart Event
- C. Gateways & Servers Tab
- D. SmartView Monitor

Correct Answer: D

Section:

Explanation:

SmartView Monitor is the tool that allows you to monitor the top bandwidth on SmartConsole. SmartView Monitor is a graphical tool that displays real-time network and security performance data, such as traffic, throughput, connections, CPU usage, memory usage, etc. You can use SmartView Monitor to identify the top bandwidth consumers and optimize your network performance.

Reference: [SmartView Monitor], [Monitoring Network Traffic]

QUESTION 8

A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

- A. The zone is based on the network topology and determined according to where the interface leads to.
- B. Security Zones are not supported by Check Point firewalls.
- C. The firewall rule can be configured to include one or more subnets in a zone.
- D. The local directly connected subnet defined by the subnet IP and subnet mask.

Correct Answer: A

Section:

Explanation:

A security zone is a group of one or more network interfaces from different centrally managed gateways that have the same security requirements. The zone is based on the network topology and determined according to where the interface leads to. For example, a zone can be defined as internal, external, DMZ, VPN, etc. Security zones are supported by Check Point firewalls and can be used to simplify security policies and network segmentation. The firewall rule can be configured to include one or more zones as source or destination objects. The local directly connected subnet defined by the subnet IP and subnet mask is not considered part of the zone, but rather a property of the interface.

Reference: [Security Zones], [Security Zones Best Practices]



QUESTION 9

Which of the following is used to initially create trust between a Gateway and Security Management Server?

- A. Internal Certificate Authority
- B. Token
- C. One-time Password
- D. Certificate

Correct Answer: C

Section:

Explanation:

A one-time password is used to initially create trust between a Gateway and Security Management Server. The administrator generates a one-time password from SmartConsole and enters it on the gateway command line interface using the cpconfig command. This establishes a Secure Internal Communication (SIC) between the gateway and the server. The other options are not used for this purpose.

Reference: [Configuring Secure Internal Communication (SIC)], [Check Point CCSA - R81: Practice Test & Explanation]

QUESTION 10

John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

- A. Logout of the session
- B. File > Save
- C. Install database
- D. Publish the session

Correct Answer: D

Section:

Explanation:

To make John's changes available to other administrators, and to save the database before installing a policy, John must publish the session. Publishing the session saves the changes to the database and makes them visible to other administrators. The other options do not achieve this goal.

Reference: Publishing a Session

QUESTION 11

Fill in the blanks: There are _____ types of software containers _____.

- A. Three; security management, Security Gateway, and endpoint security
- B. Three; Security gateway, endpoint security, and gateway management
- C. Two; security management and endpoint security
- D. Two; endpoint security and Security Gateway

Correct Answer: A

Section:

Explanation:

There are three types of software containers: security management, Security Gateway, and endpoint security. A software container is a set of software blades that provide specific functionality. A security management container manages the security policy and configuration for one or more Security Gateways. A Security Gateway container enforces the security policy on the network traffic. An endpoint security container protects the data and network access of an endpoint device. The other options are not valid types of software containers.

Reference: Software Containers

QUESTION 12



Fill in the blank: In Office mode, a Security Gateway assigns a remote client to an IP address once_____.

- A. the user connects and authenticates
- B. office mode is initiated
- C. the user requests a connection
- D. the user connects

Correct Answer: A

Section:

Explanation:

In Office mode, a Security Gateway assigns a remote client to an IP address once the user connects and authenticates. Office mode allows a remote client to get an IP address from the internal network of the organization. The IP address is assigned during the IKE negotiation, after the user has successfully authenticated with the Security Gateway³. The other options are not correct timings for assigning an IP address in Office mode.

Reference:Office Mode

QUESTION 13

Which Identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

- A. AD Query
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

Correct Answer: C

Section:

Explanation:

Endpoint Identity Agent and Browser-Based Authentication are the identity sources that provide the highest level of security for sensitive servers, as they require user authentication and can enforce granular access rules based on user identity. AD Query, Terminal Servers Endpoint Identity Agent, and RADIUS and Account Logon are less secure, as they rely on passive methods of identity acquisition or do not support identity-based access control¹².

QUESTION 14

Which statement describes what Identity Sharing is in Identity Awareness?

- A. Management servers can acquire and share identities with Security Gateways
- B. Users can share identities with other users
- C. Security Gateways can acquire and share identities with other Security Gateways
- D. Administrators can share identities with other administrators

Correct Answer: C

Section:

Explanation:

Identity Sharing is a feature that allows Security Gateways to acquire and share identities with other Security Gateways, enabling identity-based access control across different network segments or domains¹³. Management servers, users, and administrators do not share identities with Security Gateways.

QUESTION 15

Fill in the blank: In order to install a license, it must first be added to the _____.

- A. User Center



- B. Package repository
- C. Download Center Web site
- D. License and Contract repository

Correct Answer: D

Section:

Explanation:

In order to install a license, it must first be added to the License and Contract repository. The License and Contract repository is a centralized database that stores all the licenses and contracts for Check Point products. It allows you to manage, activate, and attach licenses to your Check Point products.

QUESTION 16

What are the three deployment considerations for a secure network?

- A. Distributed, Bridge Mode, and Remote
- B. Bridge Mode, Remote, and Standalone
- C. Remote, Standalone, and Distributed
- D. Standalone, Distributed, and Bridge Mode

Correct Answer: C

Section:

Explanation:

The three deployment considerations for a secure network are Remote, Standalone, and Distributed³. Remote deployment means that the Security Management Server and Security Gateway are installed on different machines. Standalone deployment means that the Security Management Server and Security Gateway are installed on the same machine. Distributed deployment means that there are multiple Security Gateways managed by one or more Security Management Servers³. Therefore, the correct answer is C. Remote, Standalone, and Distributed.

QUESTION 17

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

- A. All Connections (Clear or Encrypted)
- B. Accept all encrypted traffic
- C. Specific VPN Communities
- D. All Site-to-Site VPN Communities

Correct Answer: C

Section:

Explanation:

The option that allows traffic to VPN gateways in specific VPN communities is Specific VPN Communities⁴. This option enables you to define which VPN communities are allowed in the rule. All Connections (Clear or Encrypted) allows traffic to any destination, regardless of whether it is encrypted or not. Accept all encrypted traffic allows traffic to any encrypted destination, regardless of the VPN community. All Site-to-Site VPN Communities allows traffic to any site-to-site VPN gateway, regardless of the VPN community⁴. Therefore, the correct answer is C. Specific VPN Communities.

QUESTION 18

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge

Correct Answer: A

Section:

Explanation:

When a Security Gateway sends its logs to an IP address other than its own, it means that the Security Gateway and the Log Server are installed on different machines. This is a characteristic of a Distributed deployment. Therefore, the correct answer is A.

QUESTION 19

One of the 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 to the rule that AdminB is currently editing.
- D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Correct Answer: B

Section:

Explanation:

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 20

When should you generate new licenses?

- A. Before installing contract files.
- B. After an RMA procedure when the MAC address or serial number of the appliance changes.
- C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
- D. Only when the license is upgraded.

Correct Answer: C

Section:

Explanation:

You should generate new licenses when the existing license expires, license is upgraded or the IP-address where the license is tied changes. These scenarios require a new license to be generated and activated on the Security Gateway or Management Server. Therefore, the correct answer is C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.

QUESTION 21

Fill in the blank: When a policy package is installed, _____ are also distributed to the target installation Security Gateways.

- A. User and objects databases
- B. Network databases
- C. SmartConsole databases
- D. User databases

Correct Answer: A

Section:

Explanation:

When a policy package is installed, user and objects databases are also distributed to the target installation Security Gateways. The user and objects databases contain information about network objects, users, groups, services, VPN domains, and more. Therefore, the correct answer is A. User and objects databases.

QUESTION 22

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

- A. Remote Access
- B. Cloud IdP (Identity Provider)
- C. Active Directory Query
- D. RADIUS

Correct Answer: B

Section:

Explanation:

Identity Awareness uses several methods for acquiring identity, such as Active Directory Query, Identity Agent, Browser-Based Authentication, Terminal Servers, Captive Portal, and RADIUS¹². Cloud IdP (Identity Provider) is not a method used by Identity Awareness¹². Therefore, the correct answer is B. Cloud IdP (Identity Provider).

QUESTION 23

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Correct Answer: D

Section:

Explanation:

The Check Point software blade that provides Application Security and identity control is Application Control³. Application Control enables network administrators to identify, allow, block, or limit usage of thousands of applications and millions of websites³. Therefore, the correct answer is D. Application Control

QUESTION 24

How are the backups stored in Check Point appliances?

- A. Saved as *.tar under /var/log/CPbackup/backups
- B. Saved as *.tgz under /var/CPbackup
- C. Saved as *.tar under /var/CPbackup
- D. Saved as *.tgz under /var/log/CPbackup/backups

Correct Answer: B

Section:

Explanation:

The backups are stored in Check Point appliances as *.tgz files under /var/CPbackup. This is the default location for backup files created by the backup command. Therefore, the correct answer is B. Saved as *.tgz under /var/CPbackup

QUESTION 25

You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

- A. backup
- B. logswitch



- C. Database Revision
- D. snapshot

Correct Answer: D

Section:

Explanation:

The back up solution that should be used to ensure your database can be restored on that device is snapshot . A snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system. A snapshot can be used to restore a Security Gateway or Security Management Server to its previous state at any time . Therefore, the correct answer is D. snapshot.

QUESTION 26

Fill in the blank: The position of an implied rule is manipulated in the _____ window.

- A. NAT
- B. Firewall
- C. Global Properties
- D. Object Explorer

Correct Answer: C

Section:

Explanation:

The position of an implied rule is manipulated in the Global Properties window. Implied rules are predefined rules that are not displayed in the rule base. They allow or block traffic for essential services such as communication with Check Point servers, logging, and VPN traffic. The position of an implied rule can be changed in the Global Properties > Firewall > Implied Rules section.

Reference: How to view Implied Rules in R80.x / R81.x SmartConsole, Implied Rules

QUESTION 27

How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

- A. By impersonating the administrator with the 'Login as...' option
- B. They cannot be seen
- C. From the SmartView Tracker audit log
- D. From Manage and Settings > Sessions, right click on the session and click 'View Changes...'

Correct Answer: D

Section:

Explanation:

The changes made by an administrator before publishing the session can be seen by a superuser administrator from Manage and Settings > Sessions, right click on the session and click 'View Changes...'. This option allows the superuser to review the changes made by another administrator in a pending session.

Reference: Check Point R81 Security Management Administration Guide

QUESTION 28

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

Section:

Explanation:

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 activities²³⁴.

Reference: Monitoring Software Blade, Check Point Integrated Security Architecture, Support, Support Requests, Training, Documentation, and Knowledge base for Check Point products and services

QUESTION 29

Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

- A. 1. Define an accept rule in Security Policy. 2. Define Security Gateway to hide all internal networks behind the gateway's external IP. 3. Publish and install the policy.
- B. 1. Define an accept rule in Security Policy. 2. Define automatic NAT for each network to NAT the networks behind a public IP. 3. Publish the policy.
- C. 1. Define an accept rule in Security Policy. 2. Define automatic NAT for each network to NAT the networks behind a public IP. 3. Publish and install the policy.
- D. 1. Define an accept rule in Security Policy. 2. Define Security Gateway to hide all internal networks behind the gateway's external IP. 3. Publish the policy.

Correct Answer: C

Section:

Explanation:

The steps you will need to do in SmartConsole in order to get the connection working behind the Internet Security Gateway are:

Define an accept rule in Security Policy. This rule allows the traffic from your internal networks to pass through the Security Gateway.

Define automatic NAT for each network to NAT the networks behind a public IP. This option translates the private IP addresses of your internal networks to a public IP address assigned by your ISP router. This way, your internal networks can communicate with the Internet using a valid IP address.

Publish and install the policy. This step applies the changes you made to the Security Gateway and activates the security and NAT rules.

QUESTION 30

True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

- A. False, log servers are configured on the Log Server General Properties
- B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
- C. True, all Security Gateways forward logs automatically to the Security Management Server
- D. False, log servers are enabled on the Security Gateway General Properties

Correct Answer: B

Section:

Explanation:

The destination server for Security Gateway logs depends on a Security Management Server configuration. This is true because the Security Management Server defines the log servers that receive logs from the Security Gateways. The log servers can be either the Security Management Server itself or a dedicated Log Server¹².

Reference: Check Point R81 Logging and Monitoring Administration Guide, Check Point R81 Quantum Security Gateway Guide

QUESTION 31

Consider the Global Properties following settings:

Global Properties



- + FireWall-1
 - NAT - Network Address
 - Authentication
- + VPN
 - Identity Awareness
 - UTM-1-Edge Gatew
- + Remote Access
 - User Directory
 - QoS
 - User Authority
 - User Accounts
 - ConnectControl
 - Stateful Inspection
- + Log and Alert
- OPSEC
- Security Managemer
- Non Unique IP Addr
- Proxy
- IPS
- UserCheck
- Hit Count
- Advanced

Select the following properties and choose the position of the rules in the Rule Base:

- Accept control connections:
- Accept Remote Access control connections:
- Accept Smart Update connections:
- Accept IPS-1 management connections:
- Accept outgoing packets originating from Gateway:
- Accept outgoing packets originating from Connections gateway:
- Accept RIP:
- Accept Domain Name over UDP (Queries):
- Accept Domain Name over TCP (Zone Transfer):
- Accept ICMP requests:
- Accept Web and SSH connections for Gateway's administration (Small Office Appliance):
- Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance):
- Accept Dynamic Address modules' outgoing Internet connections:
- Accept VRRP packets originating from cluster members (VSX IPSO VRRP):
- Accept Identity Awareness control connections:

Track _____

Log Implied Rules

The selected option "Accept Domain Name over UDP (Queries)" means:

- A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
- B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
- C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
- D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Correct Answer: A

Section:

Explanation:

The selected option "Accept Domain Name over UDP (Queries)" means that UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy. This option enables the Security Gateway to accept DNS queries from external hosts and forward them to internal DNS servers. The queries are accepted by an implied rule that is applied before the explicit rules in the Security Policy. The implied rule only allows queries from interfaces that have external anti-spoofing groups defined .

