100% Money Back Guarantee

**Vendor:**CheckPoint

**Exam Code:**156-215.81

**Exam Name:**Check Point Certified Security Administrator R81

**Version:**Demo

**QUESTION 1**

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

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 analysis. The other options are not the purpose of a clean-up rule. References: Clean-up Rule,

---

**QUESTION 2**

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

The correct answer is A because session unique identifiers are passed to the web api using the X-chkp-sid http header option. The X-chkp-sid header is used to authenticate and authorize API calls. The other options are not related to session unique identifiers. References: Check Point R81 Security Management Administration Guide

---

**QUESTION 3**

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

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. References: INSTALLATION AND UPGRADE GUIDE R81.10, Chassis R81 Installation and Upgrade Guide, Check Point R81.10

---

**QUESTION 4**

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

A. Firewall

B. Application Control

C. Anti-spam and Email Security

D. Anti-Virus

Correct Answer: D

Anti-Virus is the Check Point software blade that prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud. Anti-Virus scans files and email attachments for viruses, worms, trojans, and other types of malware. It also uses ThreatCloud, a collaborative network that delivers real- time dynamic security intelligence, to detect unknown malware based on their behavior. Firewall is a software blade that enforces security policy by inspecting and controlling network traffic. Application Control is a software blade that enables administrators to control access to web applications. Anti-spam and Email Security is a software blade that protects email infrastructure from spam, phishing, and malware attacks.

---

**QUESTION 5**

What needs to be configured if the NAT property `Translate destination on client side\\' is not enabled in Global properties?

A. A host route to route to the destination IP

B. Use the file local.arp to add the ARP entries for NAT to work

C. Nothing, the Gateway takes care of all details necessary

D. Enabling `Allow bi-directional NAT\\' for NAT to work correctly

Correct Answer: C

If the NAT property `Translate destination on client side\\' is not enabled in Global properties, nothing needs to be configured on the client side, because the Gateway takes care of all details necessary. The Gateway translates the destination IP address before sending the packet to the client, so the client does not need to know about the NAT rule or add any host route or ARP entry. References: Check Point Security Engineering Study Guide, p. 136-137

---

**QUESTION 6**

You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

A. Open SmartLog and connect remotely to the wireless controller

B. Open SmartEvent to see why they are being blocked

C. Open SmartDashboard and review the logs tab

D. From SmartConsole, go to the Log and Monitor and filter for the IP address of the tablet.

Correct Answer: D

From SmartConsole, go to the Log and Monitor and filter for the IP address of the tablet is the correct answer. This is because the Log and Monitor view in SmartConsole allows you to view and analyze logs and events from various sources, such as Security Gateways, Security Management Servers, and SmartEvent Servers. You can use filters to search for specific logs and events based on different criteria, such as source IP, destination IP, action, time, etc. References: [Logging and Monitoring Administration Guide R80.20]

---

**QUESTION 7**

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

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 8**

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

A. IPS blade

B. IPSEC VPN Blade

C. Identity Awareness Blade

D. Firewall Blade

Correct Answer: A

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

---

**QUESTION 9**

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

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. References: [Check Point R81 Threat Prevention Administration Guide], page 9.

---

**QUESTION 10**

John is using Management HA. Which Smartcenter should be connected to for making changes?

A. secondary Smartcenter

B. active Smartcenter

C. connect virtual IP of Smartcenter HA

D. primary Smartcenter

Correct Answer: B

The SmartCenter that should be connected to for making changes is the active SmartCenter. The active SmartCenter is the one that is currently synchronizing its configuration with the secondary SmartCenter and handling the communication with the gateways . The primary SmartCenter is the one that was initially configured as the main server, but it may become inactive if a failover occurs. The virtual IP of SmartCenter HA is used to access the SmartConsole, not to make changes. References: [Security Management Server High Availability (HA) R81 Administration Guide], [], [How to configure ClusterXL High Availability on Security Management Server]

---

**QUESTION 11**

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

The port used for full synchronization between cluster members is TCP port 265. 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. References: How does the Cluster Control Protocol function in working and failure scenarios for gateway clusters?

---

**QUESTION 12**

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

A. Next Generation Threat Prevention

B. Next Generation Threat Emulation

C. Next Generation Threat Extraction

D. Next Generation Firewall

Correct Answer: B

The Next Generation Threat Emulation software blade package uses CPU-level and OS- level sandboxing in order to detect and block malware, p. 41. It emulates files in a virtual environment and inspects their behavior for malicious activity. , Check Point Threat Emulation Administration Guide R81