



Exam : 156-310

Title : Check Point CCSE NG

Ver : 11.24.08

QUESTION 1:

Which of the following statements about IKE Encryption are TRUE? (Choose three)

- A. The final packet size is increased after it is encrypted.
- B. TCP and IP headers are encrypted, along with the payload.
- C. IKE uses in-place encryption.
- D. IKE can use the FWZ1 encryption algorithm.
- E. IKE uses tunneling encryption.

Answer: A, B, E

Explanation:

IKE Encryption Scheme

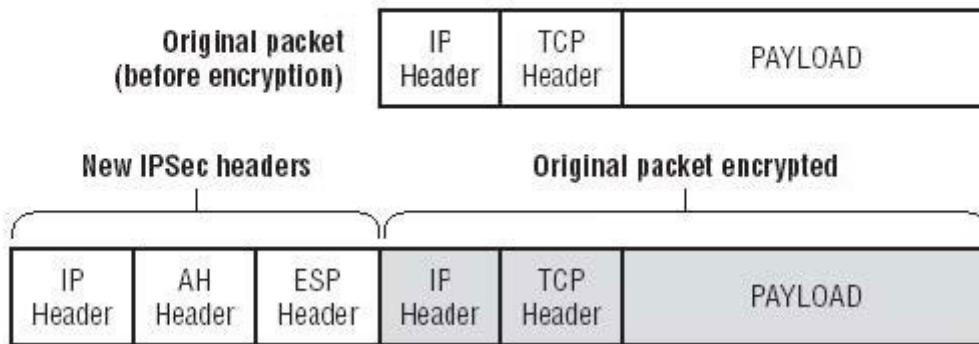
A long time ago (about four years in real time), Check Point supported many different encryption schemes: Manual IPSec, Simple Key Management for Internet Protocols (SKIP), FWZ (Check Point's own proprietary scheme), and Internet Key Exchange (IKE). As the industry began to settle on a standard and it became apparent that different vendors' VPN products needed to work together, the schemes were whittled down to only one: IKE.

IKE is a hybrid protocol that combines the Internet Security Association and Key Management Protocol (ISAKMP) and the Oakley Key Exchange Protocol. ISAKMP is responsible for the generation and maintenance of Security Associations, and Oakley is responsible for key exchanges. Both ISAKMP/Oakley and IKE are described in the IETF standard for encryption using the IP Security Protocol (IPSec). (The terms IKE and IPSec are frequently used interchangeably.)

You can find more on IPSec and its related protocols in RFCs 2401-2411 and 2451.

IPSec provides the access control, integrity of the packet, authentication, rejection of replayed packets, encryption, and non-repudiation (there's that PAIN acronym coming into play). IPSec does so by using the protocols Authentication Header (AH) and Encapsulating Security Payload (ESP). Each protocol-IPSec, AH, and ESP-is incorporated into its own header in the IPSec packet. IKE is also a tunneling protocol, which means it encrypts the entire original packet and adds new headers to the encrypted packet.

IPSec packet



Tunneling encrypts the entire original packet and adds new headers, which increases packet size and the likelihood of packet fragmentation. In-place encryption was Check Point's proprietary FWZ scheme supported in versions before FP2. It only encrypted the payload, and left the headers alone; therefore packet size did not increase. Although FWZ is no longer supported as of FP2, this information could still be used for a valid NG test question.

The new IP header uses the IPSec protocol and replaces the true source and destination of the packet (which are now encrypted) with the source and destination IP addresses of the firewalls involved in the VPN tunnel.

The AH header provides data integrity and authentication by using a message digest (instead of a digital signature, which is too slow for this process) and a Security Parameters Index (SPI). The SPI is like a pointer that tells your VPN partner which methods were selected for this VPN session. The SPI references the Security Association (SA), which was negotiated by the VPN participants. A good analogy to describe the SA is a large spreadsheet that contains all the possible combinations for key exchange, encryption, data integrity, and so forth that could be used for this connection. The SPI is the pointer that tells each partner which parts of the spreadsheet will be used for this specific tunnel. The ESP header provides confidentiality as well as authentication. It gives a reference to the SPI as well as an Initialization Vector (IV), which is another data integrity check.

IKE supports a variety of different encryption algorithms, but VPN-1 supports only DES, Triple-DES, CAST, and AES.

Encryption Standards Support by IKE and VPN-1

Algorithm	Description
DES	Data Encryption Standard (standard in the U.S. for the last 20 years). A symmetric key encryption method that uses 56-bit keys.
Triple DES	A variation on DES that addresses the problem of short, easily breakable keys. Encrypts with three different DES keys in succession, which increases the effective key strength to 168 bits.

Encryption Standards Support by IKE and VPN-1 *(continued)*

Algorithm	Description
CAST	Named for its inventors, Carlisle Adams and Stafford Tavares. Similar to DES and supports variable key lengths from 40–128 bits.
AES	Advanced Encryption Standard. The new Federal Information Processing Standard (FIPS) standard. Also known as Rijndael (pronounced “rhine-doll”) for its inventors, Vincent Rihmen and Joan Daemen.

For a more detailed explanation of encryption, IPSec, and cryptography, we recommend Applied Cryptography (John Wiley & Sons, 1995), RSA Security's Official Guide to Cryptography (McGraw-Hill, 2001) and IPSec Securing VPNs (McGraw-Hill Osborne Media, 2001).

Encryption is not an easy topic to grasp, especially in an abbreviated format within a study guide. But this background information is essential before we go into detail about how IKE negotiates keys and eventually encrypts data. Let's forge ahead and tackle the IKE phases of key negotiation.

QUESTION 2:

When upgrading a configuration to NG with Application Intelligence: (Choose the FALSE answer)

- A. Upgrade the SmartConsole.
- B. Upgrade each module's version in SmartDashboard manually.
- C. Upgrade the VPN-1/Firewall-1 Enforcement Modules.

- D. Copy \$FWDIR/state from one version of VPN-1/FireWall-1 to another version of VPN-1/FireWall-1.
- E. Upgrade the SmartCenter server. The version is set during the upgrade.

Answer: D

Explanation:

Upgrading to VPN-1/FireWall-1 NG

Now that you've performed a successful installation of FireWall-1 NG, it's time to understand how to upgrade from a previous version of VPN-1/FireWall-1. At the time of this writing, many companies are looking to upgrade from an older version of VPN-1/FireWall-1 (usually 4.1 SP3 or higher) to NG FP3. You can upgrade to NG FP1 from version 4.0 and higher. If you are running a version older than 4.0, you must upgrade to version 4.0 first, and then upgrade to NG.

With the many enhancements in NG, it's better to create a fresh install of NG and then migrate your existing configuration files over to the newly created NG firewall. The upgrade technique discussed here will upgrade version 4.1 Service Pack 6 configuration files to NG configuration files. It is recommended that the 4.1 files are upgraded to Service Pack 6 before converting them to NG. In many instances, companies are viewing the NG upgrade as an opportunity to upgrade the current platform on which their firewalls are running. For example, this is an chance to upgrade operating systems from Solaris 2.6 to 2.8, or to upgrade hardware from a Pentium II machine with limited hard drive space and memory to a Pentium IV with lots of hard drive space and much more memory.

In order to make the NG upgrade a smooth and convenient process, Check Point has developed an upgrade script that helps convert 4.1 configuration files to NG configuration files. This script automates the conversion by using the confmerge command on the objects.C, fwauth.NDB, and rulebases.fws files. (This script is not meant for people who are moving from a Windows machine to a Unix machine, or for people running Flood-Gate.) The script is in a zipped file called upgrade.4.3.tgz and can be downloaded from the support.checkpoint.com website. Here are the steps to use the upgrade script:

1. Create a new SmartCenterServer machine with the desired Feature Pack version of NG (FP1, FP2 or FP3), based on the installation guidelines previously discussed. This upgrade procedure will upgrade to FP3.
2. Download and unzip the upgrade.4.3.tgz file. This file opens into a directory named upgrade.
3. Place the 4.1 SP6 files on the SmartCenter Server under upgrade/4.1:
 - a. objects.C.
 - b. fwauth.NDB. On Windows machines, this file is only the pointer to the real database file-for example, fwauth.NDB522. In this case, take the real database file (fwauth.NDB522), rename it fwauth.NDB, and put it in the \upgrade\4.1 directory.

c. rulebases.fws.

4. Stop the FireWall-1 Services (cpstop), cd to the ,
and issue the following command

in Windows (upgrade from 4.1 to FP3):

upgrade.bat < upgrade_directory>\upgrade FP3 4.1

In Unix, enter this command (upgrade from 4.1 to FP3):

upgrade.csh < upgrade_directory>/upgrade FP3 4.1

5. Restart the FireWall Services (cpstart) and log in to the GUI.

After you have successfully run the script, in order to transfer the remaining configuration files (such as gui-clients, masters, and so on), copy the following files from the VPN-1/FireWall-1 4.1 \$FWDIR/conf directory to the VPN-1/FireWall-1 NG \$FWDIR/conf directory:

xlite.conf, aftpd.conf, smtp.conf, sync.conf, masters,
clients, fwusers, gui-clients, slapd.conf, serverkeys,
product.conf

In addition to understanding which configuration files are important in upgrading to Check Point NG, it's important to understand which configuration files need to be saved for backup in case of a failure or loss of files. The next section talks about backup and restore options and identifies the critical configuration files needed for backup.

QUESTION 3:

When you upgrade VPN-1/FireWall-1, what components are carried over to the new version? (Choose two)

- A. Licenses
- B. VPN-1/FireWall-1 database
- C. OPSEC database
- D. Backward Compatibility
- E. Rule Base

Answer: A, B

Explanation:

Upgrading to VPN-1/FireWall-1 NG

Now that you've performed a successful installation of FireWall-1 NG, it's time to understand how to upgrade from a previous version of VPN-1/FireWall-1. At the time of this writing, many companies are looking to upgrade from an older version of VPN-1/FireWall-1 (usually 4.1 SP3 or higher) to NG FP3. You can upgrade to NG FP1 from version 4.0 and higher. If you are running a version older than 4.0, you must upgrade to version 4.0 first, and then upgrade to NG.

With the many enhancements in NG, it's better to create a fresh install of NG and then migrate your existing configuration files over to the newly created

NG firewall. The upgrade technique discussed here will upgrade version 4.1 Service Pack 6 configuration files to NG configuration files. It is recommended that the 4.1 files are upgraded to Service Pack 6 before converting them to NG. In many instances, companies are viewing the NG upgrade as an opportunity to upgrade the current platform on which their firewalls are running. For example, this is an chance to upgrade operating systems from Solaris 2.6 to 2.8, or to upgrade hardware from a Pentium II machine with limited hard drive space and memory to a Pentium IV with lots of hard drive space and much more memory.

In order to make the NG upgrade a smooth and convenient process, Check Point has developed an upgrade script that helps convert 4.1 configuration files to NG configuration files. This script automates the conversion by using the confmerge command on the objects.C, fwauth.NDB, and rulebases.fws files. (This script is not meant for people who are moving from a Windows machine to a Unix machine, or for people running Flood-Gate.) The script is in a zipped file called upgrade.4.3.tgz and can be downloaded from the support.checkpoint.com website. Here are the steps to use the upgrade script:

1. Create a new SmartCenterServer machine with the desired Feature Pack version of NG (FP1, FP2 or FP3), based on the installation guidelines previously discussed. This upgrade procedure will upgrade to FP3.

2. Download and unzip the upgrade.4.3.tgz file. This file opens into a directory named upgrade.

3. Place the 4.1 SP6 files on the SmartCenter Server under upgrade/4.1:

- a. objects.C.

- b. fwauth.NDB. On Windows machines, this file is only the pointer to the real database file-for example, fwauth.NDB522. In this case, take the real database file (fwauth.NDB522), rename it fwauth.NDB, and put it in the \upgrade\4.1 directory.

- c. rulebases.fws.

4. Stop the FireWall-1 Services (cpstop), cd to the , and issue the following command in Windows (upgrade from 4.1 to FP3):

```
upgrade.bat < upgrade_directory>\upgrade FP3 4.1
```

In Unix, enter this command (upgrade from 4.1 to FP3):

```
upgrade.csh < upgrade_directory>/upgrade FP3 4.1
```

5. Restart the FireWall Services (cpstart) and log in to the GUI.

After you have successfully run the script, in order to transfer the remaining configuration files (such as gui-clients, masters, and so on), copy the following files from the VPN-1/FireWall-1 4.1 \$FWDIR/conf directory to the VPN-1/FireWall-1 NG \$FWDIR/conf directory:

xlite.conf, aftp.conf, smtp.conf, sync.conf, masters, clients, fwmusers, gui-clients, slapd.conf, serverkeys, product.conf

In addition to understanding which configuration files are important in upgrading to Check Point NG, it's important to understand which configuration

files need to be saved for backup in case of a failure or loss of files. The next section talks about backup and restore options and identifies the critical configuration files needed for backup.

QUESTION 4:

Which of the following is NOT a function of the Internal Certificate Authority (ICA)?

- A. Provides certificates for users and Security Administrators.
- B. Generated certificates for HTTPS Web server.
- C. Establishes SIC between OPSEC applications and Check Point products.
- D. Authentications SecureClient traffic to Enforcement Modules for VPNs.
- E. Establishes SIC between Check Point products.

Answer: B

Explanation:

internal certificate authority (ICA)

The certificate authority generated

during the installation of a Check Point SmartCenter Server. Certificates generated by the ICA are used for encryption and authentication.

QUESTION 5:

Which of the following FTP Content Security settings prevents internal users from sending corporate files to external FTP Servers, while allowing users to retrieve files?

- A. Use an FTP resource, and enable the GET and PUT methods.
- B. Use an FTP resource and enable the GET method.
- C. Use an FTP resource and enable the PUT method.
- D. Block FTP_PASV.
- E. Block all FTP traffic.

Answer: B

Explanation:

FTP

The FTP (File Transfer Protocol) SmartDefense group essentially has two purposes: It can protect your system against a specific FTP attack called FTP Bounce, and it lets you configure your FTP Security Server.

SmartDefense for FTP



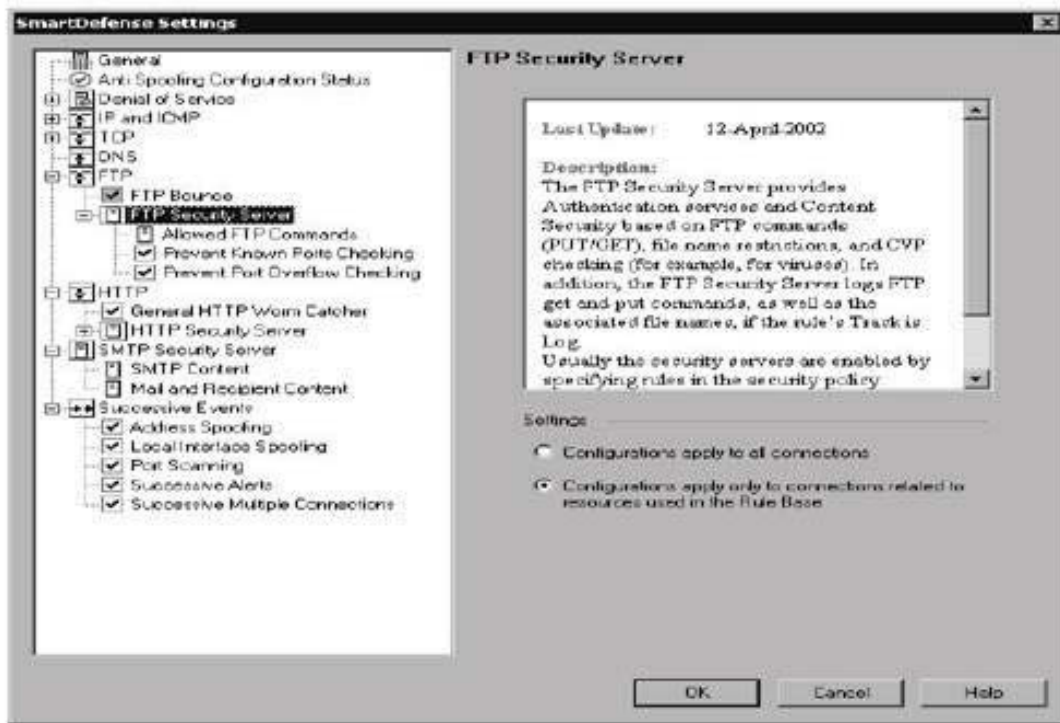
FTP Bounce

The FTP Bounce attack takes advantage of a design flaw in FTP. Port 20 is where the FTP PORT command negotiates a random high port for PASV transport of FTP data files. RFC 959, which describes FTP, dictates that the negotiated high port be allowed to any IP address and any port. The FTP Bounce attack takes advantage of this and the attacker can open a connection to a machine of their choosing for illegitimate purposes. You can select the Track option for notification if a FTP Bounce attack is detected.

FTP Security Server

The firewall FTP Security Server provides authentication and content security services (see Chapter 4, "Content Security," for more details on the FTP Security Server). Usually the FTP Security Server (showing below) is invoked by rules in your rule base that specify an FTP Resource or User Authentication. Selecting the Configurations Apply To All Connections radio button forces all FTP connections through the FTP Security Server regardless of whether your rule base contains an authentication or resource rule.

FTP Security Server

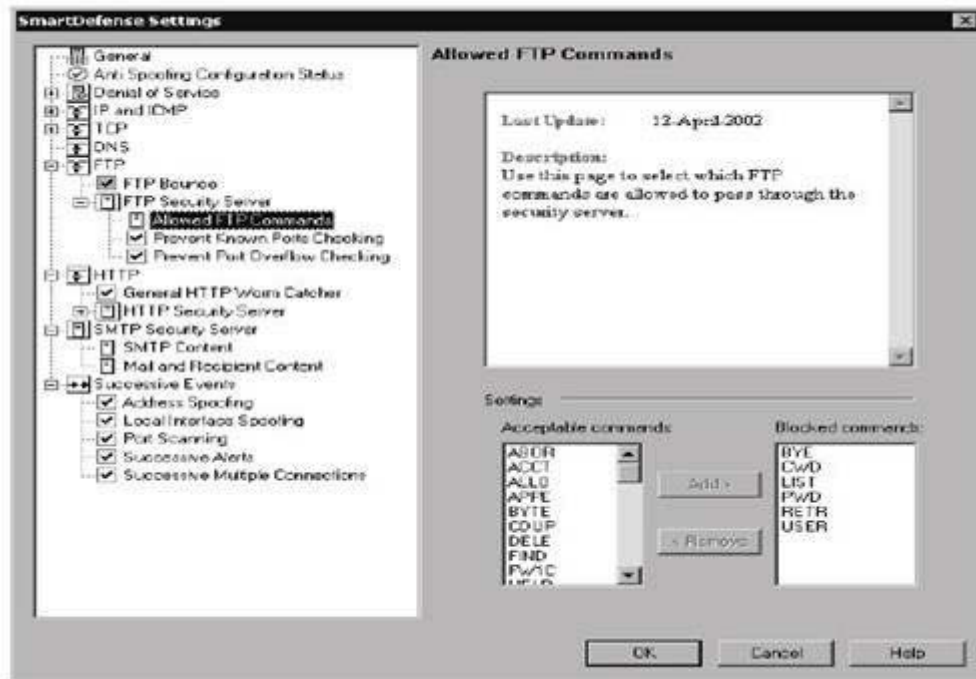


Selecting the default option of Configurations Apply Only To Connections Related To Resources Used In The Rule Base will cause the FTP Security Server to be invoked only when a resource or authentication rule in the rule base triggers it.

