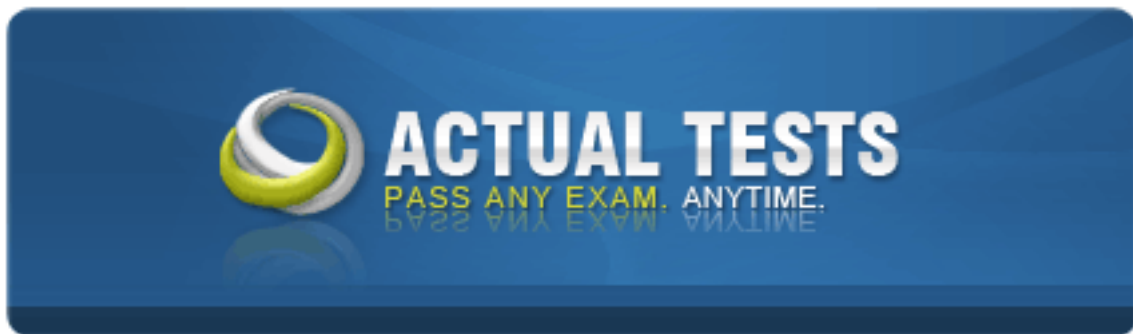# Checkpoint 156-210

156-210.4 Check Point NG with Application Intelligence - Management I

Practice Test

Version 1.2

QUESTION NO: 1

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

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

Answer: A,C

Explanation:
: Object can be renamed and the properties can be edited even after establishing the SIC and issue the certificate
Incorrect Answers:
B: Once SIC has been established and a certificate has been issued, certificate can not be renamed
D: If SIC is reset, the trust has to be re-established, hence this is wrong
E: Type of the object created can not be modified once the certificate has been issued.

QUESTION NO: 2

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

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

Answer: A,C

QUESTION NO: 3

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

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

C. objects_5_0.c

D. $CPDIR/temp directory

E. $FWDIR/state directory

Answer: A,B,C

QUESTION NO: 4

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

A. The General HTTP Worm Catcher can detect only worms that are part of a URI.

B. Security Administrators can configure the type of notification that will take place, if a worm is detected.

C. SmartDefense allows you to configure worm signatures, using regular expressions.

D. The General HTTP Worm Catcher's detection takes place in the kernel, and does not require a Security Server.

E. Worm patterns cannot be imported from a file at this time.

Answer: A

QUESTION NO: 5

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

A. Local licenses are IP specific.

B. A license can be installed and removed on a VPN-1/Firewall-1 version 4.1, using SmartUpdate.

C. You must contact Check Point via E-mail or telephone to create a license for an Enforcement Module.

D. Licenses cannot be installed through SmartUpdate.

E. Licenses are obtained through the Check Point User Center

Answer: A,E

QUESTION NO: 6

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

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

B. Stores VPN-1/FirWall-1 logs.

C. Manages the User Database.

D. Replicates state tables for high availability.

E. Compiles the Rule Base into an enforceable Security Policy.

Answer: B,C,E

QUESTION NO: 7

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

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

Which address translation solution BEST meets your requirements?

A. Hide NAT

B. The requirements cannot be met with any address translation solution.

C. Dynamic NAT

D. IP Pool Nat

E. Static NAT

Answer: E

QUESTION NO: 8

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

A. If most incoming connections are HTTP, but the rule that accepts HTTP at the bottom of the Rule Base, before the Cleanup Rule

B. Use a network object, instead of multiple host-node objects.

C. Do not log unnecessary connections.

D. Keep the Rule Base simple.

E. Use IP address-range objects in rules, instead of a set of host-node objects.

Answer: A

QUESTION NO: 9

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

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

Answer: C

QUESTION NO: 10

Network attacks attempt to exploit vulnerabilities in network applications, rather than targeting firewalls directly.
What does this require of today's firewalls?

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

Answer: C

QUESTION NO: 11

What function does the Audit mode of SmartView Tracker perform?

A. It tracks detailed information about packets traversing the Enforcement Modules.
B. It maintains a detailed log of problems with VPN-1/FireWall-1 services on the SmartCenter Server.
C. It is used to maintain a record of the status of each Enforcement Module and SmartCenter server.
D. It maintains a detailed record of status of each Enforcement Module and SmartCenter Server.
E. It tracks changes and Security Policy installations, per Security Administrator, performed in SmartDashboard.

Answer: E

QUESTION NO: 12

In the SmartView Tracker, what is the difference between the FireWall-1 and VPN-1 queries?
Choose three.

A. A VPV-1 query only displays encrypted and decrypted traffic.
B. A FireWall-1 query displays all traffic matched by rules, which have logging activated.
C. A FireWall-1 query displays all traffic matched by all rules.
D. A FireWall-1 query also displays encryption and decryption information.
E. Implied rules, when logged, are viewed using the VPN-1 query.

Answer: A,B,D

QUESTION NO: 13

Network topology exhibit
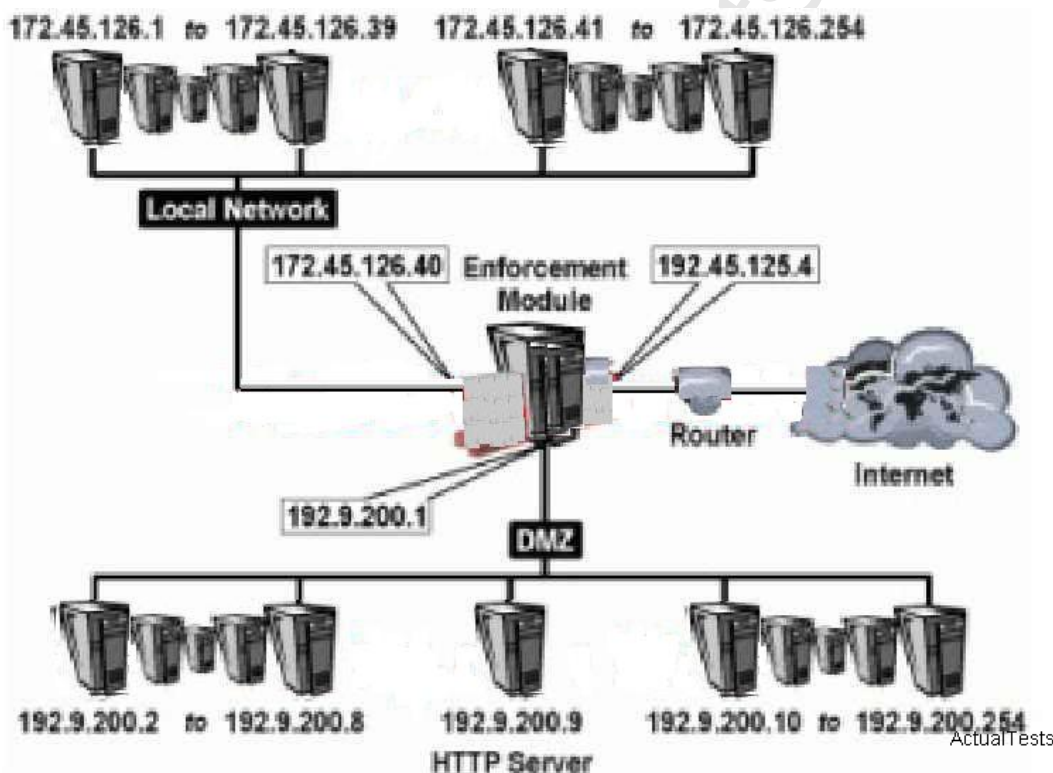
You want hide all localnet and DMZ hosts behind the Enforcemenet Module, except for the HTTP
Server (192.9.200.9). The HTTP Server will be providing public services, and must be accessible
from the Internet.
Select the two BEST Network Address Translation (NAT) solutions for this scenario,

A. To hide Local Network addresses, set the address translation for 192.9.0.0

B. To hide Local Network addresses, set the address translation for 192.9.200.0

C. Use automatic NAT rule creation to hide both DMZ and Local Network.

D. To hide Local Network addresses, set the address translation for privatenet.

E. Use automatic NAT rule creation, to statically translate the HTTP Server address.

Answer: C,E

QUESTION NO: 14

The SmartDefense Storm Center Module agent receives the Dshield.org Block List, and:

A. Populates CPDShield with blocked address ranges, every three hours.

B. Generates logs from rules tracking internal traffic.

C. Submits the number of authentication failures, and drops, rejects, and accepts.

D. Generates regular and compact log digest.

E. Populates the firewall daemon with log trails.

Answer: A

QUESTION NO: 15

What are the advantages of central licensing? Choose three.

A. Only the IP address of a SmartCenter Server is needed for all licences.

B. A central licence can be removed from one Enforcement Module, and installe don another Enforcement Module.

C. Only the IP address of an Enforcement Module is needed for all licences.

D. A central license remains valid, when you change the IP address of an Enforcemente Module.

E. A central license can be converted into a local license.

Answer: A,B,D

QUESTION NO: 16

A security Administrator wants to review the number of packets accepted by each of the Enforcement modules. Which of the following viewers is the BEST source for viewing this information?

A. SmartDashboard

B. SmartUpdate

C. SmartMap

D. SmartView Status

E. SmartView Tracker

Answer: D

QUESTION NO: 17

Hidden (or masked) rules are used to:

A. Hide rules from administrators with lower privileges.

B. View only a few rules, without distraction of others.

C. Temporarily disable rules, without having to reinstall the Security Policy.

D. Temporarily convert specifically defined rules to implied rules.

E. Delete rules, without having to reinstall the Security Policy.

Answer: B

QUESTION NO: 18

Which of the following characteristics BEST describes the behaviour of Check Point NG with Application Intelligence?

A. Traffic not expressly permitted is prohibited.

B. All traffic is expressly permitted by explicit rules.

C. Secure connections are authorized by default. Unsecured connectdions are not.

D. Traffic is filtered using controlled ports.

E. TELNET, HTTP; and SMTP are allowed by default.

Answer: A

QUESTION NO: 19

SmartUpdate CANNOT be used to:

A. Track installed versions of Check Point and OPSEC products.

B. Manage licenses centrally.

C. Update installed Check Point and OPSEC software remotely, from a centralized location.

D. Uninstall Check Point and OPSEC software remotely, from a centralized location.

E. Remotely install NG with Application Intelligence for the first time, on a new machine.

Answer: E

QUESTION NO: 20

Which of the following statements about Client Authentication is FALSE?

A. In contrast to User Authentication that allows access per user. Client Authentication allows access per IP address.
B. Client Authentication is more secure than User Authentication, because it allows multiple users and connections from an authorized IP address or host.
C. Client Authentication enables Security Administrators to grant access privileges to a specific IP address, after successful authentication.
D. Authentication is by user name and password, but it is the host machine (client) that is granted access.
E. Client Authentication is not restricted to a limited set of protocols.

Answer: B

QUESTION NO: 21

Why is Application Layer particularly vulnerable to attacks? Choose three

A. Malicious Java, ActiveX, and VB Scripts can exploit host system simply by browsing.
B. The application Layer performs access-control and legitimate-use checks.
C. Defending against attacks at the Application Layer is more difficult, than at lower layers of the OSI model.
D. The Application Layer does not perform unauthorized operations.
E. The application Layer supports many protocols.

Answer: A,C,E

QUESTION NO: 22

You have created a rule that requires users to be authenticated, when connecting to the Internet using HTTP. Which is the BEST authentication method for users who must use specific computers for Internet access?

A. Client
B. Session
C. User

Answer: A

QUESTION NO: 23

What function does the Active mode of SmartView Tracker perform?

A. It displays the active Security Policy.
B. It displays active Security Administrators currently logged into a SmartCenter Server.
C. It displays current active connections traversing Enforcement Modules.
D. It displays the current log file, as it is stored on a SmartCenter Server.
E. It displays only current connections between VPN-1/FireWall-1 modules.

Answer: C

QUESTION NO: 24

You are importing product data from modules, during a VPN-1/Firwall-1 Enforcement Module upgrade. Which of the following statements are true? Choose two.

A. Upgrading a single Enforcement Module is recommended by Check Point, since there is no chance of mismatch between installed product versions.
B. SmartUpdate queries license information, from the SmartConsole runging locally on the Enforcement Module.
C. SmartUpdate queries the SmartCenter Server and Enforcement Module for product information.
D. If SmartDashboard and all SmartConsoles must be open during input, otherwise the product-data retrieval process will fail

Answer: A,C

QUESTION NO: 25

Which if the following components functions as the Internal Certificate Authority for all modules in the VPN-1/FireWall-1 configuration?

A. Enforcement Module
B. INSPECT Engine
C. SmartCenter Server
D. SmartConsole
E. Policy Server

Answer: C

QUESTION NO: 26

Which of the following is NOT a security benefit of Check Point's Secure Internal Communications (SIC)?

A. Generates VPN certificates for IKE clients.
B. Allows the Security Administrator to confirm that the Security Policy on an Enforcement Module came from an authorized Management Server.
C. Confirms that a SmartConsole is authorized to connect a SmartCenter Server
D. Uses SSL for data encryption.
E. Maintains data privacy and integrity.

Answer: A

QUESTION NO: 27

You are administering one SmartCenter Server that manages three Enforcement Modules. One of the Enforcement Modules does not appear as a target in the Install Policy screen, when you attempt to install the Security Policy. What is causing this to happen?

A. The licence for the Enforcement Module has expired.
B. The Enforcement Module requires a reboot.
C. The object representing the Enforcement Module was created as a Node->Gateway.
D. The Enforcement Module was not listed in the Install On column of its rule.
E. No Enforcement Module Master filer was created, designating the SmartCenter Server

Answer: C

QUESTION NO: 28

You are the Security Administrator with one SmartCenter Server managing one Enforcement Moduel. SmartView Status displays a computer icon with an "I" in the Status column. What does this mean?

A. You have entered the wrong password at SmartView Status login.
B. Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module.
C. The SmartCenter Server cannot contact a gateway.
D. The VPN-1/Firewall-1 Enforcement Module has been compromised and is no longer controlled by this SmartCenter Sever.
E. The Enforcement Module is installed and responding to status checks, but the status is problematic.

Answer: E

QUESTION NO: 29

Check Point's NG with Application Intelligence protects against Network and Transport layer attacks by: (Choose two)

A. Preventing protocol-anomaly detection-

B. Allowing IP fragmentation-

C. Preventing validation of compliance to standards.

D. Preventing non-TCP denial-of-service attacks, and port scanning.

E. Preventing malicious manipulation of Network Layer protocols.

Answer: D,E

QUESTION NO: 30

Which of the following locations is Static NAT processed by the Enforcement Module on packets from an external source to an internal statically translated host?

Static NAT occurs.

A. After the inbound kernel, and before routing.

B. After the outbound kernel, and before routing.

C. After the inbound kernel, and aftter routing.

D. Before the inbound kernel, and after routing.

E. Before the outbound kernel, and before routing.

Answer: C

QUESTION NO: 31

Which of the following does a Check Point security gateway access, analyze, and use? Choose three.

A. Communications information

B. Communication-derivec state

C. Packet sniffing

D. Information mapping

E. Application-derived state

Answer: A,B,E

QUESTION NO: 32

Which NG with Application Intelligence feature allows a Security Administrator to granularly control acceptable FTP commands?

A. FTP Security Server object settings
B. Check Point Gateway object, Security Server settings
C. SmartDefense, FTP Security Server settings
D. Rule Base Service field
E. Global Properties, Security Server settings.

Answer: C

QUESTION NO: 33

You are Security Administrator preparing to deploy a new hot-fix to ten Enforcement Modules at five geographically separated locations. What is the BEST method to implement this hot-fix?

A. Use SmartView installer to deploy the hot-fix to each Enforcement Module.
B. Send a CDROM with the hot-fix to each location, and have local personnel install it.
C. Send a Certified Security Engineer to each site to perform the update.
D. Use SmartInstaller to install the packages to each of the Enforcement Models remotely.
E. Use SmartUpdate to install the packages to each of the Enforcement Models remotely.

Answer: E

QUESTION NO: 34

Implicit rules do NOT allow what types of VPN-1/FireWall-1 Control Connections by default?

