TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

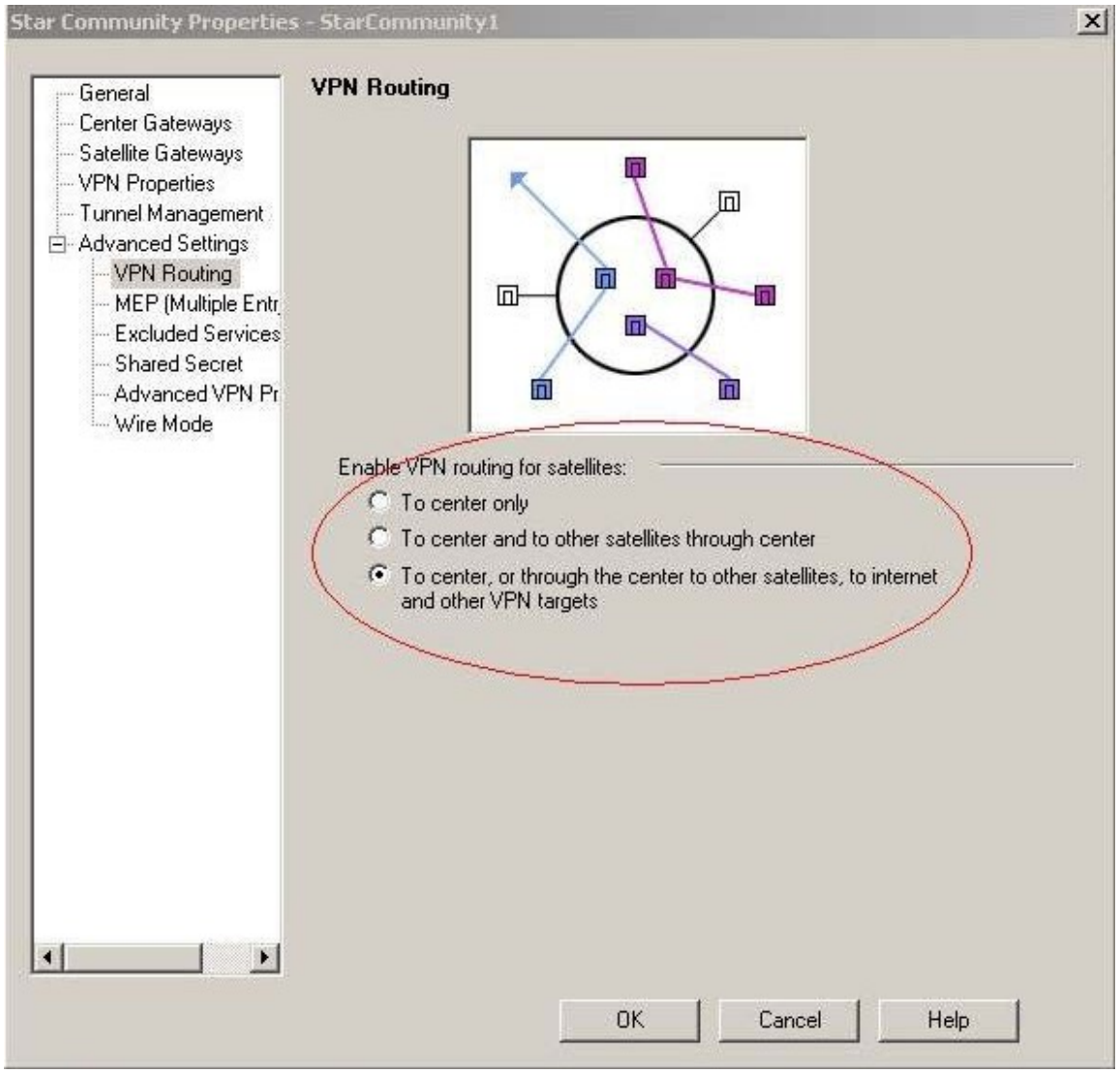
Exam : **156-315**

Title : Check Point Security Administration NGX II

Version : DEMO

1.You work a network administrator for KillTest .com. You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default
Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic passing through the QoS Module matches both rules, which of the following is true?
A. Neither rule will be allocated more than 10% of available bandwidth.
B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
C. 50% of available bandwidth will be allocated to the H.323 rule.
D. 50% of available bandwidth will be allocated to the Default Rule
E. Each H.323 connection will receive at least 512 Kbps of bandwidth.
Answer: B