Reference: Check Point R81 Quantum Security Gateway Guide, Implied Rules

QUESTION 32

How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

Correct Answer: B

Section:

Explanation:

The communication between different Check Point components is secured in R80 by using SIC. SIC stands for Secure Internal Communication and it is a mechanism that ensures the authenticity and confidentiality of communication between Check Point components, such as Security Gateways, Security Management Servers, Log Servers, etc. SIC uses certificates issued by the Internal CA (ICA) and encryption algorithms such as AES-25634.

Reference: Check Point R81 Quantum Security Gateway Guide, Check Point R81 Quantum Security Management Administration Guide

QUESTION 33

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

Section:

Explanation:

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 .

Reference: [Check Point R81 Remote Access VPN Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

QUESTION 34

What is the purpose of the CPCA process?



- A. Monitoring the status of processes
- B. Sending and receiving logs
- C. Communication between GUI clients and the SmartCenter server
- D. Generating and modifying certificates

Correct Answer: D

Section:

Explanation:

The purpose of the CPCA process is generating and modifying certificates. CPCA stands for Check Point Certificate Authority and it is a process that runs on the Security Management Server or Log Server. It is responsible for creating and managing certificates for internal communication between Check Point components, such as SIC .

Reference: [Check Point R81 Quantum Security Management Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

QUESTION 35

The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

- A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
- B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and assign role to the user.
- C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
- D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.

Correct Answer: A

Section:

Explanation:

To achieve the requirement of giving the Network Operations Center administrator access to Check Point Security devices mostly for troubleshooting purposes, but not to the expert mode, and still allowing her to run tcpdump, you need to:

Add tcpdump to CLISH using add command. This command adds a new command to the Command Line Interface Shell (CLISH) that allows running tcpdump without entering the expert mode .

Create a new access role. This option defines a set of permissions and commands that can be assigned to a user or a group of users.

Add tcpdump to the role. This option grants the permission to run tcpdump to the role.

Create new user with any UID and assign role to the user. This option creates a new user account with any User ID (UID) and assigns the role that has tcpdump permission to the user.

QUESTION 36

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

- A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
- B. Windows registry is available for future Security Management Server authentications.
- C. There is no memory used for saving a fingerprint anyway.
- D. SmartConsole cache is available for future Security Management Server authentications.

Correct Answer: D

Section:

Explanation:

When logging in for the first time to a Security Management Server through SmartConsole, a fingerprint is saved to the SmartConsole cache and is available for future Security Management Server authentications. The fingerprint is a unique identifier of the Security Management Server that is used to verify its identity and prevent man-in-the-middle attacks. The SmartConsole cache is a local folder on the client machine that stores temporary files and settings.

QUESTION 37

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

- A. SHA-256
- B. SHA-200
- C. MD5
- D. SHA-128

Correct Answer: A

Section:

Explanation:

By default, the SIC certificates issued by R80 Management Server are based on the SHA-256 algorithm¹. SHA-256 is a secure hash algorithm that produces a 256-bit digest. SHA-200, MD5, and SHA-128 are not valid algorithms for SIC certificates.

Reference:SHA-1 and SHA-256 certificates in Check Point Internal CA (ICA)

QUESTION 38

Which message indicates IKE Phase 2 has completed successfully?

- A. Quick Mode Complete
- B. Aggressive Mode Complete
- C. Main Mode Complete
- D. IKE Mode Complete

Correct Answer: A

Section:

Explanation:

Quick Mode Complete is the message that indicates IKE Phase 2 has completed successfully². IKE Phase 2 is also known as Quick Mode or Child SA in IKEv1 and IKEv2 respectively. Aggressive Mode and Main Mode are part of IKE Phase 1, which establishes the IKE SA. IKE Mode is not a valid term for IKE negotiation.

Reference:How to Analyze IKE Phase 2 VPN Status Messages,IKEv2 Phase 1 (IKE SA) and Phase 2 (Child SA) Message Exchanges,Understand IPsec IKEv1 Protocol

QUESTION 39

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

| No. | Name | Source | Destination | VPN | Services & Applications | Action | Track | Install On |
|-----|---|---------------|-------------------|-------|-------------------------|--------|--------|------------------|
| 1 | NetBIOS Noise | * Any | * Any | * Any | NBT | Drop | - None | * Policy Targets |
| 2 | Management | Net_10.28.0.0 | GW-R7730 | * Any | https ssh | Accept | Log | * Policy Targets |
| 3 | Stealth | * Any | GW-R7730 | * Any | * Any | Drop | Log | * Policy Targets |
| 4 |  DNS | Net_10.28.0.0 | * Any | * Any | * Any | Accept | Log | * Policy Targets |
| 5 | Web | Net_10.28.0.0 | * Any | * Any | http https | Accept | Log | * Policy Targets |
| 6 | DMZ Access | Net_10.28.0.0 | DMZ_Net_192.0.2.0 | * Any | ftp | Accept | Log | * Policy Targets |
| 7 | Cleanup rule | * Any | * Any | * Any | * Any | Drop | Log | * Policy Targets |

What is the possible explanation for this?

- A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
- B. Another administrator is logged into the Management and currently editing the DNS Rule.
- C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Correct Answer: B

Section:

Explanation:

The padlock sign next to the DNS rule in the Rule Base indicates that another administrator is logged into the Management and currently editing the DNS Rule¹. This is a feature of R80 that allows multiple administrators to work on the same policy simultaneously. The padlock sign prevents other administrators from modifying the same rule until the editing administrator publishes or discards the changes². The other options are not valid explanations for the padlock sign.

Reference: 156-215.80 : Check Point Certified Security Administrator (CCSA R80) : Part 19, Multi-User Policy Editing

QUESTION 40

Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

- A. Down
- B. No Response
- C. Inactive
- D. Failed

Correct Answer: A

Section:

Explanation:

When tunnel test packets no longer invoke a response, SmartView Monitor displays Down for the given VPN tunnel¹. This means that the VPN tunnel is not operational and there is no IKE or IPsec traffic passing through it. No Response, Inactive, and Failed are not valid statuses for VPN tunnels in SmartView Monitor.

Reference: Smart View Monitor displays status for all S2S VPN tunnels - Phase1 UP



QUESTION 41

Which is a suitable command to check whether Drop Templates are activated or not?

- A. fw ctl get int activate_drop_templates
- B. fwaccel stat
- C. fwaccel stats
- D. fw ctl templates --d

Correct Answer: B

Section:

Explanation:

The command fwaccel stat shows the status of SecureXL, including whether Drop Templates are enabled or not¹.

Reference: Check Point SecureXL R81 Administration Guide

QUESTION 42

Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAIa management CLI?

- A. hostname myHost12 ip-address 10.50.23.90
- B. mgmt add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt add host name emailserver1 ip-address 10.50.23.90

Correct Answer: D

Section:

Explanation:

The correct syntax for adding a host using GAiA management CLI is `isgmt add host name <name> ip-address <ip-address>2`.

Reference:Check Point GAiA R81 Command Line Interface Reference Guide

QUESTION 43

The CDT utility supports which of the following?

- A. Major version upgrades to R77.30
- B. Only Jumbo HFA's and hotfixes
- C. Only major version upgrades to R80.10
- D. All upgrades

Correct Answer: D

Section:

Explanation:

The CDT utility supports all upgrades, including major version upgrades, Jumbo HFA's, and hotfixes3.

Reference:Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent

QUESTION 44

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL



Correct Answer: A

Section:

Explanation:

The Sticky Decision Function (SDF) can only be changed for Load Sharing implementations, not for High Availability implementations4.

Reference:Check Point ClusterXL R81 Administration Guide

QUESTION 45

What command would show the API server status?

- A. `cpm status`
- B. `api restart`
- C. `api status`
- D. `show api status`

Correct Answer: D

Section:

Explanation:

The command `api status` shows the API server status, including whether it is enabled or not, the port number, and the API version1.

Reference:Check Point R81 API Reference Guide

QUESTION 46

How Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications
- B. Capsule Workspace can provide access to any application
- C. Capsule Connect provides Business data isolation
- D. Capsule Connect does not require an installed application at client

Correct Answer: A

Section:

Explanation:

Capsule Connect provides a Layer 3 VPN that allows users to access corporate resources securely from their mobile devices². Capsule Workspace provides a secure container on the mobile device that isolates business data and applications from personal data and applications³. Capsule Workspace also provides a desktop with usable applications such as email, calendar, contacts, documents, and web applications³.

Reference: Check Point Capsule Connect, Check Point Capsule Workspace

QUESTION 47

Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- C. Time object to a rule to make the rule active only during specified times.
- D. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Correct Answer: D

Section:

Explanation:

Sub Policies are a new feature in R80.10 Gateway that allow creating and attaching sets of rules to specific rules in the main policy⁴. Sub Policies are useful for delegating permissions, managing large rule bases, and applying different inspection profiles⁴. The other options are not new features in R80.10 Gateway.

Reference: Check Point R80.10 Security Management Administration Guide

QUESTION 48

What are the three components for Check Point Capsule?

- A. Capsule Docs, Capsule Cloud, Capsule Connect
- B. Capsule Workspace, Capsule Cloud, Capsule Connect
- C. Capsule Workspace, Capsule Docs, Capsule Connect
- D. Capsule Workspace, Capsule Docs, Capsule Cloud

Correct Answer: D

Section:

Explanation:

The three components for Check Point Capsule are Capsule Workspace, Capsule Docs, and Capsule Cloud¹²³. Capsule Workspace provides a secure container on the mobile device that isolates business data and applications from personal data and applications². Capsule Docs protects business documents everywhere they go with encryption and access control¹. Capsule Cloud provides cloud-based security services to protect mobile users from threats³.

Reference: Check Point Capsule, Check Point Capsule Workspace, Mobile Secure Workspace with Capsule

QUESTION 49

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Correct Answer: B

Section:

Explanation:

The port used for full synchronization between cluster members is TCP port 2654. This port is used by the Firewall Kernel to send and receive synchronization data, such as connection tables, NAT tables, and VPN keys. UDP port 8116 is used by the Cluster Control Protocol (CCP) for internal communications between cluster members.

Reference: How does the Cluster Control Protocol function in working and failure scenarios for gateway clusters?

QUESTION 50

What is true about the IPS-Blade?

- A. in R80, IPS is managed by the Threat Prevention Policy
- B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. in R80, IPS Exceptions cannot be attached to "all rules"
- D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Correct Answer: A

Section:

Explanation:

In R80, IPS is managed by the Threat Prevention Policy. The Threat Prevention Policy defines how to protect the network from malicious traffic using IPS, Anti-Bot, Anti-Virus, and Threat Emulation software blades. The IPS layer in the Threat Prevention Policy allows configuring IPS protections and actions for different network segments. The other options are not true about the IPS-Blade.

Reference: Check Point IPS Datasheet, Check Point IPS Software Blade, Quantum Intrusion Prevention System (IPS)

QUESTION 51

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

- 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

Correct Answer: B

Section:

Explanation:

The correct answer is B because after installing a new multicore CPU, the administrator needs to configure CoreXL to make use of the additional cores and reboot the Security Gateway. Installing the Security Policy is not necessary because it does not affect the CoreXL configuration.

Reference: Check Point R81 Security Management Administration Guide

QUESTION 52

When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

- A. Any size

- B. Less than 20GB
- C. More than 10GB and less than 20 GB
- D. At least 20GB

Correct Answer: D

Section:

Explanation:

The correct answer is D because the recommended size of the root partition for a dedicated R80 SmartEvent server is at least 20GB². Any size, less than 20GB, or more than 10GB and less than 20GB are not sufficient for the SmartEvent server.

Reference:Check Point R80.40 Installation and Upgrade Guide

QUESTION 53

Which firewall daemon is responsible for the FW CLI commands?

- A. fwd
- B. fwm
- C. cpm
- D. cpd

Correct Answer: A

Section:

Explanation:

The correct answer is A because the fwd daemon is responsible for the FW CLI commands³. The fwm daemon handles the communication between the Security Management server and the GUI clients. The cpm daemon handles the communication between the Security Management server and SmartConsole. The cpd daemon monitors the status of critical processes on the Security Gateway.

Reference:Check Point Firewall Processes and Daemons

QUESTION 54

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

Correct Answer: A

Section:

Explanation:

The correct answer is A because renaming the hostname of the Standby member to match exactly the hostname of the Active member is not a recommended step to prevent data loss.The hostname of the Standby member should be different from the hostname of the Active member¹.The other steps are necessary to ensure a smooth failover and synchronization between the Active and Standby Security Management Servers².

Reference:Check Point R81.20 Administration Guide,156-315.81 Checkpoint Exam Info and Free Practice Test

QUESTION 55

Using R80 Smart Console, what does a "pencil icon" in a rule mean?

- A. I have changed this rule
- B. Someone else has changed this rule
- C. This rule is managed by check point's SOC

D. This rule can't be changed as it's an implied rule

Correct Answer: A

Section:

Explanation:

The correct answer is A because a pencil icon in a rule means that you have changed this rule³. The pencil icon indicates that the rule has been modified but not published yet. You can hover over the pencil icon to see who made the change and when³. The other options are not related to the pencil icon.

Reference: Check Point Learning and Training Frequently Asked Questions (FAQs)

QUESTION 56

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

Section:

Explanation:

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's³. The Management API's support HTTPS protocol only, not HTTP³. The other methods are valid ways to communicate using the Management API's³.