A. Outgoing traffic, originating from the gateway
B. RIP for routing configuration
C. IKE and RDP-traffic, for communication and encryption
D. VPN-1/Firewall-1 specific traffic, such as logging, management, and key exchange
E. RADIOUS; CVP, UFP, and LDAP

Answer: B

QUESTION NO: 35

In Secure Internal Communicators (SIC), the SmartCenter Server and its components are identified by a(n):

A. SIC entry in the host file
B. Random seed
C. Port number
D. Distinguished Name
E. IP address

Answer: D

QUESTION NO: 36

Which of the following statements BEST describes Dynamic Network Address Translation (Hide NAT)?

A. Allow you to hide an entire network behind one IP address.
B. Translates private external IP addresses to public IP addresses.
C. Allows you to hide an entire network behind public IP addresses.
D. Translates public internal IP addresses to private IP addresses.
E. Allow you to hide an entire network behind random IP addresses.

Answer: A

QUESTION NO: 37

What type of TCP attack is a bandwidth attack, where a client fools a server into sending large amount of data, using small packets?

A. SMURF
B. SYN-Flood
C. Host System Hogging
D. Small PMTU
E. LAND

Answer: D

QUESTION NO: 38

How is the Block Intruder request used?

A. It is used in place of the HTTP Security Server.
B. SmartDefense automatically uses this capability.
C. It is used in the Log mode of SmartView Tracker to kill active connections.
D. It is activated in SmartDashboard through the Security Policy.
E. It blocks access from a Source, or to a Destination, for a specified amount of time, or indefinitely.

Answer: E

QUESTION NO: 39

A conflict between anti-spoofing and Network Address Translation (NAT) occurs when:

A. The Translate destination on the client-side option is not enabled when using Static NAT:
B. NAT is performed on the client side.
C. Manual NAT rules are used.
D. The Translate destination on the client-side option is enabled.
E. The Translate destination on the server-side option is enabled.

Answer: A

QUESTION NO: 40

One of the most important tasks Security Adminstrators perform is log maintenance. By default, when an administrator clicks File > Switch Active file from SmartView Tracker, the SmartCenter server:

A. Purges the current log file, and prompts the Security Administrator for the mode of the new log.
B. Opens a new window with a previously saved log for viewing.
C. Saves the current log file, names the save file by date and time and starts a new log.
D. Prompts the Security Administrator for the name of the current log, saves it, and then prompts the Security Administrator for the mode of the new log.
E. Purges the current log file, and starts a new log.

Answer: C

QUESTION NO: 41

A VPN-1/FireWall-1 SmartDashboard is used to perform which of the following tasks? Choose two.

A. Allows the Security Administrator to configure Network Address Translation.

B. Stores VPN-1/Firewall-1 logs

C. Compiles the Rule Base into an enforceable Security Policy.

D. Stores the User Database.

E. It is used to crate and define a Security Policy.

Answer: A,E

QUESTION NO: 42 CORRECT TEXT

Exhibit

NO	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK
1	Any	WebServer	Any	TCP http	accept	Log
2	Any	Any	Any	Any	drop	Log

Assuming the default settings in the Global Properties have not changed, which of the following types of traffic will be allowed through a firewall with the Rule Base displayed in the exhibit?

Answer: HTTP

QUESTION NO: 43

In SmartView Status, what does a status of Untrusted tell you?

A. The Enforcement Module is offlien.

B. The Security Administrator has entered the wrong password at SmartView Status login.

C. Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module

D. The SmartCenter Server cannot contact a gateway

E. An Enforcement Module is installed and responding to status checks, but the status is problematic.

Answer: C

QUESTION NO: 44

For which of the following objectd types can Network Address Translation be configured?

A. Domains, host nodes, network.

B. Domains, networks, users

C. Host nodes, networks, OSE devices

D. Host nodes, networks, address ranges

E. Networks, OSE Devices logical servers.

Answer: D

QUESTION NO: 45

Howa re Storm Center Block Lists activated? Choose the correction order.

Security Adminstrators define a CPDShield object and place it in the Rule Base appropriately.The Storm Center Module agent on the Enforcement Module retrieves the Block list, and replaces the CPDSHield object with a list of blocked IP addresses.The Storm Center Module agent periodically checks for updates to the Block list.

A. 3, 2, 1

B. 1, 2, 3

C. 2, 3, 1

D. 3, 1, 2

E. 2, 1, 3

Answer: B

QUESTION NO: 46

Network topology exhibit
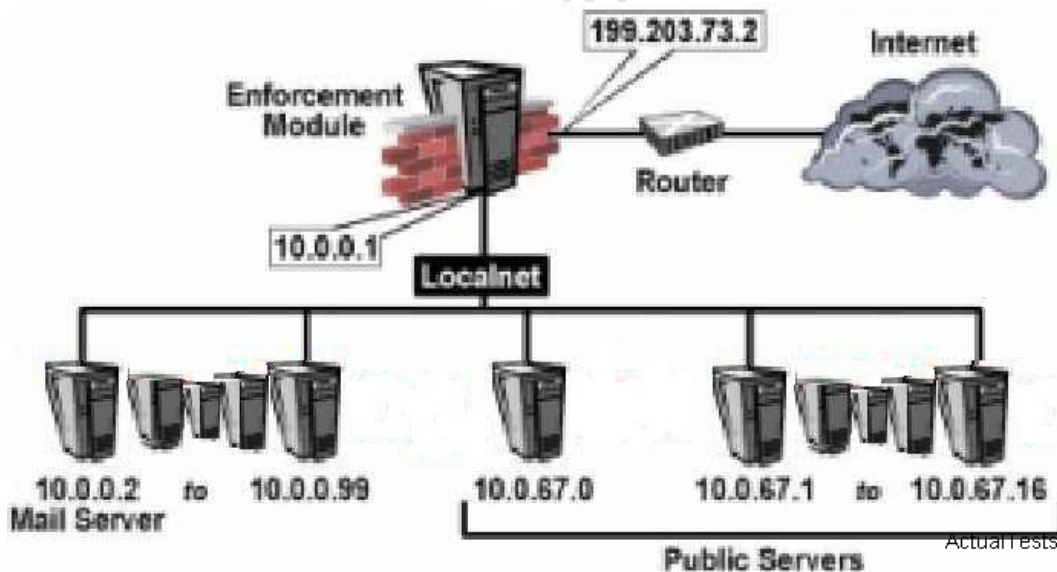
In the network displayed in the exhibit, the public servers accept and initiate connections from the Internet.

The public servers must:

A. Be moved to the other side of the Enforcement Module, and give public addresses.

B. Use Reverse Network Address Translation.

C. Use Static Network Address Translation.

D. Use Dynamic Network Address Translation

E. Network Address Translation is not required.

Answer: C

QUESTION NO: 47

What Blocking Scope options are available when using Block Intruder? Choose three.

A. Block access from this Source.

B. Block source and destination

C. Block access to this Destination.

D. Block only this connection

E. Block all traffic

Answer: A,C,D

QUESTION NO: 48

TO be MOST effective, where should Anti-Spoofing be configured?

A. Only on interfaces facing internal networks.

B. Only on external and DMZ interfaces.

C. Only on DMZ interfaces

D. Only on external interfaces.

E. On all interfaces.

Answer: E

QUESTION NO: 49

Choose the two responses that BEST describe a VPN-1/Firewall-1 Rule Base.
A Rule Base is:

A. A collection of corporate guidelines used to structure the network Security Policies for users operating behind the firewall.

B. A collection of system settings that make up implicit rules defining network security.

C. The process by which secure communications are established between different VPN-1/Firewall-1 Modules, operating within an enterprise security environment.

D. A repository of DLL files, each provides a specific security function.

E. A set of explicitly and implicitly defined rules used to define network security.

Answer: A,E

QUESTION NO: 50

When defining objects, why should you NOT change the name or IP address of the system-created SmartCenter Server objects? Choose two.

A. Changes the certificate of the system-created object

B. Causes a fault-tolerance error on the VPN-1/Firewall-1 Enforcement Module

C. Interferes with Security Policy Installation

D. Does not change the object name in the Rule Base.

E. Negatively affects the Internal Certificate Authority.

Answer: A,E

QUESTION NO: 51 CORRECT TEXT

You are the Security Administrator with one SmartCenter Server managing one Enforcement Module. SmartView Status displays a computer icon with an "?" in the Status column.
What does this mean?

Answer: The VPN-1/FireWall-1 Enforcement Module has been compromised and is no longer controlled by this SmartCenter Server.
Answer: Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module.
Answer: The Enforcement Module is installed and responding to status checks, but the status is problematic.
Answer: You have entered the wrong password at SmartView Status login.
Answer: The SmartCenter Server cannot contact the gateway.
Answer: Pending

QUESTION NO: 52 CORRECT TEXT

Which statement below BEST describes how VPN-1/FireWall-1 handles hidden rules?
Hidden rules are:

Answer: Not included when the Security Policy is installed.
Answer: Removed from the existing Security Policy.

Answer: Enforced when the Security Policy is installed.

Answer: Automatically installed, when the Unhide All option is selected from the Hide Rules menu.

Answer: Enforced as implied rules, before the explicitly defined Rule Base.

Answer: Pending

QUESTION NO: 53 CORRECT TEXT

Which of the following is NOT included in SVN Foundation?

Answer: Watch Dog for Critical Services

Answer: License Utilities

Answer: CPShared Daemon

Answer: SmartDefense

Answer: SNMP Daemon

Answer: Pending

QUESTION NO: 54 CORRECT TEXT

Which of the following BEST describes the function of Dynamic Network Address Translation (Dynamic NAT)?
Dynamic NAT:

Answer: Allows you to configure more public IP addresses than you have hosts.

Answer: Reduces the load on the Enforcement Module.

Answer: Limits the number of internal hosts that may access the Internet.

Answer: Reduces the number of connections to your Web server.

Answer: Allows you to configure for more hosts than you have public IP addresses.

Answer: Pending

QUESTION NO: 55 CORRECT TEXT

Which Block Intruder options block suspicious connections? (Choose three)

Answer: Block Connections by Packet Size.

Answer: Block Access from that Source.

Answer: Block Connections using Specific Services.

Answer: Block Access to the Destination.

Answer: Block Selected Connection.

Answer: Pending

QUESTION NO: 56 CORRECT TEXT

Which of the following denial-of-service attacks does SmartDefense defeat? (Choose three)

Answer: Ping of Death
Answer: Rouge Applets
Answer: Teardrop
Answer: Host System Hogging
Answer: LAND
Answer: Pending

QUESTION NO: 57 CORRECT TEXT

What are the benefit of Stateful Inspection? (Choose two)
Stateful Inspection:

Answer: Shuts down the upper-range ports, to secure an internal network.
Answer: Uses state information derived from past communications and other applications, to make control decisions for new communication attempts.
Answer: Leaves the upper range of ports (greater than 1023) open, to allow for file-transfer sessions.
Answer: Duplicates the number of sessions, acting as a proxy broker between a client and server.
Answer: Examines every packet, and applies a defined Security Policy to each.
Answer: Pending

QUESTION NO: 58 CORRECT TEXT

Which of the following are core functions of Application Intelligence? (Choose two)

Answer: Validating compliance to standards.
Answer: Validating simple protocols, without controlling application logic.
Answer: Validating Data and Physical Layer attacks.
Answer: Limiting the ability of applications to carry malicious data.
Answer: Allowing Application Layer operations.
Answer: Pending

QUESTION NO: 59 CORRECT TEXT

One of the functions of the SmartDefense console is to:

Answer: Add rules to block and log attacks.

Answer: Configure user options for tracking attacks.

Answer: Display real-time information about attacks.

Answer: Configure logging options for attack forensics.

Answer: Configure auditing and reporting options.

Answer: Pending

QUESTION NO: 60 CORRECT TEXT

The SANS Dshield.org Storm center integrates with SmartDefense, by: (Choose two)

Answer: Reviewing VPN-1/FireWall-1 logs.

Answer: Providing Storm Center audit trails.

Answer: Setting up the SmartDefense Subscription service.

Answer: Adding the Storm Center Block List report to the Security Policy.

Answer: Updating SmartDefense attack signatures in real time.

Answer: Pending

QUESTION NO: 61 CORRECT TEXT

Systems needing to be accessed from the Internet should use which type of address translation?

Answer: IP Pool NAT

Answer: Hide NAT

Answer: NAT cannot be used

Answer: Static NAT

Answer: Dynamic NAT

Answer: Pending

QUESTION NO: 62 CORRECT TEXT

VPN-1/FireWall-1 logs are exportable to other applications, such as spreadsheets or databases, using which of the following?

Answer: FW Log Unification Engine

Answer: Secure Internal Communications (SIC)

Answer: Check Point logs are not exportable

Answer: Log Export Application (LEA)

Answer: Log Identification Unique ID (LUUID)

Answer: Pending

QUESTION NO: 63 CORRECT TEXT

Which of the following is NOT configured under Application Intelligence in SmartDefense?

Answer: FTP

Answer: DNS

Answer: Dynamic Ports

Answer: Rlogin

Answer: VoIP

Answer: Pending

QUESTION NO: 64 CORRECT TEXT

Which type of rule should be placed above the Stealth Rule?

Answer: User Authentication

Answer: Client Authentication

Answer: Network Address Translation

Answer: Cleanup

Answer: Session Authentication

Answer: Pending

QUESTION NO: 65 CORRECT TEXT

Bad weather and a UPS failure caused your remote Enforcement Module to reboot. Earlier that day, a tornado destroyed the building where the SmartCenter Server was located. You have not yet recovered or replaced the SmartCenter Server.
Which of the following statements is false? (Choose two)
Because the Enforcement Module cannot connect to the SmartCenter Server.

Answer: The Enforcement Module will log locally.

Answer: The Enforcement Module will continue to enforce the last Security Policy installed.

Answer: No Security Policy is installed, and all traffic will be dropped.

Answer: No Security Policy is installed, and all traffic will be allowed.

Answer: The Enforcement Module attempts to fetch a Security Policy from the SmartCenter Server, and install it.

Answer: Pending

QUESTION NO: 66 CORRECT TEXT

Which of the following is NOT included in Application Intelligence Web Security?

Answer: HTTP Worm Catcher
Answer: Peer-to-Peer traffic over HTTP
Answer: Cross-Site Scripting
Answer: HTTP Format Size
Answer: HTTP Java Blocker
Answer: Pending

QUESTION NO: 67 CORRECT TEXT

Which of the following statements are TRUE of VPN-1/FireWall-1 groups? (Choose two)

Answer: Groups can be nested in groups.
Answer: The contents of one group can be imported into another group.
Answer: Services and network objects can be placed in the same group.
Answer: User groups can be nested, but network-object groups cannot.
Answer: Users and services can be placed in the same group.
Answer: Pending

QUESTION NO: 68 CORRECT TEXT

You have locked yourself out, with a rule or an incorrectly configured Security Policy. What would you do to recover communication between your SmartCenter Server and Enforcement Module?

Answer: fw push localhost
Answer: pw unloadlocal
Answer: fw unlocklocal
Answer: cpstop localhost
Answer: cpdelete localhost
Answer: Pending

QUESTION NO: 69 CORRECT TEXT

How does SmartDefense Integrate with network Storm Centers? (Choose two)

Answer: Security Administrators can decide to send logs to a Storm Center to help other organizations.
Answer: The SmartDefense Storm Center Module downloads the Block List Report directly, adding it to the Security Policy.

Answer: Security Administrators must manually compile log files before sending them to Storm Centers.
Answer: Security Administrators must create network objects for each of the systems on the Storm Center Block List, then install a new Security Policy.
Answer: By default, logs are automatically delivered to a Storm Center.
Answer: Pending

QUESTION NO: 70 CORRECT TEXT

Which of the following statements is TRUE of transparent authentication in NG with Application Intelligence? (Choose three)

Answer: Unknown users are prompted three times for a password, and are then disconnected.
Answer: Unknown users receive error messages, indicating that the Enforcement Module does not recognize user names.
Answer: NG with Application Intelligence does not allow connections from users who do not know the name or IP address of the Enforcement Module.
Answer: NG with Application Intelligence prompts for user names, event though authentication data may not be recognized by the Enforcement Module.
Answer: NG with Application Intelligence allows connections from authenticated users, and does not require that users know the IP address or name of the firewall.
Answer: Pending

QUESTION NO: 71 CORRECT TEXT

At Certpaper, auditors are Check Point Security Administrators with a customized permissions profile. Auditors must have the ability to review information from SmartView Tracker, SmartView Status, and SmartView Monitoring, but they may not make changes to the information. Auditors are not permitted to view security Policies or the objects database.