2.KillTest .com has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 SecureClient users to access KillTest .com resources. For security reasons, KillTest .com's Secure policy requires all Internet traffic initiated behind the VPN-1 Edge gateways first be inspected by your headquarters' VPN-1 Pro Security Gateway. How do you configure VPN routing in this star VPN Community?



A. To the Internet an other targets only
B. To the center and other satellites, through the center
C. To the center only
D. To the center, or through the center to other satellites, then to the Internet and other VPN targets
Answer: D

3.You are preparing to configure your VoIP Domain Gatekeeper object. Which two other object should you have created first?
A. An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed.
B. An object to represent the PSTN phone network, AND an object to represent the IP phone network
C. An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed.
D. An object to represent the Q.931 service origination host, AND an object to represent the H.245 termination host

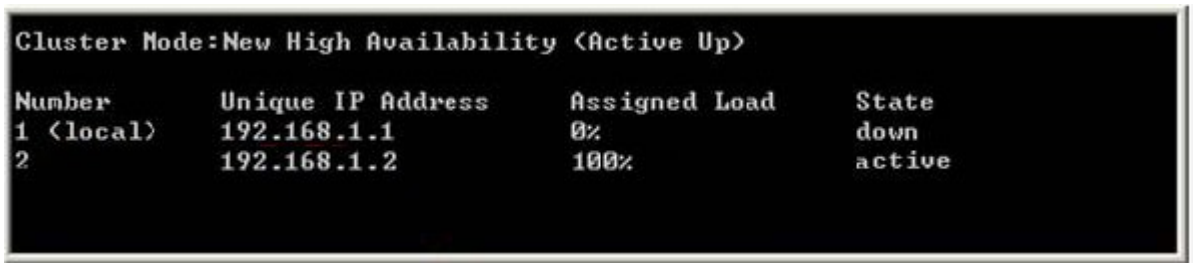
E. An object to represent the call manager, AND an object to represent the host on which the transmission router is installed.
Answer: C

4.Which Check Point QoS feature is used to dynamically allocate relative portions of available bandwidth?
A. Guarantees
B. Differentiated Services
C. Limits
D. Weighted Fair Queuing
E. Low Latency Queing
Answer: D

5.Which operating system is NOT supported by VPN-1 SecureClient?
A. IPSO 3.9
B. Windows XP SP2
C. Windows 2000 Professional
D. RedHat Linux 8.0
E. MacOS X
Answer: A

6.You want to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 Gateway to SecurePlatform NGX R60 via SmartUpdate.
Which package is needed in the repository before upgrading?
A. SVN Foundation and VPN-1 Express/Pro
B. VNP-1 and FireWall-1
C. SecurePlatform NGX R60
D. SVN Founation
E. VPN-1 Pro/Express NGX R60
Answer: C

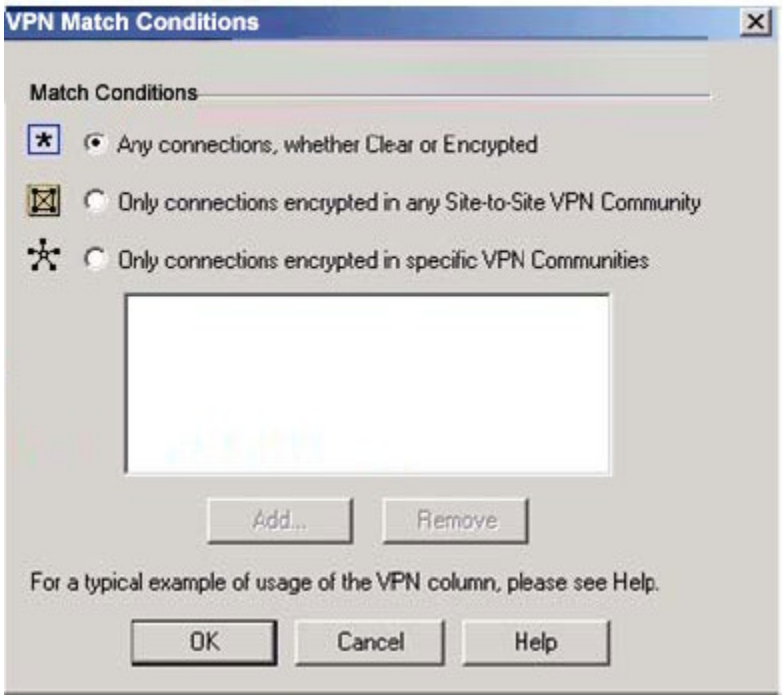
7.Exhibit:



