



www.chinatag.com

CHINATAG

CheckPoint 156-310

VPN-1/FireWall-1 Management II NG
CCSE

Q&A

DEMO Version

Copyright (c) 2003 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. Our IT certification products start at only **\$7.99**.

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 180 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

Users must enter a username and a password on the first attempt while using Secure Client Authentication window to connect to a site. Passwords are shared in memory instead of being written to disk, and are erased upon reboot.

- A. True
- B. False

Answer: A

COMMENTS: This is true, the passwords are saved in the Secure Client Daemon, instead of being written to disk, they are erased when you reboot. See Page 12.31 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 2

The IKE encryption scheme encrypts the original TCP and IP headers along with the packet data.

- A. True
- B. False

Answer: A

COMMENTS: IKE uses Tunneling-mode encryption, which work by encapsulating the entire packet, and then adding its own encryption protocol header to the encrypted packet. See Page 7.15 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 3

When licensing a VPN-1/Firewall-1 Management Server, for central licensing you must provide:

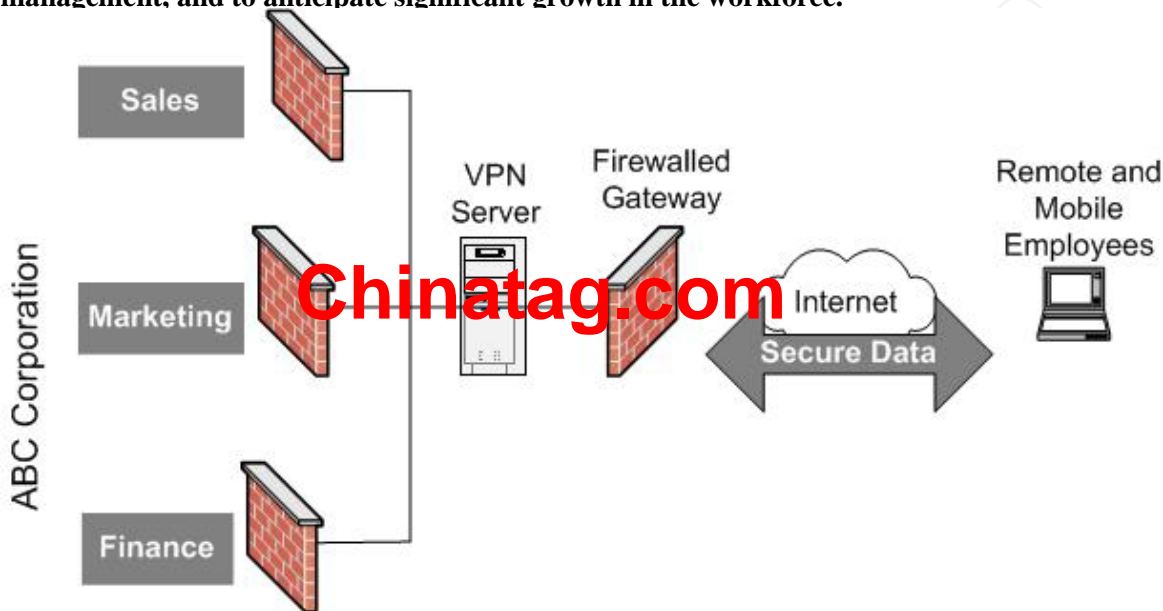
- A. A host IP address, license expiration date, product feature string and license key.
- B. A host IP address, license purchase date, product feature string and license key.
- C. A host IP address, license expiration date, product feature string and Certificate Authority Key.
- D. A host IP address, license purchase date, validation code and license key.
- E. A host IP address, number of firewall nodes, validation code and license key.

Answer: A

Explanation: As we can see in the licenses tab of the NG Configuration at "CPConfig", for the management server license at installation we have to provide the Host IP address, the expiration date of it, the features of the license and it's key, you can clearly see those fields when you provide license info. See Page L1.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 4

You are developing secure communications for a virtual corporation. There is a main office with a variety of shared resources, but most employees work either from home, or on the road. The most common interface between these employees and the central database is a modem-equipped Laptop. Reliability and quality are major issues for your users, and security requirements include the need for strong authentication of the remote and mobile users. You are expected to provide centralized management, and to anticipate significant growth in the workforce.