You need to take into consideration three further settings when setting up the FTP Security Server: Allowed FTP Commands, Prevent Known Port Checking, and Prevent Port Overflow Checking:

Allowed FTP Commands The Allowed FTP Commands option, illustrated in Figure below, gives you granular control over the FTP commands the FTP Security Server will respond to. You can set Acceptable commands and Blocked commands.

Allowed FTP commands



Prevent Known Port Checking The Prevent Known Port Checking option allows you to specify whether you want the FTP Security Server to allow connections to well-known ports. This option also provides another line of defense against the FTP Bounce attack by not allowing a connection to a well-known port.

Prevent Port Overflow Checking Prevent Port Overflow Checking is another component to help prevent the FTP Bounce Attack. Turning on this option turns off the checks that prevent numerous instances of connections from/to the same port.

QUESTION 6:

All of the following are steps for implementing UFP, EXCEPT:

- A. While the UFP Server is analyzing the requests, the Enforcement Module HTTP Proxy Server initiates a request to the destination. The HTTP Proxy server then waits for a response from the UFP Server before allowing the request.
- B. The client invokes a connection through the VPN-1/FireWall-1 Enforcement Module.
- C. The Content Server inspects the URLs and returns the validation result message to the Enforcement Module.
- D. The Enforcement Module takes the action defined in the Rule Base for the resource.
- E. The Security Server uses UFP to send the URL to a third-party UFP Server categorization.

Answer: A

Explanation:

Content-Filtering Protocols

As mentioned earlier, Check Point utilizes two different protocols to filter the content of HTTP, FTP, SMTP, and TCP traffic: CVP and UFP. Each protocol runs on a specific port and offers a different functionality, as described in the following sections. The Application Program Interface (API) information for each of these protocols can be found at

www.opsec.com

. CheckPoint encourages vendors to program their content filtering products to interface with FireWall-1.

Content Vectoring Protocol (CVP)

Content Vectoring Protocol (CVP)

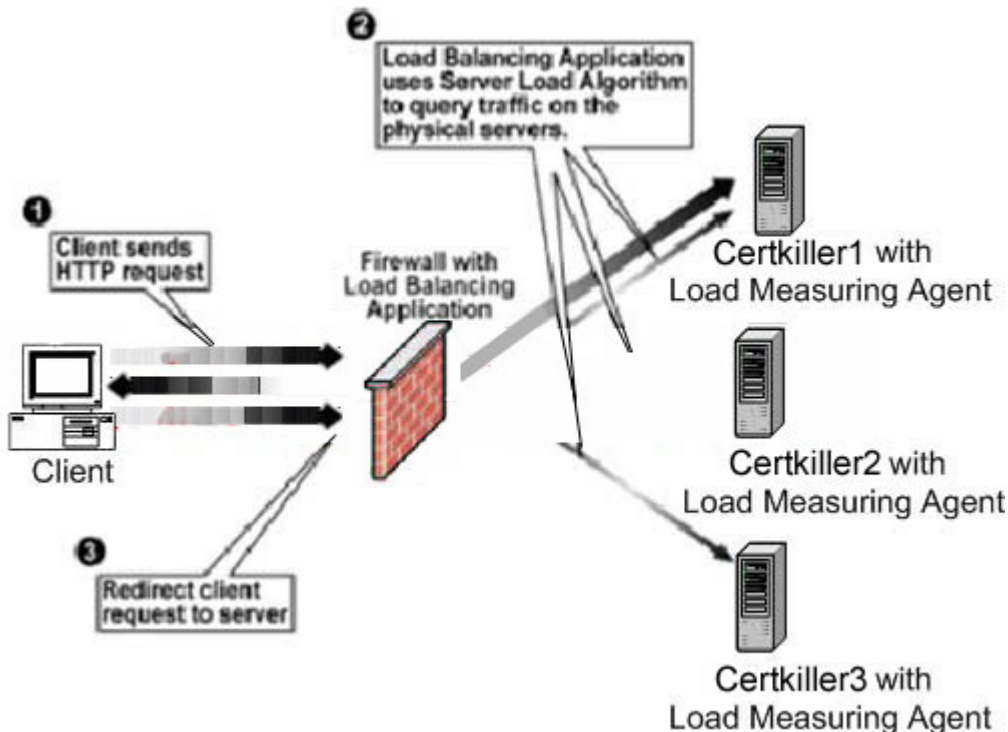
allows FireWall-1 to send a connection

on port 18181 to a CVP server to perform content checking. This API scans HTTP, FTP, SMTP, or other TCP data streams for viruses and malicious Java and ActiveX code. Some of the products also perform security for e-mail message content, but the CVP's main function is virus scanning.

URL Filtering Protocol (UFP)

URL Filtering Protocol (UFP) allows FireWall-1 to send data on port 18182 to a UFP server to perform URL filtering. This API allows organizations to monitor and/or eliminate network traffic to Internet sites deemed inappropriate or otherwise undesirable, as well as control the content viewed by the end user.

QUESTION 7:



The _____ algorithm determines the load of each physical server and requires a Load Measuring Agent be installed on each server.

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

Answer: A

Explanation:

server load A load balancing algorithm in which each server in the server farm has a load-measuring agent installed, which communicates its load to the Logical Server. The server in the server farm with the lightest load gets the connection.

QUESTION 8:

Which of the following is NOT a method of Load Balancing with VPN-1/FireWall-1?

- A. Domain Load Balancing
- B. Round Robin
- C. Server Load
- D. Round Trip
- E. Quantum Load Balancing

Answer: E

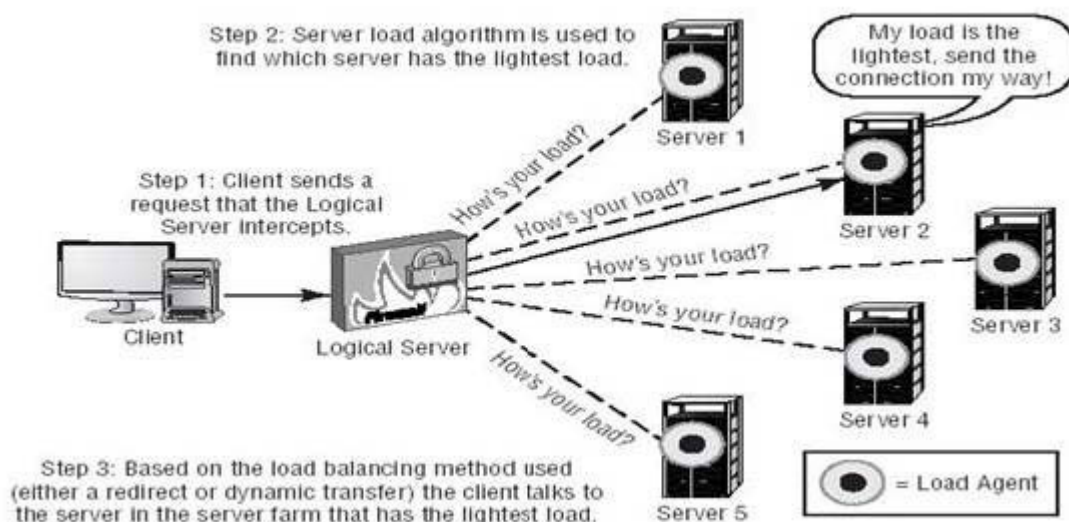
Explanation:

Load Balancing Algorithms

Now that you've learned about the methodologies the logical server/firewall uses to route traffic, you need to consider the algorithms used to decide which server in the server farm will get the load-balanced connection. Check Point provides five algorithms for the logical server; the administrator decides which of these algorithms to use. The algorithms are called server load , ,round trip , ,round robin , ,random , and domain . We'll describe these algorithms next.

The server load algorithm, shown in Figure below, works in conjunction

Server load algorithm



with a load agent that runs on each server in the server farm. The load agent is a small program that communicates to the firewall how busy the machine is. The machine with the lightest load is sent the next packet.

You can download this

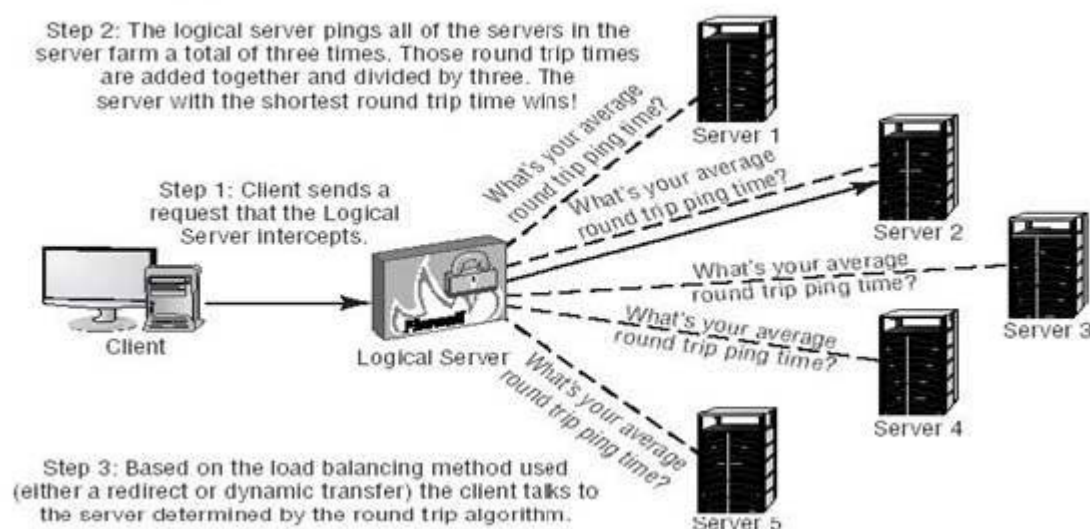
load agent

from Check Point's website (only available for Solaris) or write one using the OPSEC APIs provided by Check Point on

the OPSEC website (www.opsec.com). The load agent uses UDP port 18212 by default. The firewall checks the load on each server at the configured time and passes the connection to the server that has the lightest load.

The round trip algorithm uses ping to decide which server gets the request, as depicted in Figure below. The round trip algorithm is much simpler

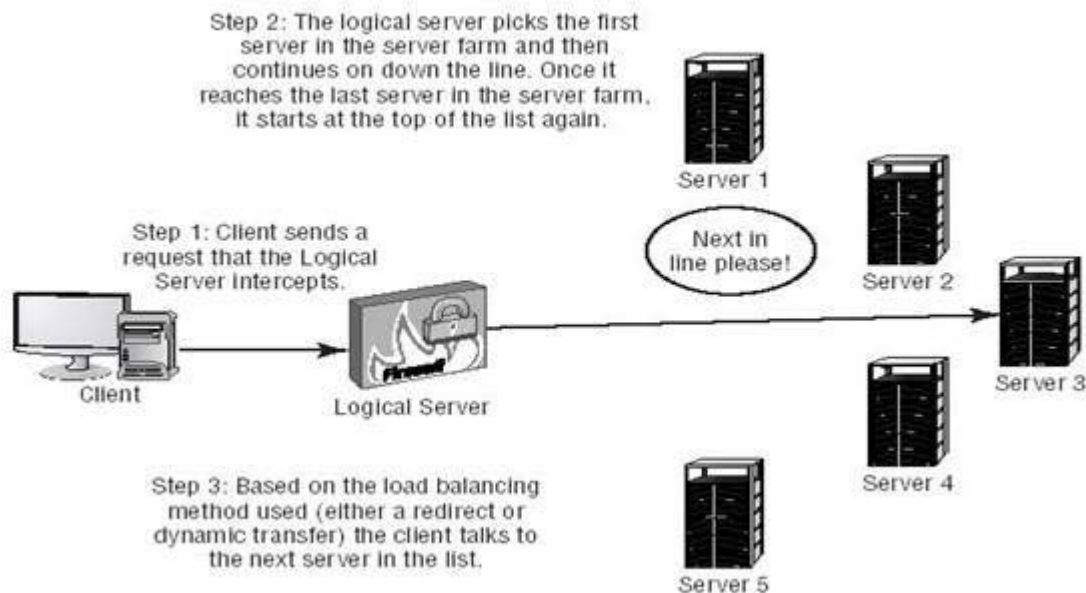
Round trip algorithm



than the server load algorithm, but not as intuitive-it cannot measure the load on the servers. Therefore, the round trip algorithm's decision is based

solely on network factors rather than the server load. When you use round trip, the server with the least traffic will answer first. The server with the most traffic will be too busy to answer, and the packet will be delivered to the machine that answers first. The drawback to using the round trip method is that the server closest to the firewall usually gets the connection. The round robin algorithm, shown in Figure below, is not very intelligent.

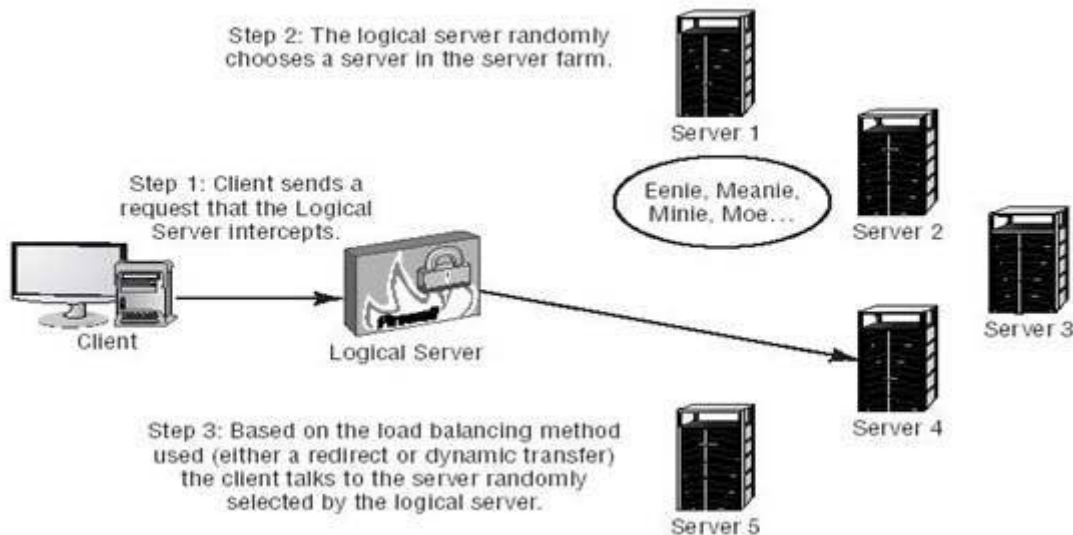
Round robin algorithm



This algorithm begins with the first server in the server farm and gives it the first connection. The second connection goes to the second server in the server farm, the third goes to the third, and so on. When the algorithm reaches the bottom of the list, it starts over.

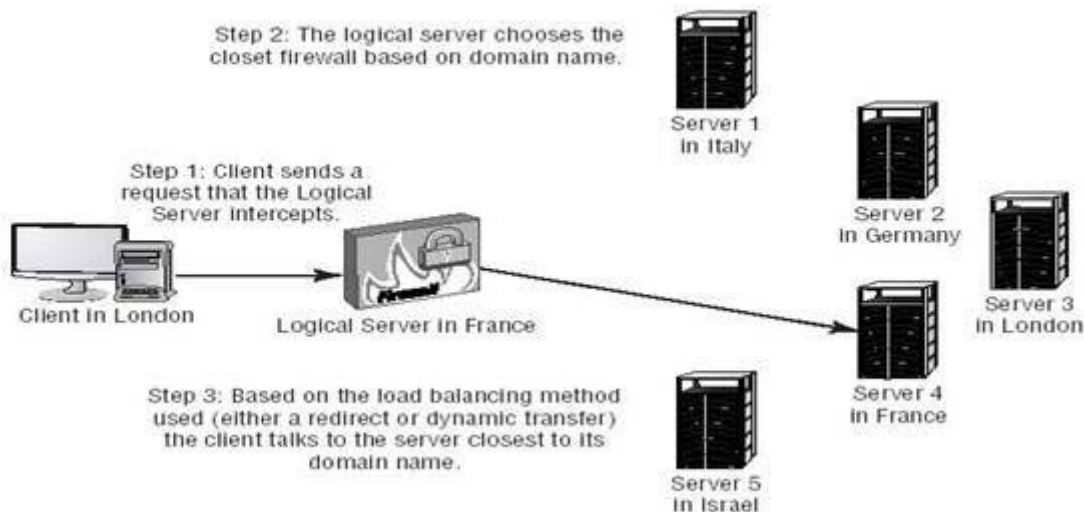
Next in the list of load balancing algorithms is random. Do you remember the method you used to choose teams when you were a kid? Eenie, Meanie, Minie, Mo! That is the same method the firewall uses. The random algorithm is illustrated in Figure below:

Random algorithm



Last is the domain algorithm. With this algorithm, the firewall chooses the closest server based on domain names. Figure below shows an illustration of the domain algorithm in action.

Domain algorithm



There is an issue with the domain algorithm. Check Point doesn't recommend using it, because it creates a noticeable delay for requests due to the required reverse DNS lookups. In today's e-business environment, any delay experienced by users accessing your website could be disastrous. This algorithm was originally designed for clients in Europe and the rest of the world, where they use country names at the end of their URLs (such as www.company.uk) Forexample, in Figure above, if a client in the U.K. is trying to connect to a website for a global company based in France, the initial connection goes to the logical server in France. At this point, the closest server is in France, and it would be

"logical" to send the connection to the server in France. Unfortunately, the domain algorithm will send packets back to the client in the U.K. and redirect them to the server located in the U.K., wasting precious time in the connection setup. This is an effective method only if all your servers are located in Europe and the client is also located in Europe.

To sum up, Check Point offers five algorithms-but in our opinion, only one is a true load balancing method. The server load algorithm is the only method that takes into account the actual load on each server. The rest of the algorithms don't consider how busy each server is in the server farm. As the administrator, you should check out all methods of load balancing (both Check Point and non-Check Point) before deciding which one is best for your situation.

QUESTION 9:

Which of the following does NOT require definition for a Voice over IP (VoIP) Domain SIP object?

- A. SIP Proxy
- B. IP Address Range
- C. VoIP Gateway
- D. Related Endpoint Domain
- E. Name

Answer: A

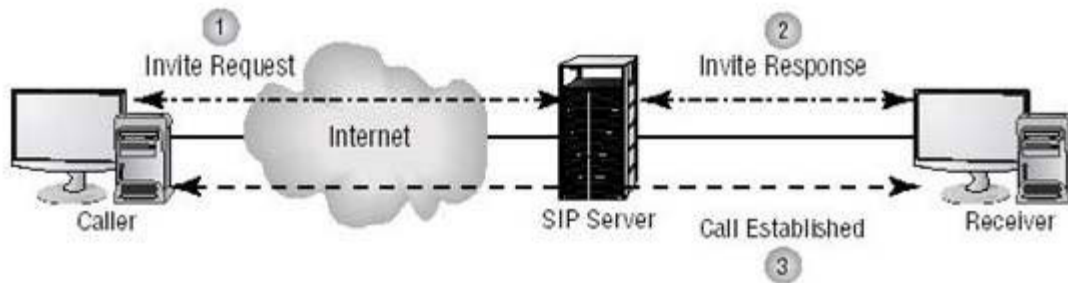
Explanation:

SIP

Session Initiation Protocol (SIP) is the IETF protocol for IP telephony. It only supports IP-based phones. It has a smaller footprint than H.323 so it's faster and more scalable. The problem lies in the fact that it's a newer protocol, and therefore fewer products exist that use it. However, SIP addresses some of the shortcomings of H.323 by making users easier to identify, making it easier to connect two circuit-switched networks across an IP network, and decreasing the delay in call setup time.

