156-310

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

VPN-1/FireWall-1 Management ll NG

Version 1.2

Important Note
Please Read Carefully

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 for an update 3-4 days before you have scheduled the exam.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Login** (upper right corner)
3. Enter e-mail and password
4. The latest versions of all purchased products are downloadable from here. Just click the links.
   Note: If you have network connectivity problems it could be better to right-click on the link and choose **Save target as**. You would then be able to watch the download progress.

For most updates it enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state

1. Exam number and version.
2. Question number.
3. Order number and login ID.

We will answer your mail promptly.

Copyright

QUESTION NO: 1
Users must enter a username and a password on the first attempt while using SecureClient Authentication window to connect to a site. Passwords are shared in memory instead if being written to disk, and are erased upon reboot.

A. True
B. False

Answer: A

QUESTION NO: 2
The IKE encryption scheme encrypts the original TCP and IP headers along with the packet data.

A. True
B. False

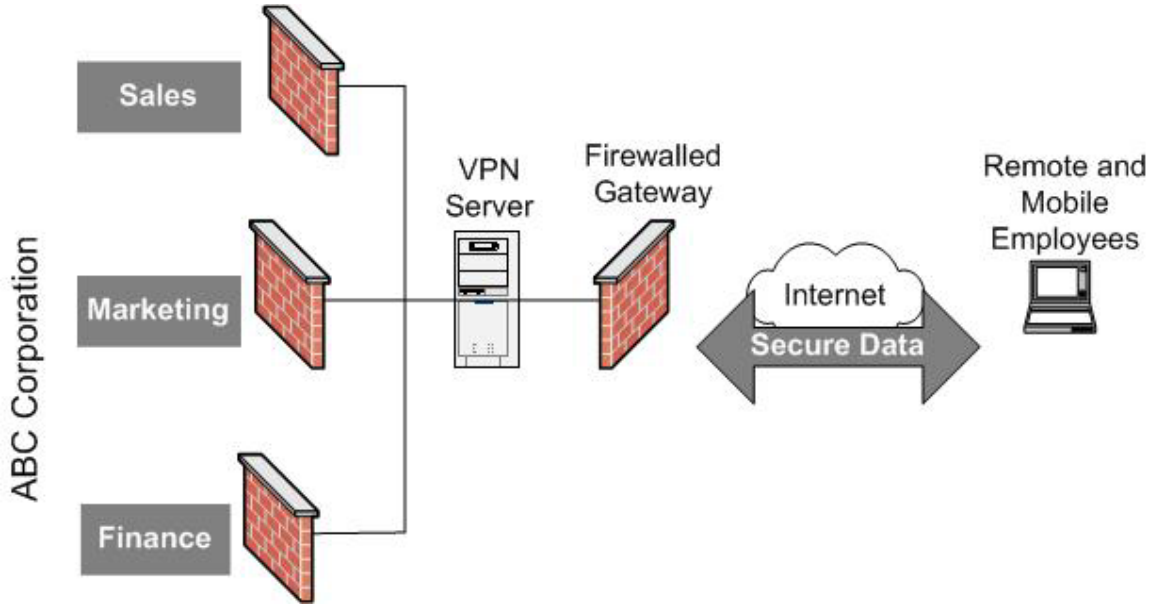
Answer: A

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

QUESTION NO: 4
You are developing secure communications for a virtual corporation. There is a main office with a variety of shared resources, but mist 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.