The type of VPN you would choose is the:

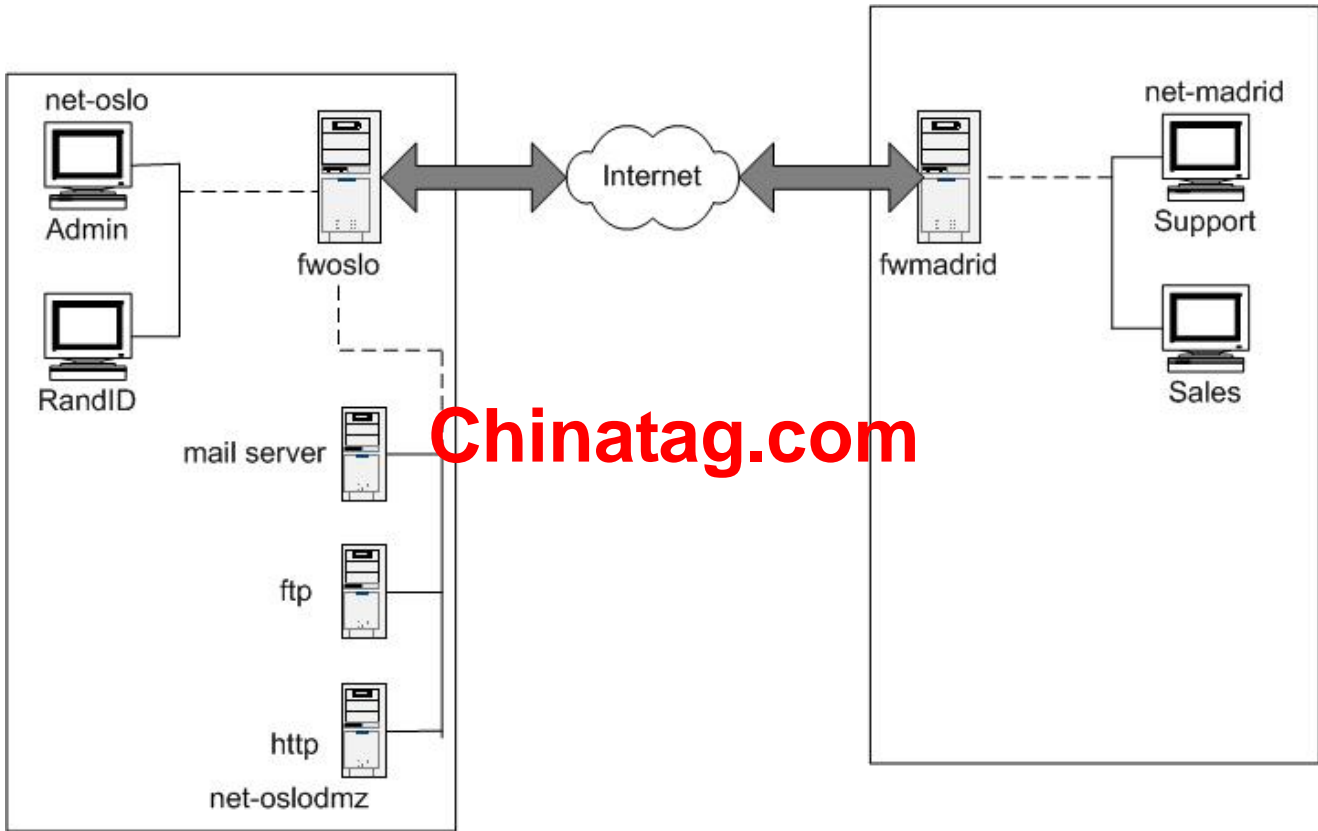
- A. Intranet VPN.
- B. Extranet VPN.
- C. Client-to-Firewall VPN.
- D. Server to Server VPN.
- E. None of the above.