SIP identifies users with a Hierarchical URL. This URL is based on a user's phone number or host name and looks similar to an e-mail address (for example, SIP: joeuser@abc.com). Figure below illustrates the SIP call process.

SIP call process



When a call is made, the caller initiates it with an invite request. This request contains the information necessary for the person you're calling to join the session: the media types and formats for the call, the destination for the media data, and perhaps requests for using H.261 video and/or G.711 audio. The invite request is sent to the user's SIP server. Because you include your available features in the invite request, the negotiation of the connection takes place in a single transaction thus call setup time is decreased (approximately 100 milliseconds).

The SIP server may or may not be a proxy server. A SIP proxy server receives the request and figures out the user's location using its internal algorithms. A non-proxy SIP server functions as a redirect server in that it sends back to the user the SIP URL that the user uses to query. In both the redirect and proxy server cases, the server's address is obtained by querying the Domain Name Service (DNS).

Once the SIP URL is found, the request finally makes it to the person you're trying to call. If the person picks up the call, the receiver's client responds to the invite request with the capabilities of its software (videoconferencing, whiteboarding, and so forth), and the connection is established.

SIP has two features that really make it unique:

- It can split an incoming call so that multiple extensions can be rung at once. When the invite request comes in, the SIP server can return to the initiator of the call a Web Interactive Voice Response (IVR) page, which contains extensions of different departments or users in a list. All you have to do is click on the link to call the appropriate person or department.

- It can return different media types.

SIP is simple and easy to deploy because its only job is to identify the user and set up the call; it relies on other protocols and applications to manage the call. It utilizes existing DNS instead of having to create a separate database for telephony. It also interfaces with circuit-switched networks (the PSTN) more easily than H.323. Does this mean SIP is the way to go? Not necessarily. It is not widely available, and (the biggest drawback at this point) it must "de-throne" Microsoft. Every version of Windows that ships has an H.323

client as part of the package (it's free!). Whether a company will purchase another client all depends on its needs and what it wants to accomplish with IP telephony.

While H.323 is the accepted VoIP protocol today, many people think that SIP will be the VoIP protocol of the future. Most of the larger vendors are developing SIP-based solutions if they haven't already. It will be beneficial to understand both protocols to make a decision on what kind of VoIP solution to deploy.

QUESTION 10:

Which of the following is NOT a valid VPN configuration option available in the VPN Manager of the Simplified Rule Base?

- A. Point-to-Point
- B. Mesh
- C. Remote Access
- D. Star with Meshed Center
- E. Star

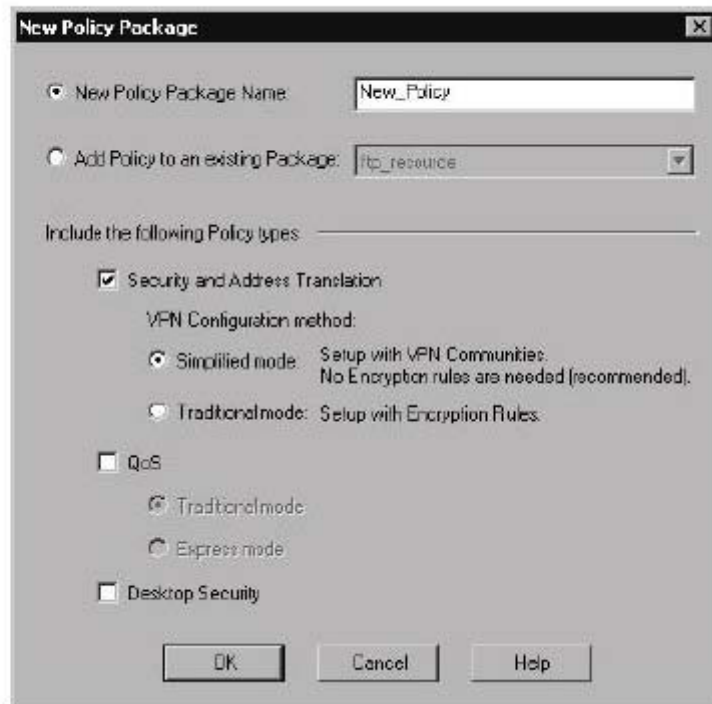
Answer: A

Explanation:

Creating the Simplified VPN Rules

Creating Simplified VPN rules is an oxymoron, because we've said you don't have to create any explicit encryption rules to make the VPN tunnels happen with a VPN community. However, you do have to create a new Simplified Policy and define access rules (unencrypted connections) and rules that specify a VPN community in the If Via column with Accept as the action (which forces this traffic through a VPN tunnel where it is encrypted). In the SmartDashboard, click on File _ New to display the New Policy Package window (Figure below). Give the policy a name (remember, no spaces and no

New Policy Package choices



dashes) and select Security And Address Translation. This option reveals the VPN Configuration methods: You can choose to create a Traditional mode policy (you write the encryption rules) or a Simplified mode policy (no encryption rules are explicitly written; they are assumed based on your VPN community definitions). After selecting Simplified Mode and clicking OK, the new Simplified Policy is now displayed in SmartDashboard. You can tell the difference between a Traditional mode policy and a Simplified mode policy by looking at the rule base. A Simplified Policy has a new column called If Via and a new tab called VPN Manager, as well as an implied VPN rule, as shown in Figure below. If you look at the options available

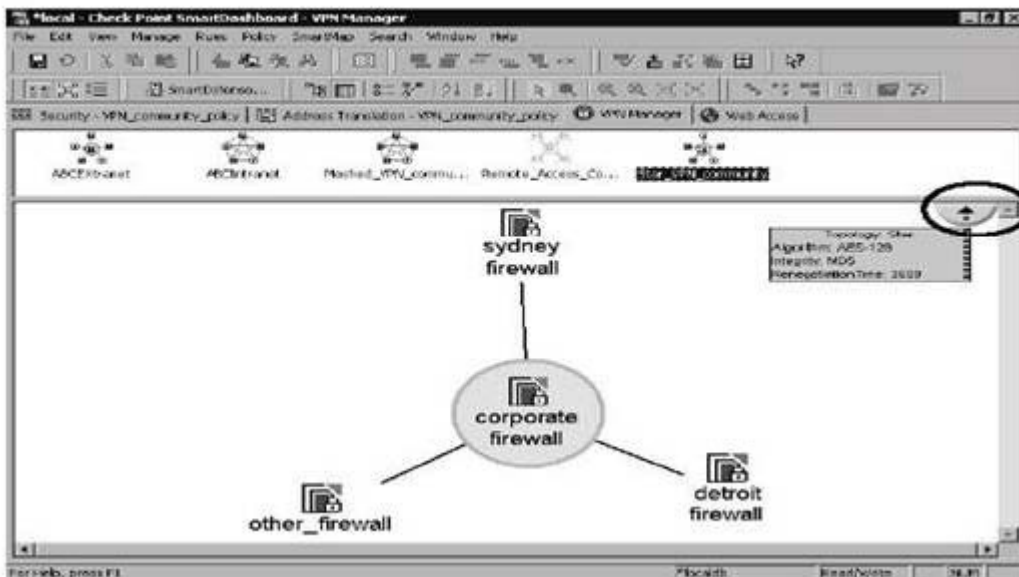
Simplified Policy in the SmartDashboard



in the Action column, you will also notice that the Encrypt options are gone. The If

Via column is used to define access rules between VPN sites participating in a VPN community. If Via is not an acronym. It's easier to understand if you "read" a rule: For example, a source of my network with a destination of another network going through (If Via) using HTTP is allowed (accepted). The addition of a VPN community in the If Via column forces all traffic matching that rule to be encrypted/decrypted even though the Action is Accept. Remember that rules created in the rule base with nothing defined in the If Via column do not affect the VPN community. To see how the VPN is configured, click on the VPN Manager tab in the SmartDashboard to display your VPN communities, as shown in Figure below.

VPN Manager tab in SmartDashboard



All VPN communities are listed here, including extranet management (discussed in Chapter 8) and remote access VPNs (discussed in Chapters 9 and 10). Select the specific VPN community in the upper window of the VPN Manager to display the topology of the VPN community in the lower pane. In Figure above, selecting the circled portion of the picture will tell you all about that VPN community: the type of topology (star, meshed, star/center-meshed), the encryption algorithm, the data integrity method, and the key renegotiation time as depicted in Figure below.

VPN community information



Aside from completing the access rules in the Security tab of the Smart-Dashboard and verifying/installing your policy, you've finished your Simplified VPN.

In Simplified mode (FP2), you could configure star and mesh intranet topologies as well as remote access topologies, but you could not configure extranets.

Traditional mode was required in order to create extranet rules as well as specific VPN rules. This is no longer true in FP3. Remote access, extranet, and site-to-site Simplified VPNs can be configured in VPN communities

QUESTION 11:

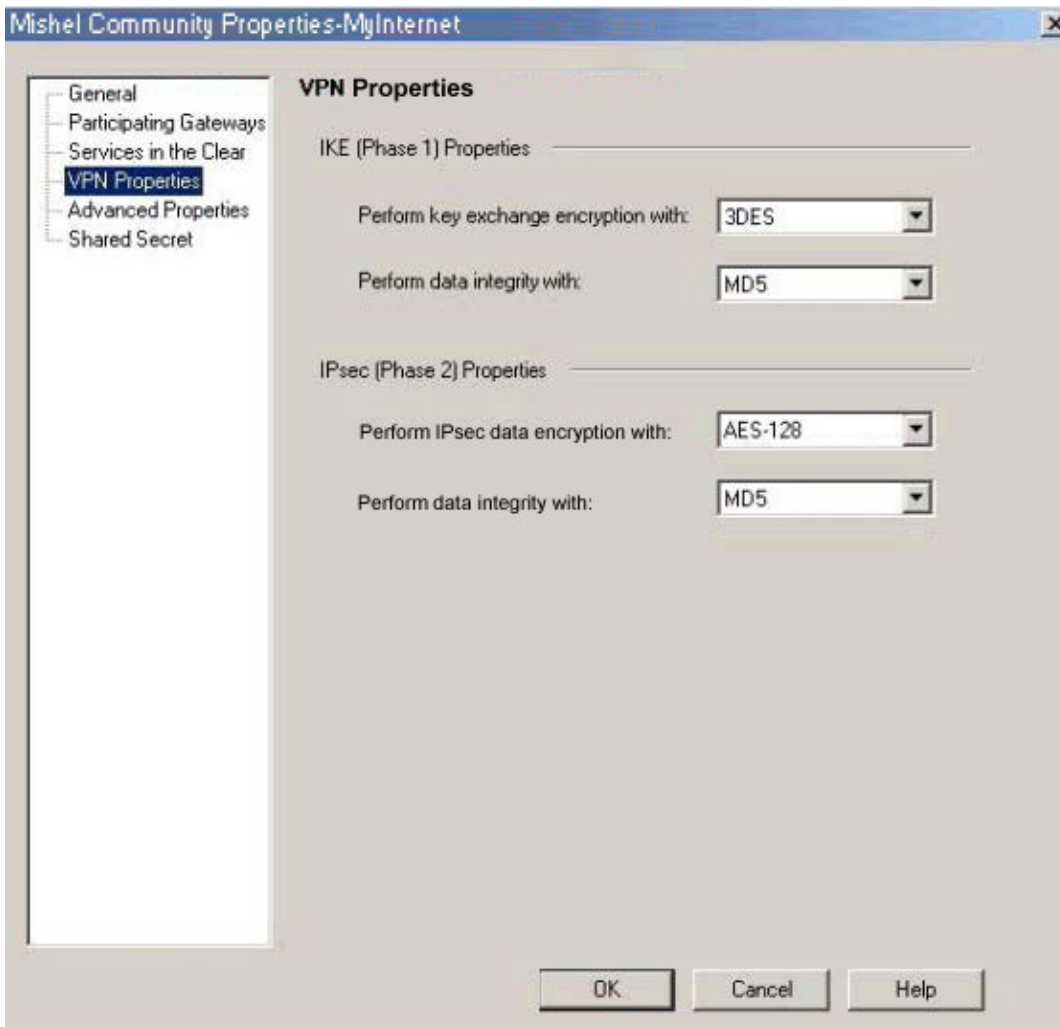
Which of the following is TRUE of the relationship between the RemoteAccess VPN Community and the Security Policy Rule Base?

- A. The RemoteAccess VPN Community defines VPN connection parameters for SecuRemote connections. The Security Policy Rule Base is used to allow access to protected resources.
- B. The RemoteAccess VPN Community is used to allow access to protected resources. The Security Policy Rule Base is used to define VPN connection parameters for SecuRemote connections.
- C. The Security Policy Rule Base is used to define VPN connection parameters for SecuRemote connections and is used to allow access to protected resources. The RemoteAccess VPN Community applies only SecureClient.
- D. The RemoteAccess VPN Community defines VPN connection parameters for SecuRemote connections and is used to allow access to protected resources. Security Policy Rules are not defined for SecuRemote.

Answer: A

QUESTION 12:

Exhibit



Jacob configured a meshed VPN Community, with VPN properties set as shown below. Which of the following statements are TRUE? (Choose two)

- A. Jacob is using the default VPN property settings for a VPN-1/FireWall-1 meshed VPN Community.
- B. Jacob's community will perform IKE Phase 1 key-exchange encryption, using the longest key VPN-1/FireWall-1 supports.
- C. Jacob must change the data-integrity settings for this VPN Community. MD5 is incompatible with AES.
- D. If Jacob changes the setting Perform IPsec data encryption with: from AES-128 to 3DES, he will increase the encryption overhead.
- E. If Jacob changes the setting, Perform key exchange encryption with: from 3DES to DES, he will enhance the VPN Community's security and reduce encryption overhead.

Answer: A, B

Note: Uncertainty due to missing exhibit. B, D also possible.

QUESTION 13:

Which of the following statements BEST explains the difference between VPN-1/FireWall-1 logs and alerts?

The difference between VPN-1/FireWall-1 logs and alerts is that:

- A. Log entries contain detailed information about traffic. Alerts contain only brief descriptions of problems. And links to the appropriate log entries.
- B. Log entries are recorded in SmartView Tracker, and are persistent. Alerts appear only in SmartView Status, and are not persistent.
- C. Logs are recorded sequentially, by date and time received. Alerts are arranged by priority and magnitude.
- D. Logging allows a Security Administrator to view historical connection information. Alerts are real-time and can be applied to a Security Policy's predefined tracking properties.
- E. Logs are generated for explicit rules, defined by Security Administrators in the Security Policy. Alerts are automatically generated by implicit rules, created as a result of Global Properties settings.

Answer: D

QUESTION 14:

Which of the following statements BEST describes the difference between VPN Domains and VPN Communities?

- A. A VPN Domain is a network, or group of networks, protected by an Enforcement Module. A VPN Community is a collection of VPN Domains and the VPN tunnels between them.
- B. A VPN Domain is a remote-access VPN, consisting of a group of SecureClients and their associated Enforcement Module. A VPN Community is a collection of Enforcement Module-to-Enforcement Module VPNs.
- C. VPN Domains are used in Microsoft environments, and allow VPN-1/FireWall-1 to communicate with Domain Controllers. VPN Communities are used in Unix environments, to allow VPN-1/FireWall-1 to communicate with authentication servers.
- D. VPN Domains specify encryption properties and access restrictions for users. VPN Communities detail encryption properties and access restrictions, for machines and processes.
- E. VPN Domains are used for Security Policies created in traditional mode. VPN Communities are used in simplified mode. VPN Domains are not available, if simplified mode is used.

Answer: A

QUESTION 15:

Ken is assisting a user whose SecureClient password has expired. The SecureClient user can no longer access resources in the VPN Domain. Which of the following solutions is likely to resolve the issue?

- A. Ken must ask the VPN-1/FireWall-1 Security Administrator to change the setting Password Expires to a date in the future. Users cannot adjust their SecureClient passwords.
- B. Ken should ask the user to change his password, using the New Password option on SecureClient's Passwords menu. The user can change his password, then stop and start SecureClient.
- C. If the SecureClient password is allowed to expire, the software will no longer function. Ken should help the user uninstall and reinstall SecureClient. The user will be prompted to supply a new password during installation.
- D. When the SecureClient password expires while a session is in progress, the session will not exit properly. Ken should ask the user to shut down and restart his computer. The user will be prompted to supply a new password after login.
- E. The user must edit the userc.C file, to change the expiration date on his password. Ken should help the user make the necessary modifications to the userc.C file, using a text editor that does not insert Unicode characters.

Answer: A

QUESTION 16:

VPN-1/FireWall-1 can be configured to enable Voice over IP (VoIP) traffic in which of the following environments? (Choose two)

- A. SIP
- B. Q.931
- C. G.723
- D. DiffServ QOS
- E. H.323

Answer: A, E

Explanation:

VoIP Methods

VoIP incorporates
signaling

, compression and encoding standards. Most
users refer to the VoIP methods by the signaling standards that control them.
Two popular signaling standards are currently in use:

—
H.323

, an
International Telecommunications Union (ITU)
standard

—
Session Initiation Protocol (SIP)
, an
Internet Engineering Task Force

(IETF)
standard

Neither of these signaling standards has been exclusively adopted by the Internet community.

Visit

<http://www.itu.int/home/index.html>

for more information about H.323,

and

<ftp://ftp.isi.edu/in-notes/rfc3261.txt>

for more information about SIP.

Which should you use? That question may be moot in the near future because the protocols may be converging. H.323 v3 has addressed some of its shortcomings, which were initial advantages to using SIP. SIP seems to be addressing some of its shortcomings as well. Whether these methods converge or not, FireWall-1 currently supports both standards. In the following sections, we'll discuss each standard in more detail.

H.323

H.323 is the most popular IP telephony protocol and has been approved by the world governments as the international standard for voice, video and data conferencing. H.323 has the flexibility of sending multimedia communications over the Internet and integrating well with the PSTN.

When H.323 was developed in the mid-1990s, its creators hoped to produce a next-generation protocol. Version 1 of H.323 was developed with a focus on multimedia communications and interoperability with other multimedia protocols and services. The version 1 standard was accepted in October 1996.

The emergence of VoIP applications and IP telephony has set the guidelines for a revision of the H.323 specification. With the development of VoIP, new requirements emerged, such as providing communication between a PC-based phone and a phone on a traditional switched circuit network; but the lack of a standard for VoIP made most of the products with these requirements incompatible. Such requirements subsequently forced the need for a standard for IP telephony. Version 2 of H.323, a packet-based multimedia communications system, was defined to accommodate these additional requirements and was accepted in January 1998.

The power of H.323 lies in its extensibility, flexibility of centralized and/or decentralized control, ease of integration with Internet protocols, worldwide acceptance, and technical capability to provide voice, video, and data convergence. In today's market, H.323 is the leader in multimedia communications and carries billions of minutes of voice, video, and data conferencing traffic over IP networks every month.