The exhibit displays the cphaprob state command output from a New Mode High Availability cluster member.
Which machine has the highest priority?
A. 192.168.1.2, since its number is 2.
B. 192.168.1.1, because its number is 1.

C. This output does not indicate which machine has the highest priority.
D. 192.168.1.2, because its stats is active
Answer: B

8.Exhibit:



KillTest tries to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. KillTest sees the screen displayed in the exhibit.
What is the problem?
A. Jack must enable directional_match(true) in the object_5_0.c file on SmartCenter server.
B. Jack must enable Advanced Routing on each Security Gateway
C. Jack must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
D. Jack must enable a dynamic-routing protocol, such as OSPF, on the Gateways.
E. Jack must enable VPN Directional Match on the gateway object's VPN tab.
Answer: C

9.Where can a Security Administator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?
A. Global Properties
B. QoS Class objects
C. Check Point gateway object properties
D. $CPDIR/conf/qos_props.pf
E. Advanced Action options in each QoS rule.
Answer: A

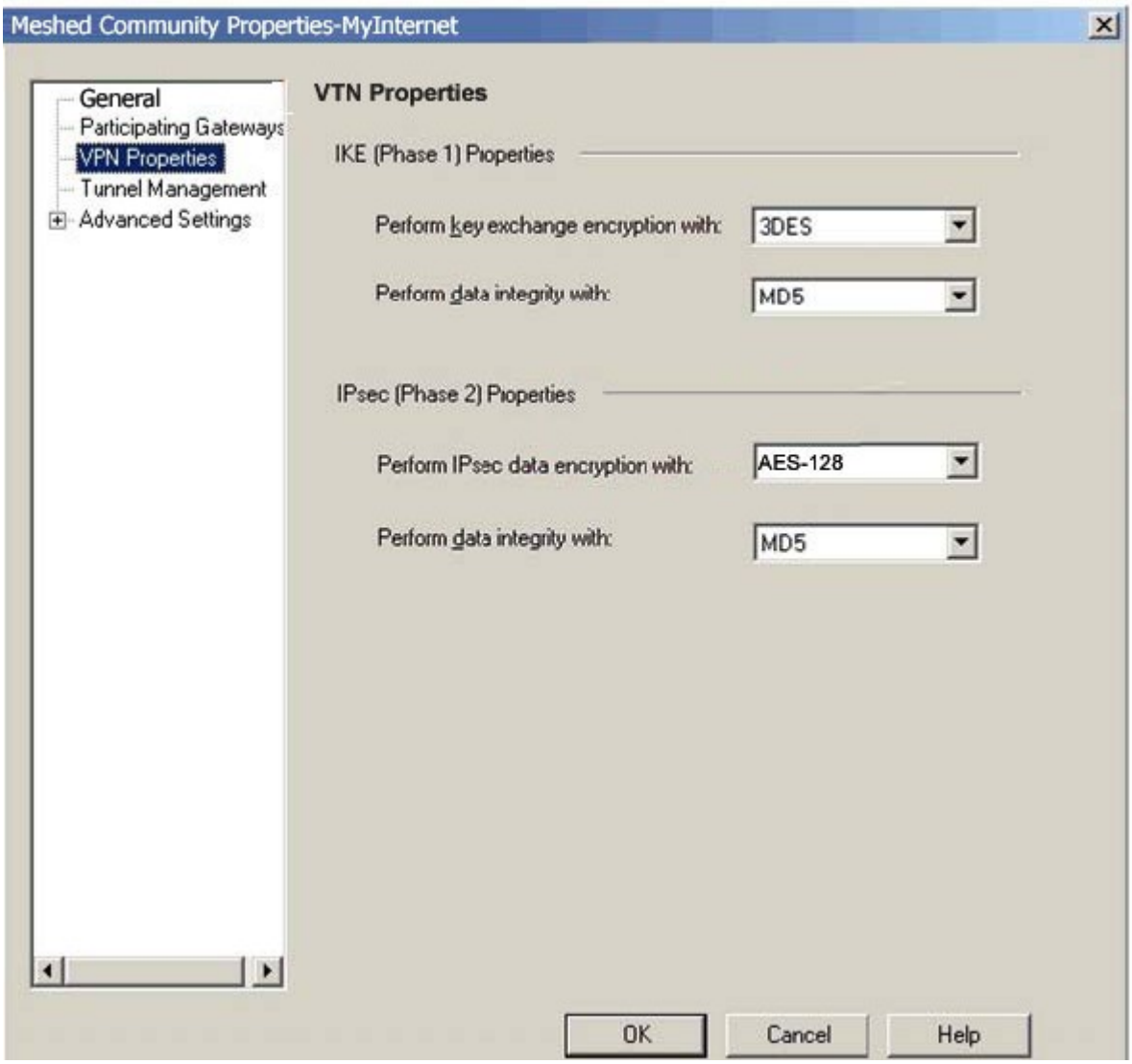
10.KillTest is the Security Administrator for KillTest .com. KillTest .com FTP servers have old hardware and software. Certain FTP commands cause the FTP

