IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **156-315.1**

Title : Check Point Certified Security Expert NGX

Version : DEMO

1. Which of the following QoS rule-action properties is an Advanced action type, only available in Traditional mode?

A. Guarantee Allocation

B. Rule weight

C. Apply rule only to encrypted traffic

D. Rule limit

E. Rule guarantee
Answer: A

2. Which of the following commands shows full synchronization status?

A. cphaprob -i list

B. cphastop

C. fw ctl pstat

D. cphaprob -a if

E. fw hastat
Answer: A

3. Greg is creating rules and objects to control VoIP traffic in his organization, through a VPN-1 NGX Security Gateway. Greg creates VoIP Domain SIP objects to represent each of his organization's three SIP gateways. Greg then creates a simple group to contain the VoIP Domain SIP objects. When Greg attempts to add the VoIP Domain SIP objects to the group, they are not listed. What is the problem?

A. The related end-points domain specifies an address range.

B. VoIP Domain SIP objects cannot be placed in simple groups.

C. The installed VoIP gateways specify host objects.

D. The VoIP gateway object must be added to the group, before the VoIP Domain SIP object is eligible to be added to the group.

E. The VoIP Domain SIP object's name contains restricted characters.
Answer: B

4. The following rule contains an FTP resource object in the Service field:

Source: local_net Destination: Any Service: FTP-resource object Action: Accept

How do you define the FTP Resource Properties > Match tab to prevent internal users from sending corporate files to external FTP servers, while allowing users to retrieve files?

A. Enable the "Get" method on the match tab.

B. Disable "Get" and "Put" methods on the Match tab.

C. Enable the "Put" and "Get" methods.

D. Enable the "Put" method only on the match tab.

E. Disable the "Put" method globally.
Answer: A

5. You are preparing to configure your VoIP Domain Gatekeeper object. Which two other objects 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

6. Your current VPN-1 NG with Application Intelligence (AI) R55 stand-alone VPN-1 Pro Gateway and SmartCenter Server run on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the SmartCenter Server, and a new machine will be the VPN-1 Pro Gateway only. You need to migrate the NG with AI R55 SmartCenter Server configuration, including such items as Internal Certificate Authority files, databases, and Security Policies.

How do you request a new license for this VPN-1 NGX upgrade?

A. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new local license for the NGX VPN-1 Pro Gateway.

B. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new central license for the NGX VPN-1 Pro Gateway.

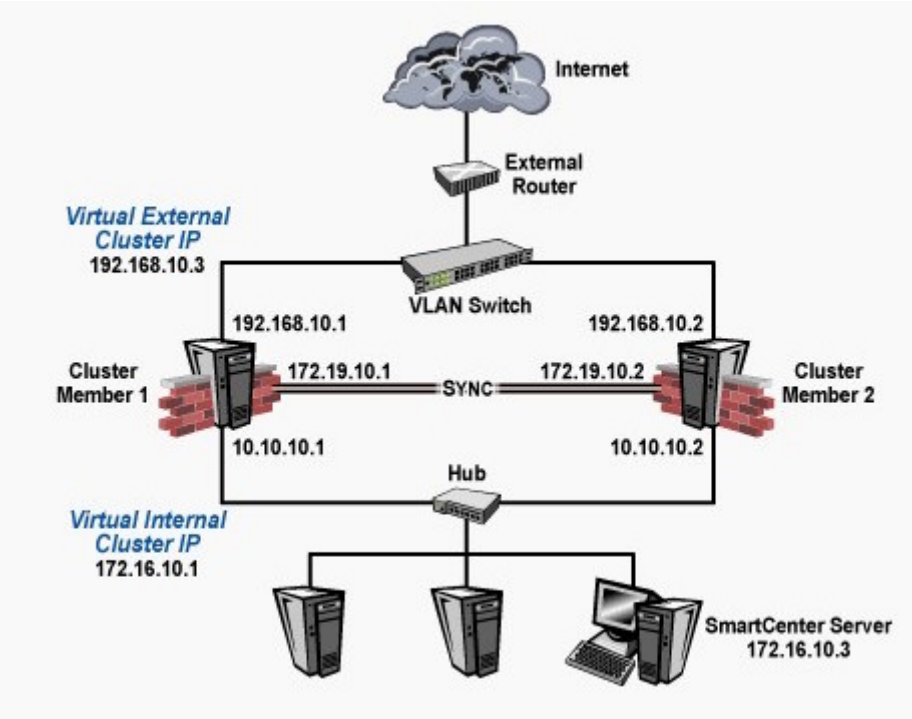
C. Request a new VPN-1 NGX SmartCenter Server license, using the NG with AI SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway.