Which of the following settings grants auditors the MOST appropriate set of permissions, based on the corporate environment, described above for Certpaper?

Answer: Read-Only SmartView Reporter
Answer: Read-Only Monitoring
Answer: Read-Only Security Policy
Answer: Read-Only SmartUpdate
Answer: Read-Only Log Consolidator
Answer: Pending

QUESTION NO: 72 CORRECT TEXT

When are Anti-Spoofing Rules enforced during packet inspection?

Answer: Before the Cleanup Rule is applied.
Answer: After the Stealth Rule is applied.
Answer: Before any rule in the Rule Base is applied.
Answer: When the packet is authorized by an Accept or Encrypt rule.
Answer: Pending

QUESTION NO: 73 CORRECT TEXT

Which of the following objects are allowed in the Source components of the Rule Base? (Choose two)

Answer: Host-Node Objects
Answer: Time Objects
Answer: LDAP Account Units
Answer: Services
Answer: User Groups
Answer: Pending

QUESTION NO: 74 CORRECT TEXT

Which of the following is TRUE, if you change the inspection order of implied rules?

Answer: You must stop and start the Enforcement Module, before the changes can take place.
Answer: After the Security Policy is installed, the order in which rules are enforced changes.
Answer: You cannot change the inspection order of implied rules.
Answer: You must stop and start the SmartCenter Server, before the changes can take place.
Answer: Security Policy installation will fail.
Answer: Pending

QUESTION NO: 75 CORRECT TEXT

Security Administrators use Session Authentication when they want users to: (Choose two)

Answer: Authenticate for all services.
Answer: Use only TELNET, FTP, Rlogin, and HTTP services.
Answer: Use only HTTP and HTTPS services.
Answer: Authenticate once, and then be able to use any service, until logging off.

Answer: Log authentication actions locally.
Answer: Pending

QUESTION NO: 76 CORRECT TEXT

Which of the following statements is TRUE concerning how NG with Application Intelligence handles the authentication of users?

Answer: Users may have different VPN-1 & FireWall-1 passwords, on Enforcement Modules managed by the same SmartCenter Server.
Answer: All users on the same gateway must use the same authentication method.
Answer: All imported users must use the same authentication method and hash.
Answer: All users in the same group must use the same authentication method and hash.
Answer: Users may be required to use different authentication methods for different services.
Answer: Pending

QUESTION NO: 77 CORRECT TEXT

Spoofing is a method of:

Answer: Making packets appear as if they came from an authorized source IP address.
Answer: Hiding your Enforcement Module from unauthorized users.
Answer: Disguising an invalid IP address behind an authorized IP address.
Answer: Detecting when someone is attacking your network.
Answer: Detecting users logging in using false or wrong authentication logins.
Answer: Pending

QUESTION NO: 78 CORRECT TEXT

Which of the following statements is TRUE when modifying user templates?

Answer: If the user template is modified, all active user connections will be dropped when the modifier user database is installed.
Answer: All users subsequently created with that template will have the new properties.
Answer: You must always create new templates. Existing user templates cannot be modified.
Answer: All users previously created using the template are automatically modified with the new properties.
Answer: If the user template is modified, you must manually re-establish user-group membership.
Answer: Pending

QUESTION NO: 79 CORRECT TEXT

As a Security Administrator, you want to force users to authenticate. You have selected Client Authentication for the type of authentication. Users will be using a Web browser to authenticate. Which of the following TCP ports will authenticate users?

Answer: 23
Answer: 261
Answer: 80
Answer: 900
Answer: 259
Answer: Pending

QUESTION NO: 80 CORRECT TEXT

Which of the following is NOT a step in the Session Authentication process?

Answer: If authentication is successful, the VPN-1/FireWall-1 Enforcement Module allows connections to pass.
Answer: The Session Agent prompts users for an authentication password, after Phase 1 of IKE negotiations is complete.
Answer: Users initiate connections directly to a server.
Answer: The Session Agent prompts users for authenticated data, and returns the information to the Enforcement Module.
Answer: The VPN-1/FireWall-1 Enforcement Module intercepts connections, and connects to t he Session Agent.
Answer: Pending

QUESTION NO: 81 CORRECT TEXT

With VPN-1/FireWall-1 central licensing, a license is linked to which of the following?

Answer: Domain name of the SmartCenter Server.
Answer: IP address of the Enforcement Module.
Answer: IP address of the SmartCenter Server.
Answer: IP address of the SmartConsole
Answer: Domain name of the Enforcement Module.
Answer: Pending

QUESTION NO: 82 CORRECT TEXT

Your organization's internal programming team developed a proprietary application for accessing the time-management system. The application uses a custom-designed protocol. As the Security Administrator, you must control user access to the time-management system.
Which is the BEST authentication method for this scenario?

Answer: NG with Application Intelligence authentication methods can only be applied to protocols included in the standard, pre-defined suite.
Answer: Implicit User Authentication
Answer: User Authentication
Answer: Session Authentication
Answer: Pending

QUESTION NO: 83 CORRECT TEXT

Which of the following is the BEST authentication for roaming users, such as doctors updating patient records via HTTP at various workstations in a hospital?

Answer: Client
Answer: Session
Answer: User
Answer: Pending

QUESTION NO: 84 CORRECT TEXT

Which of the following statements is specifically TRUE of user groups?

Answer: Non-authentication rules require a user group in the Source field.
Answer: Authentication rules require a user group in the Source field.
Answer: User groups must be created, in order to implement authentication.
Answer: Authentication rules require a user group in both the Source and Destination field.
Answer: User groups cannot be used in authentication rules.
Answer: Pending

QUESTION NO: 85 CORRECT TEXT

You have created a SmartConsole Administrator with Read Only privileges in the Check Point Configuration Tool.
Which of the following actions can this administrator perform? (Choose three)

Answer: Filter log files in the SmartView Tracker.

Answer: Review saved policies.

Answer: Change network object properties.

Answer: Install policies

Answer: Log in to the SmartDashboard.

Answer: Pending

QUESTION NO: 86 CORRECT TEXT

VPN-1/FireWall-1 supports User Authentication for which of the following services?
Select the response below that contains the MOST complete list of supported services.

Answer: FTP, FTPS, HTTP, HTTPS

Answer: Rlogin, TELNET, HTTP, FTP

Answer: POP3, SMTP, HTTPS, FTPS

Answer: TELNET, HTTP, FTP, SMTP

Answer: Rlogin, TELNET, HTTP, SMTP

Answer: Pending

QUESTION NO: 87 CORRECT TEXT

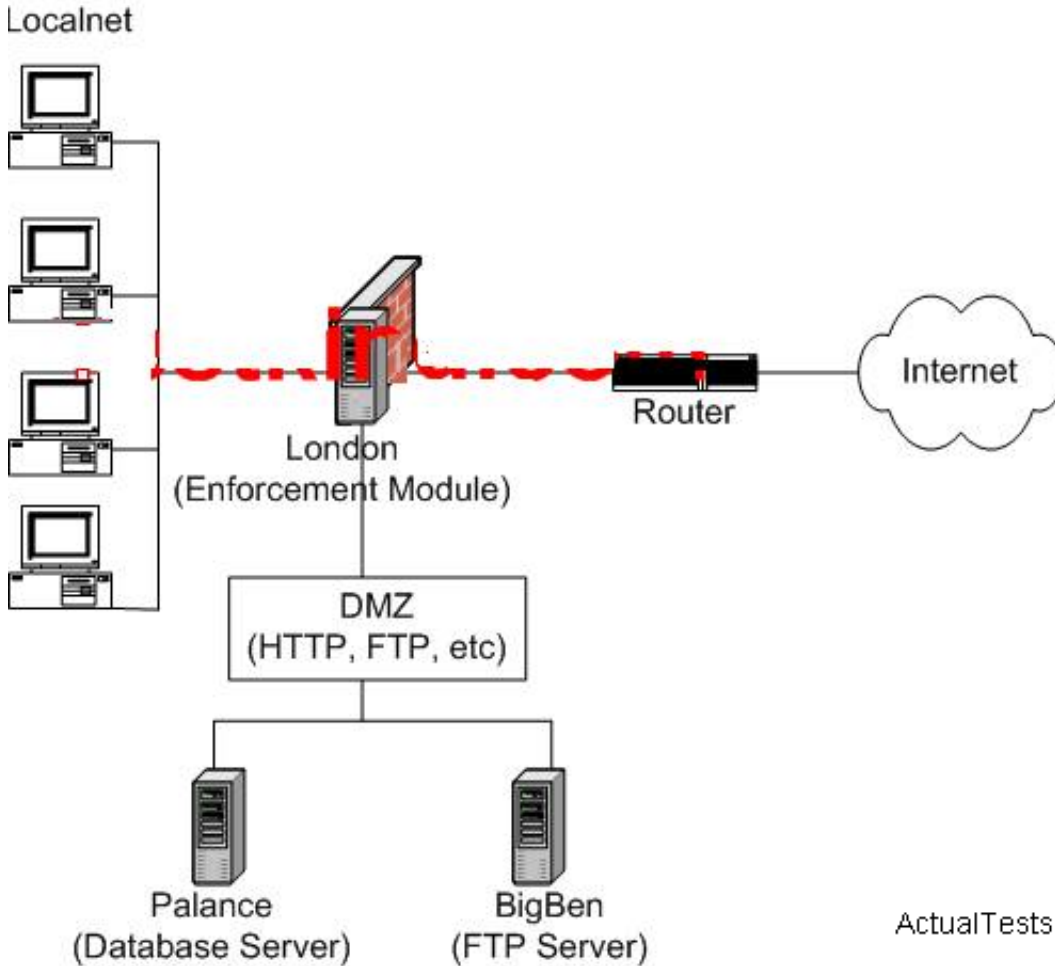User Authentication supports all of the following services, EXCEPT:

Answer: SSH

Answer: FTP

Answer: HTTP

Answer: RLOGIN

Answer: TELNET

Answer: Pending

QUESTION NO: 88 CORRECT TEXT

Localnet

London
(Enforcement Module)

Router

Internet

DMZ
(HTTP, FTP, etc)

Palance
(Database Server)

BigBen
(FTP Server)

ActualTests

In the diagram, a group of users in the QA Department requires frequent access to the Palace Server. Access to Palace is allowed from localnet hosts. Each user can log in at the beginning of the day, and can use the service for a specified time period and number of sessions. If a user forgets to log out, the connection to Palace is closed at the end of the authorization period.

Which of the following rules allows access to the Palace Server, from QA users on the local network? QA users' source (un the Rule Base) is QA@Localnet.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	QA@Localnet	Palace	sqlnet1	Client Auth	Log	Policy Targets	Any
2	QA@Localnet	London	sqlnet1	Client Auth	Log	Policy Targets	Any
3	QA@Localnet	BigBen	sqlnet1	Client Auth	Log	Policy Targets	Any
4	QA@Localnet	Palace	sqlnet1	Session Auth	Log	Policy Targets	Any

Answer: Rule 3

Answer: Rule 4

Answer: None of these rules allows access

Answer: Rule 1

Answer: Rule 2

Answer: Pending

QUESTION NO: 89 CORRECT TEXT

Which authentication method could be used for H.323 services? (Choose two)

Answer: Client Authentication
Answer: VoIP Authentication
Answer: User Authentication
Answer: No Authentication can be used for H.323
Answer: Session Authentication
Answer: Pending

QUESTION NO: 90 CORRECT TEXT

Which authentication method could be used for SIP services? (Choose two)

Answer: Client Authentication
Answer: No authentication can be used for SIP
Answer: VoIP Authentication
Answer: Session Authentication
Answer: User Authentication
Answer: Pending

QUESTION NO: 91 CORRECT TEXT

When the Client Authentication method requires Manual Sign On, users must connect to which of the following ports?

Answer: TELNET to port 70, or HTTP to port 443
Answer: TELNET to port 161, or HTTP to port 136
Answer: TELNET to port 21, or HTTP to port 80
Answer: TELNET to port 165, or HTTP to port 514
Answer: TELNET to port 259, or HTTP to port 900
Answer: Pending

QUESTION NO: 92 CORRECT TEXT

In the Client Authentication Action Properties dialog box, the Manual Sign On method is selected. This means:

Answer: If a connection matches the Rule Base and the service is an authenticated service, the client is signed on after a successful authentication.

Answer: The user must TELNET to the target server on port 250.

Answer: If a connection using any service matches the Rule Base, the client is authenticated.

Answer: If authentication is successful, access is granted from the network that initiated the connection.

Answer: the user must initiate a Client Authentication session to the gateway.

Answer: Pending

QUESTION NO: 93 CORRECT TEXT

Which of the following responses is TRUE about creating user templates? (Choose two)

Answer: By default, users can authenticate 24 hours a day, 7 days a week.

Answer: If not specific source or destination is selected users can authenticate to any source or destination.

Answer: If no password options are selected, users will still be able to authenticate, by creating their passwords during login.

Answer: When you create new users, you must create a new template for each user.

Answer: If no encryption method is selected, users will only be able to authenticate when they receive their Certificate Authority.

Answer: Pending

QUESTION NO: 94 CORRECT TEXT

What is the advantage of using VPN-1/FireWall-1 Password for the authentication scheme, rather than using OS Password?

Answer: The OS Password authentication scheme can only be used with services available to user's local machine.

Answer: There is not advantage, because VPN-1/FireWall-1 Password can only be used, if a user has an operating-system account on the network.

Answer: The OS Password authentication scheme can only be used with users who are present on the local network protected by the Enforcement Module. No external users can be configured for OS Password authentication.

Answer: VPN-1/FireWall-1 Passwords can be cached on the Enforcement Module. If a user in the user database attempts a connection, that user will not be prompted to re-enter the password.

Answer: VPN1-/FireWall-1 Passwords can be used, even if a user does not have an operating-system account on the network.

Answer: Pending

QUESTION NO: 95 CORRECT TEXT

Which of the following statements accurately describes VPN-1/FireWall-1 Session Authentication? (Choose three)

Answer: Session Authentication allows unlimited connections from a single host or IP address.
Answer: Session Authentication does not result in any additional connections to the Enforcement Module.
Answer: Session Authentication is restricted to a limited number of service.
Answer: Session Authentication requires that an authentication agent be installed on client computers.
Answer: Session Authentication requires an authentication procedure for each connection.
Answer: Pending

QUESTION NO: 96 CORRECT TEXT

You have created a rule so that every time a user wants to connect to the Internet using HTTP, that user must be authenticated. You want an authentication scheme that provides transparency for the user, and administrative control for you. The user must be able to log in from any location. Which authentication scheme meets your needs?

Answer: Client
Answer: Session
Answer: Users
Answer: Pending

QUESTION NO: 97

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

Explanation:
as stated in the Checkpoint Official Website, the User interface of the NG suite is composed of 3 components:

The Security Policy Editor (Where you create the rulebase entries).

The Visual Policy Editor (That let you see a graphical view of you Checkpoint Deployment).

The Object Tree (Where you can find the created objects of your Checkpoint implementation).

Incorrect Answers:

B: Those are components of the infrastructure, not from the user interface.

C: The inspection module is not a part of the user interface, it's the part of code installed on the firewall that makes the actual inspection.

D: The security server is not part of the interface, and there is not such a thing like System GUI.

E: Those are components of the infrastructure, not of the Interface.

QUESTION NO: 98

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?

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

Answer: A

Explanation:

The client authentication will not be performed because rule 1 states that every packet that is destined to fw.chicago.com will be dropped (without creating a log entry) for any kind of traffic, the firewall will not accept any connection to it, therefore the authentication request will be dropped either at port 259 for Telnet or port 900 with HTTP.

Incorrect Answers:

B: This rule provide the authentication.

C: This rule is not related to FTP.

D: This is the clean-up rule, perfectly correct at the end of the rule base.