servers to malfunction. Upgrading the FTP Servers is not an option this time.
Which of the following options will allow KillTest to control which FTP
commands pass through the Security Gateway protecting the FTP servers?
A. Global Properties->Security Server ->Security Server->Allowed FTP Commands
B. SmartDefense->Application Intelligence->FTP Security Server
C. Rule Base->Action Field->Properties
D. Web Intelligence->Application Layer->FTP Settings
E. FTP Service Object->Advanced->Blocked FTP Commands
Answer: B

11.You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway, bound for all site-to-site VPN Communities, including Remote Access Communities.
How should you configure the VPN match rule
A. internal_clear>All-GwToGw
B. Communities>Communities
C. Internal_clear>External_Clear
D. Internal_clear>Communities
E. Internal_clear>All_communities
Answer: E

12.You receive an alert indicating a suspicious FTP connection is trying to connect to one of your internal hosts. How do you block the connection in real time and verify the connection is successfully blocked?
A. Highlight the suspicious connection in SmartView Tracker>Active mode. Block the connection using Tools>Block Intruder menu. Use the active mode to confirm that the suspicious connection does not reappear.
B. Highlight the suspicious connection in SmartView Tracker>Log mode. Block the connection using Tools>Block Intruder menu. Use the Log mode to confirm that the suspicious connection does not reappear.
C. Highlight the suspicious connection in SmartView Tracker>Active mode. Block the connection using Tools>Block Intruder menu. Use the active mode to confirm that the suspicious connection is dropped.
D. Highlight the suspicious connection in SmartView Tracker>Log mode. Block the connection using Tools>Block Intruder menu. Use the Log mode to confirm that the suspicious connection is dropped.
Answer: C

13.Exhibit:



KillTest is using a mesh VPN Community to create a site-to-site VPN. The VPN properties in this mesh Community is displayed in the exhibit.

Which of the following statements are true?

A. If Jack changes the settings, "Perform key exchange encryption with" from "3DES" to "DES", she will enhance the VPN Community's security and reduce encryption overhead.

B. Mrs Bill must change the data-integrity settings for this VPN Community. MD5 is incompatible with AES.

C. If KillTest changes the setting "Perform IPSec data encryption with" from "AES-128" to "3DES", Jack will increase the encryption overhead.