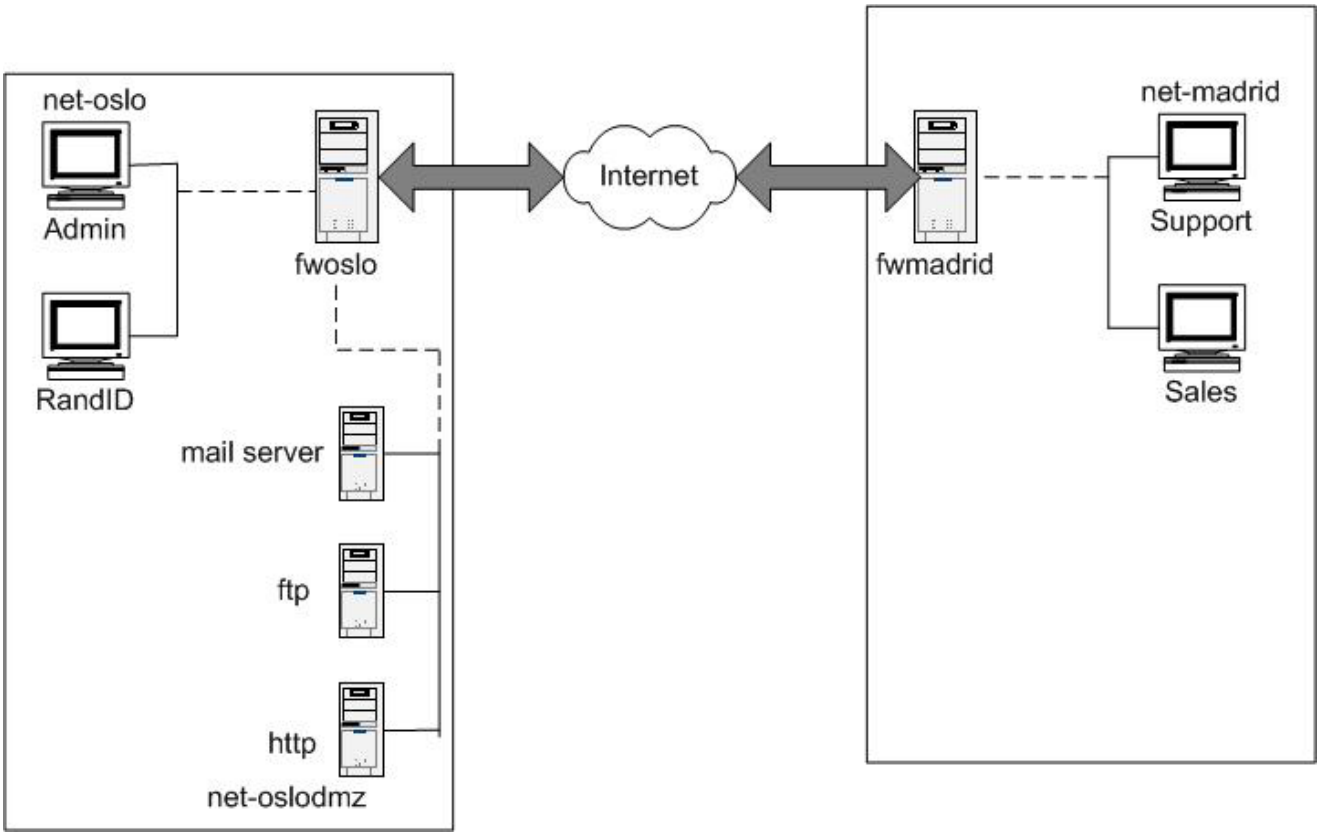


The type of VPN you would choose is the:

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

Answer: B

QUESTION NO: 5
You are setting up and 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 RFC1 818 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

QUESTION NO: 6
SecureClient supports desktop policies.

A. True
B. False

Answer: A

QUESTION NO: 7
You are the VPN-1/Firewall-1 administrator for a company whose extranet requires encryption. You must 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. Rj indal
B. FWZ
C. IKE
D. IKE
E. Triple DES.
F. Manual IPSec.

Answer: C

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

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

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

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

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

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

QUESTION NO: 14
The ABS 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

QUESTION NO: 15
The Check Point SecureClient packaging tool enables system administrators:

A. To create customized SecuRemote/SecureClient 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/SecureClient installation.
D. A and B.
E. All of the above.

Answer: E

QUESTION NO: 16
If you have modified your network configuration by removing the firewall adapters, you can reinstall these adapters by re-installing SecureClient.

A. True
B. False

Answer: B

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

QUESTION NO: 18
How do you enable connection logging to the Policy Server when using SecureClient?

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 ´Enable Logging´ under options in the tool menu of the SecureClient GUI.

Answer: A

QUESTION NO: 19
The encryption key for SecuRemote connections, for two phase exchange, remains valid by default for _____.

A. About 15 minutes.
B. About 30 minutes.
C. About 45 minutes.
D. About 60 minutes.
E. The entire remote user operating session.

Answer: A

QUESTION NO: 20
What is the purpose of HTML weeding when a defining a URI resource?

A. A HTML weeding changes specified code from an HTML page containing a reference to JAVA or ActiveX code.
B. HTML weeding strips JAVA code from incoming HTTP, and blocks JAVA applets.
C. HTML wedding stops applets when JAVA code is incorporated in a HTML document.
D. HTML weeding fetches JAVA code directly.
E. HTML weeding prompts users when a JAVA or ACTIVEX is available from an HTML page being viewed.

Answer: B

QUESTION NO: 21
When using IKE in a Firewall-to-Firewall VPN, _____ is used to manage session keys, encryption method and data integrity.

A. UDP
B. RDP
C. ICMP
D. FTP
E. RWS

Answer: B

QUESTION NO: 22
Before installing VPN-1/Firewall-1 on Windows NT, you MUST confirm that:

A. Your network is properly configured, with special emphasis on routing.
B. The host and the gateway can see each other.
C. X/Motif client is installed.
D. You can log on and TELNET to each of the hosts in the internal networks.
E. You have completed hardening your operating system.

Answer: A

QUESTION NO: 23
CRL lookups from VPN-1/Firewall-1 modules, or the SecuRemote Server, to the LDAP Server. When problems occur with CRL verification, how would you verify that the IP addresses and port numbers are correctly referencing the CA and LDAP Servers?

A. Check the **ca.ini** file.
B. Check the CA object configuration.
C. Check the CRL timeout.
D. Run **fw checkcaintegrity –f –n** from a command-line prompt.
E. Run **cpconfig**.

Answer: B

QUESTION NO: 24
What are the disadvantages of Shared Secret Key encryption?

A. A secure channel is required by which correspondents can agree on a key before their first encrypted communication.
B. Correspondents may have to agree on a key by some other fairly secure method, such as by mail or telephone.
C. The number of keys required can quickly become unmanageable since there must be a different key pair fir each pair of possible correspondents.
D. B and C.
E. A, B and C.

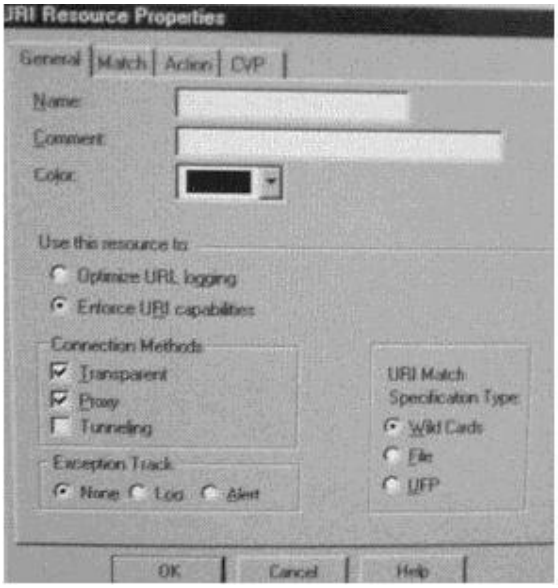
Answer: D

QUESTION NO: 25
An external UFP server, can perform which if the following?

A. Find out java, JavaScript, Active X.
B. Deny or allow access to URLs using categories.
C. Integrate Firewall-1 with an external user database.
D. Check for viruses and malicious contents.
E. All of the above.

Answer: B

QUESTION NO: 26
Which of the following statements best describe the purpose of the Transparent Connection method shown below in the URI Resources Properties window?



