



**156-215.1**

**Check Point Certified Security Administrator NGX**

Q&A

DEMO Version

Copyright (c) 2007 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 Frank wants to know why users on the corporate network cannot receive multicast transmissions from the Internet. An NGX Security Gateway protects the corporate network from the Internet. Which of the following is a possible cause for the connection problem?**

- A. NGX does not support multicast routing protocols and streaming media through the Security Gateway.
- B. Frank did not install the necessary multicast license with SmartUpdate, when he upgraded to NGX.
- C. The Multicast Rule is below the Stealth Rule. NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule.
- D. Multicast restrictions are not configured properly on the corporate internal network interface properties of the Security Gateway object.
- E. Anti-spoofing is enabled. NGX cannot pass multicast traffic, if anti-spoofing is enabled.

**Answer: D**

**Question No: 2 In NGX, what happens if a Distinguished Name (DN) is NOT found in LDAP?**

- A. NGX takes the common-name value from the Certificate subject, and searches the LDAP account unit for a matching user id.
- B. NGX searches the internal database for the username.
- C. The Security Gateway uses the subject of the Certificate as the DN for the initial lookup.
- D. If the first request fails or if branches do not match, NGX tries to map the identity to the user id attribute.
- E. When users authenticate with valid Certificates, the Security Gateway tries to map the identities with users registered in the external LDAP user database.

**Answer: B**

**Question No: 3 Gary is a Security Administrator in a small company. He needs to determine if the company's Web servers are accessed for an excessive number of times from the same host. How would he configure this setting in SmartDefense?**

- A. Successive multiple connections
- B. HTTP protocol inspection
- C. Successive alerts
- D. General HTTP worm catcher
- E. Successive DoS attacks

**Answer: A**

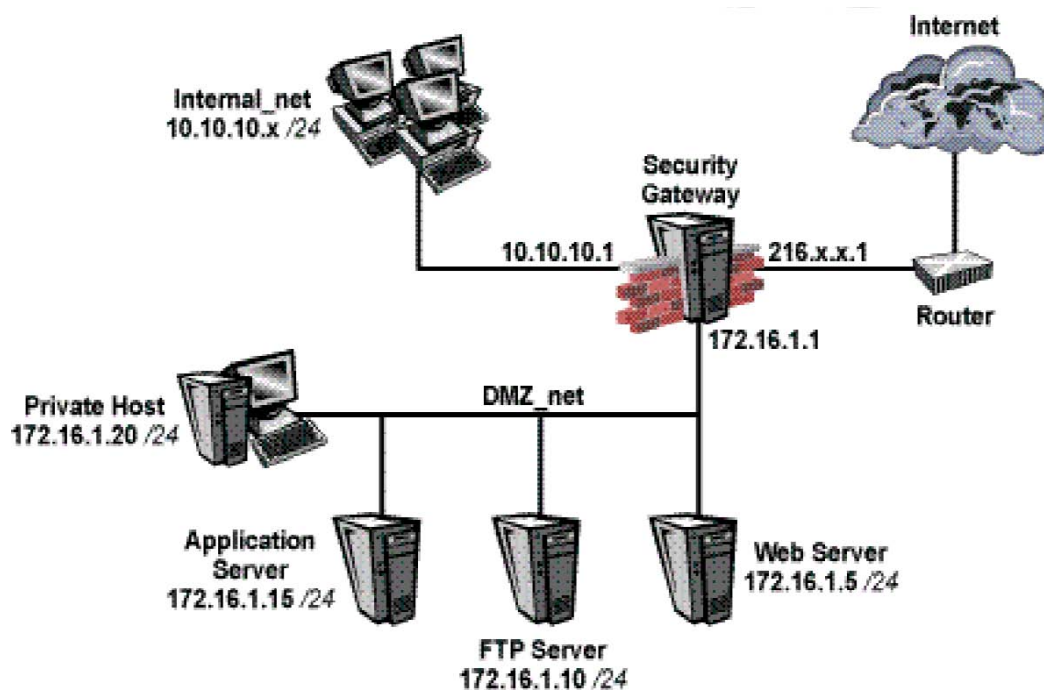
**Question No: 4** In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs. What can you do to keep old log files, when free space falls below 45 MB?

- A. Define a secondary SmartCenter Server as a log server, to transfer the old logs.
- B. Configure a script to archive old logs to another directory, before old log files are deleted.
- C. Do nothing. Old logs are deleted, until free space is restored.
- D. Use the fwm logexport command to export the old log files to other location.
- E. Do nothing. The SmartCenter Server archives old logs to another directory.

**Answer: B**

**Question No: 5** Brianna has three servers located in a DMZ, using private IP addresses. She wants internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal\_net 10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.

What is the best configuration for 10.10.10.x users to access the DMZ servers, using the DMZ servers' public IP addresses?



- A. Configure automatic Static NAT rules for the DMZ servers.
- B. Configure manual Static NAT rules to translate the DMZ servers, when connecting to the Internet.

- C. Configure manual static NAT rules to translate the DMZ servers, when the source is the internal network  
 Configure Hide NAT for the DMZ network behind the DMZ interface of the Security Gateway, when connecting to internal network 10.10.10.x.  
 Configure Hide NAT for 10.10.10.x behind DMZ's interface, when trying to access DMZ servers.

**Answer: C**

**Question No: 6 You are setting up a Virtual Private Network, and must select an encryption scheme. Network performance is a critical issue - even more so than the security of the packet. Which encryption scheme would you select?**

- A. In-place encryption
- B. Tunneling mode encryption
- C. Either one will work without compromising performance

**Answer: A**

**Question No: 7 Larry is the Security Administrator for a software-development company. To isolate the corporate network from the developers' network, Larry installs an internal Security Gateway. Larry wants to optimize the performance of this Gateway. Which of the following actions is most likely to improve the Gateway's performance?**

- A. Remove unused Security Policies from Policy Packages.
- B. Clear all Global Properties check boxes, and use explicit rules.
- C. Use groups within groups in the manual NAT Rule Base.
- D. Put the least-used rules at the top of the Rule Base.
- E. Use domain objects in rules, where possible.

**Answer: A**

**Question No: 8 If a digital signature is used to achieve both data-integrity checking and verification of sender, digital signatures are only used when implementing:**

- A. A symmetric encryption algorithm.
- B. CBL-DES.
- C. ESP.
- D. An asymmetric encryption algorithm.
- E. Triple DES.

**Answer: D**

**Question No: 9 Ellen is performing penetration tests against SmartDefense for her Web server farm. She needs to verify that the Web servers are secure against traffic hijacks. She has selected the "Products > Web Server" box on each of the node objects. What other settings would be appropriate? Ellen:**

- A. needs to configure TCP defenses such as "Small PMTU" size.
- B. should enable all settings in Web Intelligence.
- C. needs to create resource objects for the web farm servers and configure rules for the web farm.
- D. must activate the Cross-Site Scripting property.
- E. should also enable the Web intelligence > SQL injection setting.

**Answer: D**

**Question No: 10 Which of the following commands is used to restore NGX configuration information?**

- A. cpconfig
- B. cpinfo -i
- C. restore
- D. fwm dbimport
- E. upgrade\_import

**Answer: E**