



156-210

Check Point CCSA NG

Q&A

DEMO Version

Copyright (c) 2009 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.

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

Once you have installed Secure Internal Communications (SIC) for a host-node object and issued a certificate for it. Which of the following can you perform? Choose two.

- A. Rename the object
- B. Rename the certificate
- C. Edit the object properties
- D. Rest SIC
- E. Edit the object type

Answer: A,C

Explanation:

: Object can be renamed and the properties can be edited even after establishing the SIC and issue the certificate

Incorrect Answers:

- B: Once SIC has been established and a certificate has been issued, certificate can not be renamed
- D: If SIC is reset, the trust has to be re-established, hence this is wrong
- E: Type of the object created can not be modified once the certificate has been issued.

QUESTION NO: 2

You are a Security Administrator preparing to implement Hide NAT. You must justify your decision. Which of the following statements justifies implementing a Hide NAT solution? Choose two.

- A. You have more internal hosts than public IP addresses
- B. Your organization requires internal hosts, with RFC 1918-compliant addresses to be assessable from the Internet.
- C. Internally, your organization uses an RFC 1918-compliant addressing scheme.
- D. Your organization does not allow internal hosts to access Internet resources
- E. Internally, you have more public IP addresses than hosts.

Answer: A,C

QUESTION NO: 3

Which critical files and directories need to be backed up? Choose three

- A. \$FWDIR/conf directory
- B. rulebase_5_0.fws

- C. objects_5_0.c
- D. \$CPDIR/temp directory
- E. \$FWDIR/state directory

Answer: A,B,C

QUESTION NO: 4

Which of the following statements about the General HTTP Worm Catches is FALSE?

- A. The General HTTP Worm Catcher can detect only worms that are part of a URI.
- B. Security Administrators can configure the type of notification that will take place, if a worm is detected.
- C. SmartDefense allows you to configure worm signatures, using regular expressions.
- D. The General HTTP Worm Catcher's detection takes place in the kernel, and does not require a Security Server.
- E. Worm patterns cannot be imported from a file at this time.

Answer: A

QUESTION NO: 5

You are a Security Administrator attempting to license a distributed VPN-1/Firewall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which of the following must be considered when licensing the deployment? Choose two.

- A. Local licenses are IP specific.
- B. A license can be installed and removed on a VPN-1/Firewall-1 version 4.1, using SmartUpdate.
- C. You must contact Check Point via E-mail or telephone to create a license for an Enforcement Module.
- D. Licenses cannot be installed through SmartUpdate.
- E. Licenses are obtained through the Check Point User Center

Answer: A,E

QUESTION NO: 6

Which of the following are tasks performed by a VPN-1/FireWall-1 SmartCenter Server? Choose three.

- A. Examines all communications according to the Enterprise Security Policy.

- B. Stores VPN-1/FirWall-1 logs.
- C. Manages the User Database.
- D. Replicates state tables for high availability.
- E. Compiles the Rule Base into an enforceable Security Policy.

Answer: B,C,E

QUESTION NO: 7

You are a Security Administrator preparing to implement an address translation solution for Certpaper.com.

The solution you choose must meet the following requirements:RFC 1918-compliant internal addresses must be translated to public, external addresses when packets exit the Enforcement Module.Public, external addresses must be translated to internal, RFC 1918-compliant addresses when packets enter the Enforcement Module.

Which address translation solution BEST meets your requirements?

- A. Hide NAT
- B. The requirements cannot be met with any address translation solution.
- C. Dynamic NAT
- D. IP Pool Nat
- E. Static NAT

Answer: E

QUESTION NO: 8

Which of the following suggestions regarding Security Policies will NOT improve performance?

- A. If most incoming connections are HTTP, but the rule that accepts HTTP at the bottom of the Rule Base, before the Cleanup Rule
- B. Use a network object, instead of multiple host-node objects.
- C. Do not log unnecessary connections.
- D. Keep the Rule Base simple.
- E. Use IP address-range objects in rules, instead of a set of host-node objects.

Answer: A

QUESTION NO: 9

You are a Security Administrator attempting to license a distributed VPN-1/Firwall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which license type is the BEST for your deployment?

- A. Discretionary
- B. Remote
- C. Central
- D. Local
- E. Mandatory

Answer: C

QUESTION NO: 10

Network attacks attempt to exploit vulnerabilities in network applications, rather than targeting firewalls directly.

What does this require of today's firewalls?

- A. Firewalls should provide network-level protection, by inspecting packets all layers of the OSI model.
- B. Firewall should not inspect traffic below the Application Layer of the OSI model, because such inspection is no longer relevant.
- C. Firewalls should understand application behavior, to protect against application attacks and hazards.
- D. Firewalls should provide separate proxy processes for each application accessed through the firewall.
- E. Firewalls should be installed on all Web servers, behind organizations' intranet.

Answer: C