A. Matches all connections that are not in proxy or Tunneling Mode.
B. Matches connections in proxy mode only.
C. Matches connections using HTTP > CONNECT method.
D. Disables all content security options in the URI specification.
E. Takes an action as a result of a logged resource definition.

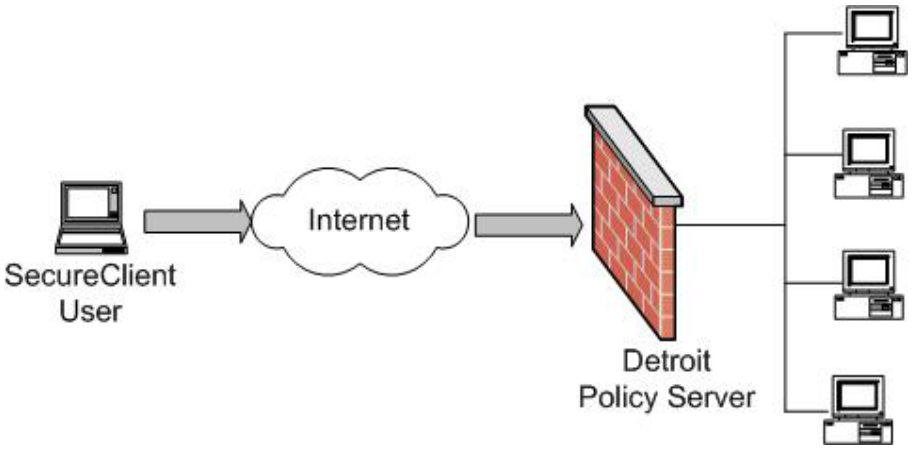
Answer: A

QUESTION NO: 27
When SecuRemote Client and Server key exchange occurs, the user will NOT be re-authenticated even if the Password Expires After timer on the SecuRemote Server has not expired.

A. True
B. False

Answer: A

QUESTION NO: 28
In the following graphic, the remote SecureClient machine does not have an installed Desktop Policy. The SecureClient user tries to connect to a host in Detroit's domain. Because Detroit is a Policy Server.



A. It will initiate explicit login and attempt to install a Desktop Policy on the SecureClient machine, before it allows a connection to its domain.
B. It will initiate implicit login and attempt to install a Desktop Policy on the SecureClient machine, before it allows a connection to its domain.
C. It will initiate implicit login only, before it allows a connection to its domain.
D. It will initiate explicit login only, before it allows a connection to its domain.
E. It will initiate implicit login and attempt to install a Desktop Policy on the SecuRemote machine, before it allows a connection to its domain.

Answer: A

QUESTION NO: 29
In the event that an unauthorized user attempts to compromise a valid SecureClient connection, the SecureClient machine can remain protected by?

A. The VPN module in the enterprise firewall.
B. Enforcing a desktop policy blocking incoming connections to the SecureClient.
C. The organization's internal firewall.
D. Network address translation performed by the gateway.
E. Using FWZ encapsulation.

Answer: B

QUESTION NO: 30
How do determine what version of firewall kernel a customer is using?

A. Fw ver.
B. Cp kernel.

C. Fw ver –k.
D. Fw kernel –v.
E. Cp cu –v.

Answer: C

QUESTION NO: 31
When you select the Pre-Shared Secret check box in the IKE Properties window:

A. The firewall can authenticate itself by a public-key signature.
B. The firewall can authenticate itself using SecuRemote only.
C. The firewall can authenticate itself by a pre-shared secret.
D. The firewall can authenticate itself using all standard and non-standard IKE authentication methods.
E. The firewall can authenticate itself using a modified pre-shared secret key.

Answer: C

QUESTION NO: 32
What is the Check Point recommended sequence for performing the following operations?

1. Install operating system.
2. Finish hardening the operating system.
3. Patch operating system.
4. Install firewall.
5. Patch firewall.

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

Answer: A

QUESTION NO: 33
To reduce the effectiveness of traffic sniffing inside the LAN, internal users should have the _____ installed in their desktop.

A. Management

B. Real Secure.
C. Enforcement
D. Policy Server.
E. SecureClient

Answer: E

QUESTION NO: 34
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

QUESTION NO: 35
If you wish to move any SecureClient files to another directory.

A. Uninstall and reinstall SecureClient first.
B. Restore the original files before uninstalling SecureClient.
C. Upgrade SecureClient, then uninstall and reinstall.
D. One of the above.

Answer: A

QUESTION NO: 36
You are installing Check Point VPN-1/Firewall-1 on a Windows NT platform. The machine will only be used to install policies on Enforcement Modules. No other machine in the network will perform the function. While installing the following installation screen of "VPN-1/Firewall-1 Enterprise Product" appears.