SIP

Session Initiation Protocol (SIP) is the IETF protocol for IP telephony. It only supports IP-based phones. It has a smaller footprint than H.323 so it's faster and more scalable. The problem lies in the fact that it's a newer protocol, and therefore fewer products exist that use it. However, SIP addresses some of

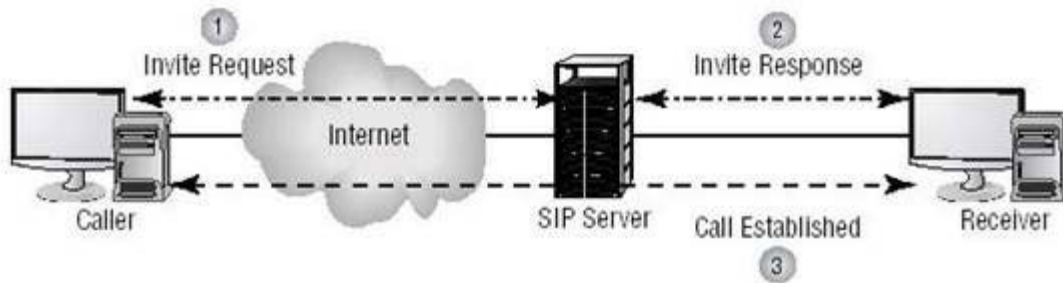
the shortcomings of H.323 by making users easier to identify, making it easier to connect two circuit-switched networks across an IP network, and decreasing the delay in call setup time.

SIP identifies users with a Hierarchical URL. This URL is based on a user's phone number or host name and looks similar to an e-mail address (for example,

SIP: joeuser@abc.com

). Figure below illustrates the SIP call process.

SIP call process



When a call is made, the caller initiates it with an invite request. This request contains the information necessary for the person you're calling to join the session: the media types and formats for the call, the destination for the media data, and perhaps requests for using H.261 video and/or G.711 audio. The invite request is sent to the user's SIP server. Because you include your available features in the invite request, the negotiation of the connection takes place in a single transaction thus call setup time is decreased (approximately 100 milliseconds).

The SIP server may or may not be a proxy server. A SIP proxy server receives the request and figures out the user's location using its internal algorithms. A non-proxy SIP server functions as a redirect server in that it sends back to the user the SIP URL that the user uses to query. In both the redirect and proxy server cases, the server's address is obtained by querying the Domain Name Service (DNS).

Once the SIP URL is found, the request finally makes it to the person you're trying to call. If the person picks up the call, the receiver's client responds to the invite request with the capabilities of its software (videoconferencing, whiteboarding, and so forth), and the connection is established.

SIP has two features that really make it unique:

— It can split an incoming call so that multiple extensions can be rung at once. When the invite request comes in, the SIP server can return to the initiator of the call a Web Interactive Voice Response (IVR) page, which contains extensions of different departments or users in a list. All you have to do is click on the link to call the appropriate person or department.

—
It can return different media types.

SIP is simple and easy to deploy because its only job is to identify the user and set up the call; it relies on other protocols and applications to manage the call. It utilizes existing DNS instead of having to create a separate database for telephony. It also interfaces with circuit-switched networks (the PSTN) more easily than H.323. Does this mean SIP is the way to go? Not necessarily. It is not widely available, and (the biggest drawback at this point) it must "de-throne" Microsoft. Every version of Windows that ships has an H.323 client as part of the package (it's free!). Whether a company will purchase another client all depends on its needs and what it wants to accomplish with IP telephony.

While H.323 is the accepted VoIP protocol today, many people think that SIP will be the VoIP protocol of the future. Most of the larger vendors are developing SIP-based solutions if they haven't already. It will be beneficial to understand both protocols to make a decision on what kind of VoIP solution to deploy

QUESTION 17:

Which of the following is NOT a feature or quality of a hash function?

- A. It is mathematically infeasible to derive the original message from the message digest.
- B. The hash function is irreversible.
- C. It is mathematically infeasible for two different messages to produce the same message digest.
- D. The hash function forms a two-way, secure communication.
- E. Encrypted with the sender's RSA private key, the hash function forms the digital signature.

Answer: D

Explanation:

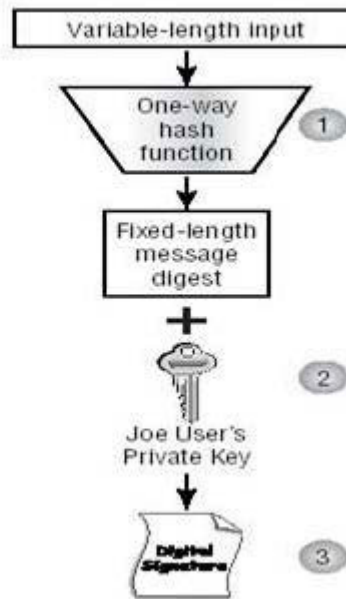
A hash is a one-way mathematical function that operates to ensure a message's integrity. It's one-way because the process is irreversible. The hash functions most routinely used are MD4, MD5, and SHA1. A one-way hash works by taking a variable-length input and putting it through a mathematical algorithm that produces a fixed-length output called a hash value or message digest

.
A one-way hash function is also known by many other names, such as contraction function, fingerprint, compression function, cryptographic checksum, message integrity check (MIC), message authentication code (MAC), and manipulation detection code (MDC).

The purpose of the one-way hash is to determine if the message you receive has changed from the original message sent. The output of the hash, or message digest, is combined with the sender's private key to generate a

digital signature as depicted in Figure below : .

One-way hash plus a private key equals a digital signature



QUESTION 18:

Which of the following is NOT a method used to configure SIP?

- A. With SIP Proxies.
- B. With a SIP Gatekeeper to a network without a proxy.
- C. From a network without a proxy to a network with a proxy.
- D. With a proxy for internal communications.
- E. Without SIP Proxies.

Answer: B

According to Check Point Management II course book > under page 119, it says that 4 listed methods are:

- (1).With Proxies
- (2).Without Proxis
- (3)From a Network without proxy to a network with Proxies
- (4).With a proxy for internal communication.

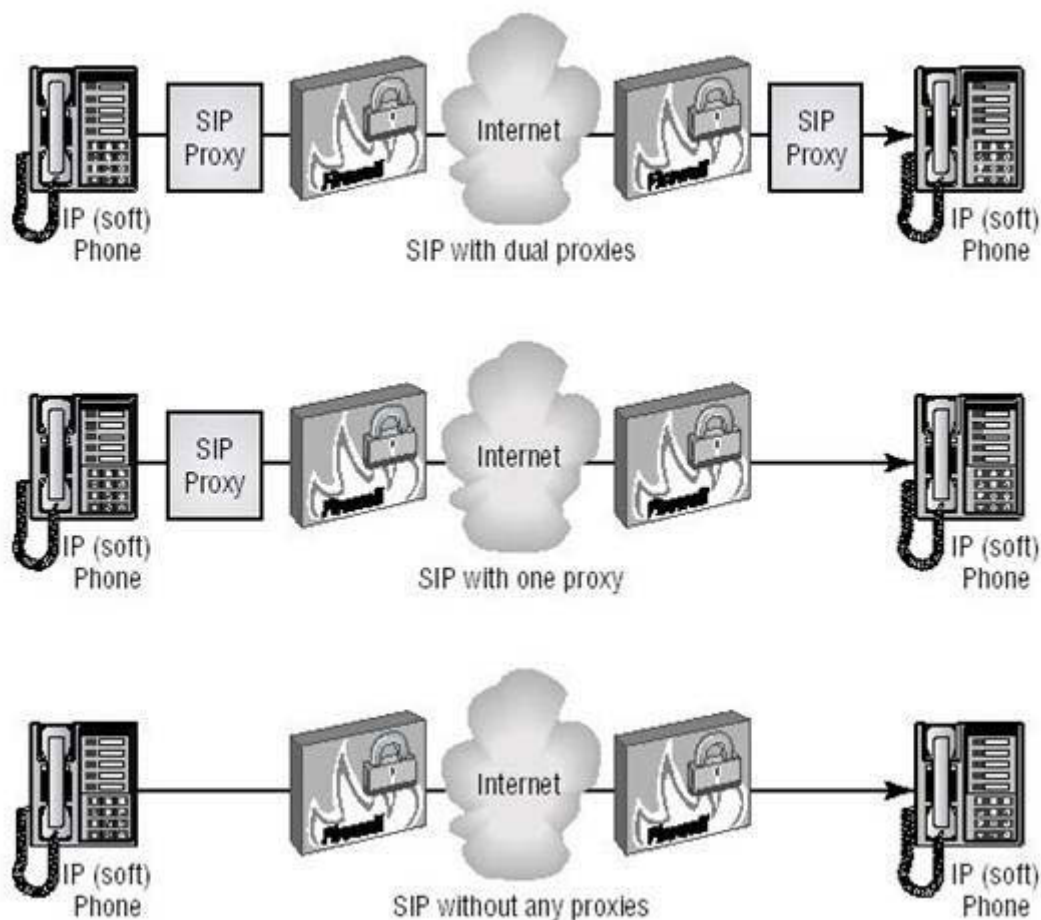
Explanation:

Configuring FireWall-1 and VoIP with SIP

There are a few different ways to configure VoIP with SIP. You can configure SIP using a SIP proxy on one or both ends of the connection, or you can use a SIP redirect server to provide DNS services to map IP addresses to SIP

URLs. You can also configure SIP without using proxies. Figure below depicts these three proxy scenarios.

Three SIP scenarios



Configuring Objects

Before configuring specific VoIP objects to the firewall, you must define Address Range or Network objects that represent the network of IP-based phones. You could also create Host Node objects to represent each phone and then put all the Host Node objects into a group. To create an Address Range object, follow these steps:

1. Go to Manage _ Network Objects and choose New _ Address Range.
2. Define the range of IP addresses that represent your IP phones, as shown in Figure below : .

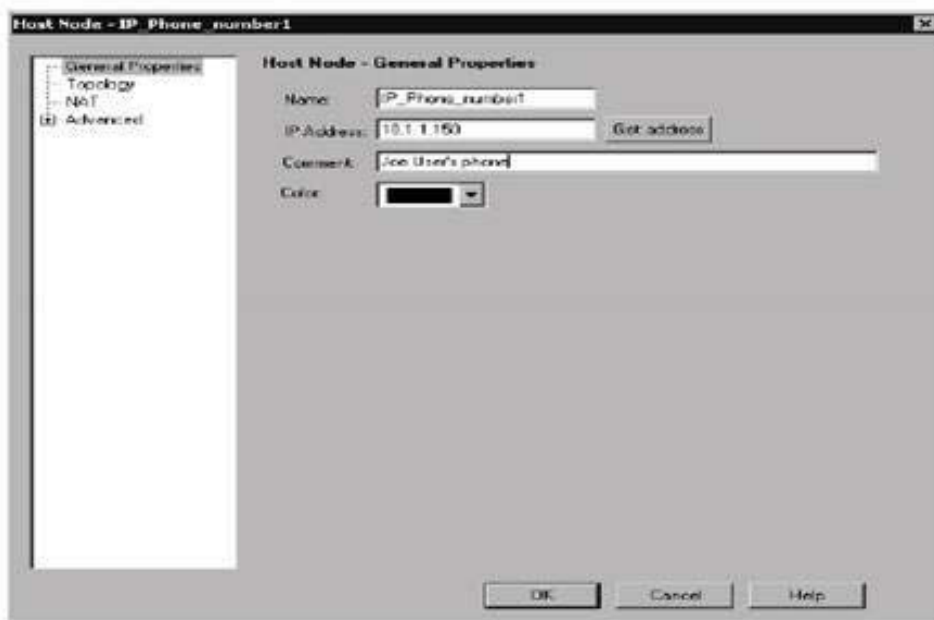
Creating an Address Range object



To create a group, follow these steps:

1. Go to Manage _ Network Objects and choose New _ Node _ Host.
2. Define an object to represent each individual phone, as depicted in Figure below :

Creating a Host Node object creation



3. Go to New _ Group _ Simple Group and define the group name.

4. Select the Host Node objects you created and move them into the In Group column, as shown in Figure below :

IP_Phone_Group object



5. At this point, if you're using a SIP proxy or a SIP redirect server, you must configure a VoIP Domain SIP object by going to Manage _ Network Objects and clicking New _ VoIP Domains _ VoIP Domain SIP. This step is demonstrated in Figure below. (We gave the object a name and then pulled the previously defined Address Range object into the Related Endpoints Domain pull-down menu. Alternatively, we could have pulled in the group object.)

SIP Domain object



6. Pull in the host node object that represents the SIP proxy.

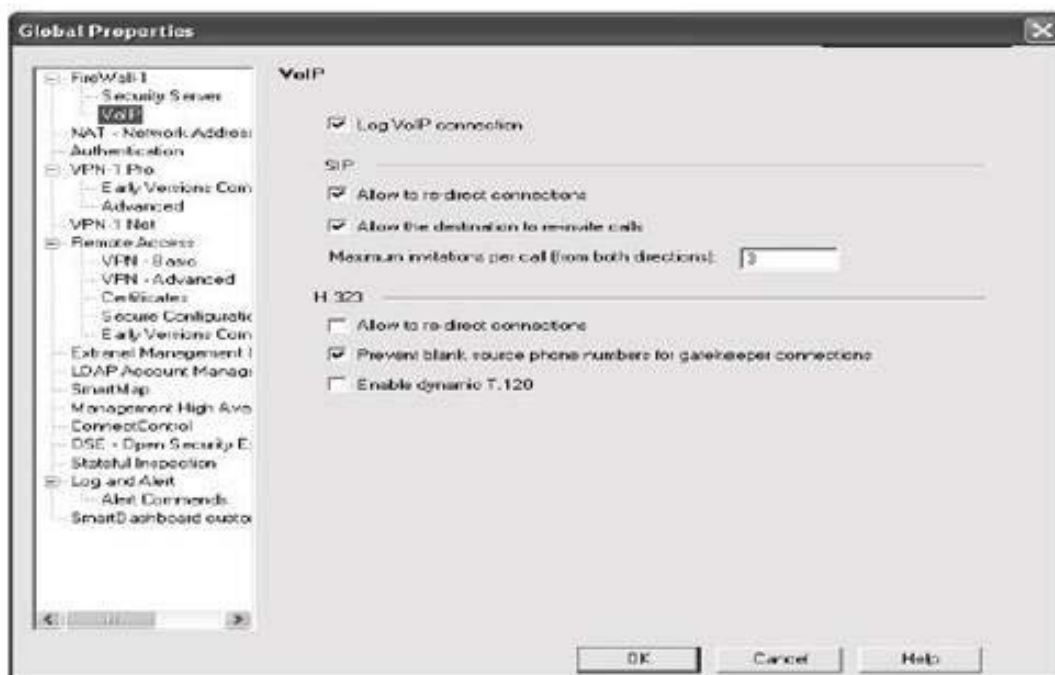
VoIP Global Properties exist as well and should be configured. Figure 5.12 shows the VoIP Global Properties options:

Allow To Re-direct Connections This option must be selected if either a SIP re-direct or proxy server is being utilized. Turn this option off only if no proxies or redirect servers are involved.

Allow The Destination To Re-Invite Calls If this option is turned on, users can take advantage of SIPs ability to initiate a new call while a call is already in progress.

Maximum Invitations Per Call (From Both Directions) This option is related to the previous one: It quantifies the maximum number of additional calls that can be placed while the initial call is still in progress.

VoIP Global Properties



Configuring the Rule Base

Creating the objects is the easy part. The tough part is creating the rules because so many different scenarios can come into play.

If the scenario does not include any proxies, you need only one rule. Figure 5.13 shows that the Source and Destination columns must include your SIP network range and the SIP network range you wish to communicate with.

SIP rule base with no proxies



Note that the Service column is populated with the SIP UDP service. For any of the SIP rules, you can select the sip service or the sip_any service. The differences between these two services are described in Table below

Explanation of sip and sip_any Services

Service	How It Works
sip	If the Source or Destination column is Any, then the firewall is not able to redirect the connection unless the gateway is configured as a SIP proxy.
sip_any	If the Source or Destination column is Any, the firewall is able to redirect the connection even if it isn't a SIP proxy, but <i>only</i> if the SIP Domain is external to the network protected by the firewall.

If the scenario includes a proxy on only one side of the connection, then a rule is needed to allow communication from the VoIP Domain SIP object (the SIP proxy), to the network object, IP address range, or destination as shown in Figure below

SIP rule base with one proxy



If the scenario includes proxies on both sides of the connection, then a rule is needed to allow the SIP proxies to communicate as shown in Figure below.

SIP rule base with two proxies



After determining what rules are needed for your scenario and configuring your rule base, all that is required is to verify and install your policy and start talking.

QUESTION 19:

You are importing a URI specification file from the Match tab on the URI Resource Properties screen. Where is the editable URI specification file stored?

- A. Policy Server
- B. SmartView Monitor
- C. Enforcement Module
- D. SmartCenter Server
- E. Enterprise Log Module

Answer: D

QUESTION 20:

You are using Hybrid IKE for Client Authentication. SecureClient produces the error Certification is badly signed. Which of the following is the MOST likely cause of the problem and the appropriate solution?

- A. Under the firewall object > VPN > IKE Properties > Support Authentication Methods, Hybrid Mode is not selected. Select the Hybrid Mode option, and stop and restart the Enforcement Module.
- B. The Distinguished Name used is too long. Change it to a shorter name in the Manage Certificate Properties screen.
- C. The certificate created by the Internal Certificate Authority (ICA) is corrupt. Create a new certificate.

- D. The SecureClient and VPN-1/FireWall-1 Enforcement Module to which it is attempting to connect are running incompatible versions. Upgrade the SecureClient to NG with Application Intelligence.
- E. The digital signature is missing. Add the digital signature to the certificate in the Manage Certificate Properties screen.

Answer: A

QUESTION 21:

Ann would like to deploy H.323 with a gatekeeper and gateway on her internal network. This network is behind a VPN-1/FireWall-1 Enforcement Module. Which of the following objects is NOT required to configure VPN-1/FireWall-1 for H.323 in this scenario?

- A. Address Range representing internal IP-addressed phones
- B. Gatekeeper Node Object
- C. Address range of external IP-addressed phones
- D. Voice over IP (VoIP) Gateway Node Object
- E. Voice over IP (VoIP) Domain Object

Answer: C

Explanation:

Configuring FireWall-1 and VoIP with H.323

Analog (conventional) telephones and digital (soft) telephones can be used in conjunction with a H.323-based VoIP solution. Conventional phones do not have IP addresses but can be connected to a H.323 gateway which converts the analog signal to digital so that it can participate in VoIP. Digital phones can be either a physical telephone that has an IP address or a computer with the appropriate software that enables it to act as a telephone. Both of these configurations are referred to as "soft phones."

The IP addresses of the gateway (if necessary) and the soft phones should be their own subnet along with the H.323 gatekeeper computer.

The gatekeeper H.323 component is the focal point for all calls within a VoIP network. It provides important services such as addressing, authorization, and authentication for the gateway and the IP phones behind it. The gatekeeper can also provide bandwidth management, accounting, billing, charging, and call-routing services.

The first step in configuring the firewall to inspect VoIP traffic is to define host node and/or network objects that represent the IP phones, the gateway computer (optional) and the gatekeeper computer. The gatekeeper and the gateway should be created as host objects. Each IP phone can be a host node object as well or you could create a network object that represents the IP address range of your VoIP network. The only portion of the H.323 architecture in which you do not have to create objects is the analog phones. Since they

don't have IP addresses, they are represented by the gateway object. If you do not have analog phones then you have no need to create a gateway object.

Creating the Gateway

If you have analog phones in your VoIP network you must create a VoIP Domain H.323 Gateway object as outlined in the following steps:

1. Go to Manage _

Network Objects and choose New _

VoIP Domains _

VoIP Domain H.323 Gateway.