Reference: Check Point Learning and Training Frequently Asked Questions (FAQs)

QUESTION 57

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

Correct Answer: A

Section:

Explanation:

The correct answer is A because session unique identifiers are passed to the web api using the X-chkp-sid http header option¹. The X-chkp-sid header is used to authenticate and authorize API calls¹. The other options are not related to session unique identifiers.

Reference: Check Point R81 Security Management Administration Guide

QUESTION 58

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete
- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Correct Answer: B



Section:**Explanation:**

The correct answer is B because Threat Extraction always delivers a file and takes less than a second to complete².Threat Extraction removes exploitable content from files and delivers a clean and safe file to the user².Threat Emulation analyzes files in a sandbox environment and delivers a verdict of malicious or benign².Threat Emulation can take more than 3 minutes to complete depending on the file size and complexity².
Reference:Check Point R81 Threat Prevention Administration Guide

QUESTION 59

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Correct Answer: A

Section:**Explanation:**

The correct answer is A because detecting and blocking malware by correlating multiple detection engines before users are affected is not a feature of the Check Point URL Filtering and Application Control Blade³.This feature is part of the Check Point Anti-Virus and Anti-Bot Blades³.The other options are features of the Check Point URL Filtering and Application Control Blade³.

Reference:Check Point R81 URL Filtering and Application Control Administration Guide

QUESTION 60

You want to store the GAiA configuration in a file for later reference. What command should you use?

- A. write mem <filename>
- B. show config -f <filename>
- C. save config -o <filename>
- D. save configuration <filename>



Correct Answer: D

Section:**Explanation:**

The correct answer is D because the command save configuration <filename> stores the Gaia configuration in a file for later reference¹.The other commands are not valid in Gaia Clish¹.

Reference:Gaia R81.10 Administration Guide

QUESTION 61

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

- A. Slow Path
- B. Medium Path
- C. Fast Path
- D. Accelerated Path

Correct Answer: A

Section:**Explanation:**

The correct answer is A because the traffic from source 192.168.1.1 to www.google.com is handled by the Slow Path if the Application Control Blade on the gateway is inspecting the traffic².The Slow Path is used when traffic requires inspection by one or more Software Blades².The other paths are used for different scenarios².

Reference:Check Point R81 Performance Tuning Administration Guide

QUESTION 62

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

Correct Answer: D

Section:

Explanation:

The correct answer is D because from SecureXL perspective, the three paths of traffic flow are Firewall Path, Accelerated Path, and Medium Path³.The Firewall Path is used when SecureXL is disabled or traffic is not eligible for acceleration³.The Accelerated Path is used when SecureXL handles the entire connection and bypasses the Firewall kernel³.The Medium Path is used when SecureXL handles part of the connection and forwards packets to the Firewall kernel for further inspection³.The other options are not valid paths of traffic flow from SecureXL perspective³.

Reference:Check Point R81 Performance Tuning Administration Guide

QUESTION 63

Fill in the blank: An identity server uses a _____ for user authentication.

- A. Shared secret
- B. Certificate
- C. One-time password
- D. Token

Correct Answer: A

Section:

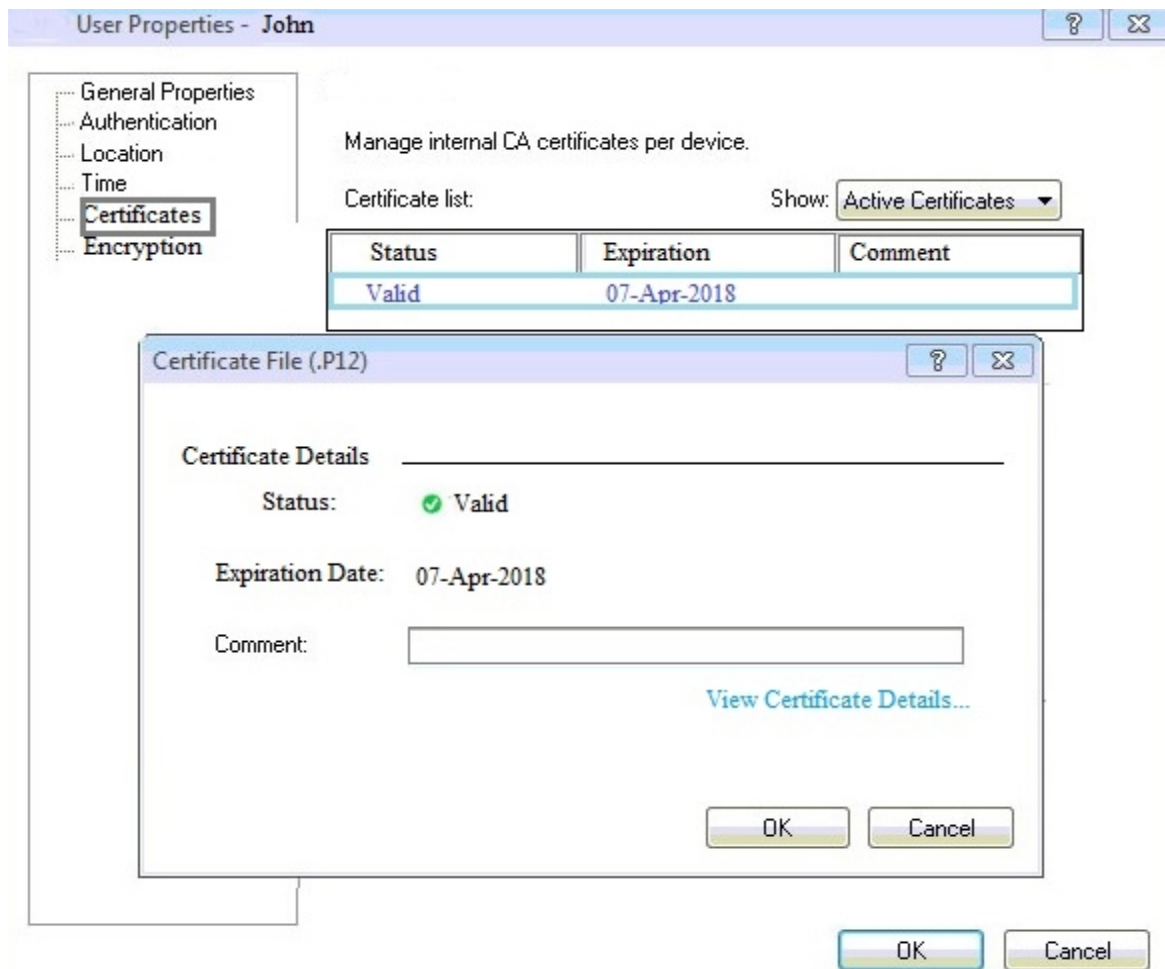
Explanation:

The answer is A because an identity server uses a shared secret for user authentication. A shared secret is a passphrase that is known by both the identity server and the user. The identity server sends a challenge to the user, who encrypts it with the shared secret and sends it back.The identity server then verifies the response and authenticates the user¹²Reference:Check Point R81 Identity Awareness Administration Guide,Check Point R81 Identity Server

QUESTION 64

You can see the following graphic:





What is presented on it?

- A. Properties of personal .p12 certificate file issued for user John.
- B. Shared secret properties of John's password.
- C. VPN certificate properties of the John's gateway.
- D. Expired .p12 certificate properties for user John.

Correct Answer: A

Section:

Explanation:

The answer is A because the graphic shows the properties of a personal .p12 certificate file issued for user John. A .p12 file is a file format that contains a user's private key and public key certificate. The graphic shows that the certificate file is valid and has an expiration date of 07-Apr-2018. The graphic also shows that the certificate file is issued by an internal CA, which is a Check Point component that manages certificates for users and gateways.

Reference: Check Point R81 Certificate Management, Check Point R81 Internal CA

QUESTION 65

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

- A. Reflected immediately for all users who are using template.
- B. Not reflected for any users unless the local user template is changed.
- C. Reflected for all users who are using that template and if the local user template is changed as well.
- D. Not reflected for any users who are using that template.

Correct Answer: A

Section:

Explanation:

The answer is A because 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, such as the server name, port, base DN, user filter, and group filter. When a User Directory template is modified, all users who are using that template will inherit the changes without requiring any additional actions.
Reference: Check Point R81 Identity Awareness Administration Guide, [Check Point R81 User Directory Templates]

QUESTION 66

Choose what BEST describes the reason why querying logs now is very fast.

- A. New Smart-1 appliances double the physical memory install
- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

Correct Answer: B

Section:

Explanation:

The answer is B because querying logs now is very fast because the Indexing Engine indexes logs for faster search results. The Indexing Engine is a component of the Smart-1 appliance that creates indexes for log fields and values, such as source, destination, action, and time. The indexes enable quick and efficient searches of large amounts of log data.

Reference: [Check Point R81 Logging and Monitoring Administration Guide], [Check Point R81 Indexing Engine]

QUESTION 67

Check Point ClusterXL Active/Active deployment is used when:

- A. Only when there is Multicast solution set up
- B. There is Load Sharing solution set up
- C. Only when there is Unicast solution set up
- D. There is High Availability solution set up



Correct Answer: B

Section:

Explanation:

Check Point ClusterXL Active/Active deployment is used when there is Load Sharing solution set up. Load Sharing enables multiple Security Gateways to share traffic and provide high availability.
Reference: Check Point R81, Check Point R81 ClusterXL Administration Guide

QUESTION 68

Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

- A. Save Policy
- B. Install Database
- C. Save session
- D. Install Policy

Correct Answer: A

Section:

Explanation:

The method to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server is Save Policy. Saving a policy updates the trusted log server with the latest policy and configuration changes.
Reference: Check Point R81 Logging and Monitoring Administration Guide

QUESTION 69

From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

- A. Verify a Security Policy
- B. Open a terminal shell
- C. Add a static route
- D. View Security Management GUI Clients

Correct Answer: A

Section:

Explanation:

From the Gaia web interface, the operation that CANNOT be performed on a Security Management Server is Verify a Security Policy. This operation can only be done from SmartConsole4.

Reference: Check Point R81 SmartConsole Online Help

QUESTION 70

Which of the following are types of VPN communities?

- A. Pentagon, star, and combination
- B. Star, octagon, and combination
- C. Combined and star
- D. Meshed, star, and combination

Correct Answer: D

Section:

Explanation:

The types of VPN communities are Meshed, Star, and Combination. A Meshed community is a group of Security Gateways that have VPN connections between every pair of members. A Star community has one Security Gateway as the center and other Security Gateways or hosts as satellites. A Combination community is a group of Meshed and Star communities.

Reference: [Check Point R81 Site-to-Site VPN Administration Guide]

QUESTION 71

What are the three types of UserCheck messages?

- A. inform, ask, and block
- B. block, action, and warn
- C. action, inform, and ask
- D. ask, block, and notify

Correct Answer: A

Section:

Explanation:

The three types of UserCheck messages are inform, ask, and block. Inform messages notify users about security events and do not require any user action. Ask messages prompt users to choose whether to allow or block an action. Block messages prevent users from performing an action and display a reason1.

Reference: Check Point R81 Logging and Monitoring Administration Guide

QUESTION 72

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network



- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

Correct Answer: B

Section:

Explanation:

The two ordered layers that make up the Access Control Policy Layer are Network and Threat Prevention. Network layer contains rules that define how traffic is inspected and handled by the Security Gateway. Threat Prevention layer contains rules that define how traffic is inspected by the Threat Prevention Software Blades.

Reference: Check Point R81 Security Management Administration Guide

QUESTION 73

Which statement is TRUE of anti-spoofing?

- A. Anti-spoofing is not needed when IPS software blade is enabled
- B. It is more secure to create anti-spoofing groups manually
- C. It is BEST Practice to have anti-spoofing groups in sync with the routing table
- D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

Correct Answer: C

Section:

Explanation:

The statement that is TRUE of anti-spoofing is that it is BEST Practice to have anti-spoofing groups in sync with the routing table. Anti-spoofing prevents attackers from sending packets with a false source IP address. Anti-spoofing groups define which IP addresses are expected on each interface of the Security Gateway. If the routing table changes, the anti-spoofing groups should be updated accordingly.

Reference: Check Point R81 ClusterXL Administration Guide, Network Defined by Routes: Anti-Spoofing

QUESTION 74

After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24 set static-route default nexthop gateway address 192.168.80.1 on save config
- B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0 add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0 add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config
- D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24 add static-route default nexthop gateway address 192.168.80.1 on save config

Correct Answer: A

Section:

Explanation:

The commands you could use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1 after the initial installation on Check Point appliance are:

set interface Mgmt ipv4-address 192.168.80.200 mask-length 24. This command sets the IPv4 address and subnet mask of the Management interface.

set static-route default nexthop gateway address 192.168.80.1 on. This command sets the default gateway for IPv4 routing.

save config. This command saves the configuration changes.

QUESTION 75

What Check Point tool is used to automatically update Check Point products for the Gaia OS?

- A. Check Point INSPECT Engine
- B. Check Point Upgrade Service Engine

- C. Check Point Update Engine
- D. Check Point Upgrade Installation Service

Correct Answer: B

Section:

Explanation:

The Check Point Upgrade Service Engine (CPUSE) is a tool that automates the process of upgrading and installing Check Point products on Gaia OS1. It can also be used to update the Gaia OS itself2. The other options are not valid tools for this purpose.

Reference: Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent, Check Point R81 Gaia Installation and Upgrade Guide

QUESTION 76

You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

- A. Open SmartLog and connect remotely to the IP of the wireless controller
- B. Open SmartView Tracker and filter the logs for the IP address of the tablet
- C. Open SmartView Tracker and check all the IP logs for the tablet
- D. Open SmartLog and query for the IP address of the Manager's tablet

Correct Answer: D

Section:

Explanation:

SmartLog is a unified log viewer that provides fast and easy access to logs from all Check Point components3. It allows the administrator to query for any log field, such as the IP address of the tablet, and filter the results by time, severity, blade, action, and more4. SmartView Tracker is a legacy tool that displays network activity logs from Security Gateways and other Check Point devices. It does not support remote connection to the wireless controller or querying for specific IP addresses.