D. Her VPN Community will perform IKE Phase 1 key-exchange encryption, using the longest key VPN-1 NGX supports.

Answer: C

14.Exhibit:
You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the configurations displayed in the exhibit.
Are these machines correctly configured for a ClusterXL deployment?
A. Yes, these machines are configured correctly for a ClusterXL deployment.
B. No, QuadCards are not supported with ClusterXL.
C. No, all machines in a cluster must be running on the same OS.
D. No, al cluster must have an even number of machines.
E. No, ClusterXL is not supported on Red Hat Linux.
Answer: C

15.You want only RAS signals to pass through H.323 Gatekeeper and other H.323 protocols, passing directly between end points. Which routing mode in the VoIP Domain Gatekeeper do you select?
A. Direct
B. Direct and Call Setup
C. Call Setup
D. Call Setup and Call Control
Answer: A

16.KillTest is concerned that a denial-of-service (DoS) attack may affect her VPN Communities. She decides to implement IKE DoS protection. Jack needs to minimize the performance impact of implementing this new protectdion.
Which of the following configurations is MOST appropriate for Mrs. Bill?
A. Set Support IKE DoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless"
B. Set Support IKE DoS protection from identified source, and Support IKE DoS protection from unidentified soruce to "Puzzles"
C. Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "Puzzles".
D. Set Support IKE DoS protection from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".
E. Set Support IKE DoS protection from identified source to "Stateless", and Support

IKE DoS protection from unidentified source to "None".
Answer: D

17.You have a production implementation of Management High Availability, at Version VPN-1 NG with application Intelligence R55.
You must upgrade two SmartCenter Servers to VPN-1.
What is the correct procedure?
A. 1. Synchronize the two SmartCenter Servers
2. Upgrade the secondary SmartCenter Server.
3. Upgrade the primary SmartCenter Server.
4. Configure both SmartCenter Server host objects version to VPN-1 NGX
5. Synchronize the Servers again.
B. 1. Synchronize the two SmartCenter Servers
2. Perform an advanced upgrade the primary SmartCenter Server.
3. Upgrade the secondary SmartCenter Server.
4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
5. Synchronize the Servers again
C. 1. Perform an advanced upgrade on the primary SmartCenter Server.
2. Configure the primary SmartCenter Server host object to version VPN.1 NGX.
3. Synchronize the primary with the secondary SmartCenter Server.
4. Upgrade the secondary SmartCenter Server.
5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
6. Synchronize the Servers again.
D. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
4. Synchronize the two servers again.
5. Upgrade the secondary SmartCenter Server.
6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
7. Synchronize the Servers again.
Answer: A

18.In a distributed VPN-1 Pro NGX environment, where is the Internal Certificate Authority (ICA) installed?
A. On the Security Gateway
B. Certificate Manager Server
C. On the Policy Server
D. On the Smart View Monitor
E. On the primary SmartCenter Server
Answer: E

19.Assume an intruder has compromised your current IKE Phase 1 and Phase 2 keys. Which of the following options will end the intruder's access, after the next Phase 2 exchange occurs?

A. Phase 3 Key Revocation
B. Perfect Forward Secrecy
C. MD5 Hash Completion
D. SH1 Hash Completion
E. DES Key Reset
Answer: B

20.You set up a mesh VPN community, so your internal networks can access your partner's network, and vice versa. Your Security Policy encrypts only FTP and HTTP traffic through a VPN tunnel. All other traffic among your internal and partner networks is sent in clear text. How do you configure the VPN community?
A. Disable "accept all encrypted traffic", and put FTP and HTTP in the Excluded services in the Community object. Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field.
B. Disable "accept all encrypted traffic" in the Community, and add FTP and HTTP services to the Security Policy, with that Community object in the VPN field.
C. Enable "accept all encrypted traffic", but put FTP and HTTP in the Excluded services in the Community. Add a rule in the Security Policy, with services FTP and http, and the Community object in the VPN field.
D. Put FTP and HTTP in the Excluded services in the Community object. Then add a rule in the Security Policy to allow Any as the service with the Community object in the VPN field.
Answer: B