D. Request a VPN-1 NGX SmartCenter Server license, using the NG with AI SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway, licensed for the existing SmartCenter Server IP address.
Answer: D

7. You are preparing a lab for a ClusterXL environment, with the following topology:

Vip internal cluster IP = 172.16.10.1; Vip external cluster IP = 192.168.10.3 Cluster Member 1: four NICs, three enabled: qfe0: 192.168.10.1/24, qfe1: 10.10.10.1/24, qfe2: 172.16.10.1/24Cluster Member 2: five NICs, three enabled; hme0: 192.168.10.2/24, eth1: 10.10.10.2/24, eth2: 172.16.10.2/24 Member Network tab on internal-cluster interface: is 10.10.10.0, 255.255.255.0 SmartCenter Pro Server: 172.16.10.3

External interfaces 192.168.10.1 and 192.168.10.2 connect to a Virtual Local Area Network (VLAN) switch. The upstream router connects to the same VLAN switch. Internal interfaces 10.10.10.1 and 10.10.10.2 connect to a hub. There is no other machine in the 10.10.10.0 network. 172.19.10.0 is the synchronization network. What is the problem with this configuration?



A. The SmartCenter Pro Server cannot be in the synchronization network.

B. There is no problem with this configuration. It is correct.

C. Members do not have the same number of NICs.

D. The internal network does not have a third cluster member.

E. Cluster members cannot use the VLAN switch. They must use hubs.
Answer: B

8. 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. VPN-1 and FireWall-1

C. SecurePlatform NGX R60

D. SVN Foundation

E. VPN-1 Pro/Express NGX R60
Answer: C

9. Which service type does NOT invoke a Security Server?

A. HTTP

B. FTP

C. Telnet

D. CIFS

E. SMTP
Answer: D

10. You want to upgrade a cluster with two members to VPN-1 NGX. The SmartCenter Server and both members are version VPN-1/FireWall-1 NG FP3, with the latest Hotfix. What is the correct upgrade procedure?

1. Change the version, in the General Properties of the gateway-cluster object.
2. Upgrade the SmartCenter Server, and reboot after upgrade.
3. Run cpstop on one member, while leaving the other member running. Upgrade one member at a time, and reboot after upgrade.
4. Reinstall the Security Policy.

A.3,2, 1, 4

B.2, 4, 3, 1

C.1, 3, 2, 4

D.2,3, 1, 4

E.1, 2, 3, 4
Answer: D

11. To change an existing ClusterXL cluster object from Multicast to Unicast mode, what configuration change must be made?

A. Change the cluster mode to Unicast on the cluster object. Reinstall the Security Policy.

B. Reset Secure Internal Communications (SIC) on the cluster-member objects. Reinstall the Security Policy.

C. Run cpstop and cpstart, to re-enable High Availability on both objects. Select Pivot mode in cpconfig.

D. Change the cluster mode to Unicast on the cluster-member object.

E. Switch the internal network's default Security Gateway to the pivot machine's IP address.
Answer: A

12. Robert has configured a Common Internet File System (CIFS) resource to allow access to the public partition of his company's file server, on \\erisco\goldenapple\files\public. Robert receives reports that users are unable to access the shared partition, unless they use the file server's IP address. Which of the following is a possible cause?

