

156-210

TEST KING



LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Checkpoint NG CCSA Exam

Version 1

Leading the way in IT testing and certification tools, www.testking.com

Important Note
Please Read Carefully

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 just cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

We are constantly adding and updating our products with new questions and making the previous versions better so email us once before your exam and we will send you the latest version of the product.

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that particular pdf file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

QUESTION NO: 1

The VPN-1/Firewall-1 NG User Interface consists of which of the following elements?

- A. Security Policy Editor, Visual Policy Editor and Object tree view.
- B. Management Server and VPN-1/FireWall-1 Module.
- C. Visual Policy Editor, Object Tree view and inspection Module.
- D. Security Policy Server, System GUI and Module Log Viewer.
- E. VPN-1/FireWall-1 Module, Inspection Module and Security Server.

Answer: A

QUESTION NO: 2

You are attempting to implement Client Authentication for FTP. You have the accept firewall control connection option unchecked in the Policies and Properties dialog box.

In the following Rule base, which rule would prevent a user from performing Client Authentication?

No	SOURCE	DESTINATION	SERVICE	ACTION
1	Any	fw.chicago.com	Any	drop
2	AllUsers@Sales.net	Any	ftp	Client Encrypt
3	Any	localNet	http telnet	Accept
4	Any	Any	Any	drop

- A. Rule 1
- B. Rule 2
- C. Rule 3
- D. Rule 4

Answer: B

QUESTION NO: 3

As a VPN-1/Firewall-1 administrator, you have an undistributed range of IP addresses for which you want to perform address translation. You can simplify your efforts through the use of ADDRESS RANGE.

- A. True
- B. False

Answer: A

QUESTION NO: 4

In the figure below, Localnet is an internal network with private addresses A corresponding set of public addresses is available as follows:

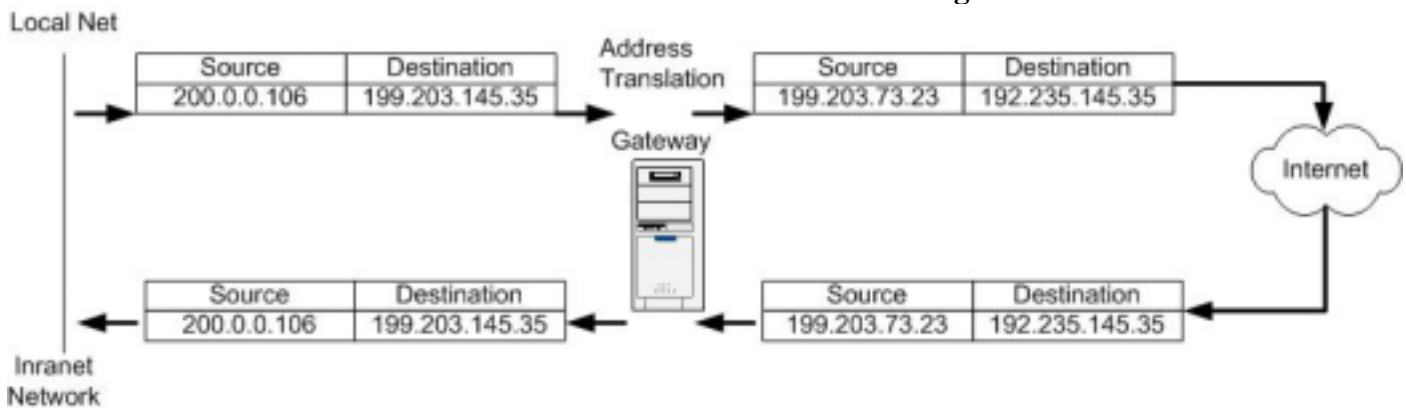
Public IP addresses

199.203.73.15-199.203.73.115

Private IP addresses

200.0.0.100-200.0.0.200

The private addresses are translated to public addresses by specifying addresses Translation in the NAT tab of Localnet's network properties window. Source addresses for the outbound packets from hosts in Localnet will be translated to 199.203.73.12 as shown in the figure below.



- A. True
- B. False

Answer: A

QUESTION NO: 5

You are working with multiple firewalls that have extensive Rule Bases. To simplify administration task, which of the following should you choose to do?

- A. Create Network range objects that restrict all applicable rules to only certain networks.
- B. Run separate GUI clients for external and internal firewalls.
- C. Eliminate all possible contradictory rules such as stealth and clean-up rules.
- D. Save a different Rule Base for each remote firewall.
- E. None of the above.

Answer: D

QUESTION NO: 6

Leading the way in IT testing and certification tools, www.testking.com

Currently, the Accounting Department is FTP-ing a file in the bank. Which Log Viewer Module would show you the activity occurring at the present time?

- A. Security Log.
- B. Active Connections Log.
- C. Accounting Log-
- D. Administrative Log.
- E. Non of the above.

Answer: B

QUESTION NO: 7

With Blocking Scope default settings, a selected connection is terminated:

- A. And all further attempts to establish a connection from the same source IP address to the same destination IP address and port will be blocked.
- B. But all further attempts to establish connections from this specific source IP address will be authenticated before being denied.
- C. And all further attempts to establish connections to this specific destination IP address will be denied.
- D. And all further attempts to establish a connection from the same source IP address to the firewall's IP address will be blocked.
- E. Both A and D.

Answer: A

QUESTION NO: 8

Consider the following Rule Base for VPN-1/Firewall-1 NG.

Assuming the default settings in global properties have NOT changed, ICMP would be allowed through the firewall.

No	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	Any	Web_Server	http	Accept	Long
2	Any	Any	Any	Any	Long

- A. True
- B. False

Answer: B

QUESTION NO: 9

Which is the correct rule in the following Rule Base?