QUESTION NO: 99

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

Explanation:

an address range is a type of object that you can use inside a rulebase only for the purposes of address translation. It allows you to consolidate IP addresses of a undistributed fashion.
Reference: Essential Check Point Firewall 1. Page 64.

Incorrect Answers:

B: We could use an address range, therefore this answer is wrong.

QUESTION NO: 100

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 Private IP addresses
199.203.73.15-199.203.73.115 200.0.0.100-200.0.0.200

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.
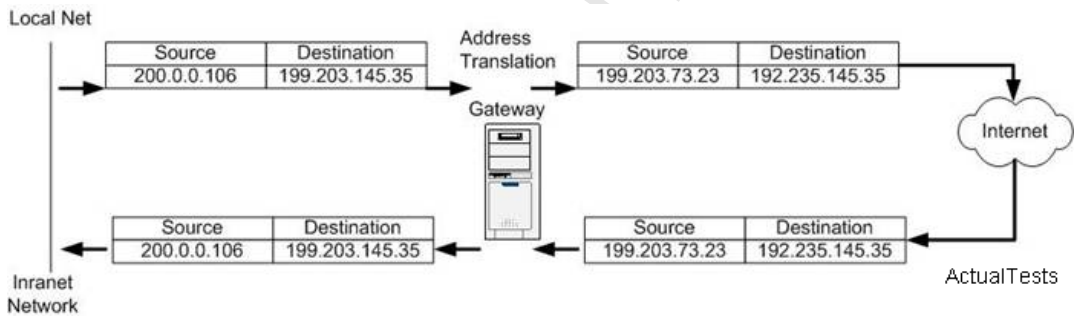
A. True
B. False

Answer: B

Explanation:

As we can see in the exhibit, this statement is wrong because when the packet is coming back with a reply from Internet to the gateway the source address should be the address of the Internet server, not the translated public address from the Checkpoint Firewall making the translation.

Incorrect Answers:

A: The exhibit cannot be true because you cannot have a reply with the same IP address in the source field that you used to make the request when you lived your gateway in your local network.

QUESTION NO: 101

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

Explanation:
this is one of the best practices recommended by Checkpoint engineers, if you have a large number of entries in your rulebase for multiple remote firewalls you can have one rulebase for each remote one, so you can simplify your administration for each of them.

Incorrect Answers:
A: This is not recommended because you could have hosts in one network sending packets through multiple firewalls modules, so you don't need to manipulate Network Range objects.
B: Checkpoint is trying to make their products as consolidated as possible, they are trying to put all the components in the same console, as is the case of the Policy Editor that includes "Object Tree", "Visual Policy Editor" and "Security Policy Editor", in the same console.
C: this is not an option because this rules are often necessary to comply with business requirements, they are best practices too.
E: is incorrect because Answer D is the only valid choice.

QUESTION NO: 102

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. None of the above.

Answer: B

Explanation:

The "active Connection" is one of the 3 available modes inside the Log Viewer, it allows you to see in real time what is the status of certain connections that are passing though the firewall, FTP connections are supported.

Incorrect Answers:

A: This does not provide real time capabilities, its not even a Log viewer mode.

C: The only component that provide real time information inside the Log Viewer is the Active Connection Log. No other provide real time capabilities.

D: The only component that provide real time information inside the Log Viewer is the Active Connection Log. No other provide real time capabilities.

E: is wrong because answer B is the right choice.

QUESTION NO: 103

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

Explanation:

this functionality is achieved by selecting "Block only this connection" from the Block Intruder Dialog Box. This is the blocking mode for intruders by default. Source: Essential Checkpoint Firewall 1.

Incorrect Answers:

B: To achieve this functionality you don't have a valid Blocking Scope option.

C: This could be achieved with "Block access to this destination", but this is not the default option.

D: To achieve this functionality you don't have a valid Blocking Scope option.

E: Only A is the correct answer, see above.

QUESTION NO: 104

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.

A. True
B. False

Answer: B

Explanation:
by default a Checkpoint NG implementation will not allow ICMP traffic through the firewall, you can change this at the Global Configuration Properties through implied rules. There are also no explicit rules in the rulebase allowing the ICMP traffic to come trough in case the implied are at the end.
Incorrect Answers:
A: By default ICMP is not allowed through the Firewall inspection module.

QUESTION NO: 105

Which is the correct rule in the following Rule Base?

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

Answer: B

Explanation:
Rule 1 is the entry to apply to our rulebase, in this rule we are including all the users defined at Chicago , giving access to any service at any destination always that the session could be authenticated. This rule is the only one that covers the needs of the questions in a 100%.
**Incorrect Answers:**
A: Rule 2 is incorrect since you cannot have the users at the same source to the same destination, in this fashion, the traffic is local and it doesn't need to pass though the gateway. That is not a good practice.
D: Putting "ANY" on the service entry is not correct because user authentication only works with HTTP, Telnet, FTP and RLogin, not with "ANY" service.

QUESTION NO: 106

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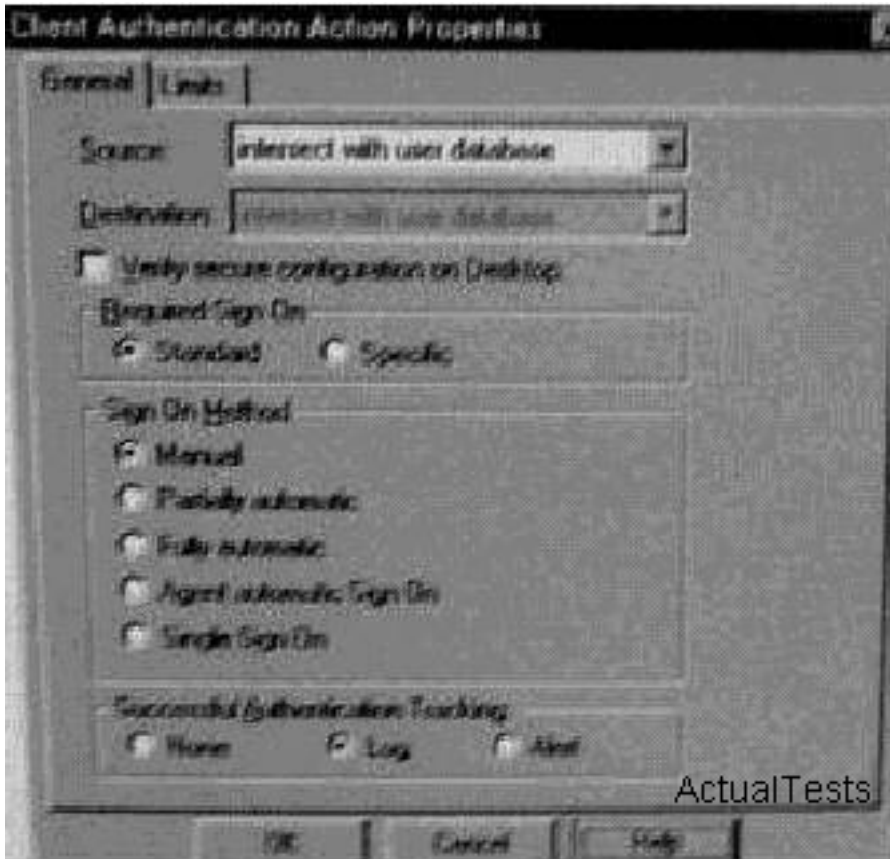
This means:

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

Explanation:
When you select the option "Manual" at the Client Authentication Action dialog box the users have to connect to port 259 with telnet or connect to port 900 with HTTP using a web browser to make the authentication process at the gateway. This process must be done manually and works for the rest of the session.
Incorrect Answers:
A: The authentication must be manual.
C: The authentication must be manual.
D: the "Manual" option tell us about connecting to the gateway to authenticate our request, not about what happen if its successful. Don't loose the focus of the question.
E: You can also connect to port 900 by HTTP, the "must" in the question make's it a wrong answer.

QUESTION NO: 107

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.
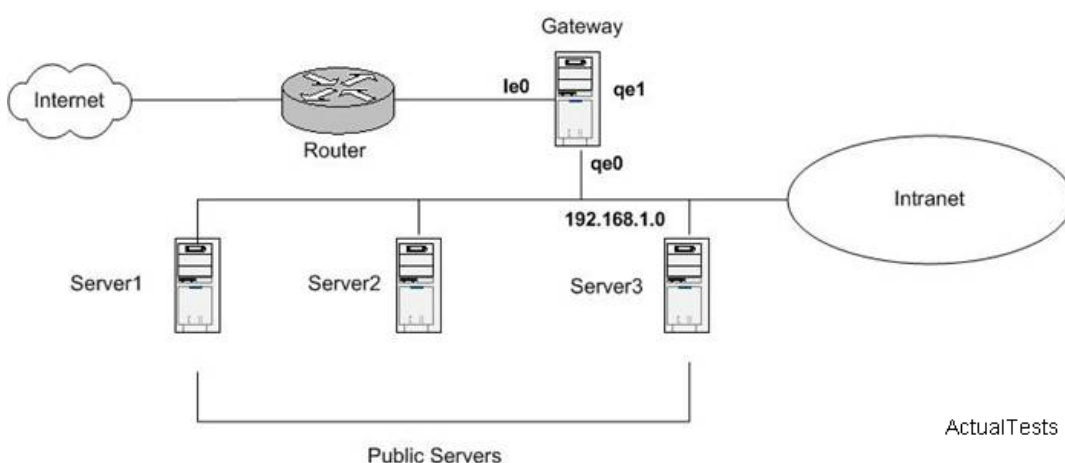
Answer: C

Explanation:
If you make changes to your configuration / rulebase and you want them to be applied to your Firewall modules you have to install the updated policy (that contains the modified rulebase) from the Install Policy button at the Policy Editor. When you are installing the policy, the Management Server translates the configuration to Inspect code and then pushes it to the applicable firewalls at their Inspection engine.
Incorrect Answers:
A: To make policy changes effective in the firewall modules you have to install it, when you save it, you are only storing the new definition, but not pushing it to the gateway modules for enforcement.
B: When you verify a policy you are only checking the syntax, the rule order and the objects, you are not enforcing the definition on the gateway modules.
D: The changes made to a policy are not enforced through the start or stop of the Firewall service in any of the components of the infrastructure.
E: The changes made to a policy are not enforced through the start or stop of the Firewall service in any of the components of the infrastructure.

QUESTION NO: 108

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

Explanation:

since you want the servers to accept connections from the outside, you cannot use Dynamic translation because the firewall will not know to which server should send the packets in the Intranet. When you require public servers inside you firewall to accept connections from the outside you have to use Static Translation, in a one-to-one IP address Public-Private translation. You can use Dynamic Translation if you only want your servers to begin connections but not receive new ones from the outside.

Incorrect Answers:

A: You can't use dynamic translation to advertise services and receive connections outside your gateway, you can use static translation in this case to achieve the desired functionality.

QUESTION NO: 109

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

Explanation:

The "fw fetch" command is issued at the gateway module and it provides a way to pull an applicable security policy from a management server and install it in the gateway kernel as inspect code. You can call it through the command line. To make a successful Fetch of a policy you need to have the firewall object defined in the Management Server through the Policy Editor. You must also have a valid trust relationship implemented through the management server and the firewall module.

Example: fw fetch 192.168.1.1

Incorrect Answers:

B: Fetch command is not used to fetch users, its used to fetch policies.

C: With the fetch command you cant make an output of the content of the policy, you can just install it on the local module.

D: This command is not related to logs, its related to policy installation.

E: The fw fetch command does not provide an interface with the system status.

QUESTION NO: 110

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

Explanation:

When a Checkpoint Gateway cannot contact one of the management servers, it will boot up and fetch the last successfully installed policy from the local disc enforcing the latest rule base available when the Management server was active. In this case the Gateway will log locally. The gateway will not get locked, it will keep running with that policy until you can contact a valid management server.

Incorrect Answers:

A: This is true, when the firewall module cannot contact its management server, it enforces the last successfully installed policy.

B: This is true, the firewall module logs locally until its Management server comes reachable again.

C: This is true, when the firewall module cannot contact its management server it fetch the last successfully installed policy from itself.

D: If you want to install a policy from a replacement management server you first need to make contact with it, and negotiate a secure channel for the data transmission containing the policy definition in inspect code.

QUESTION NO: 111

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

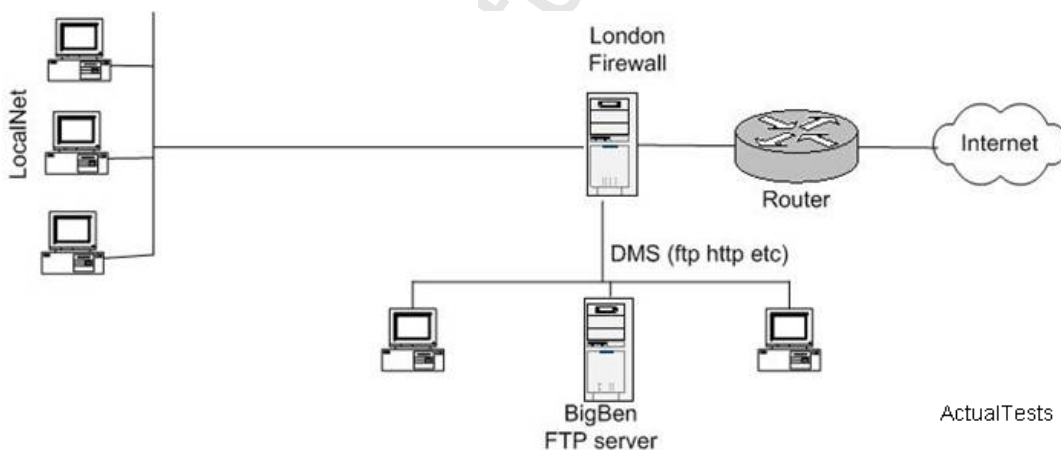E. None of the above.

Answer: C

Explanation:

When you are configuring anti-spoofing on a Checkpoint gateway you have the following 3 options: "Not Defined" that will disable anti-spoofing, "Network Defined by the Interface and Net Mask" that will calculate the topology in base of you current network and "Specific" where you can specify a range of addresses or a group of networks. "Security Policy Installed" is not a valid option.

Incorrect Answers:

A: This is one of the 3 options provided at the properties of the firewall module.

B: Yes, you could have it disabled, This is also one of the 3 options provided at the properties of the firewall module.

D: This is one of the 3 options provided at the properties of the firewall module. Its defined by yourself.

E: Option C is incorrect, so this answer is wrong.

QUESTION NO: 112

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.

A. Rule 1.

B. Rule 2.

C. Rule 3.

D. Rule 4.

E. None of these rules allow access.

Answer: A

Explanation:

Rule 1 is the appropriate rule in here because since we want the managers to access from any location we have the "@any" at the end of the source with an user authentication action that is the most appropriate authentication method because the local managers group wants to make FTP connections and User authentication provides advanced proxy services for FTP. It also supports HTTP, Telnet and Rlogin.

Incorrect Answers:

B: Rule 2 is incorrect because we want the managers to access from anywhere.

C: Rule 3 is incorrect because Session authentication does not provide the advanced capabilities of User authentication in the case of the FTP service

D: Rule 4 is incorrect because we want the managers to access from anywhere.

E: This is incorrect because answer A provide the desired results.

QUESTION NO: 113

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

Explanation:

As stated in the official checkpoint documentation, for default there is a time-out of 40 seconds for UDP activity in a dynamic connection. For the other part, the time-out for TCP connections is more than 2500 seconds by default. This could be changed through the Global Configuration at the policy editor. (See Checkpoint NG Help Online).

Incorrect Answers:

A: The time out is 40 seconds for default, see NG Help Online.

B: The time out is 40 seconds for default, see NG Help Online.

D: The time out is 40 seconds for default, see NG Help Online.

E: The time out is 40 seconds for default, see NG Help Online.

QUESTION NO: 114

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

Explanation:
by default, in the case of Telnet (Port TCP 23) you only need one rule allowing the traffic from the inside or from the outside of the firewall, any reply to that Telnet connection request will be allowed by the firewall because of the connection tracker database located at the gateway. This behavior can be configured to work in a different fashion depending on the implementation requirements.
Incorrect Answers:
A: You don't need 2 rules for a Telnet request and a Telnet reply because if the connection is allowed with the first rule through the gateway, the reply is expected in connection tracker database inside the gateway.