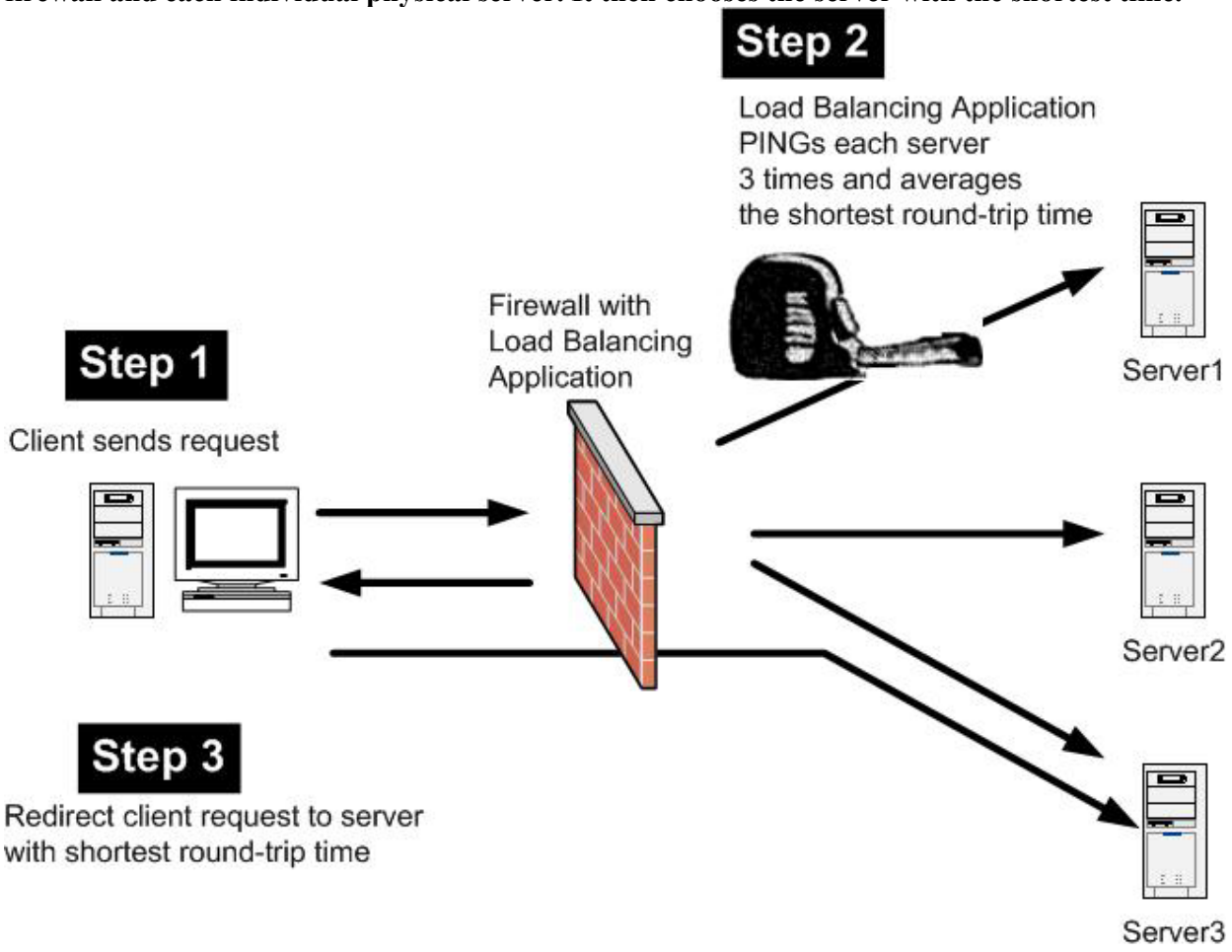
The screen shows "Please select the VPN-1/Firewall-1 Product Type you are about to install". Which option should you choose?

A. Enterprise Primary Management.

B. Enterprise Security Management.
C. Enforcement Module & Primary Management.
D. Enforcement Module.

Answer: A

QUESTION NO: 37
The _____ load balancing algorithm uses ICMP to determine the shortest time to and from the firewall and each individual physical server. It then chooses the server with the shortest time.



A. Server Load.
B. Router Load.
C. Round Trip
D. Round Robin
E. Domain

Answer: C

QUESTION NO: 38
Patrick has been hired to devise a security solution for a company that provides in-home care. Visiting Nurses use Internet connections to transmit confidential patient data to a database server located at the corporate office.
The visiting Nurses at the remote locations must have a secure connection to the database server to protect patient confidentiality. The database server itself must also be protected from external threats. The human resources department would like to have access to information about their Nurses access the database server. Accounting would like to offer Nurses the option of submitting their time sheets from remoter locations, provided this can be accomplished in a secure manner.

Patrick proposes installing Check Point VPN/Firewall-1 at the perimeter of the corporate LAN. He recommends installing Check Point SecureClient in the laptops used by the visiting Nurses. Patrick suggests rules allowing only client-authenticated traffic to the accounting server. To reduce resource consumption, Patrick advises his customer not to log any traffic passing through the Enforcement Module. Choose the one phrase below that best describes Patrick's proposal.

A. The proposed solution meets the required objectives and none of the desired objectives.
B. The proposed solution meets the required objectives and only one of the desired objectives.
C. The proposed solution meets the required objectives and all desired objectives.
D. The proposed solution does not meet the required objective.

Answer: B

QUESTION NO: 39
When using the Load Measuring Agent, you can add a new server without stopping and starting anything. Review the steps listed below and select the response demonstrating the correct order for adding a new server for Load Measuring.

1. Install the agent on the server.
2. Add the object for the new server to the existing rule in the Rule Base.
3. Re-install the Security Policy.

A. 1, 2, 3.
B. 2, 1, 3.
C. 2, 3, 1.
D. 1, 3, 2.
E. 3, 2, 1.

Answer: A

QUESTION NO: 40
What is the purpose of cplic check?

A. Allow you to perform the license installation.
B. Verification of the license expiration data.
C. It is a alternate to the **printlic** command.
D. Validates a license feature.
E. Verification of the external IP address.

Answer: D

QUESTION NO: 41
If you have modified your network configuration by removing the firewall adapters, you can reinstall these adapters by reinstalling SecureClient.

A. True
B. False

Answer: B

QUESTION NO: 42
Hector is a security administrator for a large, global enterprise that is preparing to implement VPN-1/Firewall-1. In the first phase of the rollout all Enforcement Modules will be installed at a central warehouse before being shipped to the final sites and final set-up. Site-specific information is not available to the warehouse installer. What are the MINIMUM elements Hector must configure to complete Enforcement Module installation?

A. Management Server IP address.
B. Certificate Authority.
C. Shared Secret Key.
D. One Time Password.
E. Security Servers.

Answer: A

QUESTION NO: 43
Which of the following statements is FALSE?

