Free Questions for 156-215.81 by certscare

Shared by Hayden on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Accept Rule and Drop Rule

B- Cleanup Rule and Stealth Rule

C- Explicit Rule and Implied Rule

D- NAT Rule and Reject Rule

Answer:

B

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 2

Question Type: MultipleChoice

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

Options:

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.

Answer:

B

Explanation:

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway doesshare 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 3

Question Type: MultipleChoice

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

Options:

A- Access Control

B- Threat Emulation

C- Threat Prevention

D- QoS

Answer:

D

Explanation:

The policy type that is used to enforce bandwidth and traffic control rules isQoS. 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 4

Question Type: **MultipleChoice**

When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

Options:

A- SmartView Monitor should be opened and then the SAM rule/s can be applied immediately. Installing policy is not required.

B- The policy type SAM must be added to the Policy Package and a new SAM rule must be applied. Simply Publishing the changes applies the SAM rule on the firewall.

C- The administrator must work on the firewall CLI (for example with SSH and PuTTY) and the command 'sam block' must be used with the right parameters.

D- The administrator should open the LOGS & MONITOR view and find the relevant log. Right clicking on the log entry will show the Create New SAM rule option.

Answer:

A

Explanation:

When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, the administrator needs to take the following action: SmartView Monitor should be opened and then the SAM rule/s can be applied immediately. Installing policy is not required. SAM stands for Suspicious Activity Monitoring and is a feature that allows administrators to block or limit connections from specific sources or destinations without modifying the security policy. SAM rules can be created from SmartView Monitor or SmartEvent based on real-time network activity or security events. Reference: [Check Point R81 SmartView Monitor Administration Guide]

Question 5

Question Type: MultipleChoice

Fill in the blanks: The _____ collects logs and sends them to the _____.

Options:

A- Log server; Security Gateway

B- Log server; security management server

C- Security management server; Security Gateway

D- Security Gateways; log server

Answer:

D

Explanation:

TheSecurity Gatewayscollect logs and send them to thelog server. The Security Gateways are the components that enforce the security policy on network traffic and generate logs for each connection that matches a rule with a tracking option. The log server is the component that receives and stores the logs from the Security Gateways and provides a centralized interface for viewing and analyzing

them. The log server can be either a dedicated server or integrated with the Security Management Server. Reference: [Check Point R81 Security Management Administration Guide]

Question 6

Question Type: MultipleChoice

Fill in the blanks: The Application Layer Firewalls inspect traffic through the _____ layer(s) of the TCP/IP model and up to and including the _____ layer.

Options:

A- Upper; Application

B- First two; Internet

C- Lower; Application

D- First two; Transport

Answer:

C

Explanation:

The Application Layer Firewalls inspect traffic through theLowerlayer(s) of the TCP/IP model and up to and including theApplicationlayer. The lower layers are the Physical, Data Link, and Network layers, which deal with the transmission and routing of packets. The Application layer is the highest layer of the TCP/IP model, which provides services and protocols for specific applications such as HTTP, FTP, SMTP, etc. The Application Layer Firewalls can inspect the content and context of the traffic and enforce granular security policies based on various criteria such as user identity, application identity, content type, etc. Reference: [Check Point R81 Firewall Administration Guide]