156-215

Check Point Security Administration NGX

DEMO

QUESTION NO: 1

What are the results of the command: fw sam [Target IP Address]?

A. Connections to the specified target are blocked without the need to change the Security Policy
B. Connections to and from the specified target are blocked without the need to change the Security Policy
C. The Security Policy is compiled and installed on the target's embedded VPN/FireWall Modules
D. Connections from the specified target are blocked without the need to change the Security Policy

Answer: B

QUESTION NO: 2

The command fw fetch causes the:

A. Security Gateway to retrieve the user database information from the tables on theSmartCenter Server.
B. SmartCenter Server to retrieve the debug logs of the target Security Gateway
C. Security Gateway to retrieve the compiled policy and inspect code from theSmartCenter Server and install it to the kernel.
D. SmartCenter Server to retrieve the IP addresses of the target Security Gateway

Answer: C

QUESTION NO: 3

Which of the following deployment scenarios CANNOT be managed by Check Point QoS?

A. Two lines connected directly to the Gateway through a hub
B. Two lines connected to separate routers, and each router is connected to separate interfaces on the Gateway
C. One LAN line and one DMZ line connected to separate Gateway interfaces
D. Two lines connected to a single router, and the router is connected directly to the Gateway

Answer: D

QUESTION NO: 4

Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services. The Gateway does not allow Telnet service to itself from any location. How

would you set up the authentication method? With a:

A. Session Authentication rule
B. Client Authentication rule using the manual sign-on method, using HTTP on port 900
C. Client Authentication for fully automatic sign on
D. Client Authentication rule, using partially automatic sign on

Answer: B

QUESTION NO: 5

You must set up SIP with a proxy for your network. IP phones are in the 172.16.100.0 network. The Registrar and Proxy are installed on the host, 172.16.101.100. To allow handover enforcement for outbound calls from SIP-net to the Internet, you have defined the following objects:

Network object: SIP-net: 172.16.100.0/24

SIP-gateway: 172.16.101.100

VoIP Domain object: VoIP_domain_A

End-point domain: SIP-net

VoIP gateway installed at: SIP-gateway host object

How would you configure the rule?

A. VoIP_domain_A / any / sip_any / accept
B. VoIP_Gateway_A / any / sip / accept
C. Unsupported because the SIP Registrar and the SIP Proxy are installed on the same host. Separate and create two VoIP Domain objects.
D. SIP-net & SIP-gateway / any / sip / accept

Answer: A

QUESTION NO: 6

A _____ rule is used to prevent all traffic going to the VPN-1 NGX Security Gateway

A. Stealth

B. Cleanup

C. SmartDefense

D. Reject

Answer: A

QUESTION NO: 7

An advantage of using central vs local licensing is:

A. Only one IP address is used for all licenses.

B. Licenses are automatically attached to their respective Security Gateways.

C. The license must be renewed when changing the IP address of a Security Gateway.

D. A license can be taken from oneSmartCenter Server and given to SmartCenter Server.

Answer: A

QUESTION NO: 8

Which command allows verification of the Security Policy name and install date on a Security
Gateway?

A. fw ver -p

B. fw show policy

C. fw stat -l

D. fw ctl pstat -policy

Answer: C

QUESTION NO: 9

What command displays the version of an already installed Security Gateway?

A. cpstat -gw

B. fw printver

C. fw ver

D. fw stat

Answer: C