Reference: SmartLog, SmartLog Queries, [SmartView Tracker]

QUESTION 77

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

Section:

Explanation:

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.

Reference: [Shared Policies Overview], [Shared Policies Best Practices]

QUESTION 78

To view statistics on detected threats, which Threat Tool would an administrator use?

- A. Protections
- B. IPS Protections
- C. Profiles

D. ThreatWiki

Correct Answer: D

Section:

Explanation:

ThreatWiki is a web-based tool that provides statistics on detected threats, such as attack types, sources, destinations, and severity. It also allows the administrator to search for specific threats and view their details and mitigation methods. The other options are not tools for viewing statistics on detected threats.

Reference: [ThreatWiki], [ThreatWiki - Threat Emulation]

QUESTION 79

What is the purpose of a Clean-up Rule?

- A. Clean-up Rules do not server any purpose.
- B. Provide a metric for determining unnecessary rules.
- C. To drop any traffic that is not explicitly allowed.
- D. Used to better optimize a policy.

Correct Answer: C

Section:

Explanation:

A clean-up rule is a rule that is placed at the end of the security policy to drop any traffic that is not explicitly allowed by the previous rules. It is a best practice to have a clean-up rule to prevent unauthorized access and log the dropped packets for analysis¹². The other options are not the purpose of a clean-up rule.

Reference: Clean-up Rule, Check Point CCSA - R81: Practice Test & Explanation

QUESTION 80

What are the two types of NAT supported by the Security Gateway?

- A. Destination and Hide
- B. Hide and Static
- C. Static and Source
- D. Source and Destination

Correct Answer: B

Section:

Explanation:

The two types of NAT supported by the Security Gateway are hide NAT and static NAT. Hide NAT translates many source IP addresses into one IP address, usually the external interface of the gateway. Static NAT translates one source IP address into another IP address, usually a public IP address³⁴. The other options are not valid types of NAT.

Reference: Network Address Translation (NAT), Check Point CCSA - R81: Practice Test & Explanation

QUESTION 81

What is the most recommended installation method for Check Point appliances?

- A. SmartUpdate installation
- B. DVD media created with Check Point ISOMorphic
- C. USB media created with Check Point ISOMorphic
- D. Cloud based installation

Correct Answer: C



Section:**Explanation:**

USB media created with Check Point ISOMorphic is the most recommended installation method for Check Point appliances, as it provides a fast and easy way to install the Gaia operating system and the latest software version. SmartUpdate installation requires an existing Gaia installation and does not support fresh installations. DVD media created with Check Point ISOMorphic is less convenient than USB media, as it requires burning the image to a DVD and inserting it into the appliance. Cloud based installation is not applicable for Check Point appliances, as it is intended for cloud environments such as AWS or Azure.

QUESTION 82

Which of the following is NOT a role of the SmartCenter:

- A. Status monitoring
- B. Policy configuration
- C. Certificate authority
- D. Address translation

Correct Answer: D

Section:**Explanation:**

Address translation is not a role of the SmartCenter, as it is performed by the Security Gateway based on the NAT policy configured in the SmartConsole. The other options are roles of the SmartCenter, as it is responsible for status monitoring, policy configuration, and certificate authority for the Security Gateways.

QUESTION 83

Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

- A. Manage and Command Line
- B. Logs and Monitor
- C. Security Policies
- D. Gateway and Servers



Correct Answer: A

Section:**Explanation:**

Manage and Command Line is not a valid application navigation tab in the R80 SmartConsole, as it does not exist in the interface. The image shows the navigation toolbar of the R80 SmartConsole, which has four tabs: Security Policies, Logs & Monitor, Gateways & Servers, and Manage & Settings. The Command Line Interface button is located in the system information area, not in the navigation toolbar.

QUESTION 84

Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.

- A. Main
- B. Authentication
- C. Quick
- D. High Alert

Correct Answer: A

Section:**Explanation:**

Phase 1 of the two-phase negotiation process conducted by IKE operates in Main mode or Aggressive mode. Main mode is more secure than Aggressive mode, as it protects the identities of the peers and uses six messages to establish the IKE SA. Authentication, Quick, and High Alert are not valid modes for IKE phase 1.

QUESTION 85

What is the BEST method to deploy Identity Awareness for roaming users?

- A. Use Office Mode
- B. Use identity agents
- C. Share user identities between gateways
- D. Use captive portal

Correct Answer: B

Section:

Explanation:

The BEST method to deploy Identity Awareness for roaming users is to use identity agents, which are software components installed on endpoints that provide user and machine identity information to the Security Gateway⁴⁵. Identity agents are more secure and reliable than other methods, as they do not require network changes or user interaction⁴. Office Mode, sharing user identities between gateways, and using captive portal are not methods to deploy Identity Awareness, but rather features or options that can be used with Identity Awareness⁴⁶.

QUESTION 86

What is the purpose of the Clean-up Rule?

- A. To log all traffic that is not explicitly allowed or denied in the Rule Base
- B. To clean up policies found inconsistent with the compliance blade reports
- C. To remove all rules that could have a conflict with other rules in the database
- D. To eliminate duplicate log entries in the Security Gateway

Correct Answer: A

Section:

Explanation:

The purpose of the Clean-up Rule is to log all traffic that is not explicitly allowed or denied in the Rule Base⁷⁸. The Clean-up Rule is the last rule in the rulebase and is used to drop and log explicitly unmatched traffic⁹⁷. To improve the rulebase performance, noise traffic that is logged in the Clean-up rule should be included in the Noise rule so it is matched and dropped higher up in the rulebase⁸. The other options are not valid purposes of the Clean-up Rule.

**QUESTION 87**

Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

- A. Application Control
- B. Threat Emulation
- C. Anti-Virus
- D. Advanced Networking Blade

Correct Answer: D

Section:

Explanation:

The Advanced Networking Blade is NOT subscription-based and therefore does not have to be renewed on a regular basis¹⁰¹¹. The Advanced Networking Blade provides advanced routing capabilities such as BGP, OSPF, VRRP, and multicast routing¹⁰. The other blades are subscription-based and require annual renewal to receive updates and support from Check Point¹⁰¹².

QUESTION 88

Fill in the blank: Back up and restores can be accomplished through_____.

- A. SmartConsole, WebUI, or CLI

- B. WebUI, CLI, or SmartUpdate
- C. CLI, SmartUpdate, or SmartBackup
- D. SmartUpdate, SmartBackup, or SmartConsole

Correct Answer: A






Section:

Explanation:

Back up and restores can be accomplished through SmartConsole, WebUI, or CLI¹. These are the methods to perform system backup and restore, which save and restore the Gaia OS configuration and the Security Management Server database¹. WebUI, CLI, or SmartUpdate are not valid methods, as SmartUpdate is used to install software packages and patches, not to back up or restore the system³. CLI, SmartUpdate, or SmartBackup are not valid methods, as SmartBackup is a feature of SmartProvisioning that allows backing up and restoring the configuration of Security Gateways and VSX clusters⁴. SmartUpdate, SmartBackup, or SmartConsole are not valid methods, as SmartConsole is used to configure and manage the Security Policy, not to back up or restore the system⁵.

QUESTION 89

What does it mean if Deyra sees the gateway status:

| Status | Name | IP | Versi... | Active Bla... |
|---|------|------------|----------|---|
|  | A-GW | 10.1.1.1 | R80 |  |
|  | SMS | 10.1.1.101 | R80 |    |

Choose the BEST answer.

- A. SmartCenter Server cannot reach this Security Gateway
- B. There is a blade reporting a problem
- C. VPN software blade is reporting a malfunction
- D. Security Gateway's MGNT NIC card is disconnected.



Correct Answer: B

Section:

Explanation:

If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem. The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention. The other options are not correct, as they do not match the status shown in the image. If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.

QUESTION 90

CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings. The following Threat Prevention Profile has been created.

Company TP Profile

Provide very wide coverage for all products and protocols, with noticeable performance impact.

General Policy

IPS

Anti-Bot

Anti-Virus

Threat Emulation

Malware DNS Trap

Blades Activation

IPS Anti-Bot Anti-Virus Threat Emulation

Activate Protections

Performance Impact:

Severity:

Activation Mode

High Confidence:

Medium Confidence:

Low Confidence:

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.
- D. Set the Performance Impact to Very Low Confidence to Prevent.

Correct Answer: B

Section:

Explanation:

The BEST way to tune the profile in order to lower the CPU load still maintaining security at good level is to set the Performance Impact to Medium or lower. This will reduce the number of packets that are inspected by the Threat Prevention blades, while still providing a high level of protection. Setting High Confidence to Low and Low Confidence to Inactive will lower the security level, as it will allow more traffic that may be malicious. The problem is likely with the Threat Prevention Profile, as it can have a significant impact on the CPU utilization of the Security Gateway. Adding more memory to the appliance will not solve the problem, as memory is not the bottleneck in this case. Setting the Performance Impact to Very Low Confidence to Prevent will increase the CPU load, as it will inspect more packets and block more traffic that may be false positives.

QUESTION 91

Which icon in the WebUI indicates that read/write access is enabled?

- A. Pencil
- B. Padlock
- C. Book
- D. Eyeglasses

Correct Answer: A

Section:**Explanation:**

The icon in the WebUI that indicates that read/write access is enabled is the Pencil icon. The Pencil icon appears next to the name of the device when it is in Read/Write mode, which allows making changes to the configuration. The Padlock icon indicates that read-only access is enabled, which prevents making changes to the configuration. The Book icon indicates that online help is available, which provides information and guidance on using the WebUI. The Eyeglasses icon indicates that a view-only mode is enabled, which allows viewing the configuration without logging in.

QUESTION 92

What is NOT an advantage of Stateful Inspection?

- A. High Performance
- B. Good Security
- C. No Screening above Network layer
- D. Transparency

Correct Answer: C

Section:**Explanation:**

The option that is NOT an advantage of Stateful Inspection is No Screening above Network layer. Stateful Inspection is a firewall technology that inspects packets at all layers of the OSI model, from layer 3 (Network) to layer 7 (Application). Stateful Inspection provides screening above Network layer, such as checking TCP flags, sequence numbers, ports, and application protocols. The other options are advantages of Stateful Inspection, as it provides high performance, good security, and transparency for legitimate traffic.

QUESTION 93

Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

- A. Kerberos Ticket Renewed
- B. Kerberos Ticket Requested
- C. Account Logon
- D. Kerberos Ticket Timed Out

Correct Answer: D

Section:**Explanation:**

The Windows Security Event that will NOT map a username to an IP address in Identity Awareness is Kerberos Ticket Timed Out. This event occurs when a Kerberos ticket expires and is not renewed, which means that the user is no longer active on the network. Identity Awareness does not use this event to map a username to an IP address, as it does not indicate a valid user session. The other events are used by Identity Awareness to map a username to an IP address, as they indicate a successful user authentication or activity on the network.

QUESTION 94

Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

- A. On all satellite gateway to satellite gateway tunnels
- B. On specific tunnels for specific gateways
- C. On specific tunnels in the community
- D. On specific satellite gateway to central gateway tunnels

Correct Answer: C

Section:**Explanation:**

Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or on specific tunnels in the community. This option allows the administrator to select which tunnels should be



permanent and which should be established on demand. The other options are not valid, as they do not match the available choices in the VPN community settings.

QUESTION 95

In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT _____.

- A. Upgrade the software version
- B. Open WebUI
- C. Open SSH
- D. Open service request with Check Point Technical Support

Correct Answer: C

Section:

Explanation:

The function that can NOT be performed in the Unified SmartConsole Gateways and Servers tab is Open SSH. SSH is a secure shell protocol that allows remote access to a device via command line interface. The Unified SmartConsole does not provide an option to open SSH from the Gateways and Servers tab, as it is not a graphical user interface. The other functions can be performed in the Unified SmartConsole Gateways and Servers tab, such as upgrading the software version, opening WebUI, or opening service request with Check Point Technical Support.

QUESTION 96

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

- A. IPS
- B. Anti-Virus
- C. Anti-Malware
- D. Content Awareness

Correct Answer: B

Section:

Explanation:

The Threat Prevention Software Blade that provides protection from malicious software that can infect your network computers is Anti-Virus. Anti-Virus is a software blade that scans files and traffic for viruses, worms, trojans, spyware, and other malware. Anti-Virus can block or clean infected files and prevent malware outbreaks. IPS is a software blade that provides protection from network attacks and exploits. Anti-Malware is not a software blade, but rather a term that refers to any software that can detect and remove malware. Content Awareness is a software blade that provides visibility and control over data that enters or leaves the network based on file types, data types, and keywords.

QUESTION 97

When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

- A. Log, send snmp trap, email
- B. Drop packet, alert, none
- C. Log, alert, none
- D. Log, allow packets, email

Correct Answer: C

Section:

Explanation:

The tracking actions that can be selected when configuring Spoof Tracking are Log, alert, none. Spoof Tracking is a feature that detects packets with spoofed source IP addresses and logs them in SmartView Tracker. The administrator can choose to log only, log and alert, or do nothing when spoofed packets are detected. The other options are not valid tracking actions for Spoof Tracking, as they are either not available or not relevant for this feature.



QUESTION 98

Access roles allow the firewall administrator to configure network access according to:

- A. remote access clients.
- B. a combination of computer or computer groups and networks.
- C. users and user groups.
- D. All of the above.

Correct Answer: D

Section:

Explanation:

Access roles allow the firewall administrator to configure network access according to remote access clients, a combination of computer or computer groups and networks, and users and user groups¹². Therefore, the correct answer is D.