QUESTION NO: 115

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: C

QUESTION NO: 116

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

A. True
B. False

Answer: A

Explanation:

this is an absolute truth for Checkpoint firewall implementations, since the cleanup rule drops all the traffic without making any logging, it should always be the last entry in the rulebase because any packets that gets through or to the firewall is dropped at the inspection engine before getting to the Network layer at the OSI model.

Incorrect Answers:

B: This is one of the basics, the clean up rule should always be the last rule in the rulebase of the installed policy.

QUESTION NO: 117

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

Explanation:

since we want to scan e-mail and check for viruses, all we need is a product that check for certain virus fingerprints, this products is the OPSEC certified Application and we link it with the firewall module with CVP (Content Vectoring Protocol). The most common in enterprise environments is to have a second server with a crossover cable to the firewall running this virus checking application, this is also a best practice.

Incorrect Answers:

A: UFP (URI Filtering Protocol) is not used for Virus scanning, it is usually for Content Management with applications like WebSense to restrict access to some URI´s (URL´s).

C: We don't need both of them, we can provide the functionality only with CVP.

D: We don't need UFP for this.

E: This is not a functionality provided by default you need to use an OPSEC application connected by Content Vectoring Protocol.

QUESTION NO: 118

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: C

Explanation:

one of the uses of the "Verify Policy" command is that it can check if two or more rules conflict with another one. For example if you have a cleanup rule as the first in the rule base it will deny access of the traffic to any other criteria below.

Incorrect Answers:

A: This is not the primary purpose of the policy verification, the main purpose of the verification is to achieve functionality and correct syntax and conflicting rules.

B: When you verify a policy you are making it at the management server, not at the enforcement modules.

D: In policy verification there is not a compression procedure.

E: This is obviously wrong, it is always good to verify your policies, is one of the best practices recommended by Checkpoint engineers, see Checkpoint Policy deployment help at their web site.

QUESTION NO: 119

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

Explanation:

This is false because we also have to create a workstation object to represent the public IP that the internal machine is going to use in the translation process.

Incorrect Answers:

A: This is wrong because you have to define the public address for translation as an additional step. See book "Checkpoint NG Administration" from Syngress. Page 236.

QUESTION NO: 120

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: B

Explanation:

this is the opposite, the time specified in the session time-out box will tell the firewall how much time the users with one time passwords can make request without re authenticating to the firewall.

Incorrect Answers:

A: The session time-out specifies how much time should it pass until the firewall ask for re-authentication to the users of one time passwords during their requests.

QUESTION NO: 121

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

Explanation:

when you see a status of "Untrusted" it means that the management module and the firewall module had been able to communicate but the management server is not the master for the enforcement module, it´s external from it´s control.

Incorrect Answers:

A: Untrusted does not mean "compromised", untrusted just tell you that the Management server is not the master for the firewall object.

B: This is wrong, because in this status the gateway is reached, its only that the management server is not the master for that gateway module.

C: Untrusted status is not related to the system status, its related to policy and management.

E: This is wrong because answer D is correct.

QUESTION NO: 122

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: C

Explanation:
all the objectives are completed because you have your mail and web server with routable addresses with static nat obtaining full connectivity from the inside and the outside, you provide video conferencing to the 8 workers with static dhcp mapping in combination of static NAT (they can request to Internet and receive incoming connections), and then you provide access to Internet access with HTTP and access to e-mail with dynamic NAT translation because you don't need the rest of the workers to receive initial connections from the Internet.
Incorrect Answers:
A: all the objectives are met, see the explanation above.
B: all the objectives are met, see the explanation above.
D: all the objectives are met, see the explanation above.

QUESTION NO: 123

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

Explanation:
this is the best practice, you have to check both, the properties of the user, to see that the correct authentication has been selected & the settings are correct and also the authentication properties of the firewall object to see if that authentication method is enabled.
Incorrect Answers:
B: we are not talking about encryption, only authentication, the question does not talk about a user performing encryption of traffic through any rule.
C: this is wrong because this option is not mandatory to achieve a successful authentication process.
D: You don't have to check client authentication, the question clearly talks only about user authentication.
E: this is not an available option for this issue.

QUESTION NO: 124

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

A. True
B. False

Answer: A

Explanation:
this is true, session authentication does not support some protocols that could be integrated with any application, see Session Authentication topic at the Checkpoint NG Online help.

Incorrect Answers:
B: session authentication doesn't support protocols that can be integrated with any application, see Checkpoint NG documentation.

QUESTION NO: 125

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

Explanation:
you can use the command "cp unload all all" to discard any policy installed in the gateway module, with this, you can reset the communication and correct the rulebase in your policy so you don't lock out the communication between the firewall and the management module.

Incorrect Answers:
A: this is not a valid command to resolve this communication problem, you have to unload the current installed policy.
B: this is not a valid option.
C: This will stop the checkpoint applications running, this answer is wrong because we need to unload a policy, and also, we need our applications running to make this.
E: This will start checkpoint applications, this answer is wrong because we need to unload a policy that is corrupting communication, we don't need to start services.

QUESTION NO: 126

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

Explanation:
this is the correct answer because with a fetch we can see if the firewall module can make a successful authentication and can install the latest security policy, confirming reach ability and integrity. Using this command you can proof that the settings are well configured between the firewall module and the Management console.

Incorrect Answers:
A: We need a masters file in this box, because it will tell where is the management module and where to log. It also says where is the firewall going to fetch its policy at boot time.
B: We need a masters file in the local box because this management console is also has a firewall module, the master file will redirect the firewall module to the local host as the management console.
D: This command is used to dump logs in ASCII format, we need to see the logs at the management module, we don't need to convert the default format of them. Its good to analyze logs with 3rd party applications.
E: This is not a valid option, we are having problems at the firewall communication level, not at the operating system level. Also we have connectivity because we receive control messages from the remote box.

QUESTION NO: 127

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: B

Explanation:

this is a well known issue, the error message "Authentication for command failed" is a Kernel related problem when it cannot contact its assigned management module, this could happen when we loose our trust relationship between the infrastructure components. See checkpoint web site documentation for more information.

Incorrect Answers:

A: This is an authentication related problem, not a rulebase one.

C: We are authenticating the command, not the administrator who issued it.

D: We don't need to fetch encryption keys when issuing a command, the kernel relies in its trust relationship.

E: This kind of authentication is used inside the rulebase for users, in the question we have a system authentication problem between the components.

QUESTION NO: 128

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: A

Explanation:

Session authentication does not result in any additional connection to the firewall, you can use one connection and use it for the rest of the session for any service, also remember that session authentication is controlled by the Session authentication agent. See the online product documentation for more info.

Incorrect Answers:

B: User authentication needs additional connection because it manages a proxy for each service.

C: Client authentication also requires additional connection because you have to connect to the firewall with HTTP or Telnet and enable the service for your use through the gateway.

D: This is not a valid authentication method.

E: This answer is wrong because answer A is correct, session authentication doesn't need additional connections to the firewall.

QUESTION NO: 129

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_todefaultext
D. Fwx_udp_timeout.
E. Fwx_udp_expiration.

Answer: D

Explanation:
if you want to prevent an UDP mapping from loosing its port you have the "Fwx_udp_time-out", you just need to extend the value, its in seconds, check the product online help .

Incorrect Answers:
A: this is not a valid variable to achieve this objective.
B: this is not a valid variable to achieve this objective.
C: this is not a valid variable to achieve this objective.
E: this is not a valid variable to achieve this objective.

QUESTION NO: 130

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

Explanation:
its a very walk trough process, just right click on the data column field and select "Hide" from the pop up menu. Remember, we do it at the GUI, not at the Menu or the Tool bar.

Incorrect Answers:
A: We have to make it from the GUI, not from the menu.
B: We question don't ask for more details, it ask to "hide" information.
C: We cannot disable information from a log, we could hide it, but is still inside it, its not an option.
E: We have to use the GUI, not the toolbar.

QUESTION NO: 131

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: D

Explanation:
Remember, we have to enable the desired authentication method in both, the user and the firewall object, in this case we use firewall 1 authentication.
Incorrect Answers:
A: we don't need to stop the firewall to achieve this kind of functionally, actually we are loosing all of it.
B: its not necessary to make a restart, we could make this configuration in a dynamic way.
C: We don't need to modify the service definition, remember that user authentication has its own telnet proxy.
E: you can have existing rules, you just need to make sure that they are below of the one that makes telnet authentication for your users.

QUESTION NO: 132

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

A. True
B. False

Answer: B

Explanation:
this is not implicit authentication, its explicit authentication because we are defining "TCP HTTP" and this is the explicit way to select a service inside a rule, with this, we are going to layer 7 of the OSI model, if we wanted implicit authentication we just have to go to Layer 4 of the model and select "TCP".
Incorrect Answers:
A: If we want implicit authentication we should have selected only "TCP" on the service field of your rule.

QUESTION NO: 133

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

Explanation:
SVN or "Secure Virtual Network" foundation is the piece of code used by all the checkpoint implementations through the different platforms to achieve infrastructure services and communication between the components.

Incorrect Answers:
A: This command is used to start/stop firewall services and its just a part of SVN foundation.
B: This is just a component of SVN foundation.
C: This is just a component of SVN foundation.
D: This is just a component of SVN foundation.

QUESTION NO: 134

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

Explanation:
this is the most correct answer because we use firewalls in networks where we need security, so we secure our network from unauthorized, and with this we can control who can get in or get out of it.

Incorrect Answers:
B: We don't need firewalls in a unsecured network, we need them in networks that require security.

C: We should not need to prevent authorized access, if it authorized, the traffic should go through.

D: We should not need to prevent authorized access, if it authorized, the traffic should go through.

E: A firewall is not a virus scanning engine, we have anti-virus for that matter, Firewalls are a form of packet analyzers that says if traffics go through, is redirected or is discarded at one of its interfaces, it doesn't look for virus patterns.

QUESTION NO: 135

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: E

Explanation:
We don't use an IF file in Checkpoint NG Suite of products.

Incorrect Answers:
A: We don't use an IF file in Checkpoint NG Suite of products, as simple as that.
B: We don't use an IF file in Checkpoint NG Suite of products, as simple as that.
C: We don't use an IF file in Checkpoint NG Suite of products, as simple as that.
D: We don't use an IF file in Checkpoint NG Suite of products, as simple as that.

QUESTION NO: 136

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

Explanation:
There is not way to see the actual content inside a data transfer with Checkpoint NG. For example its not possible to display what's the content of an HTML site viewed trough the HTTP protocol from Log Viewer.

Incorrect Answers:

A: There is no component inside checkpoint NG suite that provides this functionality.

B: There is no component inside checkpoint NG suite that provides this functionality.

C: There is no component inside checkpoint NG suite that provides this functionality.

D: There is no component inside checkpoint NG suite that provides this functionality.

QUESTION NO: 137

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

Explanation:

when you select the alert button in the properties of the interface at the topology tab, you achieve to main things: the action specified at the anti-spoof alert in the global properties is executed and the action of the alert pop up command at the Global Properties gets executed too. The configuration of these action is made from the policy editor at the Global Configuration of the Checkpoint infrastructure.

Incorrect Answers:

A: This is wrong, the action taken is in the Anti-Spoofing Alert field in the Global properties window is taken, not at the action field of the rule base.

B: This is only part of the answer.

C: This is only part of the answer

D: This in wrong because it includes answer A that is incorrect.

QUESTION NO: 138

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

Explanation:
You can check it out in the Syngress Book "Checkpoint NG: Next Generation Security Administration", the "!" means that the firewall module does not have a security policy installed, so its insecure. This could happen if your firewall module becomes corrupted and it can't fetch a valid security policy either from the management module or from the local host.

Incorrect Answers:
A: when we have an object as external, we can't see the status of it because we are not managing it from that management console, we don't either get a "!" next to it.
B: The rulebase doesn't resolve IP address, it doesn't make sense.
C: The "!" is not a valid representation for a halted firewall, it's a representation for a unsecured one.
E: a "!" status next to one of our modules it's a bad thing, it means that we have our gateway unsecured, without enforcing any security policy.

QUESTION NO: 139

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: B

Explanation:
with session authentication we can authenticate all the services in a transparent way because all the authentication request are made between the session authentication agent and the firewall object. The user doesn't worry about authenticating each type of service.

Incorrect Answers:
A: This is not the case, remember that we have the session authentication agent installed in the PC.
C: This is the case of User authentication, not Session authentication.
D: This is not true, because by default we have an expiration time for our sessions.
E: This answer is wrong because it takes answer "D" as correct.

QUESTION NO: 140

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

Explanation:
As it says in the question, the administrator wants granular control and that requires authentication in a user basis, he also wants logging from any place, so the best option is to use "User Authentication" because we can have a centralized user database that will provide successfully provide the mobility requirements exposed in the question.
Incorrect Answers:
A: Session authentication does not provide the mobility requirements because the user will have to install the session authentication agent on every PC and that's not a transparent experience for him.
C: Client authentication does not provide a transparent experience to the user because he / she have to make a manual logon to the firewall with Telnet or HTTP.
D: This is not one of the 3 authentication methods supported by the NG suite.
E: This is not one of the 3 authentication methods supported by the NG suite.

QUESTION NO: 141

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

Explanation:
to achieve this functionality we need static NAT, remember that dynamic NAT does not provide access for an external client to an internal machine, the firewall doesn't know where to redirect the service incoming requests when the mappings are one to many, this is the case of Dynamic NAT.

Incorrect Answers:

A: You can't provide this functionality with dynamic NAT, you have to use Static NAT in this case.

QUESTION NO: 142

The Enforcement Module (part if 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. Us usually installed on a multi-homed machine.

E. All of the above.

Answer: E

Explanation:

An enforcement module is all of the above, it has to analyze the traffic according to the Security policy that gets from a management server as inspect code, it makes this passing all the traffic through the inspect engine between the top of the layer 2 and the layer 3 of the OSI model, it usually have 2 or 3 interfaces, one internal and the other external, the third one for the advertisement of public services (DMZ). It can also provide authentication through various methods like the proprietary Firewall 1.

Incorrect Answers:

A: this is only part of the answer.

B: this is only part of the answer.

C: this is only part of the answer.

D: this is only part of the answer.

QUESTION NO: 143

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 Riles.

C. Client Authentication Rules.

D. Pseudo Rules.

E. Default Rules.

Answer: C

Explanation:

you cannot place the stealth rule above the client authentication rule because the stealth rule will deny any connection to the firewall, so when the users try to authenticate with telnet or HTTP as they should for Client Authentication, they can't make it, because the stealth rule is preventing all the connections.

Incorrect Answers:

A: Stealth rule should always be above the clean up rule, the clean up rule should be the last explicit one in the rulebase.

B: Implicit rules are not visible on the rule base, they are always at the very beginning of the rulebase or at the very end of it, those are configured in the global properties.

D: Pseudo Rules could be below the Stealth rule.

E: There is not such a thing like "default rules".

QUESTION NO: 144

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

Explanation:

of course, in the checkpoint statefull firewall engine the rulebase is examined sequentially from top to bottom, so if you change the order of any of the implied rules at the global configuration properties, the rules are enforced in a different order .

Incorrect Answers:

B: The enforcement of the rules inside the policy changes because the rulebase is applied sequentially from top to bottom until it gets a match.

QUESTION NO: 145

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

A. True
B. False

Answer: A

Explanation:

with "fw fetch" command you can specify an IP address to fetch a policy from, so you just need to specify the IP address of the management server that has the right policy destined to your firewall

module. Remember that you need to have a trust relationship established through SIC certificates. (Secure Internal Communications).

Example: fw fetch 192.168.1.1.

Incorrect Answers:

B: Since you can specify an IP address with the "fw fetch" command, you can specify the policy that you want to install, just type the IP of the management module that have the desired policy.

QUESTION NO: 146

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

A. True
B. False.

Answer: B

Explanation:

as stated by checkpoint engineers in the checkpoint web site, the objects corresponding to the Visual Policy Editor cannot be edited until they are actualized, and that actualization takes place when the topology calculations get to a consistent state, this makes the Visual Policy editor gets to a convergent state and let you edit the VPE's.