Answer: B

COMMENTS: Since we want to provide centralized management and strong security, the best option is to set up a Extranet, this is a private network that makes use of Internet / Intranet technology to provide secure network connectivity through an extended network for external entities like vendors and workers. This extended network is usually behind a firewall and is viewed as part of an organization intranet. See Page 9.11 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 5

You are setting up an IKE VPN between the VPN-1/Firewall-1 modules protecting two networks. One network is using a RFC 1918 compliant address range of 10.15.0.0 and the other network is using a RFC 1918 compliant address range 192.168.9.0. What method of address translation would you use?



- A. Static Source.
- B. Static destination.
- C. Dynamic source.
- D. Dynamic
- E. None

Answer: A

COMMENTS: Since we have private, non-rutable addresses behind the firewall we need to use a method of address translation, because those hosts are located behind the firewall and need to receive connections from the other end of the firewall we need to use Static NAT, with it, the clients can make their packets leave with an address valid at the other side of the tunnel. See “Static Source NAT” at the NG Online Documentation.

QUESTION NO: 6

Secure Client supports desktop policies.

- A. True
- B. False

Answer: A

COMMENTS: Secure Client allows administrators to enforce desktop security policies on the network, and remotely enforce desktop security policies for remote users. A desktop policy is one security policy for all Secure Clients within a Policy Server's domain. Any secure Client not using the correct policy can be denied access. See Page 12.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 7

You are the VPN-1/Firewall-1 administrator for a company whose extranet requires encryption. You must use an encryption scheme with the following features:

Portability	Standard
Key Management Automatic, external PKI	
Session Keys	Change at configured times during a connection's life time

Which encryption scheme do you choose?

- A. Rijndael
- B. FWZ
- C. IKE
- D. IKE
- E. Triple DES.
- F. Manual IPsec.

Answer: C

COMMENTS: Those are features provided by IKE, it provides support for external PKI for the management of certificates and renewal of the session keys through the life of the connection, you can configure the interval, this info can be checked at Page 7.17 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 8

When adding users to firewall, an administrator can install just the User Database without re-installing the entire Security Policy.

- A. True
- B. False

Answer: A

COMMENTS: This is true, with the option "Install Users Database" you can propagate the users database defined in the management server to the selected modules. This option is available from both, the policy menu and the User Management function. Also note that the user database is also loaded when a security policy is published. See Syngress Book "Checkpoint NG - Next Generation Security Administration" Page 219.

QUESTION NO: 9

Both, RSA and Diffie-Hellman are asymmetric encryption techniques generating a one-way trust model for encryption and decryption messages.

- A. True
- B. False

Answer: B

COMMENTS: In checkpoint NG implementation, RSA is used to create and verify digital signatures in conjunction with HASH functions. In contrast to Diffie-Hellman, RSA key pairs are used for signing and verifying certificates. Diffie-Hellman is used for encrypting and decrypting messages. See Page 7.6 and 7.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 10

VPN-1/Firewall-1 gateway products (other than the GUI) are supported on Windows NT Workstation.

- A. True
- B. False

Answer: B

COMMENTS: Checkpoint NG Suite requires a Server based operating system for supporting the various components other than the GUI, for example the enforcement modules and the management module. Also remember, Windows NT workstation is limited to 10 concurrent connections, this is not suitable for any other component other than the GUI.

QUESTION NO: 11

For each connection that is established through a VPN-1/Firewall-1 Security Server, security administrators control specific access according to information defined in the Resource field.

- A. True
- B. False

Answer: A

COMMENTS: For each connection that is established through VPN1/Firewall1 Security Server, the administrator controls specific access through the use of Resources from the specified Server. A Resource specification defines a set of entities which can be acceded by a specified protocol, you can define resources based on HTTP, FTP and SMTP. When you specify a resource, the security server will transfer the

connection to a VCP or UFP server. See Page 5.4 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 12

When a SecuRemote Client and Server key exchange occurs, the user will be re-authenticated if the password has been erased.