A. Mapped shares do not allow administrative locks.

B. The CIFS resource is not configured to use Windows name resolution.

C. Access violations are not logged.

D. Remote registry access is blocked.

E. Null CIFS sessions are blocked.
Answer: B

13. 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?

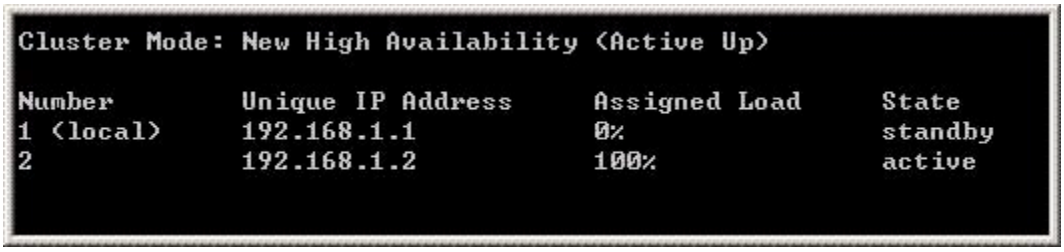
A. Disable "accept all encrypted traffic", and put FTP and HTTP in the Excluded services in the Community object. Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field.

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

14. The following is cphaprob state command output from a ClusterXL New mode High Availability member:When member 192.168.1.2 fails over and restarts, which member will become active?



A. 192.168.1.2

B. 192.168.1.1

C. Both members' state will be standby

D. Both members' state will be active
Answer: B

15. How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queues when using a Check Point QoS solution?

A. Low latency class

B. DiffServ rule

C. guaranteed per connection

D. Weighted Fair Queuing

E. guaranteed per VoIP rule
Answer: A

16. If you check the box "Use Aggressive Mode", in the IKE Properties dialog box:

A. The standard three-packet IKE Phase 1 exchange is replaced by a six-packet exchange.

B. The standard six-packet IKE Phase 2 exchange is replaced by a three-packet exchange.

C. The standard three-packet IKE Phase 2 exchange is replaced by a six-packet exchange.

D. The standard six-packet IKE Phase 1 exchange is replaced by a three-packet exchange.

E. The standard six-packet IKE Phase 1 exchange is replaced by a twelve-packet exchange.
Answer: D

17. Regarding QoS guarantees and limits, which of the following statements is FALSE?

A. The guarantee of a sub-rule cannot be greater than the guarantee defined for the rule above it.

B. If a guarantee is defined in a sub-rule, a guarantee must be defined for the rule above it.

C. A rule guarantee must not be less than the sum defined in the guarantees' sub-rules.

D. If both a rule and per-connection limit are defined for a rule, the per-connection limit must not be greater than the rule limit.

E. If both a limit and guarantee per rule are defined in a QoS rule, the limit must be smaller than the guarantee.
Answer: E

18. You are preparing to deploy a VPN-1 Pro Gateway for VPN-1 NGX. You have five systems to choose from for the new Gateway, and you must conform to the following requirements:

Operating-system vendor's license agreementCheck Point's license agreement Minimum operating-system hardware specificationMinimum Gateway hardware specification Gateway installed on a supported operating system (OS)

Which machine meets ALL of the following requirements?

A. Processor: 1.1 GHz RAM: 512 MB Hard disk: 10 GB OS: Windows 2000 Workstation

B. Processor: 2.0 GHz RAM: 512 MB Hard disk: 10 GB OS: Windows ME

C. Processor: 1.5 GHz RAM: 256 MB Hard disk: 20 GB OS: Red Hat Linux 8.0

D. Processor: 1.67 GHz RAM: 128 MB Hard disk: 5 GB OS: FreeBSD

E. Processor: 2.2 GHz RAM: 256 MB Hard disk: 20 GB OS: Windows 2000 Server
Answer: E

19. 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

20. VPN-1 NGX supports VoIP traffic in all of the following environments, EXCEPT which environment?

A. H.323

B. SIP

C. MEGACO

D. SCCP

E. MGCP
Answer: C

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.