2. In the General tab, define the gateway's Name, Comment, and Color.

Choose the network object that represents the IP addresses of your VoIP subnet in the Related Endpoints Domain pull-down menu. Keep in mind that if different H.323 protocols are carried on different interfaces, then a separate host node object has to be created to represent each interface. These host node objects should then be grouped together and defined in the VoIP Installed field. If there is a single interface carrying the protocols that make up H.323 then only one host node object (which represents the H.323 gateway) should be defined in the VoIP Installed At field.

Gatekeeper General Properties



3. In the Routing Mode tab, you'll see two options: the Call Setup and Call Setup And Call Control. Call Setup (Q.931) handles the setup and termination of the calls whereas Call Setup And Call Control does that as well as negotiating the parameters necessary for multimedia. At

least one of the choices must be checked, depending on the VoIP product that you are using.

Most people are not familiar with the H.323 protocol but have experienced using it if they've ever used Microsoft's NetMeeting product.

Creating the Gatekeeper

The gatekeeper object must be created to securely pass H.323 traffic through your firewall. To create a gatekeeper object, follow these steps:

1.

Go to Manage _

Network Objects Go to the Network Objects window

and choose New _

VoIP Domains _

VoIP Domain H.323 Gatekeeper.

2. In the General tab, shown in Figure below, define the gatekeeper's Name, Comment, and Color. The network object or address range object that represents your soft phones subnet and/or the object that represents your gateway (if you're using analog phones) should be defined in the Related Endpoints Domain field. If you are using a combination of analog and digital phones then combine the gateway and the network range in a Simple Group and define it here. The host node object that represents your H.323 gatekeeper machine should be defined in the VoIP Installed At field.

3. Under the Routing Mode tab of the gatekeeper properties, you can choose from three allowed routing modes. This option identifies which connections will be rerouted from your VoIP gatekeeper to the VoIP gatekeeper on the other end. At least one of the following choices must be checked depending on the VoIP equipment that is being utilized:

Direct The H.225 and Q.931 protocols, which allow gatekeeper to gatekeeper communication and call setup and breakdown respectively, are rerouted if this check box is selected.

Call Setup (Q.931) H.245 which is the control protocol used by H.323 for multimedia communication will be rerouted from gatekeeper to gatekeeper along with the Q.931 protocols.

Call Setup (Q.931) and Call Control (H.245) Connections that deal with video, audio and controls connections associated with video and audio will be rerouted gatekeeper to gatekeeper.

VoIP is a large set of protocols that are not easily understood. A good resource to learn more about VoIP is <http://www.voip-calculator.com/>.

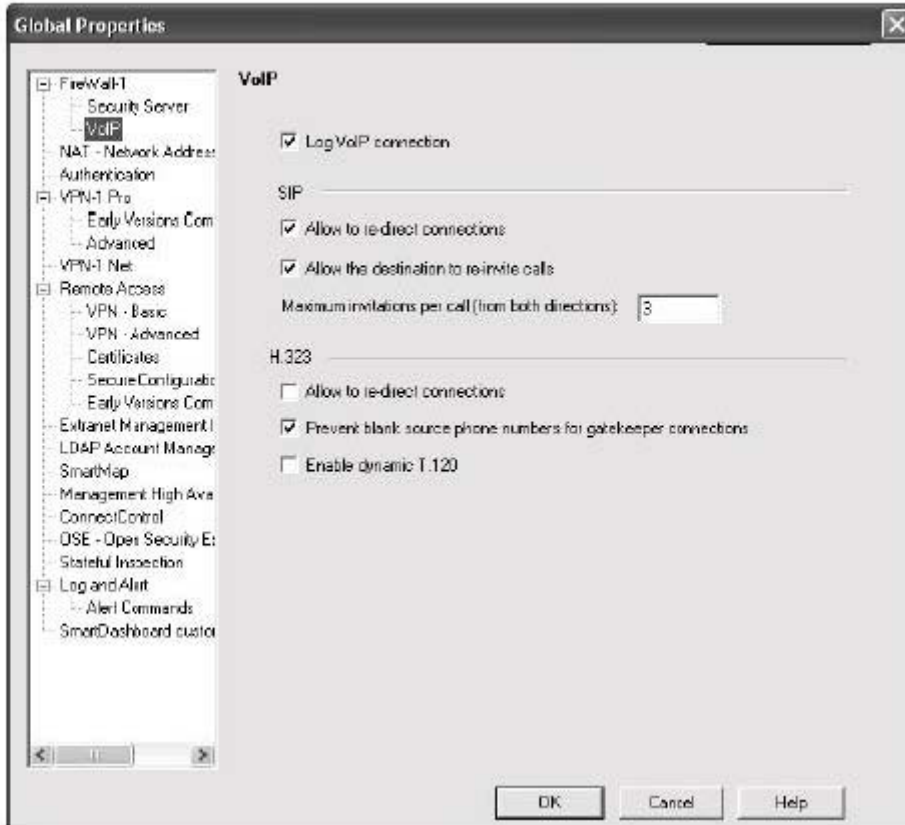
Configuring Global Properties

In the VoIP page of the Global Properties window, shown in Figure below, you can change the VoIP parameters from their default settings. If the Log VoIP Connection option is checked, every VoIP (SIP and H.323) connection will be logged including the telephone number information. Under the H.323 section, Allow to Re-direct Connections is a H.323 function that allows call

forwarding and call waiting to occur. Disallow Blank Source Phone Numbers

is what we commonly know as blocking CallerID. Enable Dynamic T.120 enables the T.120 protocol which most recognize as the whiteboarding feature of NetMeeting.

VoIP Global Properties



Configuring the Rule Base

Now that you have created your network objects and configured your VoIP global parameters, it's time to configure the rule base to filter H.323 traffic. The concept in creating the rule is to allow traffic to pass from gatekeeper to gatekeeper or from gateway to gateway using the H.323 service. You have more than one H.323 service to choose from: H.323_any provides all the required services for VoIP, and H.323_ras includes only the RAS part of the H.323 protocol. If you wish to use more than just H.323_ras then you will have to define additional services for this rule or create additional rules to allow the other protocols (e.g. T.120 or H.450) necessary for the call to be completed.

For our purposes in this book, Figure below displays a good example of an H.323 VoIP rule. The gatekeepers of Detroit and Madrid are listed in both the Source and Destination columns of the rule. The Service is H.323_any, and the Action is Accept.

H.323 VoIP rule

NO.	SOURCE	DESTINATION	SERVICE	ACTION
1	 Detroit-Gatekeeper  Madrid_VoIP_GW	 Detroit-Gatekeeper  Madrid_VoIP_GW	 H323_any	 accept

You now have an understanding of how to configure the firewall for H.323-based VoIP systems. Now look at the next section where you will learn how to configure SIP-based VoIP systems.

QUESTION 22:

If you are using SIP or SIP_ANY, and the Source or Destination is Any, which of the following statements are TRUE concerning SIP Services? (Choose two)

If the Service is:

- A. SIP_Any, and the Source is Any, the object represented by Any (internal or external) is SIP Proxy.
- B. SIP_Any, and the Destination is Any, the object represented by Any (external only) is not a SIP Proxy.
- C. SIP, and the Source is Any, the object represented by Any is allowed to redirect the connection, unless it is a SIP Proxy.
- D. SIP, and the Destination is ANY, the object represented by Any is allowed to redirect the connection, so it must be a SIP Proxy.
- E. SIP_Any, and the Source or Destination is Any, the object represented by Any (internal or external) is always a SIP Proxy.

Answer: B, C

According to Check Point Mgmt II, page 121, it says this.

Service = SIP

Description= If Source or Destination is Any, the object represented by Any is not allowed to redirect a connection, unless it is a SIP proxy
 Service = SIP_ANY Description= If Source or Destination is Any, the object represented by Any is not a SIP proxy(This is only true, if the object is external to a network protected by an Enforcement Module).

QUESTION 23:

Vered is a Security Administrator preparing to migrate her organization's IKE VPNs from pre-shared secrets to PKI with certificates. Vered's organization has client-to-site VPNs between SecureClients and Enforcement Modules, and site-to-site VPNs between Enforcement Modules. Vered will use the

VPN-1/FireWall-1 Internal Certificate Authority (ICA), to generate and maintain certificates. Which of the following statements is TRUE?

Vered can:

- A. Install and configure an OPSEC-certified Certificate Authority product. Vered cannot use the Internal Certificate Authority (ICA) to accomplish this task.
- B. Migrate the organization's site-to-site VPNs, but she cannot migrate the organization's client-to-site VPNs.
- C. Either migrate the PKI with certificates for her VPNs, or use the ICA for certificate generation and maintenance. Vered cannot do both.
- D. Migrate both the site-to-site VPNs and the client-to-site VPNs. She can use the ICA to generate and maintain certificates.
- E. Migrate the organization's client-to-site VPNs, if she moves from SecureClient to SecuRemote. She cannot migrate the site-to-site VPNs.

Answer: D

QUESTION 24:

Mark is preparing to install VPN-1/FireWall-1 and has created the installation plan below.

1. Perform the following operations below in sequential order.
2. Install the operating system.
3. Configure routing and IP forwarding.
4. Configure name resolution.
5. Patch the operating system.
6. Set \$FWDIR and \$CPDIR environment variables.
7. Install VPN-1/FireWall-1.
8. Patch VPN-1/FireWall-1,

Which step in Mark's installation plan is NOT necessary?

- A. Operating-system patches should not be applied, until after VPN-1/FireWall-1 is installed. Applying operating-system patches before VPN-1/FireWall-1 is installed will result in an unsecured system.
- B. VPN-1/FireWall-1 configures name resolution automatically. Name resolution should not be part of the installation plan.
- C. There is nothing wrong with Mark's installation plan.
- D. Routing and IP Forwarding should be configured after VPN-1/FireWall-1 is installed. Configuring routing and IP forwarding before VPN-1/FireWall-1 is installed will result in an unstable system.
- E. VPN-1/FireWall-1 configures environment variables automatically. Configure environment variables should not be part of the installation plan.

Answer: E

QUESTION 25:

Diffie-Hellman uses which type of key exchange?

- A. Static
- B. Dynamic
- C. Symmetric
- D. Asymmetric
- E. Adaptive

Answer: D

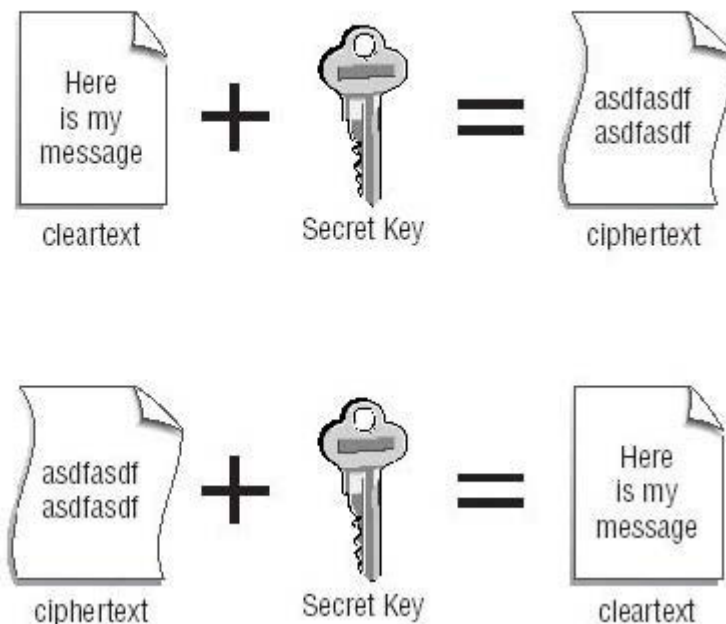
Explanation:

Symmetric Encryption

Symmetric encryption

is best described graphically, as shown in Figure below

Symmetric encryption



The original message shown in Figure 6.1 is referred to as being in cleartext

because it's readable. When this original message is combined with the secret key the result is the encrypted message (referred to as ciphertext

). The message

can only be decrypted by someone who holds the same secret key. When the process is reversed, the encrypted message together with the secret key will produce the original cleartext message.

The process is relatively simple and very quick, but it has some drawbacks; the most basic is that the same key used to encrypt is also used to

decrypt. The secret key must be created and then securely delivered to the person with whom you want to share encrypted messages. The safest way is to put it on a floppy disk and physically carry it to the person, but it is not always possible to do so. It's not secure to send this key via e-mail, because anyone could intercept it and read all of your encrypted messages. Even if you're able to physically get the key to the person, it is good security practice to change the key on a regular basis. When you're exchanging messages with one person, this is not a big deal-but with multiple people, it would be a daunting task. With symmetric encryption you should have a separate key for each person with whom you want to share encrypted information. If you used the same key for everyone, then everyone would be able to read all the messages sent. So you need to generate one key for every person with whom you wish to encrypt. As the number of keys grows, key management becomes an issue.

We're not saying that symmetric encryption doesn't have a place in a VPN. However, you'll have to address the problem of key management. This leads us to asymmetric encryption.

Asymmetric Encryption

Asymmetric encryption

uses two keys for encrypting/decrypting data. This is also referred to as public/private key encryption. Figure below depicts asymmetric encryption.

Asymmetric encryption



The public/private key pair is generated by the person who wants to encrypt. The private key is secured by the generator of the keys, and the public key is handed out freely to whoever wants to share encrypted information with the generator of the keys (the Pretty Good Privacy [PGP] program originally

worked this way). The person who wishes to encrypt a message gets a copy of the public key and encrypts the message with it. Only the holder of the private key will be able to decrypt the message.

The public key is mathematically related to the private key; it is impossible to reverse-engineer the public key to get the value of the private key. For more details about the mathematics involved in encryption, see

Applied Cryptography

by Bruce Schneier (John Wiley & Sons, 1995).

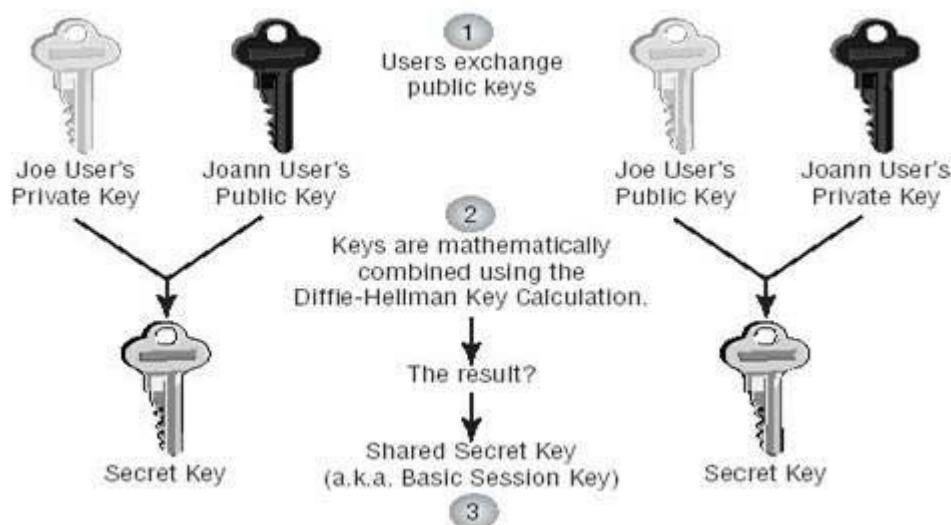
As is true for symmetric encryption, the keys should be regenerated on a regular basis or any time you think they have been compromised. Although asymmetric encryption reduces number of keys that must be managed, as an encryption process it is 1,000 times slower than symmetric encryption. What we need is a methodology that combines the assets of asymmetric and symmetric encryption. That's where the Diffie-Hellman key exchange method comes into play.

Diffie-Hellman Key Exchange Mechanism

The Diffie-Hellman

key exchange uses the public/private key pair to generate a secret key. This process is illustrated in Figure below.

Diffie-Hellman key exchange



In step 1, users exchange public keys. When you're using asymmetric encryption, the exchange of public keys is all that is required to begin encrypting. But Diffie-Hellman combines asymmetric and symmetric processes. Each user's private key is combined with their encrypting partners' public key using the Diffie-Hellman key calculation, as shown in step 2. As we stated earlier, the public and private keys that each user creates are mathematically related; that's how the users can exchange keys, apply the Diffie-Hellman key calculation, and both end up (in step 3) with mathematically identical keys.

Different mathematical groups can be used to generate the identical keys. The Diffie-Hellman standard supports three groups: DH groups 1, 2, and 5. The larger the group number, the larger the prime number used to generate the key pair. The larger groups are more secure but require more CPU cycles to generate the keys. Check Point also gives you the ability to expand the database of groups by adding custom groups.

The process depicted in Figure above solves two problems. First, you have generated the secret key necessary to perform symmetric encryption without having to physically exchange the secret key with your encrypting partner. Second, you can use that key to symmetrically encrypt data much more quickly than you can using asymmetric encryption alone. The best aspects of both encryption techniques are combined to yield a process that's better than each individual technique. The encryption processes we've described fill out the P in PAIN, but they are useless unless you get the correct key from your encrypting partner. The next section addresses how to verify that the key is from the correct source and explains the AIN in PAIN.

QUESTION 26:

If the Use Aggressive Mode check box in the IKE Properties dialogue box is enabled:

- A. The standard six-packet IKE Phase 1 exchange is replaced by a three-packet exchange.
- B. The standard three-packet IKE Phase 2 exchange is replaced by a six-packet exchange.
- C. The standard three-packet IKE Phase 1 exchange is replaced by a six-packet exchange.
- D. The standard six-packet IKE Phase 2 exchange is replaced by a three-packet exchange.
- E. The standard three-packet IKE Phase 3 exchange is replaced by a six-packet exchange.

Answer: A

Explanation:

ISAKMP Phase 1: SA Negotiation

In Phase 1 of the SA negotiation, the firewalls involved in the VPN negotiate an SA that is used to encrypt and authenticate Phase 2 exchanges. Phase 1 is a CPU-intensive process, and by default VPN-1 performs it only once every 1,440 minutes (24 hours). VPN-1 supports two modes for Phase 1: aggressive mode, which exchanges three packets; and main mode (the default mode in NG), in which six packets are exchanged. The three-packet difference is due to a cookie exchange that precedes the actual SA negotiation. The cookie exchange identifies the parties involved in the VPN, thus preventing

man-in-the-middle

attacks (to which the Diffie-Hellman key exchange is vulnerable). The SA that is negotiated includes the keys, authentication, and encryption methods.

Phase 1 negotiates the following:

- _ The encryption algorithm (the choices are DES, 3DES, AES, and CAST)
- _ The hash algorithm (the choices are MD5 or SHA1)
- _ The Diffie-Hellman group (the choices are Group 1, 2, or 5). The addition of DH group choices in NG increases the likelihood that a VPN tunnel can be established with non-Check Point firewalls.

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange. The strength of any key derived depends in part on the strength of the Diffie-Hellman group on which the prime numbers are based. The larger the group, the stronger the key-but, conversely, the more CPU-intensive the computation.

The second step in Phase 1 is the exchange of public keys and the use of the Diffie-Hellman key calculation to generate the shared secret key. The shared secret key is used to authenticate each firewall's identity. This is accomplished by hashing and encrypting the firewall's identity with the shared secret key. If the identity of each firewall is authenticated, then we move on to Phase 2.