A. A policy Server extends security to the desktop by allowing administrators to enforce a Security Policy on desktops –both inside a LAN and connecting from the Internet –this preventing authorized connections from being compromised.
B. A Policy Server must be on a firewalled machine with CP shared installed.
C. A Policy Server supports all platforms.
D. To use Policy Server in a network, you must have Policy Server from which SecureClient obtains its Desktop Policy.
E. To use Policy Server in a network, you must have SecureClient software.

Answer: C

QUESTION NO: 44
Content Vectoring Protocol (CVP), by default uses TCP port 10101, and:

A. Is designed to reroute data streams to an external virus scanning server.
B. Enhances security further by allowing virus detection capabilities by third party OPSEC certified solutions.
C. Passes files to a packet scanning server for filtering.
D. A and B.
E. A and C.

Answer: D

QUESTION NO: 45
Paul will be installing all of the components of VPN-1/Firewall-1 on a single machine. Company growth will require moving to a distributed environment as additional Enforcement Modules are added over the next six months. While installing, which option should Paul select to facilitate the transition six months from now?

A. Enterprise Primary Management.
B. Enterprise Security Management.
C. Enforcement Module & Primary Management.
D. Enforcement Module.

Answer: C

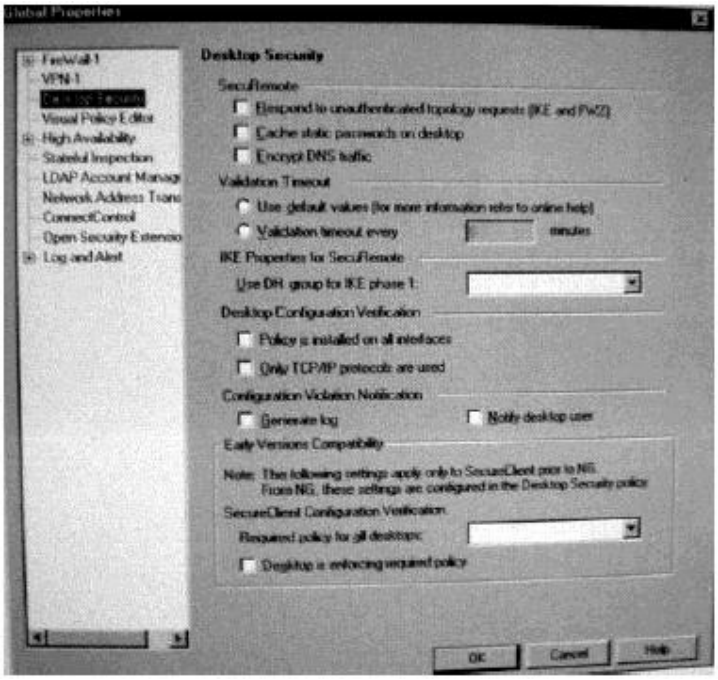
QUESTION NO: 46
In the IKE properties window, you can use the Data Integrity drop-down menu to select:

A. The cryptographic checksum method to be used for ensuring data integrity.
B. The Certificate Authority to be used for ensuring data integrity.
C. The shared secret to be used for ensuring data integrity.
D. The CA checksum method to be used for ensuring data integrity.
E. The shared-secret checksum method to be used for ensuring data integrity.

Answer: A

QUESTION NO: 47
You must configure your firewall for Hybrid IKE SecureClient connections. Which of the following fields MUST be selected to allow backward compatibility with earlier version of the SecureClient?

A. Respond to Unauthenticated topology requests (IKE and PF1).
B. Cache static passwords on desktop.
C. Required policy for all desktops and Desktop if enforcing the required policy.
D. A and B.
E. A and C.



Answer: E

QUESTION NO: 48
Your Manager has requested that you implement a policy that prevents users on the network from transferring confidential files out of the intranet using FTP. You also want to check for virus signatures on those files entering the intranet. You setup an FTP resource and add it to the Service field of a rule. You have only redefined the FTP resource and selected the Get option under the Match tab. Does this meet all of the requirements of your maneger?

A. Yes
B. No

Answer: B

QUESTION NO: 49
SecureClient syntax checking can be used to monitor usersc.C file parameters. The checking is used to prevent errors causing the site, to which it belongs from being deleted.

A. True
B. False

Answer: A

QUESTION NO: 50
The Service drop-down menu in the OPSEC Definition Properties window allows you to select a service for communication with a server from the drop-down list.
The service contains the port number to watch the filer server listens. For UFP Server, the service is:

A. FW1_UFP
B. FW1_sam
C. UFP_FW1
D. FWNG_UFP
E. FW1_NG_UFP

Answer: D

QUESTION NO: 51
You are concerned that an electronically transmitted message may be intercepted and manipulated as if it came from you. This would compromise the accuracy of the communications. To secure the validity of the original message sent, you attach a _____.

A. Tag
B. Sender flag.
C. Diffie-Hellman verification.
D. Private key.
E. Digital signature.

Answer: E

QUESTION NO: 52
When designing your company's content security solution, where should you place the CVP anti-virus server for the best performance?

A. On the company's internal Web Server.
B. On the firewall itself.
C. In any server with the internal network.
D. On a server on an internal dedicated network connected to a separate NIC in the firewall.
E. None of the above.