Incorrect Answers:

A: You can't edit VPO objects until the VPO gets to a consistent state through the topology calculations.

QUESTION NO: 147

Stateful inspection is a firewall technology introduced in Checkpoint VPN-1/Firewall-1 software. It is designed to meet which if 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

Explanation:

statefull inspection technology provides all these security features, as answer A says you can analyze the packet from layer 2 to layer 7 to get the most information from the encapsulation process including the application data content of the packet itself, the technology also manages session information for the services for security verifications through matching connection internal databases, it can also evaluate flexible expressions derived from information of various applications and can also provide authentication capabilities embedded in the technology.

In the checkpoint implementation of the statefull inspection technology, the inspect engine is placed at the top of the layer 2 of OSI model.

Incorrect Answers:

A: This is only part of the features of statefull inspection.

B: This is only part of the features of statefull inspection.

C: This is only part of the features of statefull inspection.

D: This is only part of the features of statefull inspection.

QUESTION NO: 148

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

Explanation:

when you are at the policy editor or the system status, you can click on the windows menu and go to the log viewer or other GUIs. When you call the GUIs this way you don't have to re-authenticate, you use your current security credentials.

Incorrect Answers:

B: This answer is incorrect because you can call the log viewer through the Windows menu in the policy editor or the system status.

QUESTION NO: 149

NAT can NOT be configured on which of the objects?

A. Hosts

B. Gateways

C. Networks

D. Users

E. Routers

Answer: D

Explanation:

you can't configure NAT in a user because there is nothing useful to translate in a user relating to NAT technologies, users do not have network addresses itself, and NAT translates just that, network addresses. The users are not identified by addresses, the hosts are.

Incorrect Answers:

A: You can make NAT on hosts, a hosts is any device with an IP addresses. If the device has an IP address you can use NAT.

B: Gateways are a type of host, so they have an address inside the network, NAT is possible.

C: You can make NAT in a Network, you can summarize a group of hosts behind a network address to create your NAT rules in your security policy.

E: Routers are also a type of host, so they have an address inside the network, NAT is possible.

QUESTION NO: 150

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: C

Explanation:

Client authentication includes verification of the IP address of the client. Access can be restricted to only specific client IP addresses.

Incorrect Answers:

A: With Session authentication you can use any computer to connect if you have the session authentication agent installed in the PC.

B: User authentication allows you to connect from any PC, it doesn't have Ip checking capabilities

to restrict the users to certain hosts.

D: This isn't one of the 3 authentication methods of the Checkpoint NG Suite.

E: This answer is wrong because client authentication provide the functionality required.

QUESTION NO: 151

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

Explanation:

this is the default behavior of a Checkpoint firewall, any traffic that is not expressly permitted is drooped, this is done by a implicit rule that is present in every security policy.

Incorrect Answers:

A: this is the opposite, remember, you have to permit the traffic expressly or implicitly, if you don't do it, the traffic will be dropped.

C: This is not the default behavior, see the explanation.

D: You have to define your permitted traffic, nothing is allowed by default.

E: False, you can also control the flow of traffic through implicit rules.

QUESTION NO: 152

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

Explanation:

this is the correct answer, when you create a new user its create by default from the "default" template. See checkpoint NG online documentation.

Incorrect Answers:

A: This is not the name of the default template. See checkpoint NG online documentation.

B: This is not the name of the default template. See checkpoint NG online documentation.

C: This is not the name of the default template. See checkpoint NG online documentation.

D: This is not the name of the default template. See checkpoint NG online documentation.

QUESTION NO: 153

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

Explanation:

the port 256 is used by the management station to push the policies to the enforcement modules, therefore it provides communication between the firewall and the management module. See the official CCSA courseware. Appendix C.4.

Incorrect Answers:

A: The communication does not take place through the standard HTTP port.

C: This port is used for client authentication through Telnet.

D: This port is used for client authentication trough HTTP.

E: This is the default port for Telnet.

QUESTION NO: 154

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

Explanation:

The .W files provides contains the information displayed graphically in the GUI regarding the rulebase upon saving or installation of the policy, its editable with a text editor. The command "fw load" will change the .W file to a *.pf file and compile into inspect code for policy installation in the enforcement module.

Incorrect Answers:

A: This command is not valid for working with .W files and installing security polices from them.

C: This command is not valid for working with .W files and installing security polices from them.

D: This command is not valid for working with .W files and installing security polices from them.

E: This command is not valid for working with .W files and installing security polices from them.

QUESTION NO: 155

In the Check Point Configuration Too, 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

Explanation:

as the name implies, a "Read Only Administrator", can do just that, read information, it cannot perform tasks that require writing privileges like create rules and change properties of network objects. You can see the definition in the official CCSA courseware (VPN1-FW1 Management 1 NG FP-1).

Incorrect Answers:

A: You can't modify or create objects policies with "read only" privileges.

QUESTION NO: 156

Hybrid Authentication allows VPN-1/Firewall-1 NG to authenticate SecuRemote/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: D

Explanation:
"Hybrid Authentication for IKE" is just that, it allows you to use existing authentication servers supported by VPN1/FW1 as shared secrets for IKE. This is supported since FW 1 4.1 SP1 and SecuRemote 4153. See Page 382 of "Essential Checkpoint Firewall 1" from Dameon Welch.

Incorrect Answers:
A: This is not the most complete answer, the most complete is answer "D".
B: This is not a kind of authentication server, its an encryption algorithm.
C: This is not the most complete answer, the most complete is answer "D".
E: This is not the most complete answer, the most complete is answer "D".

QUESTION NO: 157

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: E

Explanation:
To install a new policy in a enforcement module you don't have to issue anything on it, you just need to select the install option in the policy editor and the management station will push the new policy as inspect code overwriting the actual policy being enforced at the remote firewall module.

Incorrect Answers:
A: You don't need to unload the current policy to make a new one effective, is not necessary.
B: The policy is pushed from the management station in a transparent fashion on installation, you don't need to issue any additional command at the remote module.
C: You don't need to issue any command.
D: You doesn't need to use any "cp" command, the overwriting is automatic.

QUESTION NO: 158

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

Explanation:
the cleanup rule should always be the last rule in the rulebase, because it will drop or log (depending on your actions) all the traffic, it will always match the traffic that gets through it.
Incorrect Answers:
B: It should be the last rule, see the explanation for details.

QUESTION NO: 159

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

A. True
B. False

Answer: A

Explanation:
when we are using client authentication with all the setting for fully automatic authentication, you can authenticate all the protocols, it doesn't matters if the protocol supports authentication. See the Client Authentication features in the Secure knowledge base of Checkpoint for more information.
Incorrect Answers:
B: You can authenticate all the protocol whatever or not they support authentication, remember, this is client authentication.

QUESTION NO: 160

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

Explanation:
this is the main difference between the listed firewall technologies, the statefull inspection, because with it, we can see the packet before it goes to the Layer 3 of the OSI model (Network Layer = O.S TCP/IP Protocol Stack), this technology has the most access to the TCP/IP packet including the top layers.

Incorrect Answers:
A: This is configurable and is not a difference between the listed firewall technologies.
C: VPN1/Firewall 1 has full access to the packet headers.
D: This is not a difference.
E: All firewall technologies has access to the network, you define what are your key locations inside it, then, you put the firewall to make that "key locations" pass the traffic through it.

QUESTION NO: 161

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

Explanation:
to reduce the installation time, you can group the different network objects into one object so you don't have to use individual network object to make your translation rules, this will improve policy install performance and will ease the administration.

Incorrect Answers:
B: We are not reducing installation time with this answer because we are creating the rules with every single network object.
C: This is not a matching problem, it's clear that we have too many network objects inside the

same rule.

D: This is not possible, you cannot corrupt the binaries with a policy definition, they don't talk directly to each other.

E: For security reasons, we should protect the internal addresses behind the external IP Address of the firewall. This is one of the purposes of NAT.

QUESTION NO: 162

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

Explanation:

the concept of transparent authentication for Checkpoint Systems relies in making the Firewall authenticate the connections from the user, but make the user experience transparent, in other words, they don't know that the firewall is authenticating their connections.

Incorrect Answers:

A: This is not the essence of transparent authentication, we will not get error messages, we will just not go through with our requests.

B: This authentication fashion does not prompt for user input, remember, this is "transparent" authentication.

D: This is not the way transparent authentication works, you can check the transparent authentication behavior at the Knowledge base of Checkpoint.

E: The user doesn't need to know the name of the firewall, it is usually configured by the administrator, the user doesn't need to know.

QUESTION NO: 163

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

Explanation:

when selecting "intersect with user database" option means that the firewall will match the settings in the user definition and the standard rule base. The connection must match both to allow the connection. See page 272 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

Incorrect Answers:

A: This is not true, because with the options selected you must match both, user definition and the standard rulebase.

QUESTION NO: 164

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?
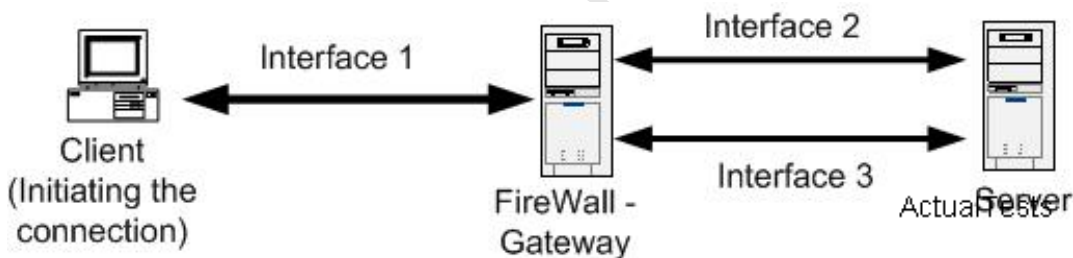
A. A connection initiated by the client will be hidden behind the IP address of the exit interface.

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

Explanation:

making this actions, you will make the packets hide behind the exit interface, this is because of the address specified. Refer to Checkpoint Online Documentation to see how the whole process work.

Incorrect Answers:

B: The connection needs to be iniciated by the client, not the server.

C: You can´t hide the IP address of the server with the client one.

D: You can´t translate a source address to 0.0.0.0.

E: You can´t translate outbound packets in the server to a 0.0.0.0. address.

QUESTION NO: 165

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

Explanation:

this is not very secure, since client authentication gives access to the host and not the user, any user could use and authenticated host to pass through the gateway. User authentication is more secure than Client authentication in this matter.

Incorrect Answers:

A: Client authentication gives access in base of the host network address.

B: When you authenticate through client authentication, its the host the one who have access, not the user.

D: This is true, you can grant certain privileges to certain IP addresses once they are authenticated, remember, this authentication method works with the hosts addresses.

QUESTION NO: 166

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

A. True

B. False

Answer: B

Explanation:

by default, any rule that you add to your rulebase for certain policy is enforced automatically once you push the updated policy to the enforcement modules from the management station. See

"Basics of Security policy Administration" at the Checkpoint Official Courseware for CCSA.

Incorrect Answers:

A: When you create a rule it is enforced as part of the security policy. See the explanation above for details.

QUESTION NO: 167

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

Explanation:

this is the only correct answer, since we are talking about "Internal" authentication scheme, the only valid answer is the Operating System authentication because the authentication occurs locally to the user.

Incorrect Answers:

A: When we talk about dynamic passwords we often talk about an external security server changing the access password in a continuos basis, the user usually see the current password with the help of a hardware Token, an example is RSA.

B: Radius is an external security server, the authentication is checked remotely.

C: AXENT is an external security server, the authentication is checked remotely.

D: TACACS is an external security server, the authentication is checked remotely.

QUESTION NO: 168

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

Explanation:

when you map a routable address with an external one, you will get the message "rule x conflicts with rule y" this is because of the behavior of the Checkpoint firewall suite in relation with the

limitations of Static NAT, this behavior will make your policy verification and installation fail.

Incorrect Answers:

B: As stated in the explanation above, you can't make this configuration because your policy verification will fail, and you will get the error message, this error makes this answer wrong.

QUESTION NO: 169

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: B

Explanation:

yes, you can use client authentication for any service and the authentication in only valid for a specific length of time, but you can't use it for any number of connection, this number is limited and can be configured. See the product online Documentation of the NG Suite for more detailed information.

Incorrect Answers:

A: This answer is not correct because you can't use client authentication for any number of connections, you have a limit.

QUESTION NO: 170

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 us 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: C

Explanation:

the traffic is being dropped because you don't have a rule allowing HTTP traffic to the internal web server, this traffic is dropped by an implicit rule.

Incorrect Answers:

A: This is not a spoofing problem, we have an implicit rule dropping the traffic.

B: You don't need to define spoofing in the external interface.

D: You don't need this rule since the web server will send reply's to existing request, you only need the inbound rule that allows the external clients the HTTP access to the internal web server.

E: This answer is wrong, because answer C is correct.

QUESTION NO: 171

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

Explanation:
When you create users in VPN/Firewall 1 you are storing them in a component, called the User Database. Note that the user database reside in the management station and si pushed / installed to the firewall modules when a policy is installed. See page 219 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

Incorrect Answers:
A: This is not the place where users are stored, this is the place where the traffic is matched to the rules inside the policies.

B: The rulebase contains the criteria for the security policy that is scanned through the inspect engine, it doesn't store the users.

D: The users aren't here, they are in the User Database, see the explanation above.

E: An inspect module is a piece of inspect code used by the inspect engine to extend the capabilities of the firewall in native form, it doesn't store the users.

QUESTION NO: 172

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

Explanation:
if a user belong to several groups and the user authenticates successfully it means that he have matched his user & authentication restrictions and also the ones of the groups he belongs to. This is the way checkpoint authentication works, you have to pass your personal authentication restrictions, and the ones in your groups to authenticate successfully.
Incorrect Answers:
B: This answer is wrong because you have to get a match in your user & group authentication restrictions to get a successful authentication. You must get a match in all of them.

QUESTION NO: 173

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

A. True
B. False

Answer: B

Explanation:
you don't have blocking rules inside your rulebase, all your blocking actions are made from "Block intruder" dialog box" at the active connection monitor in the log viewer. To unlock connection you could unload the firewall module (fwstop command) or remove it manual, this is done without modifying the existing rulebase in policy editor. See page 108 from book "Essential Checkpoint Firewall 1".
Incorrect Answers:
A: You don't have to modify the current rulebase from the policy editor. You take you unblocking action unloading the firewall or unblocking the connections manually. See explanation above for more information.

QUESTION NO: 174

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

Explanation:

this command is the same as "fw fetch", it is issued at the enforcement module and it retrieves a security policy as inspect code from the management module. It´s a way to fetch a policy from the remote end.

Incorrect Answers:

A: The fetch command is not related to users, its related to policies. Note than when you fetch a policy you are also including the user database from the management server.

C: This command is not issued in the management module, is issued at the enforcement module.

D: This command is not issued in the management module, is issued at the enforcement module.

E: This answer is wrong because answer "B" is the correct answer.

QUESTION NO: 175

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

Explanation:

when an UDP packets enters to the Inspect engine inside the firewall, the database that contains the pending connections is reviewed and the packet is delivered if its a reply to a request, we know this because there is an entry expecting the reply in the pending connections database, this is the first case. The second case that allows the deliver of the UDP packet is if it is allowed by the rulebase, for example, a rule that allows DNS Query traffic through port 53 UDP.

Incorrect Answers:

A: A request cannot pass the firewall unless there is a rulebase permitting that service.

B: This is only part of the correct answer. This is only 1 of the 2 cases.

C: Source routed request are not allowed unless there is a rule permitting it.

D: This is only part of the correct answer. This is only 1 of the 2 cases.

QUESTION NO: 176

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: E

Explanation:

the default time for Dynamic NAT TCP connections is 3600 seconds until it gets to a time-out state. You can check this at the global configuration properties of the firewall to see the default, or you can check the online Checkpoint NG documentation.

Incorrect Answers:

A: The correct default time out for Dynamic NAT on TCP connections is 3600 seconds.

B: The correct default time out for Dynamic NAT on TCP connections is 3600 seconds.

C: The correct default time out for Dynamic NAT on TCP connections is 3600 seconds.