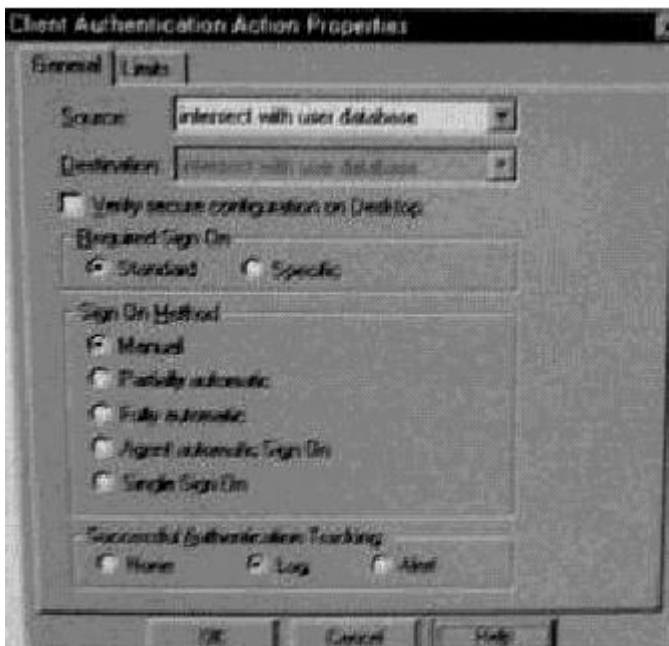
No	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	AllUsers@Chicago	Any	Any	Session Auth	Log
2	AllUsers@Chicago	Chicago	Any	Session Auth	Log
3	AllUsers@Any	Any	Any	Session Auth	Log
4	AllUsers@Chicago	Any	Any	User Auth	Log

- A. Rule 2
- B. Rule 1
- C. Rule 3
- D. Rule 4
- E. None of the rules allow access.

Answer: D

QUESTION NO: 10

In the Client Authentication Action Properties window (below), for the required Sign On Method section, Manual is selected.



This means:

- A. If a connection matches the Rule Base the service is an authenticated service, the client is signed on after a successful authentication.

- B. The user must initiate the Client Authentication Session to the gateway.
- C. If a connection using any service matches Rule Base, the client is authenticated.
- D. If authentication is successful, access is granted from the network that initiated the connection.
- E. The user must TELNET to the target server on port 259.

Answer: B

QUESTION NO: 11

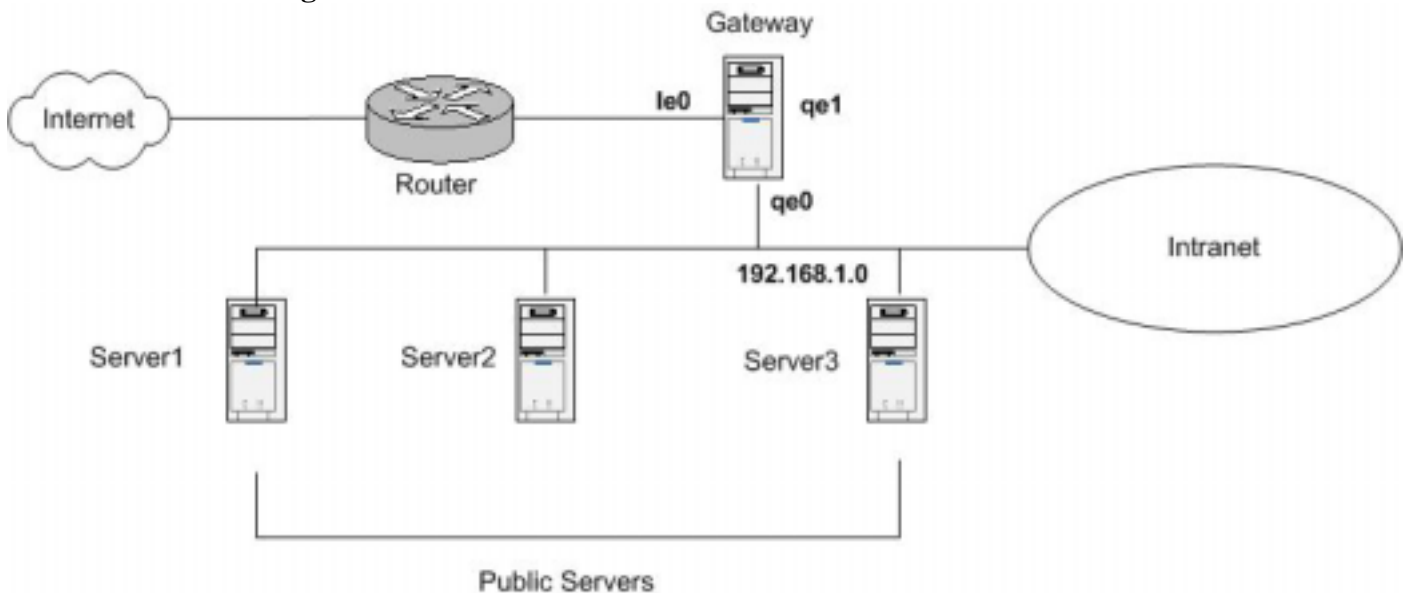
Changes made to the Security Policy do not take effect on the Enforcement Module until the administrator performs which of the following actions?

- A. Saves the policy.
- B. Verifies the policy.
- C. Install the policy.
- D. Stops firewall services on the Enforcement Module.
- E. Stops firewall services on the Management module.

Answer: C

QUESTION NO: 12

Consider the following network:



The public servers are a web form. Since the web servers accepts and initiate connections Dynamic translation is required.

- A. True

B. False

Answer: B

QUESTION NO: 13

The fw fetch command perform the following function:

- A. Attempts to fetch the policy from the Management Server.
- B. Fetches users from the Management server.
- C. Produces an output screen of the Rule Base.
- D. Fetches the logs.
- E. Fetches the systems status.