Answer: D

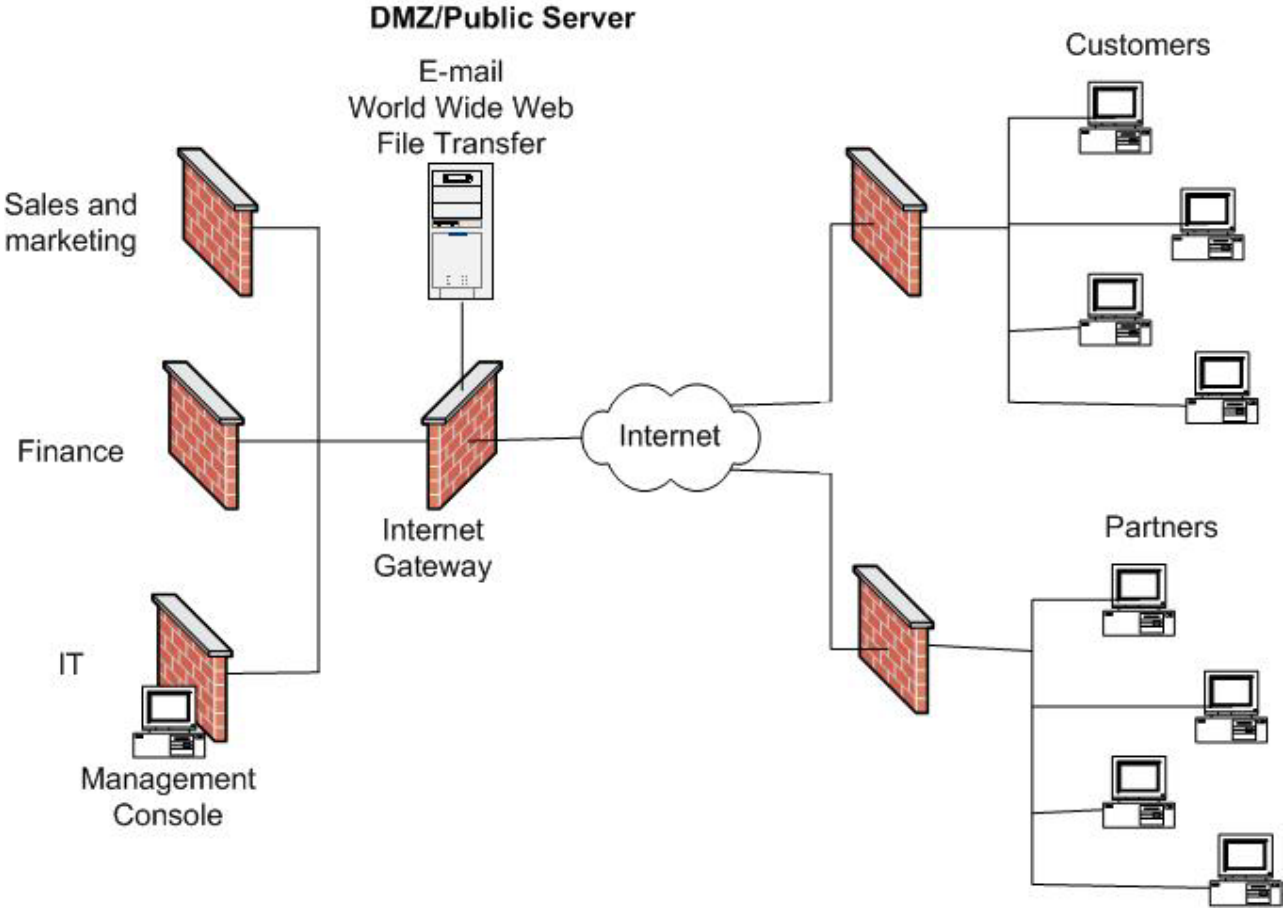
QUESTION NO: 53
You are using Hybrid IKE. The certificate is not created in the Certificates tab of the VPN-1/Firewall-1 network object; even after "Internal CA created successfully" is displayed "fw internalca create" is displayed as having been issued. Which if the following lists the most likely cause of the problem, and the appropriate remedy?

A. The distinguished name used in the "fw internalca create" and "fw interalca certify" commands is too long. In this case, use a shorter name.
B. Perform fwstop and move the objects.sav objects.bak and other files with objects.* from $FWDIR/conf directory except the objects.c file. Perform the "fw interalca create" and "fw interalca certify" again with the **–force** option.
C. Under the Firewall object> VPN> IKE> Support Authentication Methods, **Hybrid** is unchecked. Select **Hybrid** and stop and start the firewall.
D. Certificate created by internal CA is somehow corrupt. Recreate the certificate with the **–force** option.
E. Options A and B.

Answer: A, B

QUESTION NO: 54

You are developing network between separate corporate partners, each having their own secure intranet. If you want to share among them, the type of VPN you should develop is a (n):



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

Answer: C

QUESTION NO: 55
TCP services must have a rule in the Policy Editor Rule Base to be used by TCP resources.

A. True
B. False

Answer: A

QUESTION NO: 56
User groups need NOT be defined to configure SecuRemote, but are required for the configuration of a Policy Server.

A. True
B. False

Answer: A

QUESTION NO: 57
SYNDefender Gateway sends a FIN/ACK packet in immediate response to a server's SYN/ACK packet.

A. True
B. False

Answer: B

QUESTION NO: 58
What are the two types of HTTP Security Server authentication methods that may be used?

A. Transparent and UFP.
B. Transparent and Proxy.
C. Non-Transparent and Proxy.
D. Non-Transparent and CVP.
E. Transparent and CRL.

Answer: B

QUESTION NO: 59
You are implementing load-balancing to your Web Server using the Connect Control module. What type of logical server would you specify, if you need to load balance between servers that may not be behind the same firewall?

A. HTTP

B. Other with **Persistent Server Mode** –checked.
C. Both A and B.
D. None of the above, it is not possible.

Answer: B

QUESTION NO: 60
Below is the Log and Alert Page of the Global Properties window.

Exhibit missing

The **Excessive log grace period** field sets the minimum amount of time (in seconds) (**The above not available picture showed 62 seconds)** between consecutive logs of similar packets. Two packets are considered similar:

A. If they have the same source address, source port, destination port and the same service was used.
B. If they have the same source port, destination address, destination port and the same service was used.
C. If they have the same source address, source port, destination port and any service was used.
D. If they have the same destination address, source address, destination port, and the same service was used.

Answer: C

QUESTION NO: 61
Which position if a URL is sent to a UFP server when using a TCP resource?