D: The correct default time out for Dynamic NAT on TCP connections is 3600 seconds

QUESTION NO: 177

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

A. True

B. False

Answer: B

Explanation:

once you disable a rule, it becomes ineffective in your policy, you don't have to verify the policy to make the disabling effective, once you want to push the policy to the enforcement modules again the disabled rule is not enforced. To disable a rule just right click the rule number and select "Disable".

Incorrect Answers:

A: You don't have to verify your policy to make a disabling action take effect over your policy, this is not necessary. See page 215 from the Syngress Book "Checkpoint NG - Next Generation Security Administration).

QUESTION NO: 178

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

A. True
B. False.

Answer: B

Explanation:

this statement is false because Static NAT translates "Private" Internal Source IP addresses to "Public" External Source IP addresses and not "Public" internal source IP addresses to "Private" external source IP addresses. Remember that our internal hosts don't have public addresses.

Incorrect Answers:

A: Remember that we have Private Internal source IP´s behind the gateway and Public external source IP´s connected to the external network. (Example: Internet).

QUESTION NO: 179

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

Explanation:

the command "FW CTL iflist" is a utility for controlling the FW1 kernel, it can be used for obtaining interface information. See Page 385, Syngress book " Check Point NG - Next Generation Security Administration".

Incorrect Answers:

C: This is not a valid command.
D: Netstat is not used to list interfaces, it gives you TCP/IP static's.
E: This is not a valid command to this matter.

QUESTION NO: 180

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: B

Explanation:

since we want the doctors to update the profile from any place in the building the best authentication method is "User" because in Client authentication you are validating the host and not the user, and Session authentication needs the Session Authentication agent installed in every machine. User authentication validates the "user" regardless of the host, this is what we need in this situation, its the best solution for roaming users.

Incorrect Answers:

A: Session authentication need the session authentication agent in every machine and our doctors are roaming users, we don't know what machines are they going to use.

C: Client authentication validates the host, we need to validate the Roaming Users.

D: This is not a valid authentication method.

E: This answer is wrong because Answer "B" matches the question requirements.

QUESTION NO: 181

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: C

Explanation:

you can issue the command "fw stat" at the enforcement modules to get a print out of the installed policy with the date and time of installation, the name of the policy and the name of the host from which it was installed. See Page 114 of the Syngress Book - Checkpoint NG "Next Generation Security Administration".

Incorrect Answers:

A: This command is used to get internal status information of Firewall 1.

B: This command is not related to policy verification.

D: This command returns the currently installed version of Firewall 1.

E: This is not a valid command.

QUESTION NO: 182

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

Explanation:

when you have firewall objects defined in the policy editor you can select between 2 options in the general tab of the object at the "Object Management" setting. The options are "Managed by another management server (External)" or "Managed by this management server (Internal)". If you select our first option (External) we will not be able to install any policy on this firewall, because our management server does not figure as the master for the object.

Incorrect Answers:

A: Our need cant be addressed by a Master file. You can have a review to the Checkpoint documentation with the functions of the Masters file.

B: This is not a licenses problem, the management station cannot see the firewall as an option.

C: We don't need to reboot the firewall to allow it to receive policy updates.

D: This is not a possible cause.

QUESTION NO: 183

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

Explanation:

when you select only one firewall object in the "install on field" of a rule, that rule is enforced only on that firewall object. In case there are other firewalls referred in the whole policy, they will have

the complete policy installed (with all the rules in the rulebase), but they will not enforce the rules that are not relevant to them. See page 175 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

Incorrect Answers:

A: When you select only one firewall object on the "install on" field of a rule, that rule is enforced only in that firewall after the policy installation.

QUESTION NO: 184

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

Explanation:

client authentication uses port 900 to authenticate over HTTP. You can check this in the Appendix "C.4" of the CCSA Official Courseware. (Management I)

Incorrect Answers:

A: This is the standard "Well-Known" Telnet port.

B: This is the standard "Well-Known" HTTP port.

C: This port is used for client authentication with Telnet.

D: This port is not used by VPN1/FW1.

QUESTION NO: 185

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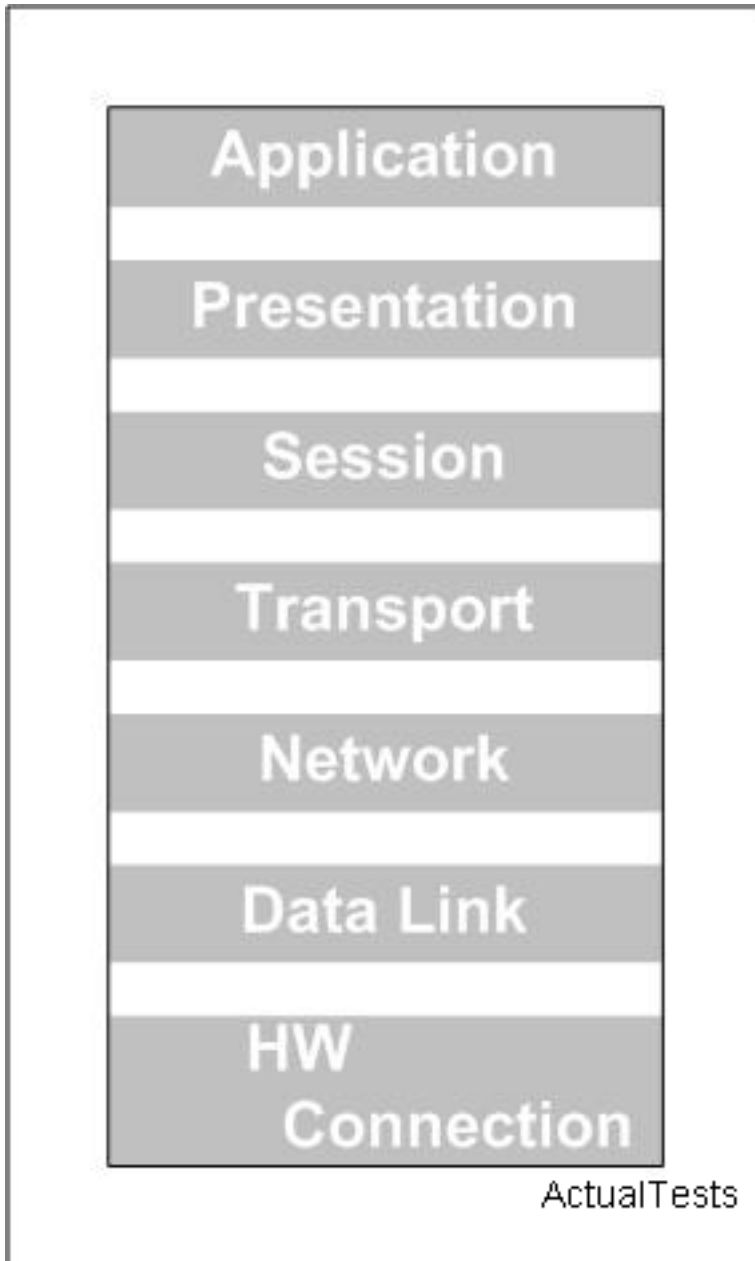
A. Data

B. Transport

C. Physical

D. Application

E. Network

Answer: E

Explanation:

VPN1/FW1 resides on the top of layer 2 (DataLink) and below Network layer of the OSI model. In this place, the firewall engine can get all the packets before they get to the TCP/IP stack of the operating system, incrementing performance and improving security.

Incorrect Answers:

A: VPN1/FW1 resides below the Network layer (3) of the OSI model.

B: VPN1/FW1 resides below the Network layer (3) of the OSI model.

C: VPN1/FW1 resides below the Network layer (3) of the OSI model.

D: VPN1/FW1 resides below the Network layer (3) of the OSI model.

QUESTION NO: 186

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

A. True
B. False

Answer: A

Explanation:
you should always place any client authentication rule above the stealth rule, the stealth rule will prevent any connection to the firewall for security purposes, the client authentication needs to make a telnet connection on port 259 TCP or an HTTP connection in port 900 TCP. So, you should always place your client authentication rules above the stealth rule or you will have your traffic dropped.

Incorrect Answers:
B: The statement at the question is true, we need the stealth rule below the client authentication rule, if we don't do it this way, our authentication request will be logged or dropped depending on our Stealth rule.

QUESTION NO: 187

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: B

Explanation:
its difficult to explain without the exhibit, but the answer is B, the statement exposed in the question is not true, its false. The NAT rules are not simply hidden.

Incorrect Answers:
A: This answer is wrong because the NAT rules aren't simply hidden, is hard to explain without the exhibit.

QUESTION NO: 188

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

Explanation:
the statement in the question is wrong,, when the packets are traveling from the client toward the server in a static destination NAT case, the first thing that takes place is routing and the we have the address translation. See "Static Destination NAT" in the book Essential Checkpoint Firewall-1 from Guru Dameon Welch.

Incorrect Answers:
A: In static destination NAT, Routing occurs first, and then we have the address translation. Remember that the packet is coming from the outside, we have to route it first.

QUESTION NO: 189

Which if the following statements are 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: D

Explanation:
This statement is false because in the inside we have Private Internal Addresses and in the outside we have Public External Addresses and not the opposite.

Incorrect Answers:
A: You can't use protocols where you can't change the ports, remember that the translation changes the sources ports to distinguish between the different NAT clients.
B: You can't use dynamic NAT to advertise servers from the inside, you have Static NAT for that matter. There is no way to distinguish the internal server from the outside.
C: When Dynamic NAT takes place, the source port number is modified by the firewall so it can know where to redirect the reply when it's coming back. The firewall have a database with this

mappings, it contains the original source port and the source port after the translation, it also contains the real source IP.

E: This is true, the firewall recognizes the different internal host with the internal source port mapping database used to make the sources port changes in the NAT process.

QUESTION NO: 190

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

Explanation:
When you update settings in a profile, the users already created with it are not updated, if you want to reflect the changes, you have to modify the profile and any single user separately. This is the behavior.

Incorrect Answers:
A: This is not true, when you update the definition of a user profile, the users already created with it are not updated.

QUESTION NO: 191

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

Explanation:
the installation time for network objects will always be lower if you populate your "hosts" file because the lookup process for the name resolution process will be much lower, since the Hosts file is always checked first upon going to resolve the name-to-IP mappings with a DNS server.

Incorrect Answers:
B: When you populate the hosts file, you can speed up the creation of network objects, this is because all the name resolution take place locally.

QUESTION NO: 192

Consider the following network:

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

Explanation:
Since we want the HTTP server to be accessible from the Internet, you have to use Static NAT, and since you need to hide the other hosts in the DMZ and in the private network, you can use Dynamic NAT to achieve the desired results.
Incorrect Answers:
A: This is only part of the correct answer, is not complete.
B: We have the hosts at the private net, What about the other hosts in the DMZ?.
C: This is just the network containing the hosts in the DMZ, what about the hosts at the internal net?
D: This is only part of the correct answer, is not complete.

QUESTION NO: 193

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: B

Explanation:
Since we want to begin an HTTP session from the outside to an illegal IP address, we need Static Destination NAT, Static Destination NAT provides a way for the firewall to translate incoming request from the outside to hosts located behind the gateway that have illegal or reserved private IP addresses. See page 239 "Static Destination NAT" in Syngress Book " Check Point NG - Next

Generation Security Administrator".

Incorrect Answers:

A: This is used to begin connections from the inside, with a host that have a reserved or illegal IP address.

C: Since we want the hosts behind the gateway to be accessible from the outside, we can't use dynamic NAT, we have to use Static NAT.

D: This answer is not correct because answer B is the correct answer.

QUESTION NO: 194

With SecureUpdate you are able to: (Select all that apply)

A. Change Central Licenses to Local Licenses
B. Track current installed versions of Check Point and OPSEC products
C. Update Check Point and OPSEC software remotely from a central location
D. Centrally manage Licenses
E. Perform a new installation of VPN-1/FW-1 remotely

Answer: B,C,D

Explanation:

Secure update is a tool for the easy management of both, the version and licensing for both Checkpoint and OPSEC products, In the GUI you have two main panels, one for the products and one for the licenses. It provides information on the version of OPSEC and Checkpoint products installed, it allows the central management of licenses for checkpoint products and also allows remote update capabilities for OPSEC and Checkpoint products.

Incorrect Answers:

A: This is not currently possible, you cannot change license from central to local, however you can do the opposite, you can change a license from local to central. See "Checkpoint licensing FAQ" in the Checkpoint web site.

E: With Secure Update you can update existing Checkpoint and OPSEC software, but you cannot perform new installations remotely from it.

QUESTION NO: 195

Which is false about SIC communications?

A. A.VPN Certificates, such as those for IKE are used for secure communications
B. B.The Policy Editior initiates an SSL based connection with the Management Server
C. The Policy Editor must be defined as being authorised to use the Management Server
D. The Management Server verifies that the Clients IP address belongs to an authorised Policy Editor Client

Answer: A

Explanation:

VPN certificates, such of those used for IKE, are used for VPNs, and should not be confused with SIC certificates, used for securing internal network communications. In SIC the management server acts as a certificate authority that issue this certificates to uniquely identify all checkpoint enabled machines. See Page 1.21 of the official CCSA NG Courseware - Management 1.

Incorrect Answers:

B: SIC for Checkpoint SVN components uses certificates for authentication and standart-based SSL for encryption for communication between components. See Page 1.20 of the official CCSA NG Courseware - Management 1.

C: For SIC communications between the management server and Policy editor, the policy editor client must be defined as being authorized to use the management server. See Page 1.22 of the official CCSA NG Courseware - Management 1.

D: The IP address of the machine trying to connect must be defined as authorized with CPConfig utility. The management server verifies that the client IP address belongs to an authorized Policy editor client. See Pages 1.20 and 1.22 of the official CCSA NG Courseware - Management 1.

QUESTION NO: 196

Within the Secure Internal Communications (SIC) framework the Management Server and Modules are identified by their SIC name. What is this commonly known as?

A. IP Address
B. Host Name
C. Friendly Name given by Administrator
D. Distinguished Name (DN)
E. Workstation Name

Answer: D

Explanation:

The management server and the modules are identified by their SIC name, also known as Distinguished Name (DN). See Page 1.22 of the official CCSA NG Courseware - Management 1.

Incorrect Answers:

A: The Checkpoint products are not recognized internally by SIC with their IP address, their are recognized with a DN (Distinguished Name).

B: The Checkpoint products are not recognized internally by SIC with their Hosts name, their are recognized with a DN (Distinguished Name).

C: The Checkpoint products are not recognized internally by SIC with a custom name defined by the administrator, their are recognized with a DN (Distinguished Name).

E: The Checkpoint products are not recognized internally by SIC with the name of the machine, their are recognized with a DN (Distinguished Name).

QUESTION NO: 197

You Enterprise Security Policy is made up of what? (Select all that apply)

A. Explicit rules created by the user
B. Implicit rules created by VPN-1/Firewall-1, and are derived from the security properties
C. something else
D. something else
E. something else

Answer: A,B

Explanation:
a security policy is the group of explicit and implicit rules created in the policy editor and pushed to the enforcement modules. The explicit rules are created by the administrator through manual definition and implicit rules are created automatically with the setting of the Global Properties in Policy Editor.
Incorrect Answers:
C: There is nothing else in a enterprise security policy.
D: There is nothing else in a enterprise security policy.

QUESTION NO: 198

The ICA creates certificates for the VPN-1/FireWall-1 Modules and any other communicating component are created via initialization of the Policy Editor. The ICA creates, signs, and delivers a certificate to the communicating component. When would the certificate become invalid? (Select all that apply)

A. If you rename the gateway
B. If you rename the rule base
C. When you Reset the ICA
D. Delete the Module object from the Policy Editor
E. something else

Answer: C,D

Explanation:
according to checkpoint documentation there are two cases when certificates become invalid, the first case is when you reset ICA, because all the certificates have to be reissued, and the second case is when you delete a module at the policy editor because the object is no longer available and the management server published a CRL invalidating the associated SIC certificate previously issued by ICA.

Incorrect Answers:

A: This is not one of the cases, remember that the internal search is made through the DN and not the alias.

B: The rulebase does not have a certificate associated with it, the certificates are issued to machines.

E: This in not one of the cases.