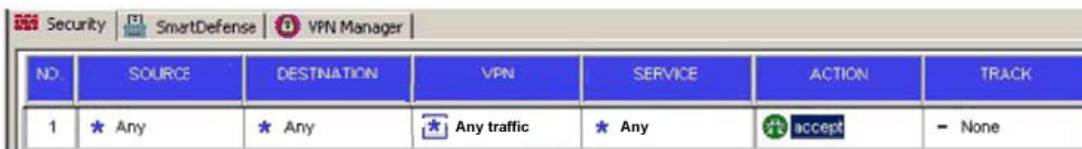
QUESTION 27:



Dr Bill is setting up a new VPN-1/FireWall-1 Enforcement Module. The Rule Base is configured to allow all traffic, and the Enforcement Module is set up as shown in the screen capture below. Dr bill cannot get the new system to pass any traffic.

What is the MOST likely cause of the problem?

System specifications:

1. Processor: 2.2 GHz
2. RAM: 256 MB
3. Hard Disk: 10 GB
4. OS: Windows 2000 Server



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	 Any traffic	* Any	 accept	- None

Results of ipconfig/all

View the following exhibit for the results of ipconfig/all.


```

Command Prompt
Results of ipconfig /all

Windows 2000 IP Configuration
Host Name . . . . . : fusingapore
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
VINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 2:
Description . . . . . : 3Com EtherLink 10/100 PCI
Physical Address. . . . . : 00-01-03-C4-3C-4E

Ethernet adapter Local Area Connection 2:
Connection: Primary DNS Suffix . . .
Description . . . . . : 3Com EtherLink 10/100 PCI #2
Physical Address. . . . . : 00-01-03-C4-3C-41
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.10.10.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.102
DNS Servers . . . . . : 172.0.0.253

```

- A. Routing is not properly configured.
- B. The machine does not have enough RAM.
- C. The processor is not fast enough.
- D. The operating system is not supported.
- E. The Rule Base is blocking traffic.

Answer: A

QUESTION 28:

Which of the following encryption algorithms supports a key length from 128-bits to 256-bits and is outlined in the new Federal Information Processing Standard publication?

- A. AES (Ridndael)
- B. CAST Cipher
- C. 3DES
- D. DES
- E. Blowfish

Answer: A

QUESTION 29:

Static passwords such as VPN-1 & FirwWall-1 and operating system passwords are cached on the desktop and users are not required to re-authenticate. Which of the following does NOT clear the password cache?

- A. Receives a policy update.
- B. Perform a disconnect from a connect mode.
- C. Selects the Stop VPN 1 SecuRemote option from the File menu.
- D. Selects the Erase Passwords option from the Passwords menu.
- E. Reboots the computer.

Answer: A

QUESTION 30:

Ann is a VPN-1/FireWall-1 Security Administrator. Her organization's solution for remote-access security is SecureClient. Ann's organization is undergoing a security audit. The auditor is concerned, because static passwords, such as VPN-1 & FireWall-1 and operating system passwords are cached on the desktop, and users are not required to re-authenticate. Which of the following explanations addresses the auditor's concerns?

- A. The auditor has incorrect information. SecureClient caches all passwords. A strong encryption algorithm protects the proprietary database used for password caching, so there is never a need to purge cached passwords.
- B. The auditor has incorrect information. SecureClient never cached passwords. SecureClient users are forced to re-authenticate for each new connection, regardless of the type of password used.
- C. Cached passwords are purged when SecureClient receives Policy and Topology updates. Most installation update Security Policies frequently, so cached passwords are rarely stored for longer than six to eight hours. Renaming the userc.C file to userc.old will also purge the password cache.
- D. Cached passwords are purged at an interval specified in the Desktop Security Policy. As long as the user.C file is encrypted, users cannot tamper with the interval setting. The interval time is in seconds from the time to SecureClient software is launched.
- E. Cached passwords are purged when SecureClient is stopped, when a connect mode is disconnected, and when the computer is rebooted. SecureClient users can manually purge the cache, by choosing the Erase Passwords option from the Passwords menu.

Answer: E

QUESTION 31:

You are preparing to deploy a new VPN-1/FireWall-1 Enforcement Module. You have five systems to choose from for your new Enforcement Module and you must meet the following requirements:

1. Comply with the operating system vendor's license agreement.
2. Comply with Check Point's license agreement.
3. Install the Enforcement Module on a supported operating system.
4. Meet minimum hardware specifications for the operating system.
5. Meet minimum hardware specifications for the VPN-1/FireWall-1 Enforcement Module.

Based on the above specifications, which of the following systems is the BEST choice?

A. Machine D Configuration

Processor: 2.0 GHz RAM: 512 MB, Hard Disk: 10 GB, OS: Windows ME

B. Machine A Configuration

Processor: 1.1 GHz, RAM: 512 MB, Hard Disk: 10 GB, OS: Windows 2000 Workstation

C. Machine B Configuration

Processor: 1.67 GHz, RAM: 128 MB, Hard Disk: 5 GB, OS: FreeBSD

D. Machine E Configuration

Processor: 2.2 GHz, RAM: 256 MB, Hard Disk: 20 GB, OS: Windows 2000 Server

E. Machine C Configuration

Processor: 1.5 GHz, RAM: 256 MB, Hard Disk: 20 GB, OS: Red Hat Linux 8.0

Answer: D

Explanation

Minimum System Requirement

Module	Operating Systems	Disk Space	Memory	Supported NICs
SmartDashboard Management GUI	Windows 98, Me, NT SP4, NT SP5, NT SP6, 2000, XP; Sun Solaris SPARC	40MB	128MB recommended	Ethernet, Fast Ethernet, GigabitEthernet, ATM, FDDI, Token Ring
SmartCenter Management Server and enforcement point	Windows NT Server SP6a; Windows 2000 Server and Advanced Server; Sun Solaris 2.7 with patch 106327-08 (2.7 supports 32-bit mode only); Solaris 2.8 with patches 108434-01 and 108435-01 (2.8 supports 32- and 64-bit mode); Red Hat Linux 6.2, 7.0, 7.1, 7.2	40MB	128MB recommended	Ethernet, Fast Ethernet, GigabitEthernet, ATM, FDDI, Token Ring

QUESTION 32:

Which of the following actions should be taken before deploying VPN-1/FireWall-1 in a production role? (Choose three)

- A. Edit the ARP table for NAT.
- B. Disable all network services.
- C. Install and patch operating system(s).
- D. Obtain licenses.
- E. Configure routing.

Answer: C, D, E

QUESTION 33:

Dr Bill is a Security Administrator whose organization maintains several IKE VPNs. Executives in Dr bill's organization want to know which mechanism VPN-1/FireWall-1 uses to guarantee the authenticity of messages. Which technology should Dr Bill explain to the executives?

- A. Application Intelligence
- B. Certificate Revocation Lists
- C. Digital Signatures
- D. Hybrid Mode Authentication
- E. Key Exchange Protocols

Answer: C

QUESTION 34:

Determine the appropriate routing mode for a Voice over IP (VoIP) Domain Gatekeeper object that supports Q.931 and H.245.

- A. Call Setup and Call Control
- B. Direct
- C. Call Proxy and Call Control
- D. Direct and Call Control
- E. Call Setup

Answer: A

Explanation:

Creating the Gatekeeper

The gatekeeper object must be created to securely pass H.323 traffic through your firewall. To create a gatekeeper object, follow these steps:

1.
Go to Manage _

Network Objects Go to the Network Objects window and choose New _

VoIP Domains _

VoIP Domain H.323 Gatekeeper.

2. In the General tab, shown in Figure below, define the gatekeeper's Name, Comment, and Color. The network object or address range object that represents your soft phones subnet and/or the object that represents your gateway (if you're using analog phones) should be defined in the Related Endpoints Domain field. If you are using a combination of analog and digital phones then combine the gateway and the network range in a Simple Group and define it here. The host node object that represents your H.323 gatekeeper machine should be defined in the VoIP Installed At field.

Gatekeeper General Properties



3. Under the Routing Mode tab of the gatekeeper properties, you can choose from three allowed routing modes. This option identifies which connections will be rerouted from your VoIP gatekeeper to the VoIP gatekeeper on the other end. At least one of the following choices must be checked depending on the VoIP equipment that is being utilized: Direct The H.225 and Q.931 protocols, which allow gatekeeper to gatekeeper communication and call setup and breakdown respectively, are rerouted if this check box is selected.

Call Setup (Q.931) H.245 which is the control protocol used by H.323 for multimedia communication will be rerouted from gatekeeper to gatekeeper along with the Q.931 protocols.

Call Setup (Q.931) and Call Control (H.245) Connections that deal with video, audio and controls connections associated with video and audio will be rerouted gatekeeper to gatekeeper.

QUESTION 35:

Dr bill is assisting a SecureClient user, who cannot access resources in the VPN Domain. Dr bill has performed the following troubleshooting tasks.

1. Confirmed that the Network Interface Card, Ethernet cable, and router port are all functioning properly.
2. Reviewed the contents of the SecureClient machine's Address Resolution Protocol table, and confirmed entries are consistent with the machine addresses of other machines in the collision domain.
3. Used Ping, to confirm connectivity with the default gateway and upstream router.
4. Completed an FTP session to an Internet host.
5. Tried to Telnet to a host in the VPN Domain, this attempt failed.

Dr bill concluded the problem is a SecureClient problem, and not a TCP/IP connectivity issue. Which of the following statements is TRUE of Dr bill's testing and conclusion?

- A. Dr bill's tests and conclusion are valid. Because SecureClient operates between the Presentation and Application Layers of the OSI model, the user's inability to access resources is a SecureClient problem.
- B. Dr bill's methodology is sound, but his tests are insufficient to determine whether or not the problem is with SecureClient. A TCP/IP problem may exist between the upstream router and target Enforcement Module.
- C. Dr bill's methodology is valid, and his conclusion is correct. Because Dr bill has tested all seven layers of the OSI Model on the SecureClient machine, the problem must be malfunctioning SecureClient software.
- D. Dr bill's methodology is flawed. Client-side testing yields no useful information when troubleshooting SecureClient issues. Eric should have initiated all tests from the Enforcement Module.
- E. Dr bill's tests and conclusion are invalid. SecureClient operates between the Presentation and Session Layers of the OSI Model, and Dr bill only tested up to the Transport Layer.

Answer: B

QUESTION 36:

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following should you do first?

- A. A shared secret must be exchanged, before certificates can be imported.
- B. A new server object must be created, to represent your partner's Certificate Authority (CA).
- C. Your partner's Certificate Revocation List must be imported manually.
- D. A new logical-server object must be created, to represent your partner's CA.

E. Your partner's Access Control List must be imported manually.

Answer: D

QUESTION 37:

How does load balancing allow several servers to share and distribute the network load in the VPN-1/FireWall-1 software?

- A. Priority routing pools are created to distribute traffic among a group of physical servers.
- B. A logical server is created on the Enforcement Module.
- C. A logical server is deployed on the SmartCenter Server.
- D. Network subnets are created to represent a group of physical servers.
- E. All traffic bound for a specific physical server is directed to a resource that proxies each connection based on a defined server object.

Answer: B

QUESTION 38:

In gateway-to-gateway encryption, gateways identify themselves by presenting their credentials. Which of the following are credentials supported by VPN-1/FireWall-1 for a gateway-to-gateway encryption? (Choose two)

- A. Certificates
- B. Cookies
- C. Tokens
- D. Pre-shared secret
- E. Tags

Answer: A, D

QUESTION 39:

Dr bill is a Security Administrator preparing to implement a VPN solution for his multisite organization. To comply with industry regulations, Dr bill's VPN solution must meet the following requirements:

1. Portability: Standard
2. Key Management: Automatic, External PKI
3. Session Keys: Changed at configured times during a connection's lifetime
4. Key Length: No less than 128 bit

5. Data Integrity: Secure against brute force and inversion attacks

Which Check Point VPN-1/FireWall-1 VPN solution meets the requirements?

- A. IKE VPNs_ AES encryption for IKE Phase 1, AES encryption for Phase 2; SHA1 hash
- B. IKE VPNs: DES encryption for IKE Phase 1, 3DES encryption for Phase 2; MD5 hash
- C. IKE VPNs: AES encryption for IKE Phase 1, DES encryption for Phase 2; SHA1 hash
- D. IKE VPNs: CAST encryption for IKE Phase 1. SHA1 encryption for Phase 2: DES hash
- E. IKE VPNs: SHA1 encryption for IKE Phase 1, MD5 encryption for Phase 2; AES hash

Answer: A

Explanation:

Encryption Standards Support by IKE and VPN-1

Algorithm	Description
DES	Data Encryption Standard (standard in the U.S. for the last 20 years). A symmetric key encryption method that uses 56-bit keys.
Triple DES	A variation on DES that addresses the problem of short, easily breakable keys. Encrypts with three different DES keys in succession, which increases the effective key strength to 168 bits.
Algorithm	Description
CAST	Named for its inventors, Carlisle Adams and Stafford Tavares. Similar to DES and supports variable key lengths from 40–128 bits.
AES	Advanced Encryption Standard. The new Federal Information Processing Standard (FIPS) standard. Also known as Rijndael (pronounced “rhine-doll”) for its inventors, Vincent Rihmen and Joan Daemen.

QUESTION 40:

Dr bill is a Security Administrator configuring SecuRemote as a remote-access solution for his company. Which of the following is NOT true?

Dr bill MUST:

- A. Obtain a SecuRemote license.
- B. Define SecuRemote connection rules in the Rule Base.
- C. Define and configure users who will be allowed access.
- D. Install SecuRemote on all remote-access clients.
- E. Implement user encryption on his network.

Answer: B

QUESTION 41:

Dr bill is troubleshooting a VPN problem. He wants to use SmartView Tracker to determine if the key exchange is successful, and if any errors are being generated. The Global Properties Log and Alert page settings for Dr bill's system uses default settings for VPN-1/FireWall-1. Will Dr bill be able to get the information he needs from SmartView Tracker?

- A. No, Dr bill will not be able to find entries in SmartView Tracker for successful VPN key exchanges. By default, only failed VPN key exchanges and VPN configuration errors are logged.
- B. No, Dr bill will not be able to find entries in SmartView Tracker for VPN configuration and key-exchange errors. By default, only successful VPN key exchanges are logged.
- C. No, Dr bill will not be able to find entries in SmartView Tracker for VPN key exchanges or VPN configuration errors. By default, these items are set to Alert, and Alerts appear in SmartView Status.
- D. Yes, Dr bill will be able to find entries in SmartView Tracker, for successful VPN key exchanges, VPN configuration and key-exchange errors. By default, these items are logged.
- E. No, Dr bill will not be able to find entries in SmartView Tracker for VPN key exchanges or VPN configuration errors. By default, VPN key exchanges and VPN configuration errors are not logged.

Answer: D

QUESTION 42:

The Certificate Authority: (Choose two)

- A. Certifies a public key by generating a certificate.

- B. Enforces preset user privileges.
- C. Is a trusted third-party from which a public key can be obtained, even via the Internet.
- D. Expires in 30 days.
- E. Stores itself on a physical device and uses an access password.

Answer: A, C

QUESTION 43:

Determine the appropriate routing mode for a Voice over IP (VoIP) Domain Gateway object that supports Q.931.

- A. Call Setup and Call Control
- B. Call Setup
- C. Direct and Call Control
- D. Call Proxy and Call Control
- E. Direct

Answer: B

Explanation:

Creating the Gatekeeper

The gatekeeper object must be created to securely pass H.323 traffic through your firewall. To create a gatekeeper object, follow these steps:

1.

Go to Manage _

Network Objects Go to the Network Objects window

and choose New _

VoIP Domains _

VoIP Domain H.323 Gatekeeper.

2. In the General tab, shown in Figure below, define the gatekeeper's Name, Comment, and Color. The network object or address range object that represents your soft phones subnet and/or the object that represents your gateway (if you're using analog phones) should be defined in the Related Endpoints Domain field. If you are using a combination of analog and digital phones then combine the gateway and the network range in a Simple Group and define it here. The host node object that represents your H.323 gatekeeper machine should be defined in the VoIP Installed At field.

Gatekeeper General Properties



3. Under the Routing Mode tab of the gatekeeper properties, you can choose from three allowed routing modes. This option identifies which connections will be rerouted from your VoIP gatekeeper to the VoIP gatekeeper on the other end. At least one of the following choices must be checked depending on the VoIP equipment that is being utilized: Direct The H.225 and Q.931 protocols, which allow gatekeeper to gatekeeper communication and call setup and breakdown respectively, are rerouted if this check box is selected.

Call Setup (Q.931) H.245 which is the control protocol used by H.323 for multimedia communication will be rerouted from gatekeeper to gatekeeper along with the Q.931 protocols.

Call Setup (Q.931) and Call Control (H.245) Connections that deal with video, audio and controls connections associated with video and audio will be rerouted gatekeeper to gatekeeper.

QUESTION 44:

A SecureClient configuration is being verified with Secure Configuration Verification (SCV) on an Enforcement Module. Which of the following is NOT true?

- A. If users log off the Policy Server or disable the Security Policy, SecureClient will indicate a Secure Configuration failure.
- B. The Enforcement Module checks the identity of users on specific machines, and verifies that the machines are securely configured.
- C. SCV cannot be verified on an Enforcement Module.
- D. Access is denied to SecureClient machines that are accidentally or intentionally misconfigured.
- E. The default SCV policy requires users to log in to the Policy Server.

Answer: C

p360 Check Point Mgmt II Student Manual

Explanation:

Secure Configuration Verification (SCV)

Secure Configuration Verification (SCV)

is a mechanism that determines

whether the SecureClient machine is securely configured (clean) or not

securely configured (dirty). SCV makes sure SecureClient machines that are

attempting to VPN with the firewall are protected by the Policy Server's policy

and their security is not being compromised.

The SCV process is done with an

SCV Manager

component running on

the Policy Server. The SCV Manager is responsible for configuration and

maintenance of the SCV state from all

SCV plug-ins

SCV plug-ins are DLLs

registered with SecureClient; they contain functions that can notify the SCV

Manager of the DLL's state. When the SCV Manager wants SCV status, it

queries all registered SCV plug-ins about the SCV state for which they are

responsible. If all SCV plug-ins indicate that the machine is securely configured,

the SCV Manager sets the general SCV state to "securely configured."

Otherwise, it considers the SecureClient machine to be not secure. One of the

files that carries the SCV information is

local.scv

; it is stored on the

SecureClient machine with its other configuration files.

Future versions of SCV will support Check Point NG and third-party SCV

plug-ins such as Open Platform for Security (OPSEC) products. Administrators

will be able to configure both the SCV plug-ins and the SCV checks.

Doing so will help the administrator customize the SCV operation and gain

more control over the SecureClient machine.

The next section discusses SecureClient, its deployment, and the Secure-

Client Packaging Tool.

QUESTION 45:

In the event that an unauthorized user attempts to compromise a valid SecureClient connection, the SecureClient machine can remain protected by:

A. Network Address Translation performed by the Enforcement Module.

B. The VPN-1/FireWall-1 feature of the enterprise Enforcement Module.

C. The organization's internal Enforcement Module.

- D. Enforcing a Desktop Policy blocking incoming connections to the SecurClient.
- E. Implementing Perfect Forward Secrecy for all SecureClient connections.

Answer: D

p351 Check Point Mgmt II Student Manual

QUESTION 46:

Which of the following statements is FALSE concerning Policy Servers?

- A. The Policy Server extends security to the desktop, by allowing administrators to enforce Desktop Policies on clients connecting from the Internet.
- B. The Policy Server may be installed on an Enforcement Module.
- C. A Policy Server extends security to the desktop, by allowing administrators to enforce Desktop Security Policies on clients connecting from an internal LAN.
- D. The Policy Server must be installed on the SmartCenter Server.
- E. The SecureClient machine obtains the Desktop Policy from the Policy Server.