Answer: A

QUESTION NO: 14

Inclement weather and a UPS-failure cause a firewall to reboot. Earlier that day a tornado destroyed the building where the firewall's Management Module was located. The Management Module was not recovered and has not been replaced.

Bases on the scenario, which of the following statements is FALSE?

- A. The firewall will continue to enforce the last rule base installed.
- B. The firewall will log locally.
- C. The firewall will fetch the last installed policy form local host and install it.
- D. Communication between the firewall and the replacement Management Module must be established before the replacement Management Module can install a policy on the firewall.
- E. Because the firewall cannot contact the Management Module, no policy will be installed.

Answer: E

QUESTION NO: 15

When configuring Anti-Spoofing for VPN-1/FireWall-1 NG on the firewall interfaces, all of the following are valid address choices except:

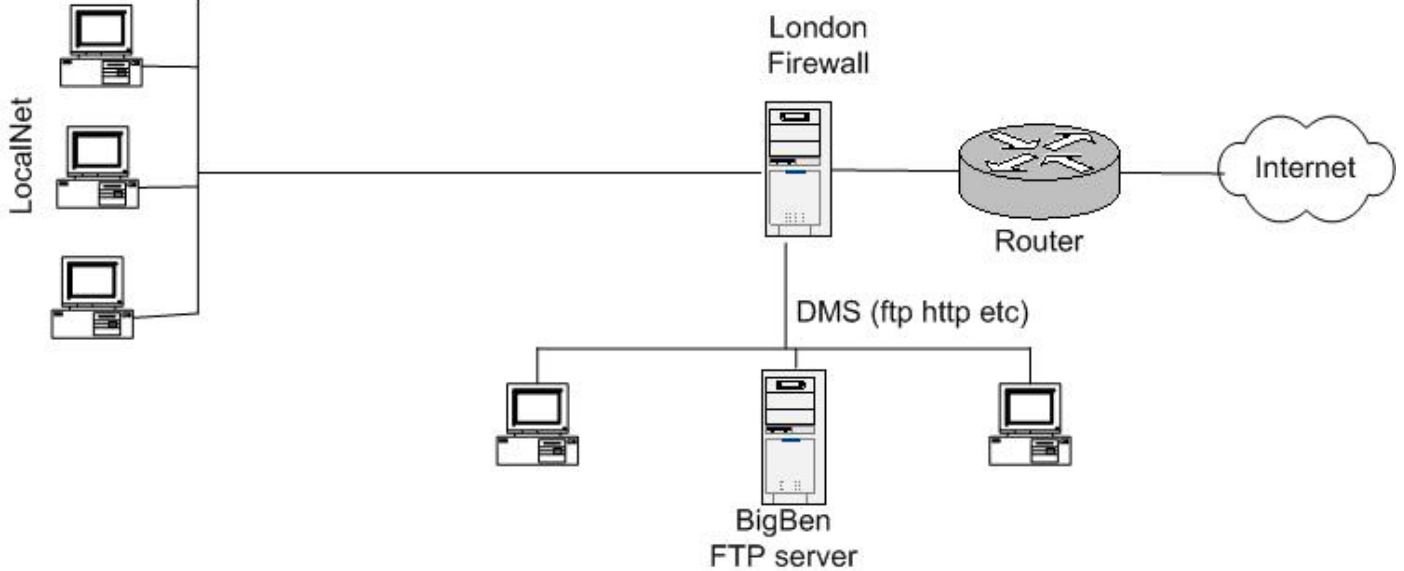
- A. Network defined by Interface IP and Net Mask.
- B. Not Defined.
- C. Security Policy Installed.
- D. Specific

E. None of the above.

Answer: C

QUESTION NO: 16

The security administrator for the following configuration only allows members of the localnet managers group access files in BigBen (the FTP Server)



Select below the rule that allows local managers to access the FTP server from any location.

No	SOURCE	DESTINATION	SERVICE	ACTION
1	LocalManageers@Any	BigBen	ftp	User Auth
2	LocalManageers@Net_London	BigBen	ftp	Client Auth
3	LocalManageers@Any	BigBen	ftp	Session Auth
4	LocalManageers@Net_Tokyo	BigBen	ftp	User Auth

- A. Rule 1.
- B. Rule 2.
- C. Rule 3.
- D. Rule 4.
- E. None of these rules allow access.

Answer: D

QUESTION NO: 17

Assume that you are working on a Windows NT operating system. What is the default expiration for a Dynamic NAT connection NOT showing any UDP activity?

- A. 30 Seconds.
- B. 60 Seconds.
- C. 40 Seconds.
- D. 600 Seconds.
- E. 3000 Seconds.

Answer: C

QUESTION NO: 18

Assume there has been no change made to default policy properties. To allow a telnet connection into your network, you must create two rules.

One to allow the initial Telnet connection in.

One to allow the destination machine to send information back to the client.

- A. True
- B. False

Answer: B

QUESTION NO: 19

In Windows NT to force log entries other than the default directory.

- A. You must use the **cpconfig** command.
- B. Change the **fwlog** environment variable.
- C. Modify the registry.
- D. Change the directory in log viewer.
- E. Use the fw log switch command.

Answer: D

QUESTION NO: 20

For most installations, the Clean-Up rule should be the last rule in Rule Base.

- A. True
- B. False

Answer: B

QUESTION NO: 21

What complements are necessary for VPN-1/FireWall-1 NG to scan e-mail, passing through the firewall, for macro viruses?

- A. UFP and OPSEC-certified scanning product.
- B. CVP and OPSEC-certified virus scanning product.
- C. UFP and CVP.
- D. UFP, CVP and OPSEC-certified content filter.
- E. None of the above, VPN-1/FireWall-1 NG scans for macro viruses by default.

