Question 1

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

Options:

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.

Answer:

B

Question 2

What are two basic rules Check Point recommends 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

Question 3

Question Type: MultipleChoice

Which command is used to add users to or from existing roles'?

Options:

A) add rba user <User Name> roles <List>

B) add user <User Name>

C) add rba user <User Name>

D) add user <User Name> roles <List>

Answer:

A

Question 4

Question Type: **MultipleChoice**

What is the order of NAT priorities'?

Options:

A) IP pool NAT static NAT. hide NAT

B) Static NAT hide NAT, IP pool NAT

C) Static NAT, IP pool NAT hide NAT

D) Static NAT automatic NAT hide NAT

Answer:

C

Question 5

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.

If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.

Which of the following is the BEST for this behavior?

Options:

A) The setting Log does not capture this level of detail for GRE. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.

B) The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE sessions. This is a known issue with GRE. Use IPSEC instead of the non-standard GRE protocol for encapsulation.

C) The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracker. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.

D) The Log Server is failing to log GRE traffic properly because it is VPN traffic. Disable all VPN configuration to the partner site to enable proper logging.
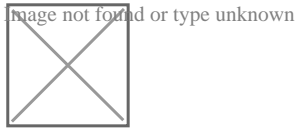
Answer:

C

Question 6

Question Type: MultipleChoice

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.

Image not found or type unknown

What is the possible for this?

Options:

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.

Answer:

B

Question 7

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

Options:

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.

Answer:

B

Question 8

Question Type: **MultipleChoice**

What is the order of NAT priorities'?

A) IP pool NAT static NAT. hide NAT

B) Static NAT hide NAT, IP pool NAT

C) Static NAT, IP pool NAT hide NAT

D) Static NAT automatic NAT hide NAT

Answer:

C

Question 9

Question Type: MultipleChoice

What are two basic rules Check Point recommends 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