QUESTION NO: 199

Doctors in your building want to be able to get access to files on an ftp server on the DMZ (there is a diagram in the exam). The doctors move around PC's in the building, what is the best authentication scheme to use so they can access the FTP server?

A. Session

B. User

C. Reverse

D. Client

E. IKE

Answer: B

Explanation:

since the users are roaming, the best authentication method to use is "User", also remember that this authentication method has advanced FTP capabilities through its FTP proxy.

Incorrect Answers:

A: This is not practical because we need the session authenticated agent installed in each machine and our users are roaming.

C: This is not a valid authentication method.

D: We need to validate the users, not the hosts, remember that our Doctors are roaming users.

E: This is not a valid authentication method.

QUESTION NO: 200

User Authentication can be used to authenticate which services? (Select all that apply.)

A. HTTP

B. HTTPS

C. RLOGIN

D. FTP

E. TELNET

Answer: A,C,D,E

Explanation:

With Session Authentication you can authenticate 4 services: HTTP, FTP, Telnet and RLogin. See Page 282 of Syngress Book " Check Point NG - Next Generation Security Administration".

the block intruder windows has 3 options available to block intruder connections, they are "Block only this source", "Block access to this source" and "Block access to this destination". See Page 376 of Syngress Book " Check Point NG - Next Generation Security Administration".

Incorrect Answers:

B: HTTPS is not supported by user authentication. See Page 282 of Syngress Book "Check Point NG - Next Generation Security Administration".QUESTION 200To block an active connection with Block Intruder, select the connection you want to block, and then select Block Intruder from the Select mune. The following default options are available from the Block Intruder window (Select all that apply.)Block access to this gatewayBlock access from this sourceBlock only this connectionBlock access for specific packets to the destinationBlock access to this destinationAnswer: B, C, E

QUESTION NO: 201

When can Hide Mode not be used?

A. Where the port number cannot be changed
B. Where the port number can be changed
C. Where the external server must distinguish between clients based on their IP address
D. something else

Answer: A,C

Explanation:

Hide mode NAT can't be used when the port number cannot change because hide mode changes the source IP port to recognize the connections, also you can't reach a host through the gateway from the outside if you are applying Hide mode NAT to it. If you have one of this 2 cases you have to use Static NAT.

Incorrect Answers:

B: If the port number can be changed, Hide mode NAT will work fine.
D: This will also make Hide Mode NAT to work.

QUESTION NO: 202

What Implicit Rules are allowed by default in the Global Properties?

A. Accept RIP

B. Accept Firewall Control Connections

C. Accept Domain Name over UDP (Queries)

D. Accept ICMP Requests

E. Accept CPRID connections (SecureUpdate)

Answer: B,E

Explanation:

by the default "Accept Firewall control connections" is allowed, it opens port 256 for firewall communications. Also CPRID connections are accepted, this port is used for Secure Update.

Incorrect Answers:

A: By default RIP is not allowed, how have to change the global configuration to change this.

C: By default DNS over port 53 UDP is not allowed, how have to change the global configuration to change this.

D: By default ICMP messages are not allowed, how have to change the global configuration to change this.

QUESTION NO: 203

What mode would you use to check if someone is pinging the firewall?

A. Security Log

B. Log Viewer

C. Active Connections

D. Accounting Log

E. Audit Log

Answer: B

Explanation:

if you want to see events relating to traffic arriving to the firewall, like ICMP messages, you have to use the Log viewer mode, See Page 4.6 of the CCSA NG Official Courseware - Management I.

Incorrect Answers:

A: This is not a Mode its a physical log file, the question ask for a mode.

C: We cannot see ICMP massages with Active Connections, the packets are send and there is no a permanent connection.

D: This is not a Mode its a physical log file, the question ask for a mode.

E: This is not a Mode its a physical log file, the question ask for a mode.

QUESTION NO: 204

What is true of the Enforcement Module? (Select all that apply)

A. Usually installed on a multihomed machine

B. Manages logging

C. Is installed on a host enforcement point

D. Examines all communications according to a Enterprise Security Policy

E. Can provide authentication and Content Security features at the application level

Answer: A,C,D,E

Explanation:

We normally use a multihomed machine to have internal, external and DMZ interfaces. It´s also installed in a enforcement point, because it will analyze the network traffic to comply with the enterprise security policy. Additionally, it can provide authentication through the supported schemes (Client, Session, User) and also some content security at the application level like stripping off Java code from HTTP connections.

Incorrect Answers:

B: Logging is maintained at the management module.

QUESTION NO: 205

Which is not a step in Session Authentication?

A. The user initiates a connection directly to the server.

B. The Session Authentication agent prompts the user for the authentication data and returns this information to the Inspection Module.

C. If the authentication is successful, then the VPN-1/Firewall-1 NG module allows the connection to pass through the gateway, and continue to the target server.

D. The Session Authentication agent prompts the user for authentication data and returns this information to the Inspection Module.

E. The Session Authentication agent prompts the user for authentication data after a valid check of (something) and returns this information to the Inspection Module.

Answer: E

Explanation:

In session authentication the session agent doesn't try to authenticate the user if the validation checking is already done.

Here is the complete process: First, the user connects directly to the destination server, then the inspection module intercepts the connection and the inspection module connects to the session agent on the client PC, then the session agent prompts the user for authentication data and returns it to the inspection engine in the firewall, at the end, if the authentication is successful, the gateway allows the connection to pass through to the target server.

Incorrect Answers:

QUESTION NO: 206

What component of CheckPoint NG allows you to export Logs to an external program such as Access or Excel.

A. ELA
B. LEA
C. Logs cannot be exported to external programs.
D. ULLLS

Answer: B

Explanation:
You can use LEA (Log export API), first Microsoft have to create an interface so it can access the information in the logs. See Appendix D.3 of the CCSA NG Courseware - Management I.

Incorrect Answers:
A: ELA is used to send information inside the checkpoint logs (import data).
C: This is possible through LEA.
D: This is not related to our question matters.

QUESTION NO: 207

What is not a feature of the SVN Foundation.

A. Watch dog for critical services
B. Cpstart/CPstop
C. CPMAD
D. Check Point Registry

Answer: C

Explanation:
CPMAD is a log analyzer for Checkpoint, it compares the logs with the rules defined for alerting. It´s not part of the SVN Foundation package. See Page 1.19 of the official CCSA NG Courseware - Management I.

Incorrect Answers:
A: This part of SVN Foundation. See Page 1.19 of the official CCSA NG Courseware - Management I.
B: This part of SVN Foundation. See Page 1.19 of the official CCSA NG Courseware - Management I.
D: This part of SVN Foundation. See Page 1.19 of the official CCSA NG Courseware -

Management I.

QUESTION NO: 208

What can NAT be performed on?

A. Domains, Networks & Workstations
B. Domains & Networks
C. Security Servers & Networks
D. Networks, Workstations, and IP ranges

Answer: D

Explanation:
NAT can be performed in all of this: Networks, Workstations, and IP ranges, just create rules inside your NAT policies and see that you can use all of this objects.
Incorrect Answers:
A: Domains should not be included in the answer.
B: This is not the most complete answer.
C: This is not the most complete answer.

QUESTION NO: 209

The system display status displays a firewall with "!". What does this mean?

A. The firewall is defined as external
B. The firewall has been turned off
C. Nothing is wrong
D. The firewall is unprotected, no security policy is loaded
E. The module is problematic

Answer: E

QUESTION NO: 210

If you want a user to authenticate every time they use the internet what authentication scheme would you use?

A. User
B. Client
C. Session

Answer: A

QUESTION NO: 211

At what level of the OSI model does the Firewall Module sit?

A. Presentation
B. Data
C. Network
D. Physical
E. Session

Answer: C

QUESTION NO: 212

User authentication cannot provide access privilege for which services?

A. HTTP
B. FTP
C. TELNET
D. RPC
E. RLOGIN

Answer: D

QUESTION NO: 213

Tess was initiating a client authentication session by beginning an HTTP session on port 259 with the gateway named London. What do you think might be wrong with the address Tess specified in the browser?

A. The user should use Session Authentication method to successfully connect to the destination server.
B. The user should be able to connect, since she was using the right port.
C. The user was using the wrong port. She needs to use port 900 to connect successfully.
D. The user should bypass the firewall at port 900 to connect successfully.
E. The user should bypass the firewall at port 259 to connect successfully.

Answer: C

QUESTION NO: 214

You can choose to hide your internal IP addresses in which of the following ways? (Select all that apply)

A. Hide behind the IP address of the gateway's external interface
B. Hide behind 255.255.255.255
C. Hide behind an imaginary IP address
D. Hide behind the IP address of the gateway's internal interface
E. Hide behind 0.0.0.0

Answer: A,E

QUESTION NO: 215

The implicit-drop rule follows the principle "that which is not expressly permitted is _____"

A. Prohibited
B. Allowed
C. Rejected
D. Dropped
E. Moved

Answer: A

QUESTION NO: 216

How would you remedy a conflict between Anti-Spoofing and NAT?

A. By adding the translated, external IP address to the Valid Addresses on the external interface
B. By removing die translated, external I? address to the invalid Addresses on the internal interface
C. By adding the translated external IP address to the Valid Addresses on the internal interface
D. Reinstall NAT rules
E. Do nothing

Answer: C

QUESTION NO: 217

From what two windows can you use to block or terminate any connection from or to a specific IP address in Log Viewer NG? (Select two.)

A. Request window

B. Intruder window

C. Block Intruder window

D. Block Request window

E. Block Request/Intruder window

Answer: C,D

QUESTION NO: 218

What are the advantages of Central Licensing? (Select all that apply.)

A. Only one IP address is needed for all licenses

B. Multiple IP address are needed for all licenses

C. The licenses remain valid when changing the IP address of a Module

D. The licenses are revoked when changing the IP address of a Module

E. A license can be removed from one Module and installed on another Module

Answer: A,C,E

QUESTION NO: 219

Select what is true of hidden rules.

A. Whether they are displayed, or not, hidden rules are made redundant when the security Policy is installed

B. Whether they are displayed, or not, hidden rules are displayed when the security Policy is installed

C. Whether they are displayed, or not, hidden rules are enforced when the security Policy is installed

D. Whether they are displayed, or not hidden rules numbering would change when the security Policy is installed

E. None of the above

Answer: C

QUESTION NO: 220

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

A. Static Source

B. Static Destination

C. Dynamic Source

D. Dynamic

E. None of the above

Answer: A

QUESTION NO: 221

What are the two components of SecureUpdate? (Select two.)

A. Central License

B. Installation Manager

C. Local Manager

D. License Manager

E. Installation Service

Answer: B,D

QUESTION NO: 222

What configuration is said to be used if the Policy Editor and the Management Server are deployed on separate machines?

A. Client/Server

B. Server/Server

C. Firewall

D. Client/Client

E. None of the above

Answer: A

QUESTION NO: 223

What is the purpose of Stealth Rule?

A. To specify users that should be allowed to connect to the firewall.

B. To disable a firewall.

C. To allow any connection to the firewall.

D. To prevent any user from connecting directly to the firewall.

E. To specify users that should be prevented from connecting to the firewall.

Answer: D

QUESTION NO: 224

Which type of authentication will require users to TELNET to port 259 or connect via HTTP at port 900 to be authenticated for a service?

A. Session authentication
B. User authentication
C. Client authentication
D. IP authentication
E. None

Answer: C

QUESTION NO: 225

What is the purpose of NAT? (Select all that apply.)

A. To conceal external computers and users from outside networks.
B. To translate internal host names to IP addresses.
C. To conceal internal computers and users from outside networks.
D. To overcome IP addressing limitations, by allowing usage of private I P address allocation and unregistered internal addressing schemes.
E. To conceal external computers and users from inside networks.

Answer: C,D

QUESTION NO: 226

If the security policy is enforced by more than two firewalls how many rule bases would you need?

A. Two rule bases.
B. Only one rule base.
C. One rule base each for each number of network objects there
D. Three rule bases.
E. No rule base is needed to implement your security policy.

Answer: B

QUESTION NO: 227

In Log Viewer GUI what option do you select to delete all entries in the log file, regardless of which entries are selected?

A. Kill
B. Delete
C. Purge
D. Cut
E. Remove

Answer: C

QUESTION NO: 228

_____ rules, defined in a firewall object's properties, are enforced before any rule in the Security Policy's Rule Base.

A. Anti-spoofing
B. Explicit
C. Implicit
D. Implicit drop
E. None of the above

Answer: A

QUESTION NO: 229

What happens to current log file when you create a new log file?

A. New Log file cannot be created when current file is opened.
B. The current file is appended to the new file.
C. The current Log file is opened in addition to the new Log file.
D. The current Log file is closed and written to disk with a name that contains the current date and time, as only one Log file can be opened in the Log Viewer at a time.
E. The current file is lost.

Answer: D

QUESTION NO: 230

The rules that you define in the Rule Base are known as _____ rules.

A. Implicit
B. Explicit
C. Properties setup
D. Stealth
E. Cleanup

Answer: B

QUESTION NO: 231

The _____ maintains the VPN-1/Firewall-1 NG database. The database includesnetwork object definitions, user definitions, security policy, and the log files.

A. Firewall Module
B. Management Server
C. Client Module
D. Server Module
E. None of the above

Answer: B

QUESTION NO: 232

What command uninstalls the currently loaded Inspection Code from selected targets?

A. cp load
B. cp putkey
C. cp unload
D. cp install
E. cp uninstall

Answer: C

QUESTION NO: 233

Why would an administrator want to negate a selected object in the Rule Base?

A. To include all objects or users and exclude a specific object or user

B. To include a specific object or user

C. To nest a specific object or user

D. To connect to any destination using tcp/ip service.

E. To connect to any destination using ftp service.

Answer: A

QUESTION NO: 234

What NAT type translates valid IP addresses to invalid IP addresses for connections initiated by external clients?

A. Static Source NAT

B. Static Destination NAT

C. Hide Mode

D. Static NAT

E. None of the above

Answer: B

QUESTION NO: 235

Check Point Registry, cpstart/cpstop, cpshared Daemon, Watch Dog for critical Services, and cpconfig are components of what?

A. CPShared

B. Enforcement Module

C. sic

D. SecureUpdate

E. Management Module

Answer: A

QUESTION NO: 236

What two services or protocols can Client Authentication uses to initiate connection to the firewall? (Select two.)

A. TELNET and HTTP

B. TELNET and RPC

C. HTTP and HTTPS

D. HTTP and UDP E. HTTP and TCP

Answer: A

QUESTION NO: 237

Why must Client Authentication rule be placed above Stealth rule in the Rule Base?

A. In order that they can have access to the local Management Server
B. In order that they can have access to the Management Server
C. In order that they can have access to the local firewall
D. In order that they can have access to the Policy Editor
E. In order that they can have access to the OS

Answer: C

QUESTION NO: 238

Which of the following ports would TELNET service use for communications?

A. 21
B. 23
C. 25
D. 29
E. 30

Answer: B

QUESTION NO: 239

What is the advantage of a VPN-1/ Firewall-1 NG password authentication scheme over the OS password authentication scheme?

A. The user does not require an OS account on the gateway to use a VPN-I/ Firewall-1 password.
B. The user does require an OS account on the gateway to use a VPN-I/ Firewall-I password.
C. The VPN-I/ Firewall-I password has no advantage over OS password.
D. Using VPN-I/ Firewall-I password will allow the authenticating user to bypass the gateway.

Answer: A

QUESTION NO: 240

SecureUpdate License Manager supports which two types of licenses for Check Point products? (Select two.)

A. PE-bound
B. Firewall-I bound
C. OS-bound
D. Management-bound
E. Module-bound

Answer: D,E

QUESTION NO: 241

Which of these is NOT a component of SecureUpdate?

A. Installation Server
B. Installation Manager
C. License Manager
D. None of the above

Answer: A

Explanation:
Note:
Note 1:
Section A contains 96 questions.
Section B contains 146 questions.
The total number of questions is 242.
Each section starts with QUESTION NO :1. There are no missing questions.

Note 2 : Answers to the unanswered questions will be provided shortly. First customer, if any, faster than us in providing answers will receive credit for each answer provided.

Send your suggestions to feedback@Certpaper.com .