QUESTION 99

Which tool is used to enable ClusterXL?

- A. SmartUpdate
- B. cpconfig
- C. SmartConsole
- D. sysconfig

Correct Answer: B

Section:

Explanation:

The tool that is used to enable ClusterXL is cpconfig. ClusterXL is a software-based Load Sharing and High Availability solution that distributes network traffic between clusters of redundant Security Gateways¹. To enable ClusterXL, you need to run the cpconfig command on each cluster member and select Enable Cluster membership for this gateway². Therefore, the correct answer is B.cpconfig.

QUESTION 100

Fill in the blank: _____ is the Gaia command that turns the server off.

- A. sysdown
- B. exit
- C. halt
- D. shut-down

Correct Answer: C

Section:

Explanation:

halt is the Gaia command that turns the server off. This command shuts down the operating system and powers off the machine. Other commands that can be used to shut down the server are shutdown and poweroff. Reference: [Gaia Administration Guide R80.40]

QUESTION 101

Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

- A. All Connections (Clear or Encrypted)
- B. Accept all encrypted traffic



- C. Specific VPN Communities
- D. All Site-to-Site VPN Communities

Correct Answer: C

Section:

Explanation:

Specific VPN Communities is the option that would only match and allow traffic to VPN gateways for one Community in common. This option allows you to define a specific VPN community that includes the VPN gateways that are allowed to communicate with each other. The other options are either too broad or too narrow for this scenario.

Reference: [Site to Site VPN in R80.x - Tutorial for Beginners]

QUESTION 102

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage & Settings
- B. Security Policies
- C. Gateway & Servers
- D. Logs & Monitor

Correct Answer: D

Section:

Explanation:

Logs & Monitor is the SmartConsole tab that is used to monitor network and security performance. This tab allows you to view and analyze logs and events from various sources, such as Security Gateways, Security Management Servers, and SmartEvent Servers. You can also use this tab to generate reports and troubleshoot issues.

Reference: [Logging and Monitoring Administration Guide R80.20]

QUESTION 103

Which of the following is NOT a policy type available for each policy package?

- A. Threat Emulation
- B. Access Control
- C. Desktop Security
- D. Threat Prevention

Correct Answer: A

Section:

QUESTION 104

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?

- A. The Gateway is an SMB device
- B. The checkbox "Use only Shared Secret for all external members" is not checked
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS
- D. Pre-shared secret is already configured in Global Properties

Correct Answer: C

Section:

Explanation:

Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS. This is because certificate based authentication provides stronger security and easier management than pre-shared secret authentication. The other options are either incorrect or irrelevant for this scenario.

Reference: [Check Point R80.10 - Part 6 - Certificate Based Authentication]

QUESTION 105

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Next-Generation Firewall
- C. Packet Filtering
- D. Application Layer Firewall

Correct Answer: B

Section:

Explanation:

The INSPECT Engine is a technology that extracts detailed information from packets and stores that information in state tables. It enables stateful inspection and application layer filtering. Reference: INSPECT Engine, Stateful Inspection

QUESTION 106

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

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

Correct Answer: B

Section:

Explanation:

The Access Role object type is used to grant network access to an LDAP user group. It defines a set of users and machines that can access a specific network resource. Reference: Access Role, LDAP User Group



QUESTION 107

View the rule below. What does the pen-symbol in the left column mean?

| | | | | |
|---|--|--|--|----------|
| 3 | | HR can access to social network applications | HR | Internet |
| 4 | | All employees can access YouTube for work purposes | Corporate LANs Branch Office LAN Data Center LAN | Internet |

- A. Those rules have been published in the current session.
- B. Rules have been edited by the logged in administrator, but the policy has not been published yet.

- C. Another user has currently locked the rules for editing.
- D. The configuration lock is present. Click the pen symbol in order to gain the lock.

Correct Answer: B

Section:

Explanation:

The pen-symbol in the left column means that the rules have been edited by the logged in administrator, but the policy has not been published yet. It indicates that the changes are not yet effective and can be discarded.

Reference: Policy Editor, Publishing Changes

QUESTION 108

What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

- A. Server, Username, Password, Path, Version
- B. Username, Password, Path, Version
- C. Server, Protocol, Username, Password, Destination Path
- D. Server, Protocol, Username, Password, Path

Correct Answer: D

Section:

Explanation:

According to the Check Point R81.10 SmartConsole for Windows1, to restore a backup, you need to supply the following data: Server, Protocol, Username, Password, and Path. The Server is the IP address or hostname of the Security Management Server. The Protocol is either SCP or SFTP. The Username and Password are the credentials for the Security Management Server. The Path is the location of the backup file on the Security Management Server.

Reference:Check Point R81.10 SmartConsole for Windows



QUESTION 109

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License & Contract
- D. License & Contract and Package Repository

Correct Answer: D

Section:

Explanation:

According to the Managing and Installing license via SmartUpdate2, there are two repositories installed on the Security Management Server by SmartUpdate: License & Contract and Package Repository. The License & Contract repository stores all licenses available and all of the assigned licenses. The Package Repository stores all packages downloaded from the Check Point Cloud or uploaded from a local device.

Reference:Managing and Installing license via SmartUpdate

QUESTION 110

Which back up method uses the command line to create an image of the OS?

- A. System backup
- B. Save Configuration
- C. Migrate
- D. snapshot

Correct Answer: D

Section:

Explanation:

According to the Hewlett Packard Enterprise Support Center³, the snapshot command uses the command line to create an image of the OS. A snapshot is a point-in-time copy of a disk partition that can be used to restore the system in case of a failure or corruption.

Reference:Hewlett Packard Enterprise Support Center

QUESTION 111

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

- A. Protections
- B. IPS Protections
- C. Profiles
- D. ThreatWiki

Correct Answer: B

Section:

Explanation:

According to the Learn More About Threat Signatures⁴, to quickly review when Threat Prevention signatures were last updated, you can use the IPS Protections tool. This tool shows you the date and time of the last update, as well as the number of signatures and their categories.

Reference:Learn More About Threat Signatures

QUESTION 112

Which of the following is considered to be the more secure and preferred VPN authentication method?

- A. Password
- B. Certificate
- C. MD5
- D. Pre-shared secret

Correct Answer: B

Section:

QUESTION 113

When a Security Gateway sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge Mode
- D. Targeted

Correct Answer: A

Section:

Explanation:

When a Security Gateway sends its logs to an IP address other than its own, it means that the deployment option is distributed. In a distributed deployment, the Security Management Server and the Security Gateway are installed on separate machines. The Security Management Server collects logs from one or more Security Gateways and manages them centrally. In a standalone deployment, the Security Management Server and the Security Gateway are installed on the same machine. The Security Gateway sends logs to its own IP address. In a bridge mode deployment, the Security Gateway acts as a transparent bridge between two network segments and does not have an IP address of its own. In a targeted deployment, the Security Gateway sends logs to a specific log server that is configured in the gateway object properties³⁴Reference:Part 4 - Installing Security

QUESTION 114

In _____ NAT, the _____ is translated.

- A. Hide; source
- B. Static; source
- C. Simple; source
- D. Hide; destination

Correct Answer: A

Section:

Explanation:

In hide NAT, the source IP address is translated. Hide NAT is also known as many-to-one NAT or PAT (Port Address Translation). It maps multiple private IP addresses to one public IP address by using different port numbers. Hide NAT allows outbound connections from the private network to the public network, but not inbound connections from the public network to the private network. In static NAT, the source or destination IP address is translated depending on the direction of the traffic. Static NAT is also known as one-to-one NAT or bi-directional NAT. It maps one private IP address to one public IP address and allows both outbound and inbound connections. In simple NAT, there is no translation of IP addresses. Simple NAT is also known as routing mode or transparent mode. It allows traffic to pass through the NAT device without any modification. There is no hide NAT for destination IP address translation.⁵⁶⁷⁸Reference:What Is Network Address Translation (NAT)?,Network address translation,Network Address Translation Definition,Network Address Translation (NAT)

QUESTION 115

An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

- A. AD Query
- B. Browser-Based Authentication
- C. Identity Agents
- D. Terminal Servers Agent



Correct Answer: B

Section:

Explanation:

Browser-Based Authentication is the best method for enabling Identity Awareness on the Check Point firewalls for users who use company issued or personal laptops. Browser-Based Authentication redirects users to a web page where they enter their credentials to access the network resources. This method does not require any installation or configuration on the user's device and supports any operating system and browser. AD Query is a method that queries Active Directory servers for user login events and maps them to IP addresses. This method does not work for personal laptops that are not joined to the domain. Identity Agents are software agents that run on Windows or macOS devices and provide user and machine identity information to the firewall. This method requires installation and management of the agents on each device, which may not be feasible for personal laptops. Terminal Servers Agent is a method that identifies users who connect to Windows Terminal Servers or Citrix servers via RDP or ICA protocols. This method does not apply to laptops that connect directly to the network.⁹¹⁰Reference:Identity Awareness Reference Architecture and Best Practices,Part 10 - Identity

QUESTION 116

Which of the following situations would not require a new license to be generated and installed?

- A. The Security Gateway is upgraded.
- B. The existing license expires.
- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

Correct Answer: A

Section:

Explanation:

Upgrading the Security Gateway does not require a new license to be generated and installed. The license is tied to the IP address or hostname of the Security Gateway, not the software version. However, if the IP address or hostname changes, the existing license expires, or the license is upgraded, a new license must be generated and installed.¹²Reference:Check Point R81,Managing and Installing license via SmartUpdate

QUESTION 117

When should you generate new licenses?

- A. Before installing contract files.
- B. After a device upgrade.
- C. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
- D. Only when the license is upgraded.

Correct Answer: C

Section:**Explanation:**

You should generate new licenses when the existing license expires, the license is upgraded, or the IP address associated with the license changes. These situations invalidate the current license and require a new one to be obtained from the Check Point User Center and installed on the Security Management Server or Security Gateway. Installing contract files or upgrading devices do not affect the validity of the license.¹²Reference:Check Point R81,Managing and Installing license via SmartUpdate

QUESTION 118

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)
- B. CloudGuard
- C. Distributed
- D. Bridge Mode



Correct Answer: B

Section:**Explanation:**

CloudGuard is not a valid deployment option for R80. CloudGuard is a product name for Check Point's cloud security solutions, not a deployment mode. The valid deployment options for R80 are all-in-one (stand-alone), distributed, and bridge mode. In an all-in-one deployment, the Security Management Server and Security Gateway are installed on the same machine. In a distributed deployment, the Security Management Server and Security Gateway are installed on separate machines. In a bridge mode deployment, the Security Gateway acts as a transparent bridge between two network segments and does not have an IP address of its own.³Reference:CloudGuard, [Part 4 - Installing Security Gateway], [Deployment Options]

QUESTION 119

Which backup utility captures the most information and tends to create the largest archives?

- A. backup
- B. snapshot
- C. Database Revision
- D. migrate export

Correct Answer: B

Section:**Explanation:**

Snapshot is the backup utility that captures the most information and tends to create the largest archives. Snapshot creates an image of the entire system, including operating system files, configuration files, databases, and logs. It can be used to restore the system in case of a failure or corruption. Backup creates a compressed file that contains configuration files and databases, but not operating system files or logs. It can be used to restore

configuration settings and policies. Database Revision creates a backup of only the database files that store policies and objects. It can be used to revert to a previous revision of the database. Migrate export creates a compressed file that contains configuration files, databases, and logs, but not operating system files. It can be used to migrate data from one machine to another with different hardware or software versions.

Reference: [Backup and Restore], [Database Revision Control], [Migrate Tools], [Hewlett Packard Enterprise Support Center]

QUESTION 120

Which of the following commands is used to monitor cluster members in CLI?

- A. show cluster state
- B. show active cluster
- C. show clusters
- D. show running cluster

Correct Answer: A

Section:

Explanation:

The command `show cluster state` is used to monitor cluster members in CLI. It displays information such as the cluster mode, the cluster members, their status, their priority, and their interfaces.

Reference: [ClusterXL Administration Guide], [Check Point CLI Reference Card]

QUESTION 121

When enabling tracking on a rule, what is the default option?

- A. Accounting Log
- B. Extended Log
- C. Log
- D. Detailed Log

Correct Answer: C

Section:

Explanation:

When enabling tracking on a rule, the default option is Log. This option generates a log entry for each connection that matches the rule. The log entry contains information such as the source, destination, service, action, and time of the connection.

Reference: [Logging and Monitoring R81], [Logging and Monitoring]

QUESTION 122

Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for what components?

- A. The Security Gateway (SG) and Security Management Server (SMS) software and the CPUSE engine.
- B. Licensed Check Point products for the Gaia operating system and the Gaia operating system itself.
- C. The CPUSE engine and the Gaia operating system.
- D. The Gaia operating system only.

Correct Answer: B

Section:

Explanation:

Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for licensed Check Point products for the Gaia operating system and the Gaia operating system itself. CPUSE is an advanced tool that automates software updates and upgrades on Gaia platforms. It can download and install packages such as hotfixes, Jumbo Hotfix Accumulators, minor versions, major versions, and OS updates.

Reference: [CPUSE - Gaia Software Updates (including Gaia Software Updates Agent)], [Check Point R81]



QUESTION 123

When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packet Filtering?

- A. Stateful Inspection offers unlimited connections because of virtual memory usage.
- B. Stateful Inspection offers no benefits over Packet Filtering.
- C. Stateful Inspection does not use memory to record the protocol used by the connection.
- D. Only one rule is required for each connection.

Correct Answer: D

Section:

Explanation:

Stateful Inspection is a firewall technology that inspects both the header and the payload of each packet and keeps track of the state and context of each connection. Packet Filtering is a firewall technology that inspects only the header of each packet and does not keep track of the state or context of each connection. A benefit that Stateful Inspection offers over Packet Filtering is that only one rule is required for each connection, whereas Packet Filtering requires two rules for each connection (one for each direction). Stateful Inspection also offers other benefits over Packet Filtering, such as enhanced security, performance, and flexibility. Stateful Inspection does not offer unlimited connections because of virtual memory usage, nor does it avoid using memory to record the protocol used by the connection.