Answer: B

QUESTION NO: 22

Why would you want to verify a Security Policy before installation?

- A. To install Security Policy cleanly.
- B. To check up the enforcement-point firewall for errors.
- C. To identify conflicting rules in your Security Policy.
- D. To compress the Rule Base for faster installation
- E. There us no benefit verifying a Security Policy before installing it.

Answer: B

QUESTION NO: 23

To completely setup Static NAT, you ONLY have to select Add Automatic Address Translation rules on the NAT tab, and specify a public NAT IP address.

- A. True
- B. False

Answer: B

QUESTION NO: 24

If you configure the Minutes interval for a firewall in the User Authentication session timeout box, as shown below on the Authentication Tab of the Workstations properties window, users of one time password must re-authenticate for each request during this time period.

- A. True
- B. False

Answer: A

QUESTION NO: 25

What does a status of Untrusted tell you?

- A. A VPN-1/Firewall-1 NG firewall module has been compromised.
- B. A gateway cannot be reached.
- C. A module is installed and responding to status checks, but the status is problematic.
- D. A gateway is connected, but the management module is not the master of the module installed on the gateway.
- E. None of the above.

Answer: D

QUESTION NO: 26

Omanan Enterprises has the premier reclamation system for scrap aluminum in the western hemisphere. Then phenomenal growth over the last 10 years has led to the decision to establish a presence in the Internet in order to their customers. To that end, Omanan Enterprise network administrator, Jason has acquired a Web Server, and email server and 14 IP addresses from their ISP. Jason also purchased a Checkpoint VPN-1/FireWall-1 stand alone gateway module, with these interfaces, to protect Omanan enterprises' corporate data their ISP will be providing DNS services. The Web Server and email server must have Static routable IP addresses. The eight member executive counsel of Omanan Enterprises would to have routable IP addresses also, so that they can video-conference with the company's suppliers. Omanan Enterprises' remaining 200 employees would like to have access to Internet, and the executive counsel believe that granting them access might improve company morale.

Jason installs and configured Checkpoint VPN-1/FireWall1 stand alone Gateway module at the perimeter of Omanan Enterprises corporate LAN. He uses the 3rd NIC in the stand alone firewall gateway module to create DMZ. Jason installs the Web server and the email server on the DMZ. He creates tools and objects on the checkpoint VPN-1/FireWall-1 stand alone gateway module to allow HTTP, POP3 and SMTP from the Internet to the DMZ. He Creates objects to represent the web and email server and configures them for Static NAT.

Jason reconfigures his DHCP server so that each of the members of the executive counsel has reserved IP address. He then sues those reservations co create Statically NAT-ed objects on the Checkpoint VPN/Firewall-1 Standalone Gateway module. Jason creates another object represents the internal network he configures this object for Dynamic NAT. He adds a rule allowing HTTP traffic from the

internal network to any destination. Jason created an additional rule to allow POP3 and SMTP traffic between the internal networks and DMZ.

Choose the one phrase below that best describes Jason'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: 27

Anna is a security administrator setting up User Authentication for the first time. She has correctly configured her Authentication rule, but authentication still does not work. What is the Check Point recommended way to troubleshoot this issue?

- A. Verify the properties of the user attempting authentication and the authentication method selected in the Authentication Properties of your firewall object.
- B. Verify the firewall settings of your firewall object, and the properties for the user attempting encryption and authentication.
- C. Verify the properties for the user attempting authentication and make sure that the file Stealth Authentication method is selected in the Authentication properties of both the peer gateway object and your firewall object.
- D. Verify both Client and User Authentication, and the authentication method selected in the Authentication properties of your Firewall object.
- E. Re-import Schema from the VPN-1/FireWall-1 NG installation CD.

Answer: A

QUESTION NO: 28

Session authentication provides an authentication method NOT supported by protocols that can be integrated with any application.

No.	Source	Destination	Service	Action	Track	Install On
1.	Any	Local_Net	telnet	Accept	Long	Gateways
2.	Pub Server1	Pub Server2	Any	Accept	Long	Gateways

- A. True
- B. False

Answer: B

QUESTION NO: 29

How do recover communications between your management module and enforcement module if you lock yourself out via a rule policy that is configured incorrectly?

- A. Cp delete all all.
- B. Cp pause all all.
- C. Cp stop all all.
- D. Cp unload all all.
- E. Cp push all all.

Answer: D

QUESTION NO: 30

You have set up a firewall and management module on one NT box and a remote module on a different location. You receive only sporadic logs from the local firewall and only and control message from remote firewall. All rules on both firewalls are logging and you know the traffic is flowing through the firewall using these rules. All the firewall related services are running and you are using NAT and you receive few logs from the local firewall.

What actions from the choices below would you perform to find out why you cannot see logs?

- A. Make sure there is no masters file in SFWDIR/conf on the remote module.
- B. Make sure there is no masters file in SFWDIR/conf on the local NT box.
- C. See if you can do a fwfetch from the module.
- D. Run the fw logexport -t -n from the command line prompt on the remote module.
- E. Use pulist.exe from the Windows NT resource kit.

Answer: C

QUESTION NO: 31

**As a firewall administrator you encounter the following you error message:
Authentication for command failed.**

What is the most logical reasoning for thus type of error message?

- A. The Rule Base has been corrupted.
- B. The kernel cannot communicate with the management module.
- C. The administrator does not have the ability to push the policy.

- D. Remote encryption keys cannot be fetched.
- E. Client authentication has failed.

Answer: E

QUESTION NO: 32

Your customer has created a rule so that every time a user wants to go to the Internet, that user must be authenticated. Firewall load is a concern for the customer. Which authentication method does not result in any additional connections to the firewall?

