



156-515.65

Check Point Certified Security Expert Plus NGX 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.

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

Which files should be acquired from a Windows 2003 Server system crash with a Dr. Watson error?

- A. drwtsn32.log
- B. vmcore.log
- C. core.log
- D. memory.log
- E. info.log

Answer: A

QUESTION NO: 2

VPN debugging information is written to which of the following files?

- A. FWDIR/log/ahttd.elg
- B. FWDIR/log/fw.elg
- C. \$FWDIR/log/ike.elg
- D. FWDIR/log/authd.elg
- E. FWDIR/log/vpn.elg

Answer: C

QUESTION NO: 3

fw monitor packets are collected from the kernel in a buffer. What happens if the buffer becomes full?

- A. The information in the buffer is saved and packet capture continues, with new data stored in the buffer.
- B. Older packet information is dropped as new packet information is added.
- C. Packet capture stops.
- D. All packets in it are deleted, and the buffer begins filling from the beginning.

Answer: D

QUESTION NO: 4

Which file provides the data for the host_table output, and is responsible for keeping a record of all internal IPs passing through the internal interfaces of a restricted hosts licensed Security

Gateway?

- A. hosts.h
- B. external.if
- C. hosts
- D. fwd.h
- E. fwconn.h

Answer: D

QUESTION NO: 5

You modified the *.def file on your Security Gateway, but the changes were not applied. Why?

- A. There is more than one *.def file on the Gateway.
- B. You did not have the proper authority.
- C. *.def files must be modified on the SmartCenter Server.
- D. The *.def file on the Gateway is read-only.

Answer: C

QUESTION NO: 6

Assume you have a rule allowing HTTP traffic, on port 80, to a specific Web server in a Demilitarized Zone (DMZ). If an external host port scans the Web server's IP address, what information will be revealed?

- A. Nothing; the NGX Security Server automatically block all port scans.
- B. All ports are open on the Security Server.
- C. All ports are open on the Web server.
- D. The Web server's file structure is revealed.
- E. Port 80 is open on the Web server.

Answer: E

QUESTION NO: 7

Which of the following types of information should an Administrator use tcpdump to view?

- A. DECnet traffic analysis
- B. VLAN trunking analysis

- C. NAT traffic analysis
- D. Packet-header analysis
- E. AppleTalk traffic analysis

Answer: D

QUESTION NO: 8

Which statement is true for route based VPNs?

- A. IP Pool NAT must be configured on each gateway
- B. Route-based VPNs replace domain-based VPNs
- C. Route-based VPNs are a form of partial overlap VPN Domain
- D. Packets are encrypted or decrypted automatically
- E. Dynamic-routing protocols are not required

Answer: E

QUESTION NO: 9

The list below provides all the actions Check Point recommends to troubleshoot a problem with an NGX product.

- A. List Possible Causes
- B. Identify the Problem
- C. Collect Related Information
- D. Consult Various Reference Sources
- E. Test Causes Individually and Logically

Select the answer that shows the order of the recommended actions that make up Check Point's troubleshooting guidelines?

- F. B, C, A, E, D
- G. A, E, B, D, C
- H. A, B, C, D, E
- I. B, A, D, E, C
- J. D, B, A, C, E

Answer: A

QUESTION NO: 10

NGX Wire Mode allows:

- A. Peer gateways to establish a VPN connection automatically from predefined preshared secrets.
- B. Administrators to verify that each VPN-1 SecureClient is properly configured, before allowing it access to the protected domain.
- C. Peer gateways to fail over existing VPN traffic, by avoiding Stateful Inspection.
- D. Administrators to monitor VPN traffic for troubleshooting purposes.
- E. Administrators to limit the number of simultaneous VPN connections, to reduce the traffic load passing through a Security Gateway.

Answer: C