Reference: [Stateful Inspection], [Packet Filtering], [Firewall Technologies]

QUESTION 124

Fill in the blanks: Gaia can be configured using _____ the _____.

- A. Command line interface; WebUI
- B. Gaia Interface; GaiaUI
- C. WebUI; Gaia Interface
- D. GaiaUI; command line interface

Correct Answer: A

Section:

Explanation:

Gaia can be configured using the command line interface (CLI) or the WebUI. The CLI is a text-based interface that allows you to configure and manage Gaia settings using commands and scripts. The WebUI is a graphical interface that allows you to configure and manage Gaia settings using a web browser. Gaia Interface and GaiaUI are not valid terms for Gaia configuration tools.

Reference: [Gaia Administration Guide], [Gaia Overview]

QUESTION 125

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

Section:

Explanation:

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.

Reference: [Sectional Titles], [SmartConsole CLI Guide], [SmartConsole API Reference Guide]



QUESTION 126

A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

- A. In the system SMEM memory pool.
- B. In State tables.
- C. In the Sessions table.
- D. In a CSV file on the firewall hard drive located in \$FWDIR/conf/.

Correct Answer: B

Section:

Explanation:

A stateful inspection firewall works by registering connection data and compiling this information in state tables. State tables are data structures that store information about the state and context of each connection, such as source, destination, service, protocol, sequence number, flags, etc. State tables enable the firewall to inspect both the header and the payload of each packet and apply security policies accordingly.

Reference: [Stateful Inspection], [State Tables]

QUESTION 127

What is the RFC number that act as a best practice guide for NAT?

- A. RFC 1939
- B. RFC 1950
- C. RFC 1918
- D. RFC 793

Correct Answer: C

Section:

Explanation:

The RFC number that acts as a best practice guide for NAT is RFC 1918. RFC 1918 defines a range of private IP addresses that are not globally routable and can be used for internal networks. NAT is a technique that maps these private IP addresses to public IP addresses that can communicate with the Internet. RFC 1918 provides guidelines and recommendations for using NAT in different scenarios and environments.

Reference: [RFC 1918], [Network Address Translation (NAT)]

**QUESTION 128**

URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

- A. WebCheck
- B. UserCheck
- C. Harmony Endpoint
- D. URL categorization

Correct Answer: B

Section:

Explanation:

URL Filtering employs a technology called UserCheck, which educates users on web usage policy in real time. UserCheck is a feature that allows the firewall to interact with the users and inform them about the web usage policy and its violations. UserCheck can also allow users to request access to blocked websites or report false positives. UserCheck helps users understand and comply with the web usage policy and reduces the workload of the administrators.

QUESTION 129

Name one limitation of using Security Zones in the network?

- A. Security zones will not work in Automatic NAT rules
- B. Security zone will not work in Manual NAT rules
- C. Security zones will not work in firewall policy layer
- D. Security zones cannot be used in network topology

Correct Answer: B

Section:

Explanation:

One limitation of using Security Zones in the network is that Security Zones will not work in Manual NAT rules. Manual NAT rules are rules that explicitly define how to translate the source and destination IP addresses and ports of each connection. Manual NAT rules do not support using Security Zones as objects, only network objects or groups. Automatic NAT rules are rules that automatically define how to translate the source and destination IP addresses and ports of each connection based on the network objects or groups properties. Automatic NAT rules support using Security Zones as objects. Security Zones can also work in firewall policy layer and network topology.

Reference: [Security Zones Best Practices], [NAT Methods]

QUESTION 130

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

Section:

Explanation:

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.

Reference: [Gaia Administration Guide], [Gaia Overview]

QUESTION 131

Which type of Check Point license ties the package license to the IP address of the Security Management Server?

- A. Central
- B. Corporate
- C. Local
- D. Formal

Correct Answer: A

Section:

Explanation:

The type of Check Point license that ties the package license to the IP address of the Security Management Server is Central license. A Central license is a license that is installed on the Security Management Server and applies to all the Security Gateways that are managed by it. The Central license is based on the IP address of the Security Management Server and cannot be transferred to another Security Management Server with a different IP address.

Reference: [Check Point R81 Licensing Guide], [Managing and Installing license via SmartUpdate]

QUESTION 132

Which of the following is NOT an advantage to using multiple LDAP servers?



- A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
- B. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- C. Information on a user is hidden, yet distributed across several servers.
- D. You gain High Availability by replicating the same information on several servers

Correct Answer: C

Section:

Explanation:

The statement that information on a user is hidden, yet distributed across several servers is not an advantage to using multiple LDAP servers. LDAP (Lightweight Directory Access Protocol) is a protocol that allows access to a centralized directory service that stores information about users, groups, devices, etc. Using multiple LDAP servers can provide advantages such as faster access time, compartmentalization, and high availability, but not hiding information. Information on a user is not hidden by using multiple LDAP servers, but rather replicated or partitioned across them. Replication means that the same information is copied to all LDAP servers, while partitioning means that different information is stored on different LDAP servers. Both methods aim to improve performance and reliability, not security or privacy.

Reference: [LDAP Integration], [LDAP]

QUESTION 133

When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

- A. The gateway is not powered on.
- B. Incorrect routing to reach the gateway.
- C. The Admin would need to login to Read-Only mode
- D. Another Admin has made an edit to that object and has yet to publish the change.

Correct Answer: D

Section:

Explanation:

When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, it indicates that another Admin has made an edit to that object and has yet to publish the change. SmartConsole supports concurrent administration, which means that multiple Admins can work on the same security policy at the same time. However, when one Admin edits an object, such as a gateway, a rule, or a network, that object is locked for other Admins until the change is published or discarded. The lock icon shows which objects are being edited by other Admins and prevents conflicts or overwrites. The gateway being powered off, incorrect routing to reach the gateway, or logging in to Read-Only mode do not cause the lock icon to appear.

Reference: [Concurrent Administration], [SmartConsole Overview]

QUESTION 134

In order to modify Security Policies, the administrator can use which of the following tools? (Choose the best answer.)

- A. SmartConsole and WebUI on the Security Management Server.
- B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
- C. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
- D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Correct Answer: B

Section:

Explanation:

In order to modify Security Policies, the administrator can use SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed. SmartConsole is a graphical tool that allows the administrator to create, edit, and manage security policies using a web browser. mgmt_cli (API) is a command-line tool that allows the administrator to perform the same tasks using commands and scripts. Both tools can connect to the Security Management Server remotely from any computer that has SmartConsole installed.

Reference: [SmartConsole Overview], [mgmt_cli (API)]

QUESTION 135

A SAM rule is implemented to provide what function or benefit?

- A. Allow security audits.
- B. Handle traffic as defined in the policy.
- C. Monitor sequence activity.
- D. Block suspicious activity.

Correct Answer: D

Section:

Explanation:

A SAM (Suspicious Activity Monitoring) rule is implemented to provide the function or benefit of blocking suspicious activity. A SAM rule is a rule that defines an action to be taken by the firewall when it detects a suspicious activity, such as an attack, a scan, or a policy violation. The action can be blocking, dropping, rejecting, or logging the traffic that triggered the suspicious activity. A SAM rule can be created manually or automatically by other security features, such as IPS, Anti-Bot, or SmartEvent.

Reference: [SAM Rules], [Suspicious Activity Rules]

QUESTION 136

Is it possible to have more than one administrator connected to a Security Management Server at once?

- A. Yes, but only if all connected administrators connect with read-only permissions.
- B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
- C. No, only one administrator at a time can connect to a Security Management Server.
- D. Yes, but only one of those administrators will have write-permissions. All others will have read-only permission.

Correct Answer: B

Section:

Explanation:

It is possible to have more than one administrator connected to a Security Management Server at once, but objects edited by one administrator will be locked for editing by others until the session is published. This feature is called concurrent administration and it allows multiple administrators to work on the same security policy at the same time. However, when one administrator edits an object, such as a gateway, a rule, or a network, that object is locked for other administrators until the change is published or discarded. The lock icon shows which objects are being edited by other administrators and prevents conflicts or overwrites.

Reference: [Concurrent Administration], [SmartConsole Overview]

QUESTION 137

In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

- A. Logging & Monitoring
- B. None - the data is available by default
- C. Monitoring Blade
- D. SNMP

Correct Answer: C

Section:

Explanation:

In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, the Monitoring Blade feature needs to be enabled on the Security Gateway. The Monitoring Blade is a software blade that collects and displays network and security performance data from the Security Gateway, such as traffic, throughput, connections, CPU usage, memory usage, etc. The Monitoring Blade can be enabled or disabled on each Security Gateway from the SmartConsole.

Reference: [Monitoring Blade], [SmartView Monitor]

QUESTION 138

What is the default shell for the command line interface?

- A. Clish
- B. Admin
- C. Normal
- D. Expert

Correct Answer: A

Section:

Explanation:

Clish is the default shell for the command line interface. It is a user-friendly shell that provides a menu-based and a command-line mode. Admin, Normal, and Expert are not valid shell names¹.

QUESTION 139

When configuring Anti-Spoofing, which tracking options can an Administrator select?

- A. Log, Alert, None
- B. Log, Allow Packets, Email
- C. Drop Packet, Alert, None
- D. Log, Send SNMP Trap, Email

Correct Answer: A

Section:

Explanation:

Log, Alert, and None are the tracking options that an Administrator can select when configuring Anti-Spoofing. Log means that the packet will be logged in SmartView Tracker. Alert means that the packet will trigger an alert in SmartView Monitor. None means that no action will be taken². The other options are not valid tracking options.

QUESTION 140

Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

- A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
- B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
- C. 192.168.1.1 AND 172.26.1.1 AND drop
- D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Correct Answer: B

Section:

Explanation:

src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop is the correct log query to show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1. The AND operator means that all conditions must be true for the query to match. The OR operator means that any condition can be true for the query to match³. The other queries will either show packets that are not dropped or packets that have different source or destination addresses.

QUESTION 141

Core Protections are installed as part of what Policy?

- A. Access Control Policy.
- B. Desktop Firewall Policy
- C. Mobile Access Policy.

D. Threat Prevention Policy.

Correct Answer: D

Section:

Explanation:

Core Protections are installed as part of the Threat Prevention Policy. Core Protections are a set of IPS protections that are essential for securing your network against malicious traffic⁴. The other policies do not include Core Protections.

QUESTION 142

In HTTPS Inspection policy, what actions are available in the 'Actions' column of a rule?

- A. 'Inspect', 'Bypass'
- B. 'Inspect', 'Bypass', 'Categorize'
- C. 'Inspect', 'Bypass', 'Block'
- D. 'Detect', 'Bypass'

Correct Answer: A

Section:

Explanation:

The actions available in the "Actions" column of a rule in HTTPS Inspection policy are "Inspect" and "Bypass". "Inspect" means that the HTTPS traffic will be decrypted and inspected according to the Access Control policy. "Bypass" means that the HTTPS traffic will not be decrypted and will be allowed without inspection¹. The other options are not valid actions for HTTPS Inspection policy.

QUESTION 143

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

- A. Captive Portal and Transparent Kerberos Authentication
- B. UserCheck
- C. User Directory
- D. Captive Portal

Correct Answer: A

Section:

Explanation:

Browser-based Authentication sends users to a web page to acquire identities using Captive Portal and Transparent Kerberos Authentication. Captive Portal is a web page that prompts users to enter their credentials. Transparent Kerberos Authentication is a method that automatically authenticates users who have a valid Kerberos ticket from the Active Directory domain controller². UserCheck is a feature that allows users to interact with the security policy, not a method of authentication. User Directory is a component that integrates with external user databases, not a web page for authentication. Captive Portal alone is not enough to fill in the blank, as it is only one of the methods used by Browser-based Authentication.

QUESTION 144

With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

- A. The complete communication is sent for inspection.
- B. The IP address of the source machine.
- C. The end user credentials.
- D. The host portion of the URL.

Correct Answer: D

Section:

Explanation:

With URL Filtering, only the host portion of the URL is sent to the Check Point Online Web Service for analysis. The host portion 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 Gateway³. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data.

QUESTION 145

Choose what BEST describes the reason why querying logs now are very fast.

- A. The amount of logs being stored is less than previous versions.
- B. New Smart-1 appliances double the physical memory install.
- C. Indexing Engine indexes logs for faster search results.
- D. SmartConsole now queries results directly from the Security Gateway.

Correct Answer: C

Section:

Explanation:

The reason why querying logs now are very fast is that Indexing Engine indexes logs for faster search results. Indexing Engine is a component of R81 Management that creates and maintains an index of log data, which enables quick and efficient log searches⁴. The other options are not related to the speed of log querying. The amount of logs being stored may vary depending on the log retention settings. New Smart-1 appliances may have improved hardware specifications, but they do not affect the log querying process directly. SmartConsole queries results from the Security Management Server, not from the Security Gateway.

QUESTION 146

Which policy type is used to enforce bandwidth and traffic control rules?

- A. Access Control
- B. Threat Emulation
- C. Threat Prevention
- D. QoS



Correct Answer: D

Section:

Explanation:

The policy type that is used to enforce bandwidth and traffic control rules is QoS. QoS stands for Quality of Service and is a software blade that allows administrators to prioritize network traffic according to various criteria such as source, destination, service, application, user, etc. QoS can also limit the bandwidth consumption of certain traffic types or guarantee a minimum bandwidth for critical applications.

Reference: [Check Point R81 QoS Administration Guide]

QUESTION 147

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

- A. Cache the data to speed up its own function.
- B. Share the data to the ThreatCloud for use by other Threat Prevention blades.
- C. Log the traffic for Administrator viewing.
- D. Delete the data to ensure an analysis of the data is done each time.