- A. Session
- B. User
- C. Client
- D. Connection
- E. None of the above.

Answer: B

QUESTION NO: 33

What variable is used to extend the interval of the Timeout in a NAT to prevent a hidden UDP connection from losing its port?

- A. Fwx_udp_todefaultextend.
- B. Fwx_udp_expdefaultextend.
- C. Fwx_udp_todefaulttext
- D. Fwx_udp_timeout.
- E. Fwx_udp_expiration.

Answer: E

QUESTION NO: 34

To hide data filed in the log viewer:

- A. Select **Hide** from the Log Viewer menu.
- B. Right-click anywhere in a column of the Log Viewer GUI and select **Show Details**.
- C. Right-click anywhere in the column of the Log Viewer GUI and select **Disable**.
- D. Right-click anywhere in the column of the Log Viewer GUI and select **Hide**.
- E. Select **Hide** from the Log Viewer tool bar.

Answer: D

QUESTION NO: 35

You are following the procedure to setup user authentication for TELNET to prompt for a distinct destination. This allows the firewall to simulate a TELNET Proxy. After you defined the user on the Firewall and use VPN-1/FireWall-1 Authentication, you would:

- A. Stop the Firewall.
- B. Restart the Firewall.
- C. Start the Policy Editor and go to Manage service, and edit TELNET service.
- D. Ensure that the Authentication method is enabled in the firewall object.
- E. Ensure that there are no existing rules already allowing TELNET.

Answer: E

QUESTION NO: 36

You have the VPN-1/Firewall-1 NG product installed. The following Rule Base order correctly implements Implicit Client Authentication fort HTTP.

No.	SOURCE	DESTINATION	SERVICE	ACTION
1	All Users@localnet	*Any	TCP ftp	User Auth
2	All Users@localnet	*Any	TCP http	User Auth

- A. True
- B. False

Answer: B

QUESTION NO: 37

What is the software package through which all Check Point products use infrastructure services?

- A. Cpstart/cpstop.
- B. Check Point Registry.
- C. CPD
- D. Watch Dog for critical services.
- E. SVN Foundation.

Answer: E

QUESTION NO: 38

Choose the BEST response to finish this statement.

A Firewall:

- A. Prevents unauthorized to or from a secured network.
- B. Prevents unauthorized to or from a unsecured network.
- C. Prevents authorized access to or from an Intranet.
- D. Prevents authorized access to or from an Internet.
- E. Prevents macro viruses from infecting the network.

Answer: A

QUESTION NO: 39

Where is the external if file located in VPN1/Firewall-1 NG?

- A. FWDIR conf directory.
- B. Database directory.
- C. State directory.
- D. Temp Directory.
- E. Not used in VPN1/Firewall-1 NG.

Answer: A

QUESTION NO: 40

Which log viewer mode allows you to actually see the contents of the files HTTP-ed by the corporation's Chief Executive Officer?

- A. Security Log.
- B. Active Connections Log.
- C. Accounting Log.
- D. Administrative Log.
- E. None of the above.

Answer: E

QUESTION NO: 41

When you select the alert radio button on the topology tab of the interface properties window:

- A. The action specified in the Action element of the Rule Base is taken.
- B. The action specified in the Anti-Spoofing Alert field in the Global properties window is taken.
- C. The action specified in the Pop up Alter Command in the Global properties window is taken.
- D. Both A and B.
- E. Both B and C.

Answer: E

QUESTION NO: 42

You are the firewall administrator with one management server managing one firewall. The system status displays a computer icon with a ‘!’ symbol in the status column. Which of the following is the most likely cause?

- A. The destination object has been defined as external.
- B. The Rule Base is unable to resolve the IP address.
- C. The firewall has been halted.
- D. The firewall is unprotected, no security policy is loaded.
- E. Nothing is wrong.

Answer: D

QUESTION NO: 43

System Administrators use session authentication when they want users to:

- A. Authenticate each time they use a supported service.
- B. Authenticate all services.
- C. Use only TENET, FTP, RLOGIN, and HTTP services.
- D. Authenticate once, and then be able to use any service until logging off.
- E. Both B and D

Answer: D

QUESTION NO: 44

Your customer has created a rule so that every time a user wants to go to Internet, that user must be authenticated. The customer requires an authentication scheme that provides transparency for the user and granular control for the administrator. User must also be able to log in from any location. Based on this information, which authentication schemes meets the customer’s needs?

- A. Session
- B. User
- C. Client
- D. Dual
- E. Reverse

Answer: B

QUESTION NO: 45

Implementing Dynamic NAT would enable an internal machine behind the firewall to act as an FTP Server for external clients.

- A. True
- B. False

Answer: B

QUESTION NO: 46

The Enforcement Module (part of the VPN-1/FireWall-1 Module):

- A. Examines all communications according to an Enterprise Security Policy.
- B. Is installed on a host enforcement point.
- C. Can provide authentication and Content Security features at the application level.
- D. Is usually installed on a multi-homed machine.
- E. All of the above.

Answer: E

QUESTION NO: 47

In most cases when you are building the Rule Base you should place the Stealth Rule above all other rules except:

- A. Clean up rules.
- B. Implicit Rules.
- C. Client Authentication Rules.
- D. Pseudo Rules.
- E. Default Rules.

Answer: C

QUESTION NO: 48

If you change the inspection order of any of the implied rules under the Security Policy Setup, does it change the order in which the rules are enforced?

- A. True
- B. False

Answer: A

QUESTION NO: 49

The fw fetch command allows an administrator to specify which Security Policy a remote enforcement module retrieves.

- A. True
- B. False

Answer: A

QUESTION NO: 50

You can edit VPE objects before they are actualized (translated from virtual network objects to real).

- A. True
- B. False.