A. The full URL is forwarded.
B. Only the IP address of the remote server is forwarded to the UFP server.
C. The URL is not forwarded to the UFP Server, it is handled by the Security Servers.
D. Only the path portion of the URL is forwarded.
E. Only the host name is forwarded.

Answer: B

QUESTION NO: 62
For standard RFC (Request for Comments) complaint IKE VPN's, a user's authentication method should be defined where?

A. In the authentication tab of the user.

B. In the Encryption tab of the firewall and the Authentication tab of the user.
C. In the Encryption tab of the firewall and the Encryption tab of the user.
D. In the Authentication tab on the firewall.
E. In the Authentication tab of the firewall and the user.

Answer: C

QUESTION NO: 63
When you install the Management Module and GUI Client on a Windows NT Server:

A. The Windows NT Server in which you install becomes the Management Module and Authentication GUI for the Enforcement Module.
B. The Administration GUI resides on the Enforcement Module and the Management Module resides on its own machine.
C. The Windows NT Server on which you install becomes the Enforcement Module.
D. The Administration GUI only resided on the Management Module.
E. The Administration GUI communicated with the Management Module on port 257.

Answer: D

QUESTION NO: 64
The following steps correctly list the actions taken by a Certificate Authority (CA)

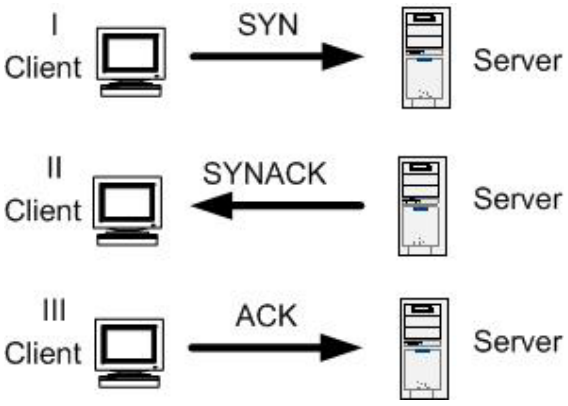
1. Users send their public keys to a CA in a secure manner.
2. The CA signs the public keys with its own private keys, creating CA public keys.
3. The CA creates certificated with its public and private keys.

Receivers then authenticate senders' public keys, by matching the CA public keys to the CA private keys on the certificates.

A. True
B. False

Answer: B

QUESTION NO: 65
This picture shows a normal three-way TCP/IP handshake.



Which of the following will cause VPN-1/Firewall-1 to reset TCP connections with a server protected by SYNDefender?

A. The client never completes the handshake with an SYN packet.
B. The client never completes the handshake with an SYN/ACK packet.
C. The server never completes the handshake with an SYN packet.
D. The client never completes the handshake with an ACK packet
E. The server never completes the handshake with an ACK packet.

Answer: D

QUESTION NO: 66
With SecureClient, if you have more than one network adapter:

A. VPN-1/Firewall-1 adapters can be bound to all of them.
B. In Windows 3x, the binding is static and takes place when SecureClient is installed.
C. On Windows NT, the binding is dynamic and takes place upon reboot.
D. On Windows 2000, the binding is static and takes place when Secure Client is installed.
E. A, B and C.

Answer: A, C

QUESTION NO: 67
Which load-balancing method chooses the physical server closest to the client, based on DNS?

A. Round Trip.
B. Server Load.
C. Round Robin.

D. Random
E. Domain

Answer: E

QUESTION NO: 68
On which the following operating systems does Check Point support installation of the VPN-1/Firewall-1 Management Server?

A. Windows NT Server 4.0 SP6A.
B. Windows NT Workstation 4.0 SP6A
C. Free BSD.
D. Solaris 2.5.
E. IOS

Answer: A

QUESTION NO: 69
SYN flood attacks are used in the Denial-of-Service (Dos) attacks, or in conjunction with other exploits to block access to a server network.

A. True
B. False

Answer: A

QUESTION NO: 70
Which of the following statements is FALSE?

A. Alter commands are executed by the **alertd** process, running on the single gateway (stand-alone) installation.
B. If logs are being sent to more than one machine, each **alertd** process will execute the alert commands.
C. The alert condition id detected on the firewall module, then the Management Server is notified and executes the alert.
D. Alert commands are executed on the Alert Module, running on the Management Server.

Answer: D

QUESTION NO: 71
Which command is used to export a group of users from VPN-1/Firewall-1?

A. Fw dbexport.
B. Ldapmodify
C. Ldabsearch
D. Ldap export.

Answer: A

QUESTION NO: 72
You are using Hybrid IKE. SecuRemote produces the error "Certificate is badly signed". Which of the following lists the most likely cause of the problem, and the appropriate remedy?

A. The distinguished name used in the "fw interalca create" and "fw interalca certify" commands is too long. In this case, use a shorter name.
B. Under the Firewall object> VPN> IKE> Support Authentication Methods, **Hybrid** is unchecked. Select **Hybrid** and stop and start the firewall.
C. The Certificate created by internal CA is corrupt. Recreate the certificate with the **–force** option.
D. SecuRemote version is lower then 4.1 SP1. Upgrade SecuRemote.
E. None of the above.

Answer: D

QUESTION NO: 73
The "Man in the Middle" threat consists of the possibility of a third party intercepting the private keys of you and another correspondent, even though you think you're communicating directly with each other.

A. True
B. False

Answer: A

QUESTION NO: 74

If you do not configure any groups during Solaris installation, ONLY the supervisor will be able to access and execute the VPN-1/Firewall-1 Module.

A. True
B. False

Answer: B

QUESTION NO: 75
When you conduct a distributed installation of VPN-1/Firewall-1:

A. The SYN Foundation component is installed on all modules.
B. The Enforcement Module is distributed among VPN-1/Firewall-1 Modules.
C. All VPN-1/Firewall-1 files are installed on multiple machines.
D. Any Windows NT server on which you install Check Point VPN-1/Firewall-1 becomes the Enforcement Module.
E. You do not need Windows NT administrative privileges.