Answer: D

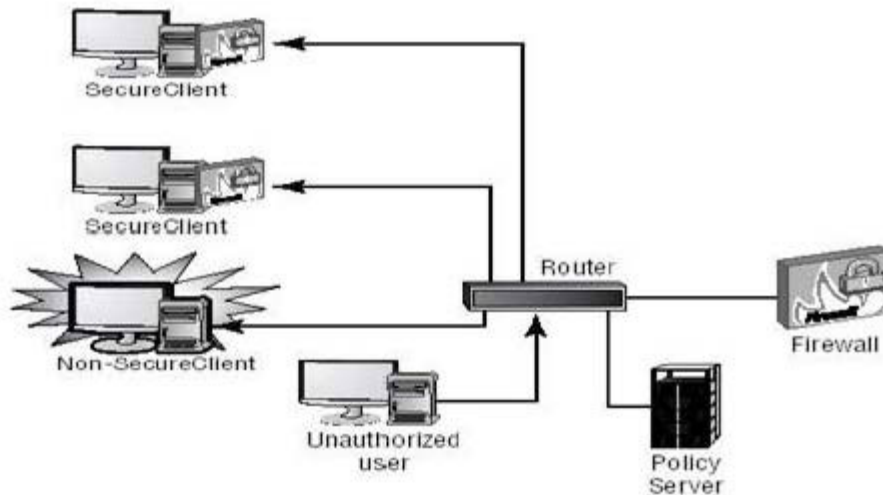
p49 CCSE Study Guide

What Is the Policy Server?

A Policy Server is a Check Point NG component that runs on a VPN-1/FireWall-1 Module. It's called a Policy Server because it allows an administrator to centrally manage desktop security by issuing a Desktop policy to SecureClient machines. The Desktop policy can be enforced on machines inside and outside a LAN, to prevent authorized connections from being compromised. In addition to enforcing a Desktop policy, the Policy Server adds security by authenticating and authorizing users, verifying memberships to user groups, and verifying secure configuration of SecureClient machines.

Figure below provides an example of how machines with SecureClient are protected from unauthorized connections. Once the SecureClient machines connect to the Policy Server and download a Desktop policy, connections that are unauthorized or not allowed by the Desktop policy will be dropped. In Figure below, as the unauthorized user tries to connect to the other machines on the network, the SecureClient machines can block the connection. Meanwhile, the machine without SecureClient is open to the unauthorized attack.

How SecureClient works



Now that you understand what the Check Point NG Policy Server is and what it does, let's look further into its technical nature. We'll discuss licensing and configuration as well as the Policy Server daemon and the files that make it work.

Licensing the Policy Server and SecureClient

It's important to understand the licensing process for the Policy Server and SecureClient. The SecureClient license is located on the SmartCenter Server and is based on the number of SecureClient users you have. The Policy Server license is located on each Policy Server and is independent of the number of users.

All SecureClient licenses contain one Policy Server license, so additional Policy Server licenses are necessary only when multiple Policy Servers are deployed. This arrangement is different from the way licensing worked in VPN-1 4.1. The NG method is more scalable for Policy Server High Availability implementations. NG includes another new feature: The Policy Server can run on gateway clusters.

The Policy Server can be installed on a Windows, Solaris, Linux, or IPSO platform. Just like the VPN-1/FireWall-1 package, the Policy Server must be installed or uninstalled in a certain order. The Policy Server must be installed on an existing FireWall Module. When you're uninstalling the Policy Server, it must be removed before the VPN-1/FireWall-1 package, which is removed before the SVN Foundation package.

QUESTION 47:

Dr bill is creating rules and objects to control Voice over IP (VoIP) traffic, through his organization's VPN-1/FireWall-1 Enforcement Module. Dr bill creates VoIP-domain SIP objects, to represent each of his organization's three SIP gateways. Dr bill then creates a simple group to contain the VoIP domain SIP objects. When Dr bill attempts to add the VoIP-domain SIP objects to the group,

they are not listed. What is the problem?

- A. VoIP-domain SIP objects cannot be placed in simple groups.
- B. The VoIP-gateway object must be added to the group, before the VoIP-domain SIP object is eligible to be added to the group.
- C. The VoIP-domain SIP object's name contains restricted characters.
- D. The related-endpoints domain specifies an address range.
- E. The installed VoIP gateways specify host objects.

Answer: A

p117 Check Point Mgmt II Student Manual

QUESTION 48:

Dr bill is a Security Administrator preparing to configure his VPN-1/FireWall-1 Rule Base, to accommodate Voice over IP (VoIP) traffic. Dr bill has the information displayed below.

1. VoIP Domain Session Initiation Protocol (SIP): Norbert
2. End Point Domain: 10.10.100.0
3. GateKeeper Server IP : 10.10.100.
4. Phone Type: Pingtel instant expressa(tm) softphone Version 1.2.1
5. RTP Port Settings: UDP Port 5079
6. RTCP Port Settings: UDP Port 5075

Does Dr bill have enough information to configure his objects and rules?

- A. Yes, Dr bill has sufficient information to configure his objects and rules.
- B. No, Dr bill does not have enough information to configure his objects and rules. Dr Bill needs to know the IP address of the VoIP gateway.
- C. Dr bill is trying to pass SIP traffic through NG with Application Intelligence. NG with Application Intelligence does not support SIP. Dr bill must use an H.323 VoIP solution for NG with Application Intelligence.
- D. No, Dr bill does not have enough information to configure his objects and rules. Dr Bill needs to know the IP address of the SIP user-agent server.
- E. No, Dr bill does not have enough information to configure his objects and rules. Dr Bill needs to know the IP address of the SIP redirect server.

Answer: C

VoIP gatekeeper and gateways are H.323 terms not SIP.

QUESTION 49:

Dr bill wants to protect internal users from malicious Java code. However, he does not want to strip Java scripts. Which is the BEST configuration option?

- A. Configure a URI resource to block Java code.
- B. Configure a CVP resource to strip block java code.
- C. Configure a URI resource to strip applet tags.
- D. Configure a URI resource to strip script tags.
- E. Configure a CVP resource to strip script tags.

Answer: A

p153 Check Point Mgmt II Student Manual

Explanation:

A URI resource

can filter out HTML codes (script tags, ActiveX tags, and so on), block Java code, scan for viruses, and redirect users to alternate web sites.

QUESTION 50:

You are a VPN-1/FireWall-1 Security Administrator. You must discover the users who are attempting to circumvent SecureClient protection mechanisms. In which of the following logs would you MOST likely find the information you need?

- A. SecureClient Control
- B. SmartView Tracker
- C. Fwd.elg
- D. Vpnd.elg
- E. Remote Acces Control

Answer: B

QUESTION 51:

Which of the following modes allows a client in a load-balancing environment to retain its connection with the same server during a session?

- A. Standby Server
- B. Active Server
- C. Persistent Server
- D. Relay Server
- E. Backup Server

Answer: C

Explanation:

Persistent Server Mode should always be turned on. This option is the "superglue" of the logical server: It makes the connection stay with the same server or service for a time frame specified by you in the Global Properties. Persistent Server Mode is helpful with services such as FTP , which involve an active connection. You want the connection to stay with the same server throughout the duration of the session. That way, if there is a break in the session, you will be able to get back to that specific server to complete the download. With Persistent Server Mode turned on (it is on by default), two persistency options are available: You can choose to make the connection persistent based on either the service being used (HTTP, FTP, and so on) or the server selected by the algorithm.

QUESTION 52:

Dr bill is a Security Administrator preparing to install and deploy VPN-1/FireWall-1 to protect his company's information assets. Dr bill only has one machine to dedicate to security enforcement. Which of the following VPN-1/FireWall-1 installation options is MOST appropriate for Dr bill's environment?

- A. Enterprise Primary Management
- B. Enforcement Module and Primary Management
- C. Enterprise Single Gateway
- D. Enforcement Module
- E. Enterprise Secondary Management

Answer: B

QUESTION 53:

Dr bill is a VPN-1/FireWall-1 Security Administrator attempting to implement SecuRemote access. Dr bill creates and configures a SecuRemote user. When he goes to his RemoteAccess Community and attempts to add the new user as a participant, the user is not listed. Why is the user NOT listed?

- A. Only administrators may be participants in the RemoteAccess Community, not default users.
- B. Dr bill did not specify an authentication method for the new user.
- C. Only user groups, not individual users, may be participants in the RemoteAccess Community.
- D. Only gateways may be participants in the RemoteAccess Community. Users are not eligible participants.
- E. Dr bill specified encryption parameters for the user that do not match the RemoteAccess Community's encryption parameters.

Answer: C
p300 Check Point Mgmt II Student Manual

QUESTION 54:

What is the proper order to uninstall VPN-1/FireWall-1 in a stand-alone configuration?

1. SmartConsole
2. SVN Foundation
3. VPN-1/FireWall-1
4. Policy Server

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

Answer: B
p71 Check Point Mgmt II Student Manual

QUESTION 55:

A digital signature:

- A. Automatically changes shared keys.
- B. Uniquely encodes the receiver of the key.
- C. Provides a secure key-exchange mechanism over the Internet.
- D. Guarantees the authenticity of a message.
- E. Decrypts data to its original form.

Answer: D

QUESTION 56:

Dr. Bill is a Security Administrator who must define a new user for SecuRemote access to his VPN-1/FireWall-1 VPN Domain. Dr. Bill has an established Remote Access VPN community for existing SecuRemote users. Dr. Bill creates a new user and populates the Login Name field. He then saves and installs the Security Policy. When Dr. Bill attempts a SecuRemote connection using the newly created user, the connection fails. Which of the following is the BEST explanation for the failure?

- A. The VPN-1/Firewall-1 Enforcement Module does not have a valid license for the new SecuRemote user.
- B. Dr bill did not configure Time properties for the new user. New users are restricted to No Time.
- C. Dr bill did not define an authentication method or generate a certificate for the new user.
- D. The new user was not placed in a group. The All Users group cannot be used for SecuRemote access.
- E. Dr bill did not configure the user's locations. The Any location is not a valid option for SecuRemote users.

Answer: C

p300 Check Point Mgmt II Student Manual

QUESTION 57:

Dr bill wants to configure a custom script to launch an application for certain rules. Which of the following should Dr bill configure?

- A. SNMP Trap Alert Script
- B. Custom scripts cannot be executed through Alert Scripts.
- C. Mail Alert Script
- D. User-Defined Alert Script
- E. Popup Alert Script

Answer: D

Explanation:

Custom User-Defined Alerts

Many companies have Intrusion Detections Systems (IDS) running on their networks to detect potential attacks. Network IDS Sensors are usually positioned on each subnet of the firewall to listen to traffic in promiscuous mode and detect attacks using either a signature-based or anomaly-based detection method. IDS sensors can detect attacks, but most products don't have the ability to stop attacks after they are detected. By the time an administrator is alerted to most attacks, the damage is already done. (It's like having a silent car alarm that sends you an alphanumeric page after someone has broken in and stolen your stereo. The text message should say, "Thank you. It has been a pleasure being your thief.")

Check Point's SmartDefense has the ability to detect an attack, block the attack, and send alerts about the attack. Using Check Point's alerting features, an administrator can configure SmartDefense to block known attacks and send a customized alert when an attack occurs. The customized alert can be

an e-mail, an alphanumeric message, a screen pop-up, or whatever else the administrator would like to use.

QUESTION 58:

Assume an intruder has succeeded in compromising your current IKE Phase 1 and Phase 2 keys. Which of the following will end the intruder's access after the next Phase 2 exchange occurs?

- A. DES Key Reset
- B. MD5 Hash Completion
- C. SHA1 Hash Completion
- D. Phase 3 Key Revocation
- E. Perfect Forward Secrecy

Answer: E

Explanation:

Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is a layer of protection that can be added to Phase 2. Using this option adds a Diffie-Hellman key exchange to Phase 2 negotiations (it normally occurs only in Phase 1). If your Phase 1 keys were compromised, an attacker could decrypt Phase 2 exchanges to get your IPSec keys (VPN session keys). This scenario is prevented by adding a Diffie-Hellman key exchange to Phase 2. Even if an attacker got your Phase I keys, they would need to get your Phase 2 keys to uncover the IPSec keys necessary to decrypt your traffic. Because Phase 2 occurs every hour, it's highly unlikely that the attacker would have time to decipher your Phase 2 keys before they were renegotiated.

QUESTION 59:

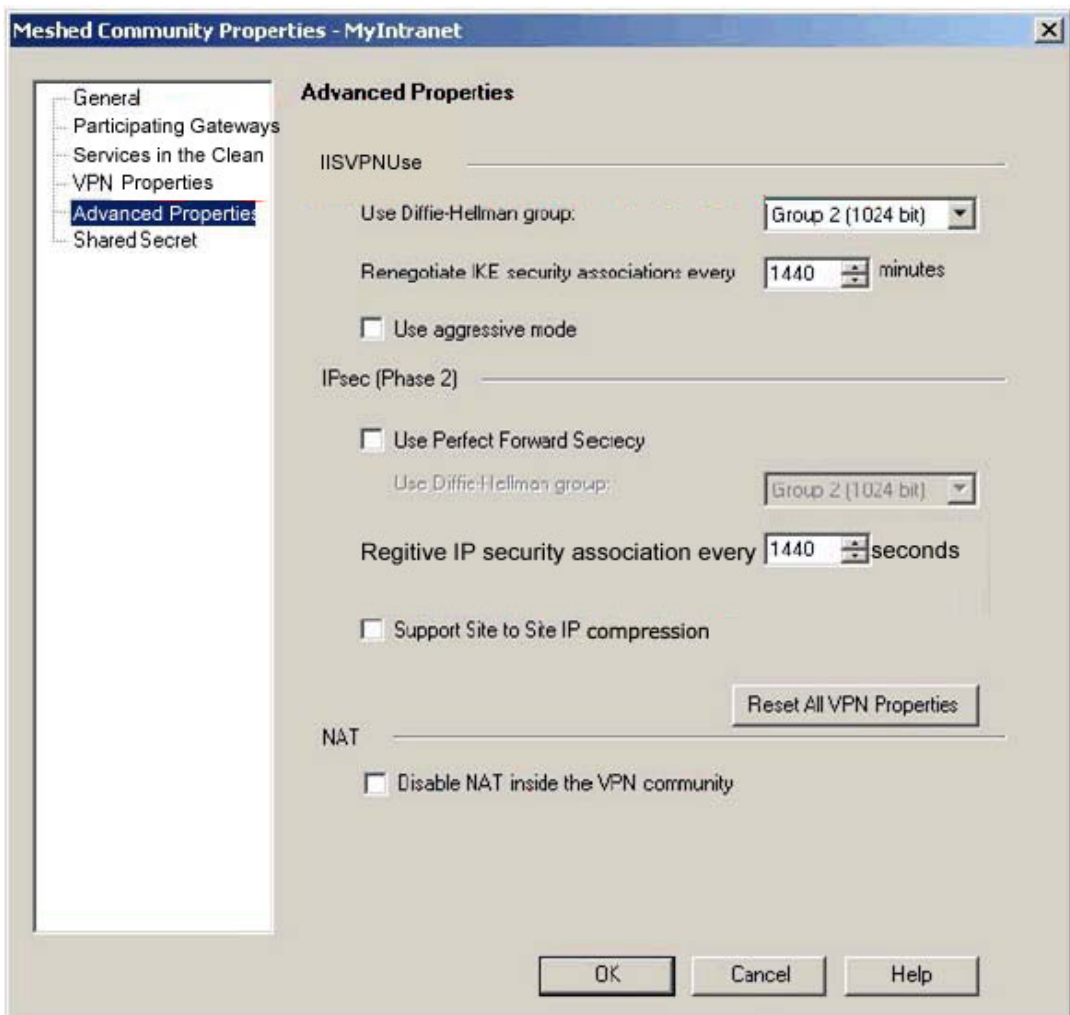
To enable session tracking, you must do which of the following? (Choose two)

- A. Create the path a packet takes after it leaves an Enforcement Module.
- B. Define which parameters of an alert are established.
- C. Define which parameters of a log are established.
- D. Create the path a packet takes between an enterprise Enforcement Module and the perimeter router.
- E. Create the path a packet has taken before reaching an Enforcement Module.

Answer: B, C

QUESTION 60:

Exhibit:



Dr bill wants to reduce encryption overhead for his meshed VPN Community, without compromising security. Which of the following helps Dr bill accomplish his goal?

- A. Check the box Support Site to Site IP compression.
- B. Check the box User aggressive mode.
- C. Change the setting Use Diffie-Hellman group: to "Group 5 (1536 bit)".
- D. Check the box Use Perfect Forward Secrecy.
- E. Reduce the setting Renegotiate IKE security associations every to "720".

Answer: B

QUESTION 61:

You are logging into a Policy Server in order to update or download a new Desktop Policy. Which of the following initiates an Explicit login?

- A. SecureClient
- B. Remote Client Manager
- C. Session Authentication Agent
- D. Policy Server
- E. LDAP Server

Answer: A

p369 Check Point Mgmt II Student Manual

QUESTION 62:

Which of the following FTP Content Security settings prevents internal users from retrieving files from an external FTP Server, while allowing users to send files?

- A. Block FTP_PASV.
- B. Use an FTP resource, and enable the GET and PUT methods.
- C. Use an FTP resource and enable the GET method.
- D. Use an FTP resource and enable the PUT method.
- E. Block all FTP traffic.

Answer: D

QUESTION 63:

If a VPN Community is included in the IF VIA field of a rule, all packets matching the rules' criteria will be _____, even though the rule shows Accept in the Action column.

- A. user authenticated
- B. encrypted
- C. dropped
- D. client authenticated
- E. rejected

Answer: B

Note: The 'If Via' column (FP3) was changed to the VPN column in NGAI (FP4).

QUESTION 64:

Which of the following is configured in a rule allowing notification through SmartView Status?

- A. Mail
- B. Account
- C. Log
- D. Alert
- E. SNMP Trap

Answer: D

QUESTION 65:

Dr bill wants to deploy SecureClient to remote users and wants to use certificate for authentication. What is the proper order to properly generate and deploy user certificates on the Internal Certificate Authority (ICA)?

1. Securely distribute the certificate.
2. Create the user.
3. Require the user to change the password protecting the certificate.
4. Generate the user certificate.

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

Answer: D

QUESTION 66:

Which of the following statements about Hybrid IKE are FALSE? (Choose two)

- A. The final packet size is increased after it is encrypted.
- B. Only pre-shared secrets or certificates may be used.
- C. SecureClient and Hybrid IKE are incompatible.
- D. TCP/IP headers are encrypted along with the payload.
- E. Any authentication mechanism supported by VPN-1/FireWall-1 is supported.

Answer: B, C

QUESTION 67:

VPN-1/FireWall-1 allows a Security Administrator to define four types of Certificate Authorities. Which of the following is NOT a type of Certificate Authority that can be defined in VPN-1/FirwWall-1?

- A. OPSEC PKI
- B. External SmartCenter Server
- C. Entrust PKI
- D. VPN-1 Certificate Manager
- E. Caching Only Certificate Manager

Answer: E

p208 Check Point Mgmt II Student Manual

Explanation:

As with any other object, a Name is given and you can define a Comment and Color. The Certificate Authority pull-down menu lists the four choices for creating a CA server object:

VPN-1 Certificate Manager This was Check Point's proprietary twist on Entrust's Certificate Manager. This product line was dropped in December 2001 but is listed to handle backward compatibility requirements.

Entrust PKI This OPSEC partner offers a PKI solution. See www.entrust.com for more details.