Answer: B

QUESTION NO: 51

Stateful inspection is a firewall technology introduced in Checkpoint VPN-1/Firewall-1 software. It is designed to meet which of the following security requirements?

1. Scan information from all layers in the packet.
2. Save state information derived from previous communications, such as the outgoing Port command of an FTP session, so that incoming data communication can be verified against it.

3. Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.
4. Evaluate and manipulate flexible expressions based on communication and application derived state information.

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

Answer: E

QUESTION NO: 52

If the security policy editor or system status GUI is open, you can open the log viewer GUI from the window menu.

- A. True
- B. False

Answer: A

QUESTION NO: 53

NAT can NOT be configured on which of the objects?

- A. Hosts
- B. Gateways
- C. Networks
- D. Users
- E. Routers

Answer: D

QUESTION NO: 54

Your customer has created a rule so that every user wants to go to Internet, that user must be authenticated. Which is the best method of authentication for users who must use specific computers for Internet access?

- A. Session

- B. User
- C. Client
- D. Connection
- E. None of the above.

Answer: B

QUESTION NO: 55

Which of the following describes the behavior of VPN-1/Firewall-1 NG?

- A. Traffic not expressly prohibited is permitted.
- B. Traffic not expressly permitted is prohibited.
- C. TELNET, SMTP and HTTP are allowed by default.
- D. Secure connections are authorized by default, unsecured connections are not.
- E. All traffic is controlled by explicit rules.

Answer: B

QUESTION NO: 56

New users are created from templates. What is the name of the standard template from which you would create a new user?

- A. New
- B. User
- C. Group
- D. Standard User.
- E. Default

Answer: E

QUESTION NO: 57

In a distributed management environment, the firewall administrator has removed the default check from Accept VPN-1/Firewall-1 control connections under the Security Policy tab of the properties setup dialogue box. In order for the management module and the Firewall to communicate, you must create a rule to allow the Management Module to communicate to the firewall on which port?

- A. 80
- B. 256
- C. 259

- D. 900
- E. 23

Answer: B

QUESTION NO: 58

What is the command for installing a Security Policy from a *.W file?

- A. Fw gen and then the name of the .W file.
- B. Fw load and then the name of .W file.
- C. Fw regen and then the name of the .W file.
- D. Fw reload and then the directory location of the .W file.
- E. Fw import and then the name of the .W file.

Answer: B

QUESTION NO: 59

In the Check Point Configuration Tool, you create a GUI administrator with Read Only privileges. This allows the Firewall-1 administrator for the authorized GUI client (GUI workstation) privileges to change network object, and create and install rules.

- A. True
- B. False

Answer: B

QUESTION NO: 60

Hybrid Authentication allows VPN-1/Firewall-1 NG to authenticate SecurRemote/SecureClient, using which of the following?

- A. RADIUS
- B. 3DES
- C. TACACS
- D. Any authentication method supported by VPN-1/Firewall-1.
- E. Both A and C.

Answer: E

QUESTION NO: 61

In order to install a new Security Policy on a remote firewall, what command must be issued on the remote firewall?

- A. Fw unload all all.
- B. Fw load new.
- C. Cp clear policy.
- D. None of the above, the command cp policy remove is issued from the manager.
- E. None of the above, the new policy will automatically overwrite the existing policy.

Answer: B

QUESTION NO: 62

As a firewall administrator if you want to log packets dropped by “implicit drop anything not covered” rules, you must explicitly define a Clean-up rule. This must be the last rule in the rule base.

- A. True
- B. False

Answer: A

QUESTION NO: 63

Fully Automatic Client authentication provides authentication for all protocols, whether supported by these protocols or not.

- A. True
- B. False

Answer: A

QUESTION NO: 64

VPN-1/Firewall-1 NG differs from Packet filtering and Application Layer Gateways, because?

- A. VPN-1/Firewall-1 NG provides only minimal logging and altering mechanism.
- B. VPN-1/Firewal-1 NG uses Stateful inspection which allows packet to be examined at the top of the layers of the OSI model.
- C. VPN-1/Firewall-1 NG has access to a limited part of the packet header only.

- D. VPN-1/Firewall-1NG requires a connection from a client to a firewall and firewall to a server.
- E. VPN-1/Firewall-1 NG has access to packets passing through key locations in a network.

Answer: B

QUESTION NO: 65

AlphaBravo Corp has 72 privately addressed internal addresses. Each network is a piece of the 10-net subnetted to a class C address. AlphaBravo uses Dynamic NAT and hides all of the internal networks behind the external IP addresses of the Firewall. The Firewall administrator for AlphaBravo has noticed that policy installation takes significantly longer since adding all 72 internal networks to the address translation rule. What should the Firewall administrator do to reduce the time it takes to install a policy?

- A. Create an object for the entire 10-net and use the object for the translation rule instead of the individual network objects.
- B. Use automatic NAT rule creation on each network object. Hide the network behind the firewall's external IP addresses.
- C. Match packets to the state table, so packets are not dropped. Increase the size of the NAT tables.
- D. Reinstall the Firewall and Security Policy Editor. The policy is corrupting Firewall's binaries.
- E. Increase the size of state table. Use automatic NAT rule creation to hide the networks behind an IP address other than firewall's external IP.

Answer: A

QUESTION NO: 66

How does VPN-1/Firewall-1 NG implement Transparent authentication?

- A. Unknown user receive error messages indicating that the firewalled gateway does not know the user names on the gateway.
- B. VPN-1/Firewall-1 NG prompts for user names even through the authentication data may not be recognized by the firewall's user database.
- C. VPN-1/Firewall-1 NG allows connections, but hides the firewall from authenticated users.
- D. Unknown users error messages indicating that the host does not know the users names on the server.
- E. VPN-1/Firewall-1 NG does not allow connections from users who do not know the name of the firewall.