Correct Answer: B

Section:

Explanation:

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does share the data to the ThreatCloud for use by other Threat Prevention blades. The ThreatCloud is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to security gateways. The Threat Prevention gateway can send and receive updates from the ThreatCloud about

new threats and malicious data signatures.

Reference: [Check Point R81 Threat Prevention Administration Guide]

QUESTION 148

Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. SmartDashboard
- B. SmartEvent
- C. SmartView Monitor
- D. SmartUpdate

Correct Answer: B

Section:

Explanation:

The product that correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices is SmartEvent. SmartEvent is a software blade that analyzes logs from various sources such as Security Gateways, Endpoint Security Servers, Identity Awareness Servers, etc. and generates security events based on predefined or custom rules. SmartEvent provides a graphical interface for viewing and managing security events in real-time or historical mode.

Reference: [Check Point R81 SmartEvent Administration Guide]

QUESTION 149

Which two Identity Awareness daemons are used to support identity sharing?

- A. Policy Activation Point (PAP) and Policy Decision Point (PDP)
- B. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
- C. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
- D. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)

Correct Answer: D

Section:

Explanation:

The two Identity Awareness daemons that are used to support identity sharing are Policy Decision Point (PDP) and Policy Enforcement Point (PEP). PDP is a daemon that runs on the Security Management Server or a dedicated Identity Awareness Server and provides identity information to other components. PEP is a daemon that runs on the Security Gateway and enforces identity-based rules based on the information received from the PDP. Identity sharing is a feature that allows PDPs and PEPs to exchange identity information across different domains or networks.

Reference: [Check Point R81 Identity Awareness Administration Guide]

QUESTION 150

What is the default shell of Gaia CLI?

- A. clish
- B. Monitor
- C. Read-only
- D. Bash

Correct Answer: A

Section:

Explanation:

The default shell of Gaia CLI is clish, which stands for Check Point command line interface shell1. It provides a user-friendly interface to configure and manage Check Point products.

Reference: Check Point Gaia Administration Guide



QUESTION 151

How many layers make up the TCP/IP model?

- A. 2
- B. 7
- C. 6
- D. 4

Correct Answer: D

Section:

Explanation:

The TCP/IP model is made up of four layers: Application, Transport, Internet, and Network Interface1, p. 10. The TCP/IP model is a simplified version of the OSI model, which has seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical.

Reference:Check Point CCSA - R81: Practice Test & Explanation, [TCP/IP Model Explained]

QUESTION 152

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

Section:

Explanation:

Resource is NOT an objects category in SmartConsole1, 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.

Reference:Check Point CCSA - R81: Practice Test & Explanation, [Check Point SmartConsole R81 Help]

QUESTION 153

Which of the following is used to enforce changes made to a Rule Base?

- A. Publish database
- B. Save changes
- C. Install policy
- D. Activate policy

Correct Answer: C

Section:

Explanation:

The option that is used to enforce changes made to a Rule Base is Install policy.Installing policy is the process of sending the security policy and the network objects from the Security Management Server to the Security Gateway1, p. 22.Publishing database and saving changes are options that are used to save changes made to a Rule Base, but they do not enforce them on the Security Gateway2. Activating policy is not a valid option in SmartConsole.

Reference:Check Point CCSA - R81: Practice Test & Explanation,Check Point SmartConsole R81 Help

QUESTION 154

What is UserCheck?

- 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

Section:

Explanation:

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 access³, p. 38. UserCheck is not a messaging tool, an administrator tool, or a notification tool.

Reference: Check Point CCSA - R81: Practice Test & Explanation, [Check Point UserCheck Administration Guide R81]

QUESTION 155

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. SmartEvent

Correct Answer: A

Section:

Explanation:

When doing a Stand-Alone Installation, you would install the Security Management Server with none of the other Check Point architecture components. A Stand-Alone Installation is a type of installation that combines the Security Management Server and the Security Gateway on one computer or appliance³, p. 14. SmartConsole, SecureClient, and SmartEvent are not Check Point architecture components, but software applications that can be installed separately.

Reference: Check Point CCSA - R81: Practice Test & Explanation, [Check Point Installation and Upgrade Guide R81]

QUESTION 156

Fill in the blank: An Endpoint identity agent uses a _____ for user authentication.

- A. Shared secret
- B. Token
- C. Username/password or Kerberos Ticket
- D. Certificate

Correct Answer: C

Section:

Explanation:

An Endpoint identity agent uses a username/password or Kerberos ticket for user authentication³, p. 28. An Endpoint identity agent is a lightweight client installed on endpoint computers that communicates with Identity Awareness gateways and provides reliable identity information. An Endpoint identity agent does not use a shared secret, a token, or a certificate for user authentication.

Reference: Check Point CCSA - R81: Practice Test & Explanation, [Check Point Identity Awareness Administration Guide R81]

QUESTION 157

What is the purpose of a Stealth Rule?

- A. A rule used to hide a server's IP address from the outside world.
- B. A rule that allows administrators to access SmartDashboard from any device.
- C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
- D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

Correct Answer: C

Section:

Explanation:

The purpose of a Stealth Rule is to drop any traffic destined for the firewall that is not otherwise explicitly allowed¹, p. 32. A Stealth Rule is usually placed at the top of the rule base, before any other rule that allows traffic to the Security Gateway², p. 13. A Stealth Rule is not used to hide a server's IP address, to allow administrators to access SmartDashboard, or to drop any traffic that is not explicitly allowed.

Reference: Check Point CCSA - R81: Practice Test & Explanation, 156-315.81 Checkpoint Exam Info and Free Practice Test

QUESTION 158

To view the policy installation history for each gateway, which tool would an administrator use?

- A. Revisions
- B. Gateway installations
- C. Installation history
- D. Gateway history

Correct Answer: C

Section:

Explanation:

To view the policy installation history for each gateway, an administrator would use the Installation history tool¹, p. 22. The Installation history tool shows the date and time of each policy installation, the name of the administrator who installed it, and the status of the installation³. Revisions, Gateway installations, and Gateway history are not valid tools in SmartConsole.

Reference: Check Point CCSA - R81: Practice Test & Explanation, Check Point SmartConsole R81 Help

QUESTION 159

How many users can have read/write access in Gaia Operating System at one time?

- A. One
- B. Three
- C. Two
- D. Infinite

Correct Answer: A

Section:

Explanation:

Only one user can have read/write access in Gaia Operating System at one time². This is to prevent conflicts and errors when multiple users try to modify the same configuration settings.

Reference: Check Point Gaia Administration Guide

QUESTION 160

In SmartConsole, on which tab are Permissions and Administrators defined?

- A. Manage and Settings
- B. Logs and Monitor
- C. Security Policies

D. Gateways and Servers

Correct Answer: A

Section:

Explanation:

Permissions and Administrators are defined on the Manage and Settings tab in SmartConsole3. This tab allows you to create and manage administrator accounts, roles, permissions, and authentication methods for accessing SmartConsole and other Check Point management interfaces.

Reference:Check Point R81 Security Management Administration Guide

QUESTION 161

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

- A. RADIUS
- B. Check Point password
- C. Security questions
- D. SecurID

Correct Answer: C

Section:

Explanation:

Security questions are not an authentication scheme used for accounts created through SmartConsole4. The available authentication schemes are Check Point password, RADIUS, TACACS, SecurID, LDAP, and Certificate.

Reference:Check Point R81 Security Management Administration Guide

QUESTION 162

The Gateway Status view in SmartConsole shows the overall status of Security Gateways and Software Blades. What does the Status Attention mean?

- A. Cannot reach the Security Gateway.
- B. The gateway and all its Software Blades are working properly.
- C. At least one Software Blade has a minor issue, but the gateway works.
- D. Cannot make SIC between the Security Management Server and the Security Gateway

Correct Answer: C

Section:

Explanation:

The Status Attention means that at least one Software Blade has a minor issue, but the gateway works1.For example, this could indicate a license expiration warning, a policy installation failure, or a blade activation problem2.

Reference:Check Point R81 SmartConsole Guide,Check Point R81 Security Management Administration Guide

QUESTION 163

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

- A. Publish changes
- B. Save changes
- C. Install policy
- D. Install database

Correct Answer: C

Section:

Explanation:

In order for changes made to policy to be enforced by a Security Gateway, an administrator must perform Install Policy³. This action transfers the policy package from the Security Management Server to the Security Gateway and activates it.

Reference:Check Point R81 Security Management Administration Guide

QUESTION 164

What is the main objective when using Application Control?

- A. To filter out specific content.
- B. To assist the firewall blade with handling traffic.
- C. To see what users are doing.
- D. Ensure security and privacy of information.

Correct Answer: D

Section:

Explanation:

The main objective when using Application Control is to ensure security and privacy of information⁴. Application Control enables administrators to control access to web applications and web sites based on risk level, user identity, and other criteria. It also provides visibility into web usage and application activity.

Reference:Check Point R81 Application Control Administration Guide

QUESTION 165

What are the three main components of Check Point security management architecture?

- A. SmartConsole, Security Management, and Security Gateway
- B. Smart Console, Standalone, and Security Management
- C. SmartConsole, Security policy, and Logs & Monitoring
- D. GUI-Client, Security Management, and Security Gateway



Correct Answer: A

Section:

Explanation:

The three main components of Check Point security management architecture are SmartConsole, Security Management, and Security Gateway⁵. SmartConsole is the graphical user interface that allows administrators to manage and monitor Check Point products. Security Management is the server that stores the security policy and configuration data. Security Gateway is the device that enforces the security policy on the network traffic.

Reference:Check Point R81 Security Management Administration Guide

QUESTION 166

In which deployment is the security management server and Security Gateway installed on the same appliance?

- A. Standalone
- B. Remote
- C. Distributed
- D. Bridge Mode

Correct Answer: A

Section:

Explanation:

A standalone deployment is when the security management server and Security Gateway are installed on the same appliance.This is suitable for small or branch office environments¹

QUESTION 167

Where can administrator edit a list of trusted SmartConsole clients?

- A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
- B. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- C. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients, via cpconfig on a Security Gateway.
- D. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.

Correct Answer: B

Section:

Explanation:

The administrator can edit a list of trusted SmartConsole clients in three ways: in cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, and in SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients

QUESTION 168

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

Section:

Explanation:

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 169

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

Section:

Explanation:

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.

QUESTION 170

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

Section:

Explanation:

A correlation unit (CU) is a component of SmartEvent that analyzes log entries on log servers and identifies events based on predefined or custom rules¹. 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 171

What is NOT an advantage of Packet Filtering?

- A. Application Independence
- B. High Performance
- C. Scalability
- D. Low Security and No Screening above Network Layer

Correct Answer: D

Section:

Explanation:

Packet filtering is a technique that controls the flow of network data by examining the headers of packets and applying a set of rules to accept or reject them. Packet filtering has some advantages, such as efficiency, cost-effectiveness, ease of use, and transparency³. However, it also has some disadvantages, such as low security and no screening above the network layer⁴. Packet filtering firewalls cannot inspect the payload of packets or the application layer protocols, which makes them vulnerable to attacks that exploit higher-level vulnerabilities

QUESTION 172

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

Section:

Explanation:

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 packet⁶. 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 173

Which software blade does NOT accompany the Threat Prevention policy?

- A. IPS
- B. Application Control and URL Filtering
- C. Threat Emulation
- D. Anti-virus

Correct Answer: B

Section:



Explanation:

The Threat Prevention policy is a unified policy that manages three software blades: IPS, Anti-Virus, and Threat Emulation. The Threat Prevention policy enables you to configure settings and actions for detecting and preventing various types of threats, such as malware, exploits, botnets, etc. Application Control and URL Filtering are not part of the Threat Prevention policy, but they are part of a separate policy that controls access to applications and websites based on categories, users, groups, and machines.

QUESTION 174

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

Section:

Explanation:

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 175

Which Check Point Software Blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering



Correct Answer: B

Section:

Explanation:

Identity Awareness is the Check Point software blade that provides visibility of users, groups and machines while also providing access control through identity-based policies. Identity Awareness enables administrators to define granular access rules based on user or machine identity, rather than just IP addresses. Identity Awareness also allows administrators to monitor user activity and generate reports based on user or machine identity.

QUESTION 176

For Automatic Hide NAT rules created by the administrator what is a TRUE statement?

- A. Source Port Address Translation (PAT) is enabled by default.
- B. Automatic NAT rules are supported for Network objects only.
- C. Automatic NAT rules are supported for Host objects only.
- D. Source Port Address Translation (PAT) is disabled by default.

Correct Answer: A

Section:

Explanation:

Automatic Hide NAT rules are created by the administrator when they configure NAT for network objects or groups in the object properties. Automatic Hide NAT rules allow multiple private IP addresses to share a single public IP address when accessing external networks. Source Port Address Translation (PAT) is enabled by default for Automatic Hide NAT rules, which means that the Security Gateway assigns a unique source port number for each connection from the same source IP address. This allows the Security Gateway to keep track of the connections and translate the reply packets correctly.

QUESTION 177

What is the user ID of a user that have all the privileges of a root user?

- A. User ID 1
- B. User ID 2
- C. User ID 0
- D. User ID 99

Correct Answer: C

Section:

Explanation:

The user ID (UID) of a user that has all the privileges of a root user is 0. The root user is the superuser account that can perform any action on the system, such as changing file ownership, binding to network ports below 1024, or executing any command. The root user is identified by the UID 0, not by the name "root", which is just a convention. It is possible to have another user account with the name "root", but not with the same UID 0.

QUESTION 178

Which command shows the installed licenses in Expert mode?