Answer: A

QUESTION NO: 76
If the Persistent Server mode check box is selected in the Logical Server Properties window, which if the following is TRUE?

A. Once a client is connected to a physical server, the client will continue to connect to that server for the duration of the session.
B. Once the server is connected to a client, the server will continue to connect to that client for the duration defined in the Logical Server Properties window.
C. Once the client is connected to a physical sever, the client will only connect to that server for a single session.
D. After a client has connected to a physical server, the client disconnects from the server.

Answer: A

QUESTION NO: 77
Which of the following statements is FALSE?

A. A SYN flood attack is an attack against a service designed to make a server unavailable.
B. A SYN flood attack exploits the limitations of the TCP/IP protocol.

C. During SYN flood attack, a client sends a SYN/NACK to a server and data exchange begins.
D. During a SYN flood attack, a server replies with a SYN/ACK identified by the source IP address in an IP header.

Answer: C

QUESTION NO: 78
When a user leaves an organization or when a key is compromised, a certificate must be revoked. The Certificate Authority does this by using and distributing a:

A. Certification Invocation List (CIL).
B. Revocation of Certification (ROC).
C. Authority Certification List (ACL).
D. Certification Revocation List (CRL).
E. Certification Key List (CKL).

Answer: D

QUESTION NO: 79
The internal program, know as alertf, allows an operator to define how many events with in a defined number of seconds before the script is executed.

A. True
B. False

Answer: A

QUESTION NO: 80
When you connect to a site referenced in your database SecuRemote:

1. Holds the first packet without transmitting it.
2. Examines the packet to determine responsible firewall.
3. Encrypts the packet and then transmits it.

A. True
B. False

Answer: B

QUESTION NO: 82
You are the VPN-1/Firewall-1 administrator for a company WAN. You want all users to communicate across WAN securely. You must use an encryption scheme that does not change packet size, to allow for better network performance. You must also be able to define the Certificate Authority from your local VPN-1/Firewall-1 Management Module. Which encryption scheme do you choose?

A. Rgindal
B. FWZ
C. IKE
D. Triple DES.
E. Manual IPSec.

Answer: B

QUESTION NO: 83
SecuRemote operates between the _____and the _____.

A. TCP/IP Protocol, hardware card.
B. Network, hardware card.
C. TCP/IP Protocol, NIC Driver.
D. NIC Driver, Hardware Card.
E. TCP/IP Protocol, network.

Answer: A

QUESTION NO: 83
By default where dies VPN-1/Firewall-1 look for a user-defined tracking script?

A. $FWDIR/root directory on the GUI client.
B. $FWDIR/local directory on the firewall.
C. $FWDIR/bin directory on the Management Server.
D. $FWVPN/bin directory on the firewall.
E. $FWDIR/bin/base directory on the Management Server.

Answer: C

QUESTION NO: 84
Which parameter, of TRUE, will automatically initiate an RDP status query with a gateway to check if it is still alive?

A. Keepalive
B. Dns_xplate
C. Active_resolver
D. Resolver_session_interval

Answer: C

QUESTION NO: 85
The SecureClient packaging tool installation generates a self-extracting auto-running executable file by saving SecuRemote properties on the Management Server and applying the properties to and open (unzipped) SecuRemote installation folder.

A. True
B. False

Answer: A

QUESTION NO: 86
You are a firewall administrator using SecuRemote. You are providing digital signatures to achieve both data integrity checking and verification of sender. Certificates are possible when using _____.

A. 3DES
B. IKE
C. IKE with SHIP.
D. IKE with Manual IPSec.

Answer: B

QUESTION NO: 87
Some VPN-1/Firewall-1 tracking options generate log entries and trigger executables. These executables take the form of:

A. User-defined executables in $FWDIR/local.
B. SNMP traps, or other functions defined by security engineers, EXCEPT socket-based applications.
C. SNMP traps, alter emails, or other functions defined by security engineers.

D. User-defined JAVA scripts in $FWDIR/bin
E. SMS traps, alert emails, or other functions defined by security engineers.

Answer: C

QUESTION NO: 88
You are using a 56-bit encryption key called DES. Your client is concerned that this is insufficient security. You reconfigure the VPN to use the strongest encryption used by the VPN-1/Firewall-1 software. Which of the following would you use?

A. AES 256.
B. BlowFish
C. RC4
D. CAST
E. 3DES 698

Answer: A

QUESTION NO: 89
The functionality of the VPN-1/Firewall-1 architecture can be divided between which workstations?

A. Enforcement Module and Policy Editor.
B. Host and Policy Editor.
C. Policy Editor, Management Server and Enforcement Module.
D. Host and Management Server.
E. Router and Management Server.

Answer: C

QUESTION NO: 90
Respond to unauthenticated topology requests (IKE and FWI) on the Desktop Security screen in Global Properties allow backward compatibility with earlier versions of the SecuRemote /SecureClient.

A. True
B. False

Answer: A

QUESTION NO: 91
You are working with a Windows NT server running the Check Point VPN-1/Firewall-1 software. Which if the following radio button options would you select from the Server Setup Properties window to configure the connect memory strategy for this configuration?

A. Minimize memory used.
B. Balance
C. Maximize Throughput File Sharing.
D. Maximize Throughput for Network Applications.
E. Make Browser Broadcast to LAN Manager 2.x Clients.

Answer: D

QUESTION NO: 92
The Solaris command to install the Enforcement Module software without using the Installation Wrapper is:

A. Pkgadd /d
B. Pkgadd –d
C. Pkgadd
D. Pkgadd /install
E. Pkgadd /setup

Answer: B

QUESTION NO: 93
When installing the SecureClient packaging tool, users must define their VPN-1/Firewall-1 sties.

A. True
B. False

Answer: B

QUESTION NO: 94
The following URL specification blocks access to the /warez/illegal.html
204.32.38.254/warez/illegal.html 1

A. True
B. False

Answer: B