Answer: C

QUESTION NO: 67

When creating user authentication rule, select intersect with user database for source and destination to allow access according to the source specified in the rules.

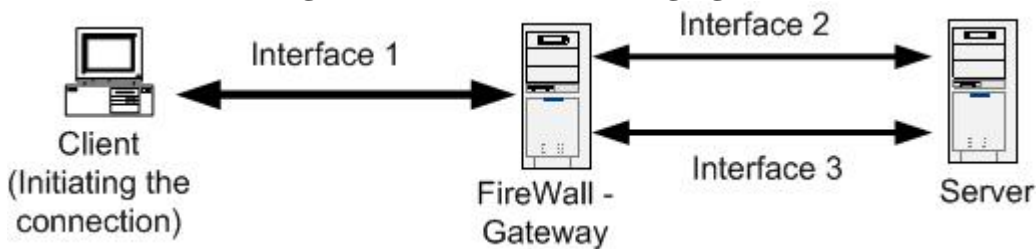
- A. True
- B. False

Answer: B

QUESTION NO: 68

A connection initiated by the client in the figure below will be hidden behind the IP address of the interface through which the connection was routed on the server side if the gateway (behind either interface 2 or interface 3). Specifying 0.0.0.0 as the address is convenient because of network address translation (NAT) is performed dynamically. And if the IP addresses of the gateway are changed, it is not necessary to reconfigure the NAT parameters.

Which of the following is true about the following figure?



- A. A connection initiated by the client will be hidden behind the IP address of the exit interface.
- B. A connection initiated by the server will be hidden behind the IP address of the exit interface.
- C. A connection initiated by the server will be hidden by the IP address of the client.
- D. Source addresses of outbound packets from the client will be translated to 0.0.0.0.
- E. Source addresses of outbound packets from the server will be translated to 0.0.0.0.

Answer: A

QUESTION NO: 69

Which if the following statements about Client Authentication are FALSE?

- A. In contrast to User Authentication, which allows access per user, Client Authentication allows access per ID address.
- B. Authentication is by user name and password, but is the host machine (client) that is granted access.
- C. Client Authentication is more secure than User Authentication, because it allows multiple users and connections from an authorized IP address or host.
- D. Client Authentication enables administration to grant access privileges to a specific IP address after successful authentication.

Answer: C

QUESTION NO: 70

When you make a rule, the rule is not enforces as part of your Security Policy.

- A. True
- B. False

Answer: B

QUESTION NO: 71

Which of the following user actions would you insert as an INTERNAL Authentication scheme?

- A. The user enters the security dynamics passcode.
- B. The user prompted for a response from the RADIUS server.
- C. The user prompted for a response from the AXENT server.
- D. The user prompted for a response from the TACACS server.
- E. The user enters an operating system account password.

Answer: E

QUESTION NO: 72

When configuring Static NAT, you cannot map the routable IP address to the external IP address of the Firewall if attempted, the security policy installation fails with the following error “rule X conflicts with rule Y”.

- A. True
- B. False

Answer: A

QUESTION NO: 73

The advantage of client authentication is that it can be used for any number of connections and for any services, but authentication is only valid for a specified length of time.

- A. True
- B. False

Answer: A

QUESTION NO: 74

You have set up Static NAT on a VPN-1/Firewall-1 to allow Internet traffic to an internal web server. You notice that any HTTP attempts to that machine being dropped in the log due to rule 0. Which of the following is the most likely cause?

- A. Spoofing on the internal interface is set to **Network defined by Interface IP and Net Mask**.
- B. Spoofing on the external interface is set to **Not Defined**.
- C. You do NOT have a rule that allows HTTP access to the internal Web Server.
- D. You do NOT have a rule that allows HTTP from the Web Server to Any destination.
- E. None of the above.

Answer: A

QUESTION NO: 75

As a firewall administrator, you are required to create VPN-1/Firewall-1 users for authentication. When you create a user for user authentication, the data is stored in the?

- A. Inspect Engine.
- B. Rule base.
- C. Users database
- D. Rulebase fws file
- E. Inspect module.

Answer: C

QUESTION NO: 76

If users authenticated successfully, they have matched the User and Authentication rule restriction of the user group to which they belong.

- A. True
- B. False

Answer: A

QUESTION NO: 77

The only way to unblock BLOCKED connections by deleting all the blocking rules from the Rule base.

- A. True
- B. False

Answer: B

QUESTION NO: 78

When you perform a cp fetch, what can you expect from this command?

- A. Firewall retrieves the user database from the tables on the Management Module.
- B. Firewall retrieves the inspection code from the remote Management Module and installs it to the kernel.
- C. Management module retrieves the IP address of the target specified in the command.
- D. Management module retrieves the interface information for the target specified in the command.
- E. None of the above.

Answer: B

QUESTION NO: 79

Each incoming UDP packet is locked up in the list of pending connections. Packets are delivered if they are _____.

- A. A request.
- B. A response to a request.
- C. Source routed.
- D. Allowed by the Rule Base.
- E. Both B and D.

Answer: E

QUESTION NO: 80

Assume an NT system. What is the default expiration for a Dynamic NAT connection NOT showing any TCP activity?

- A. 30 Seconds.
- B. 60 Seconds.
- C. 330 Seconds.
- D. 660 Seconds.
- E. 3600 Seconds.

Answer: B

QUESTION NO: 81

When you disable a rule the rule is NOT disabled until you verify your Security Policy.

- A. True
- B. False

Answer: B

QUESTION NO: 82

Static Source NAT translates public internal source IP addresses to private external source IP addresses.

- A. True
- B. False.

Answer: B

QUESTION NO: 83

What is the command that lists the interfaces to which VPN-1/FireWall-1 bound?