- A. print cplic
- B. show licenses
- C. fwlic print
- D. cplic print

Correct Answer: D

Section:

Explanation:

The command that shows the installed licenses in Expert mode is cplic print. This command displays information about the licenses that are installed on the local machine or a remote machine¹. The other commands are not valid for showing licenses in Expert mode.

QUESTION 179

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

Section:

Explanation:

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 rules². 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 users³. The other options are not basic rules for building a security policy, but rather types or categories of rules.

QUESTION 180

Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

- A. Full



- B. Custom
- C. Complete
- D. Light

Correct Answer: A

Section:

Explanation:

The type of Endpoint Identity Agent that includes packet tagging and computer authentication is Full. The Full Identity Agent is a client-side software that provides full identity awareness features, such as user authentication, computer authentication, packet tagging, identity caching, and identity sharing. The other types of Endpoint Identity Agents are Custom, Complete, and Light, which have different features and capabilities.

QUESTION 181

Which of the following is TRUE regarding Gaia command line?

- A. Configuration changes should be done in mgmt_di and use CLISH for monitoring. Expert mode is used only for OS level tasks
- B. Configuration changes should be done in mgmt_cli and use expert-mode for OS-level tasks.
- C. Configuration changes should be done in expert-mode and CLISH is used for monitoring
- D. All configuration changes should be made in CLISH and expert-mode should be used for OS-level tasks.

Correct Answer: D

Section:

Explanation:

The statement that is true regarding Gaia command line is that all configuration changes should be made in CLISH and expert-mode should be used for OS-level tasks. CLISH is the default shell of Gaia CLI that provides a limited set of commands for basic configuration and troubleshooting. Expert mode is an advanced shell that allows running Linux commands and accessing the file system. Configuration changes should not be done in expert-mode, as they may cause inconsistencies or errors in the system. The other statements are false regarding Gaia command line.

QUESTION 182

When a gateway requires user information for authentication, what order does it query servers for user information?

- A. First - Internal user database, then LDAP servers in order of priority, finally the generic external user profile
- B. First the Internal user database, then generic external user profile, finally LDAP servers in order of priority.
- C. First the highest priority LDAP server, then the internal user database, then lower priority LDAP servers, finally the generic external profile
- D. The external generic profile, then the internal user database finally the LDAP servers in order of priority.

Correct Answer: B

Section:

Explanation:

When a gateway requires user information for authentication, it queries servers for user information in the following order: first the internal user database, then the generic external user profile, and finally LDAP servers in order of priority. The internal user database is a local database that stores user information on the Security Gateway or Security Management Server. The generic external user profile is a predefined profile that allows users to authenticate with any external server that supports RADIUS or TACACS protocols. LDAP servers are external servers that use the Lightweight Directory Access Protocol to store and retrieve user information. The gateway queries LDAP servers according to the priority that is defined in the LDAP Account Unit object properties.

QUESTION 183

Fill in the blank RADIUS Accounting gets _____ data from requests generated by the accounting client

- A. Location
- B. Payload
- C. Destination

D. Identity

Correct Answer: D

Section:

Explanation:

RADIUS Accounting gets identity data from requests generated by the accounting client. RADIUS Accounting is a feature that allows tracking and measuring resource usage of network services by users. The accounting client, which is usually a network access server (NAS), sends accounting requests to a RADIUS server with information about user sessions, such as start and stop times, bytes transmitted and received, IP addresses, etc. The RADIUS server records this information in a database for billing, auditing, or reporting purposes. One of the mandatory attributes that the accounting client must include in every accounting request is the User-Name attribute, which identifies the user who is accessing the network service.

QUESTION 184

SmartConsole provides a consolidated solution for everything that is necessary for the security of an organization, such as the following

- A. Security Policy Management and Log Analysis
- B. Security Policy Management. Log Analysis. System Health Monitoring. Multi-Domain Security Management.
- C. Security Policy Management Log Analysis and System Health Monitoring
- D. Security Policy Management. Threat Prevention rules. System Health Monitoring and Multi-Domain Security Management.

Correct Answer: A

Section:

Explanation:

SmartConsole provides a consolidated solution for everything that is necessary for the security of an organization, such as Security Policy Management and Log Analysis. Security Policy Management is the process of defining and enforcing rules that control the access and protection of network resources. Log Analysis is the process of collecting, analyzing, and reporting on log data that is generated by network devices and applications.

SmartConsole is a unified graphical user interface that allows administrators to manage multiple security functions from a single console. The other options are not part of SmartConsole, but rather separate software blades or features that can be integrated with SmartConsole.

QUESTION 185

By default, which port does the WebUI listen on?

- A. 8080
- B. 80
- C. 4434
- D. 443

Correct Answer: B

Section:

Explanation:

By default, the WebUI listens on port 80. The WebUI is a web-based interface that allows administrators to configure and monitor Gaia OS settings and features from a web browser. The WebUI uses the HTTP protocol to communicate with the Gaia machine, which by default uses port 80 as the standard port number. The other port numbers are not used by the WebUI by default, but they can be changed by modifying the Gaia configuration file or using CLISH commands.

QUESTION 186

Fill in the blank Backup and restores can be accomplished through

- A. SmartUpdate, SmartBackup. or SmartConsole
- B. WebUI. CLI. or SmartUpdate
- C. CLI. SmartUpdate, or SmartBackup
- D. SmartConsole, WebUI. or CLI

Correct Answer: D

Section:

Explanation:

Backup and restores can be accomplished through SmartConsole, WebUI, or CLI. SmartUpdate and SmartBackup are not valid options¹.

QUESTION 187

Which of the following is NOT a type of Endpoint Identity Agent?

- A. Custom
- B. Terminal
- C. Full
- D. Light

Correct Answer: A

Section:

Explanation:

There are three types of Endpoint Identity Agents: Full, Light, and Terminal. Custom is not a valid type².

QUESTION 188

An administrator wishes to use Application objects in a rule in their policy but there are no Application objects listed as options to add when clicking the '+' to add new items to the 'Services & Applications' column of a rule. What should be done to fix this?

- A. The administrator should drag-and-drop the needed Application objects from the Object Explorer into the new rule
- B. The 'Application Control' blade should be enabled on a gateway
- C. 'Applications & URL Filtering' should first be enabled on the policy layer where the rule is being created.
- D. The administrator should first create some applications to add to the rule.

Correct Answer: C

Section:

Explanation:

To use Application objects in a rule, the "Applications & URL Filtering" blade should be enabled on the policy layer where the rule is being created. Enabling the "Application Control" blade on a gateway is not enough³.

QUESTION 189

Which Threat Prevention Software Blade provides comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

- A. IPS
- B. Anti-Virus
- C. Anti-Spam
- D. Anti-bot

Correct Answer: A

Section:

Explanation:

The IPS (Intrusion Prevention System) Software Blade provides comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities. The other options are not related to this function.

QUESTION 190

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

- A. Windows Management Instrumentation (WMI)
- B. Hypertext Transfer Protocol Secure (HTTPS)
- C. Lightweight Directory Access Protocol (LDAP)
- D. Remote Desktop Protocol (RDP)

Correct Answer: C

Section:

Explanation:

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using LDAP (Lightweight Directory Access Protocol). The other protocols are not used for this purpose.

QUESTION 191

Which of the completed statements is NOT true? The WebUI can be used to manage Operating System user accounts and

- A. add users to your Gaia system.
- B. assign privileges to users.
- C. assign user rights to their home directory in the Security Management Server.
- D. edit the home directory of the user.

Correct Answer: C

Section:

Explanation:

The WebUI can be used to manage Operating System user accounts and add users to your Gaia system, assign privileges to users, and edit the home directory of the user. However, it cannot assign user rights to their home directory in the Security Management Server. This is done by the SmartConsole1.



QUESTION 192

Fill in the blank RADIUS protocol uses _____ to communicate with the gateway

- A. UDP
- B. CCP
- C. TDP
- D. HTTP

Correct Answer: A

Section:

Explanation:

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.

QUESTION 193

Choose what BEST describes a Session

- A. Sessions ends when policy is pushed to the Security Gateway.
- B. Starts when an Administrator logs in through SmartConsole and ends when the Administrator logs out.
- C. Sessions locks the policy package for editing.
- D. Starts when an Administrator publishes all the changes made on SmartConsole

Correct Answer: B

Section:

Explanation:

A session starts when an Administrator logs in through SmartConsole and ends when the Administrator logs out. A session allows multiple administrators to work on the same policy simultaneously, without overwriting each other's changes.

QUESTION 194

Where can alerts be viewed?

- A. Alerts can be seen in SmartView Monitor
- B. Alerts can be seen in the Threat Prevention policy.
- C. Alerts can be seen in SmartUpdate.
- D. Alerts can be seen from the CLI of the gateway.

Correct Answer: A

Section:

Explanation:

Alerts can be viewed in SmartView Monitor, which is a graphical tool that provides real-time information about the network and security activities, such as traffic, VPN tunnels, threats, and performance.

QUESTION 195

If there is an Accept Implied Policy set to 'First', what is the reason Jorge cannot see any logs?

- A. Log Implied Rule was not set correctly on the track column on the rules base.
- B. Track log column is set to Log instead of Full Log.
- C. Track log column is set to none.
- D. Log Implied Rule was not selected on Global Properties.



Correct Answer: D

Section:

Explanation:

If there is an Accept Implied Policy set to "First", Jorge cannot see any logs because Log Implied Rule was not selected on Global Properties. The Log Implied Rule option enables logging for all implied rules, such as DHCP, anti-spoofing, and cleanup rules.

QUESTION 196

A layer can support different combinations of blades. What are the supported blades:

- A. Firewall, URLF, Content Awareness and Mobile Access
- B. Firewall (Network Access Control), Application & URL Filtering, Content Awareness and Mobile Access
- C. Firewall, NAT, Content Awareness and Mobile Access
- D. Firewall (Network Access Control), Application & URL Filtering and Content Awareness

Correct Answer: D

Section:

Explanation:

A layer can support different combinations of blades, but the supported blades are Firewall (Network Access Control), Application & URL Filtering, and Content Awareness. These blades provide granular control over network traffic based on applications, users, content, and risk. Mobile Access is not a supported blade in a layer.

QUESTION 197

Fill in the blank: Once a license is activated, a _____ should be installed.

- A. Security Gateway Contract file
- B. Service Contract file
- C. License Management file
- D. License Contract file

Correct Answer: B

Section:

Explanation:

Once a license is activated, a Service Contract file should be installed. This file contains information about the license expiration date, support level, and other details. The other options are not valid file names.

QUESTION 198

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored?

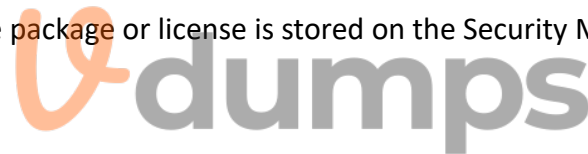
- A. SmartConsole installed device
- B. Check Point user center
- C. Security Management Server
- D. Security Gateway

Correct Answer: C

Section:

Explanation:

When you upload a package or license to the appropriate repository in SmartUpdate, the package or license is stored on the Security Management Server. SmartUpdate is a tool that allows you to centrally manage software updates and licenses for all Check Point products on your network.



QUESTION 199

What technologies are used to deny or permit network traffic?

- A. Stateful Inspection, Firewall Blade, and URL/Application Blade
- B. Packet Filtering, Stateful Inspection, and Application Layer Firewall
- C. Firewall Blade, URL/Application Blade and IPS
- D. Stateful Inspection, URL/Application Blade, and Threat Prevention

Correct Answer: A

Section:

Explanation:

The technologies that are used to deny or permit network traffic are Stateful Inspection, Firewall Blade, and URL/Application Blade. Stateful Inspection is a technology that inspects network traffic at the packet level and maintains the state and context of each connection. Firewall Blade is a software blade that enforces security policy and prevents unauthorized access to protected resources. URL/Application Blade is a software blade that enables administrators to control access to millions of websites and applications based on users, groups, and machines.

QUESTION 200

To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

- A. The Access Control and Threat Prevention Policies.
- B. The Access Control Policy.
- C. The Access Control & HTTPS Inspection Policy.
- D. The Threat Prevention Policy.

Correct Answer: D

Section:

Explanation:

To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity. The administrator should install the Threat Prevention Policy after Publishing the changes. The Threat Prevention Policy defines how the Security Gateway inspects and protects against threats such as port scans, bot attacks, and zero-day exploits.

Reference: Check Point R81 Firewall Administration Guide, Check Point R81 Threat Prevention Administration Guide

QUESTION 201

When changes are made to a Rule base, it is important to _____ to enforce changes.

- A. Publish database
- B. Activate policy
- C. Install policy
- D. Save changes

Correct Answer: A

Section:

Explanation:

When changes are made to a Rule base, it is important to Publish database to enforce changes. Publishing database saves the changes to the database and makes them available to other administrators. Installing policy applies the changes to the Security Gateways.

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

QUESTION 202

The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?

- A. The Smart Licensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
- B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
- C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.
- D. The cpinfo command must be run on the firewall with the switch -online-license-activation.

Correct Answer: C

Section:

Explanation:

The Online Activation method is available for Check Point manufactured appliances. The administrator uses the Online Activation method by using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts. This method requires internet access and a valid User Center account.

Reference: [Check Point Licensing and Contract Operations User Guide], [Check Point R81 Gaia Installation and Upgrade Guide]

QUESTION 203

Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

- A. Manual NAT can offer more flexibility than Automatic NAT.
- B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
- C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
- D. Automatic NAT can offer more flexibility than Manual NAT.

Correct Answer: A

Section:

Explanation:

Manual NAT can offer more flexibility than Automatic NAT because it allows the administrator to define the NAT rules in any order and position¹. Automatic NAT creates the NAT rules automatically and places them at the top or bottom of the NAT Rule Base².

Reference: Check Point R81 Firewall Administration Guide, Check Point R81 Security Management Administration Guide