- A. True
- B. False

Answer: A

COMMENTS: That's true, if the password has been deleted from the repository, every time there is a IKE (every 24 hours for one time password users) or FW1 key exchange (every hour for one time password users), the user must re-authenticate, this is because there is no way for the Client and the server to know that the connection is still valid. See "VPN Client - SecuRemote" chapter of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 13

There are certain general recommendations for improving the performance of Check Point VPN-1/Firewall-1, Choose all that apply.

1. Use Domain objects when possible.
2. User Network instead of Address Ranges.
3. Combine similar rules to reduce the number of rules.
4. Enable VPN-1/Firewall-1 control connections.
5. Keep Rule Base small and simple.

- A. 1, 2, 3.
- B. 1, 2, 4.
- C. 2, 3, 5.
- D. 1, 2, 3, 4, 5.
- E. 1, 3, 5.

Answer: C

COMMENTS: Since all the answers except "C" includes the use of Domain objects when possible, the answer C is obviously right. Domain objects are not recommended by checkpoint because they degrade performance with the name resolution and translation process. Of course, keeping the rule base simple and consolidating your similar rules is always a best practice. Also it's better to use Network objects because an address range is not always in continuous fashion.

QUESTION NO: 14

The **AES** algorithm (Rjindal) is used with IKE encryption, VPN-1/Firewall-1 supports which version of AES?

- A. 256-bit.
- B. 168 and 256-bit.
- C. 112-, 168- and 256-bit.
- D. 40- and 56-bits.
- E. 25- and 112-bit.

Answer: A

COMMENTS: The advanced encryption standard (AES) is the new FIPS publication that use US. Government organizations to protect sensitive information. The AES algorithm is “Rijndael”. A key length of 128 to 256 bits is supported. The more bits that are added, the stronger the encryption is. See Page 7.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 15

The Check Point Secure Client packaging tool enables system administrators:

- A. To create customized SecuRemote/Secure Client installation packages to distribute to users.
- B. To configure SecuRemote properties for users before installation.
- C. To customize the flow of end users’ installation processes before SecuRemote/Secure Client installation.
- D. A and B.
- E. All of the above.

Answer: E

COMMENTS: Secure Client Packaging Tool provides all of these features, you can customize the packages before the installation so the users don’t have to configurate ev erything themselves. It’s with this customization that the administrator is allowed to configure the SecuRemote properties before installation and control the flow of end user installation process. For example you can already define the site a user belongs without its intervention upon installation of the package. See Page 12.41 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 16

If you have modified your network configuration by removing the firewall adapters, you can reinstall these adapters by re-installing Secure Client.

- A. True
- B. False

Answer: B

COMMENTS: If you have modified your network configuration by removing FW1 Adapter, you can reinstall these adapters, without reinstalling secure client, by selecting Re-bind adapters from the tools menu. FW1 can be bound to more than one adapter, in Windows 98 the binding is static and takes place when Secure Client is installed, in Windows NT / 2000, the binding is dynamic and takes place upon reboot. See Page 12.35 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION NO: 17

Which of the following selections lists the three security components essential to guaranteeing the security of network connections?

- A. Encryption, inspection, routing.
- B. NAT, traffic control, topology.
- C. Static addressing, cryptosystems, spoofing.
- D. Encryption, authentication, integrity.
- E. DHCP, quality of service, IP pools.

Answer: D

COMMENTS: those 3 are the pillars of network security, with Encryption you can make the information visible only to the parties involved (the ones that have the decryption keys), everyone else will only see garbage, this provides privacy. With authentication you can validate that an entity is really it, authentication can be provided with something you have, something you know, or a combination of both. And with Integrity, you can validate that the information has not changed from source to destination, this could be achieved with the use of Digital Signatures. The best security is achieved with a combination of the 3.

QUESTION NO: 18

How do you enable connection logging to the Policy Server when using Secure Client?

- A. Go to the registry and add key EnableLogging=1.
- B. Create the file st.log in the log directory.
- C. Set logging to Alert in the Tracking field of the Rule Base.
- D. Enable logging in the Policy server.
- E. Select ;äEnable Logging; under options in the tool menu of the Secure Client GUI.

Answer: A