- A. Fw ct1 iflist
- B. Ifconfig -a
- C. Ifconfig \all
- D. Netstat -m
- E. Cp bind -all

Answer: B

QUESTION NO: 84

Your customer has created a rule so that every time a user wants to go to Internet, that user must be authenticated. Which if the following is the best authentication method for roaming users, such as doctors updating patient records at various floor stations in a hospital?

- A. Session
- B. User
- C. Client
- D. Connection
- E. None of the above.

Answer: A

QUESTION NO: 85

Which command utility allows verification of the Security Policy installed on a firewall module?

- A. Fw ct1 pstat.
- B. Fw printlic.
- C. Fw stat.
- D. Fw ver.
- E. Fw pol.

Answer: E

QUESTION NO: 86

You are a firewall administrator with one Management Server managing 3 different Enforcement Modules. One of the Enforcement Modules does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is the most likely cause?

- A. No master file was created.
- B. License for multiple firewalls has expired.
- C. The firewall has NOT been rebooted.
- D. The firewall was NOT listed in the Install On column of the rule.
- E. The firewall is listed as “Managed by another Management Module (external)” in the Workstation Properties dialog box.

Answer: E

QUESTION NO: 87

In the Install On column of a rule, when you select a specific firewall object as the only configuration object, that rule is enforced on all firewalls with in the network, with related configurations.

- A. True
- B. False.

Answer: B

QUESTION NO: 88

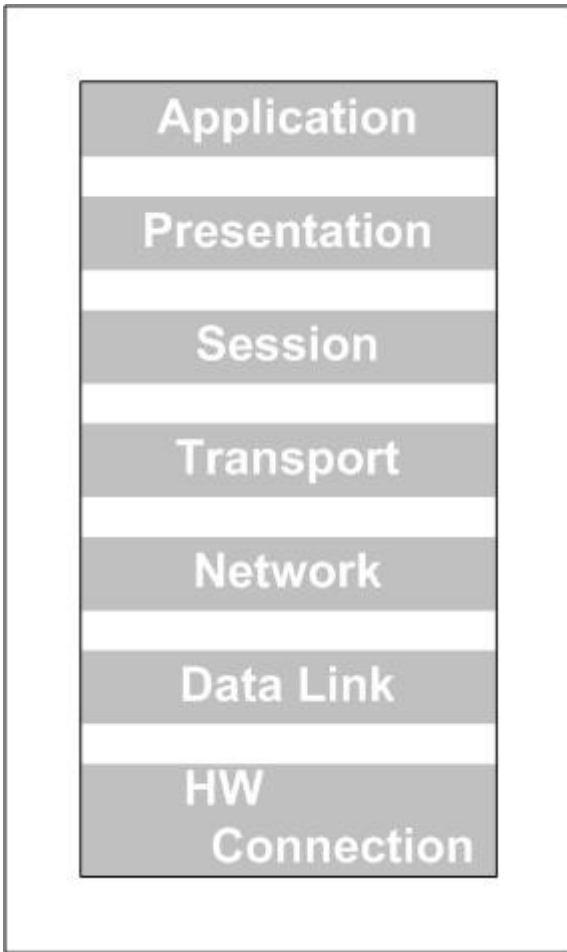
As an administrator, you want to force your users to authenticate. You have selected Client Authentication as your authentication scheme. Users will be using a Web browser to authenticate. On which TCP port will authentication be performed?

- A. 23
- B. 80
- C. 259
- D. 261
- E. 900

Answer: E

QUESTION NO: 89

Once installed the VPN-1/FireWall-1 NG resides directly below what layer of the TCP/IP stack?



- A. Data
- B. Transport
- C. Physical
- D. Application
- E. Network

Answer: E

QUESTION NO: 90

Client Authentication rules should be placed above the Stealth rule, so users can authenticate to the firewall.

- A. True
- B. False

Answer: A

QUESTION NO: 91

The following rule base tells you any automatically created NAT rules have simply hidden but have not been deleted from the Rule Base.

- A. True
- B. False

Answer: A

QUESTION NO: 92

You are using static Destination NAT. You have VPN-1/FireWall-1 NG running on Windows NT/Solaris platform. By default, routing occurs after the address translation when the packet is passing form the client towards the server.

- A. True
- B. False

Answer: B

QUESTION NO: 93

Which if the following statements is FALSE?

- A. Dynamic NAT cannot be used for protocols where the port number cannot be changed.
- B. Dynamic NAT cannot be used when an external server must distinguish between clients bases on their IP addresses.
- C. With Dynamic NAT, packet's source port numbers are modified.
- D. In Dynamic NAT, public internal addresses are hidden behind a single private external address using dynamically assigned port numbers to distinguish between them.
- E. Dynamically assigned post numbers are used to distinguish between hidden private addresses.

Answer: B

QUESTION NO: 94

When you modify a User Template, any users already operating under that template will be updates to the new template properties.

- A. True

B. False

Answer: B

QUESTION NO: 95

Installation time for creating network objects will decrease if you list machine names and IP addresses in the hosts files.

- A. True
- B. False

Answer: A

QUESTION NO: 96

Consider the following network:

No	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service

The administrator wants to take all the local and DMZ hosts behind the gateway except the HTTP server 192.9.200.9. The http server will be providing public services and must be accessible from Internet. Select the best NAT solution below that meets these requirements.

- A. Use automatic NAT that creates a static NAT to the HTTP server.
- B. To hide the private addresses set the address translation for Private Net.
- C. To hide the private address set the address translation for 192.9.200.0.
- D. Use automatic NAT rule creation to hide NAT Local net and private Net.
- E. Both A and D.

Answer: E

QUESTION NO: 97

What NAT made is necessary if you want to start and HTTP session on a Reserved or Illegal IP address?

- A. Static Source.
- B. Static destination.

- C. Dynamic
- D. None of the above.

Answer: C