



**133-S-713.4**

**Check Point Security Administration NGX II R65**

Q&A

DEMO Version

Copyright (c) 2010 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1**

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?

```
Cluster Mode: New High Availability (Active Up)
```

Number	Unique IP Address	Assigned Load	State
1 <local>	192.168.1.1	0%	standby
2	192.168.1.2	100%	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**

**QUESTION NO: 2**

What is the command to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 SmartCenter Server to VPN-1 NGX using a CD?

- A. cd patch add
- B. fwm upgrade\_tool
- C. cppkg add
- D. patchadd
- E. patch addcd

**Answer: E**

**QUESTION NO: 3**

You have a production implementation of Management High Availability, at version VPN-1 NG with Application Intelligence R55. You must upgrade your two SmartCenter Servers to VPN-1 NGX. 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 on 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: B**

#### **QUESTION NO: 4**

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Pro Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server, without making any changes to the existing primary SmartCenter Server? (Changes can include uninstalling and reinstalling.)

- A. You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- B. The new machine cannot be installed as the Internal Certificate Authority on its own.
- C. The secondary Server cannot be installed on a SecurePlatform Pro machine alone.
- D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server.

**Answer: A**

#### **QUESTION NO: 5**

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use four machines with the following configurations:

Cluster Member 1: OS: SecurePlatform. NICs: QuadCard. memory: 256 MB. Security Gateway

version: VPN-1 NGX

Cluster Member 2: OS: SecurePlatform, NICs: four Intel 3Com, memory: 512 MB, Security Gateway version: VPN-1 NGX

Cluster Member 3: OS: SecurePlatform, NICs: four other manufacturers, memory: 128 MB, Security Gateway version: VPN-1 NGX

SmartCenter Pro Server: MS Windows Server 2003, NIC: Intel NIC (one), Security Gateway and primary SmartCenter Server installed version: VPN-1 NGX

Are these machines correctly configured for a ClusterXL deployment?

- A. No, the SmartCenter Pro Server is not using the same operating system as the cluster members.
- B. Yes, these machines are configured correctly for a ClusterXL deployment.
- C. No, Cluster Member 3 does not have the required memory.
- D. No, the SmartCenter Pro Server has only one NIC.

**Answer: B**

#### **QUESTION NO: 6**

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**

#### **QUESTION NO: 7**

How does a standby SmartCenter Server receive logs from all Security Gateways, when an active SmartCenter Server fails over?

- A. The remote Gateways must set up SIC with the secondarySmartCenter Server, for logging.
- B. Establish Secure Internal Communications (SIC) between the primary and secondary Servers. The secondary Server can then receive logs from the Gateways, when the active Server fails over.
- C. On the Log Servers screen (from the Logs and Masters tree on the gateway object's General Properties screen), add the secondary SmartCenter Server object as the additional log server. Reinstall the Security Policy.
- D. Create a Check Point host object to represent the standby SmartCenter Server. Then select "Secondary SmartCenter Server" and Log Server", from the list of Check Point Products on the General properties screen.
- E. The secondary Server's host name and IP address must be added to the Masters file, on the remote Gateways.

**Answer: C**

#### **QUESTION NO: 8**

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**

#### **QUESTION NO: 9**

Which component functions as the Internal Certificate Authority for VPN-1 NGX?

- A. VPN-1 Certificate Manager
- B. SmartCenterServer
- C. SmartLSM
- D. Policy Server
- E. Security Gateway

**Answer: B**

#### **QUESTION NO: 10**

:

You are configuring the VoIP Domain object for a Skinny Client Control Protocol (SCCP)

environment protected by VPN-1 NGX. Which VoIP Domain object type can you use?

- A. CallManager
- B. Gatekeeper
- C. Gateway
- D. Proxy
- E. Transmission Router

**Answer: A**