OPSEC PKI This option encompasses non-Entrust OPSEC PKI solutions. For a listing of current OPSEC-certified PKI solutions, go to http://www.opsec.com/solutions/sec_pki.html.

External Management Server This option is for Check Point certificates that you import from other Check Point SmartCenter Servers.

NG's implementation of IKE supports X.509 digital certificates from these sources. Keep in mind that you can have only one certificate from each CA, and each CA must have a unique DN.

Certificate Authority Properties window



QUESTION 68:

Dr bill is a Security Administrator assisting a SecuRemote user who must switch from using a pre-shared secret, to using certificates for access to the VPN domain. The user is physically located on a different continent then Dr bill. Until the user has her certificate, she cannot access the resources she needs to perform her duties. Which of the following options is the BEST method for Dr bill to deliver the certificate to the user?

- A. Initiate the user's certificate, and send the user the registration key. Allow the user to complete the registration process.
- B. Generate the certificate and save it to a floppy disk. Mail the floppy disk to the user's location.
- C. The user should mail her laptop to Dr bill. Dr bill needs physical to the SecuRemote machine to load the certificate.
- D. Dr bill must delete the user's account and create a new account. It is not possible to change encryption settings on existing users.
- E. Generate the certificate, and place it on FTP Server in the VPN Domain. Ask the user to fetch the certificate.

Answer: E

p271 Check Point Mgmt II Student Manual

QUESTION 69:

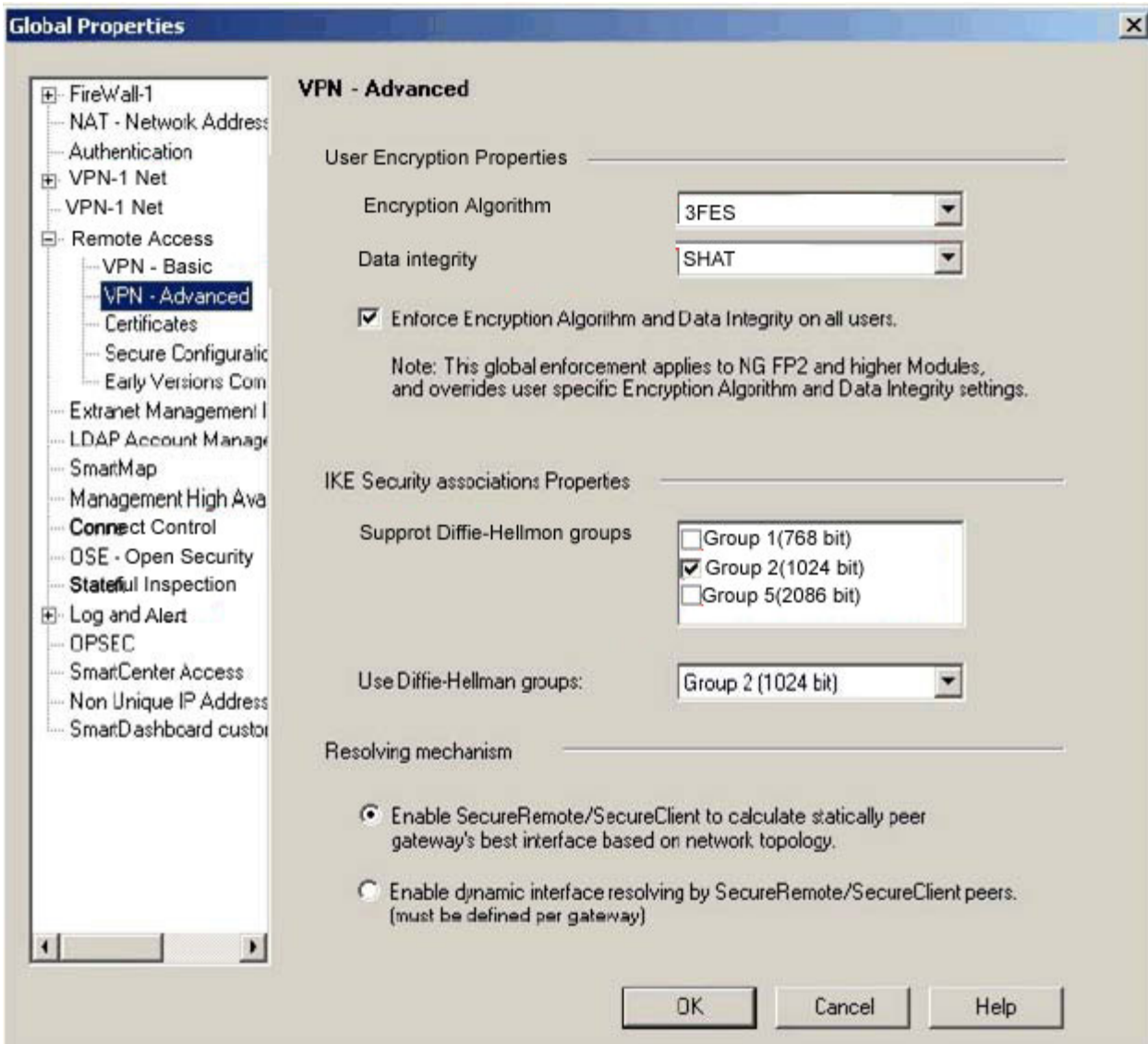
The Internal Certificate Authority (ICA) is installed on which of the following?

- A. SmartCenter Server
- B. Policy Server
- C. Enterprise Log Module
- D. SmartConsole
- E. Enforcement Module

Answer: A

QUESTION 70:

Exhibit



Dr bill is adjusting the Global Properties > Remote Access > VPN - Advanced settings in SmartDashboard. Which of Dr bill's VPN Communities will be affected by these changes?

- A. All mesh VPN Communities
- B. MyIntranet only
- C. RemoteAccess only
- D. All VPN Communities, regardless of type
- E. All star VPN Communities

Answer: C

QUESTION 71:

How many certificates can one entity have from a single Certificate Authority?

- A. Two
- B. One
- C. Four
- D. Five
- E. Three

Answer: B

QUESTION 72:

Which of the following statements correctly describes a difference between pre-shared secrets and certificates, as implemented in gateway-to-gateway encryption in VPN-1/FireWall-1?

- A. A pre-shared secret is an attribute of a single entity, but a certificate is an attribute of a pair of entities.
- B. A pre-shared secret is an attribute of a pair of entities, but a certificate is an attribute of a single entity.
- C. Both a pre-shared secret and a certificate are attributes of a pair of entities.
- D. Both a pre-shared secret and certificate are attributes of a single entity.
- E. None of the above.

Answer: B

QUESTION 73:

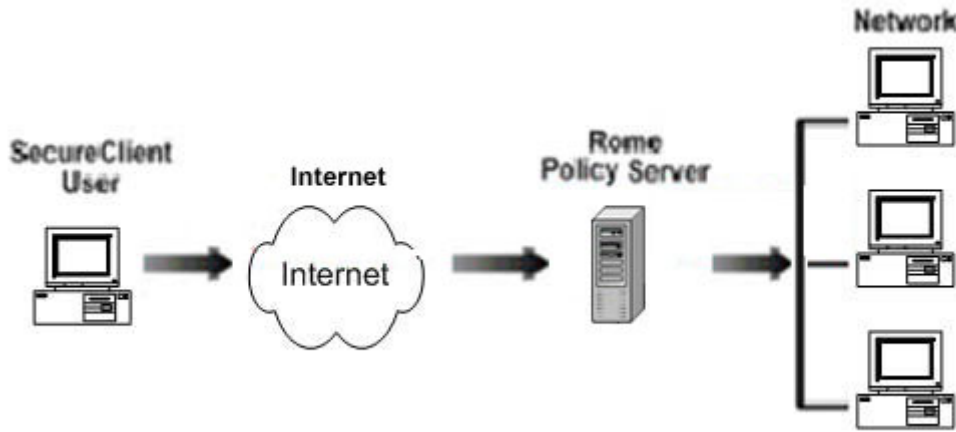
Dr Bill is assisting a SecureClient user who is not able to access resources in the VPN Domain. Which of the following is NOT a possible cause for the user's inability to access resources?

- A. A key-exchange protocol is initiated with the VPN-1/FireWall-1 Enforcement Module. The user's ISP may be blocking the protocol.
- B. SecureClient holds the first packet without transmitting it. If the user's Internet connection is very slow, the connection may be timed out.
- C. SecureClient challenges users for authentication. The user may be supplying an incorrect user name or password.
- D. The VPN-1/FireWall-1 Enforcement Module pushes topology information to the SecureClient. If the user's is behind a NAT device, the Enforcement Module cannot push the topology.
- E. SecureClient examines the packet, to determine the responsible Enforcement Module. The user may have supplied incorrect information about the Enforcement Module.

Answer: E

QUESTION 74:

In the following graphic, the remote SecureClient machine does not have an installed Desktop Policy.



The SecureClient User tries to connect to a host in Rome's VPN Domain. Because Rome is a Policy Server:

- A. It will initiate Explicit Logon only, before it allows a connection to its VPN Domain.
- B. It will initiate Explicit Logon and attempt to install a Desktop Policy on the SecureClient machine, before it allows a connection to its VPN Domain.
- C. The SecureClient user will not be allowed to connect to a host in Rome's VPN Domain.
- D. It will initiate Implicit Logon and attempt to install a Desktop Policy on the SecureClient machine, before it allows a connection to its VPN Domain.
- E. It will initiate Implicit Logon only, before it allows a connection to its VPN Domain.

Answer: D

p369 Check Point Mgmt II Student Manual

QUESTION 75:

Dr. Bill is a Security Administrator for a financial firm with very strict policies for remote access. Preventing users from modifying settings is a priority. Dr. Bill has selected SecureClient as his firm's remote access solution. Dr. Bill is reviewing site definition solutions and attempting to decide which is appropriate for his environment. Which of the following should he choose?

- A. Allow SecureClient users to connect to a trusted, third party site-distribution server and download the site.
- B. Allow SecureClient users to download the site information from a VPN-1/FireWall-1 Enforcement Module.
- C. Configure a SecureClient User Access Token, and allow users to attach the token to

the client.

D. Establish a SecureClient connection and allow subsequent SecureClient connections to fetch site information from their peers.

E. Prepare a standard userc.C file for SecureClient users and predefine the site for them

Answer: B

p385 Check Point Mgmt II Student Manual

QUESTION 76:

Which of the following Action column options is NOT available for use in a simplified mode Rule Base?

A. Drop

B. Accept

C. Reject

D. Client Auth

E. Encrypt

Answer: E

QUESTION 77:

Dr bill is preparing to implement remote-access VPNs, using VPN-1/FireWall-1 and SecureClient. When Dr bill selects an authentication method, it must meet the following requirements:

1. The authentication method must support existing authentication methods, including OS passwords and RADIUS, for ClientAuthentication.

2. The Enforcement Module must use certificates, to authenticate itself to the client.

3. The authentication method must be flexible, allowing other authentication solutions to be added, including SecureID and TACACS.

Which authentication method should Dr bill choose?

A. Digital Certificates

B. Pre-shared Secrets

C. LDAP

D. Public Key Signatures

E. Hybrid Mode

Answer: E

QUESTION 78:

Dr bill is a security consultant. Dr bill's client uses a 56-bit DES encryption key for its VPN-1/FireWall-1 VPNs. Dr bill informs his client that as a banking concern, the client is not using a long enough key to comply with new industry regulations. New industry regulations require a key length of no less than 120 bits. The new industry standards expressly prohibit the use of proprietary algorithms. Which of the following solutions could Dr bill suggest to his client, to help the client achieve regulatory compliance? (Choose two)

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

Answer: C, D

QUESTION 79:

Arne is a Security Administrator for a small company in Oslo. He has just been informed that a new office is opening in Madrid, and he must configure each site's Enforcement Module to encrypt all data being passed between the offices. Because Arne controls both sites, he decides to use a shared-secret key to configure an IKE VPN. Which of the following tasks does Arne NOT need to perform to configure the IKE VPN?

- A. Configure the Rule Base to allow encrypted traffic between the VPN Domains.
- B. Configure IKE encryption parameters for the Madrid and Oslo Enforcement Modules.
- C. Establish a secure channel for the exchange of the shared secret.
- D. Define VPN Domains for the Madrid and Oslo Enforcement Modules.
- E. Create certificates for the Madrid and Oslo Enforcement Modules.

Answer: E

QUESTION 80:

A Security Administrator wants to reduce the load on Web servers located in a DMZ. The servers are configured with the same Web pages for the same domain, and with identical hardware. Which of the following is the BEST answer to help balance the load on the Web servers?

- A. Round Trip
- B. Round Robin
- C. Server Load
- D. Domain

E. Cluster

Answer: C

'Round Robin' does not take into account the actual load on a server, it just passes from one to another. 'Server Load' would be better solution as it measures the actual load each server is under.

Explanation:

Load Balancing Algorithms

After learning about the methodologies the logical server/firewall uses to route traffic, you need to consider the algorithms used to decide which server in the server farm will get the load-balanced connection. Check Point provides five algorithms for the logical server; the administrator decides which of these algorithms to use. The algorithms are called server load, round trip, round robin, random, and domain. We'll describe these algorithms next.

1. The server load algorithm, shown in Figure below, works in conjunction with a load agent that runs on each server in the server farm. The load agent is a small program that communicates to the firewall how busy the machine is. The machine with the lightest load is sent the next packet.

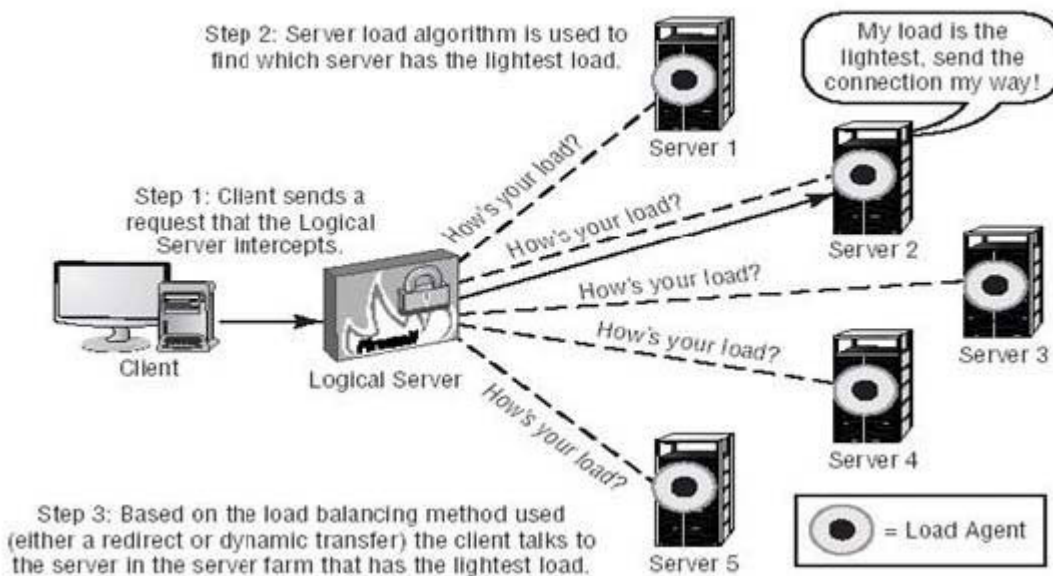
You can download this load agent

from Check Point's website (only available for Solaris) or write one using the OPSEC APIs provided by Check Point on the OPSEC website (www.opsec.com).

The load agent uses UDP port 18212

by default. The firewall checks the load on each server at the configured time and passes the connection to the server that has the lightest load.

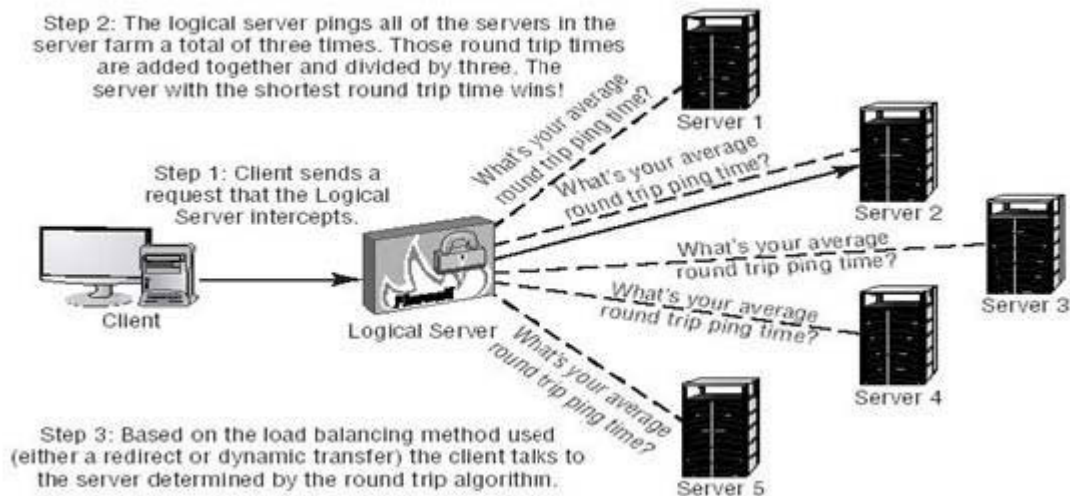
Server load algorithm



2. The round trip algorithm uses ping to decide which server gets the request, as depicted in Figure below. The round trip algorithm is much simpler than the server

load algorithm, but not as intuitive-it cannot measure the load on the servers. Therefore, the round trip algorithm's decision is based solely on network factors rather than the server load. When you use round trip, the server with the least traffic will answer first. The server with the most traffic will be too busy to answer, and the packet will be delivered to the machine that answers first.

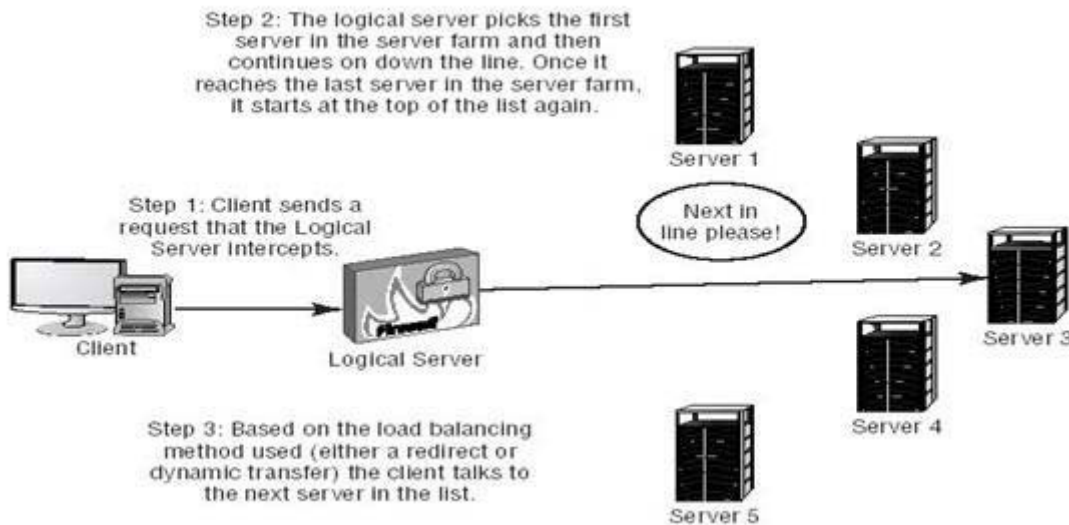
Round trip algorithm



The drawback to using the round trip method is that the server closest to the firewall usually gets the connection.

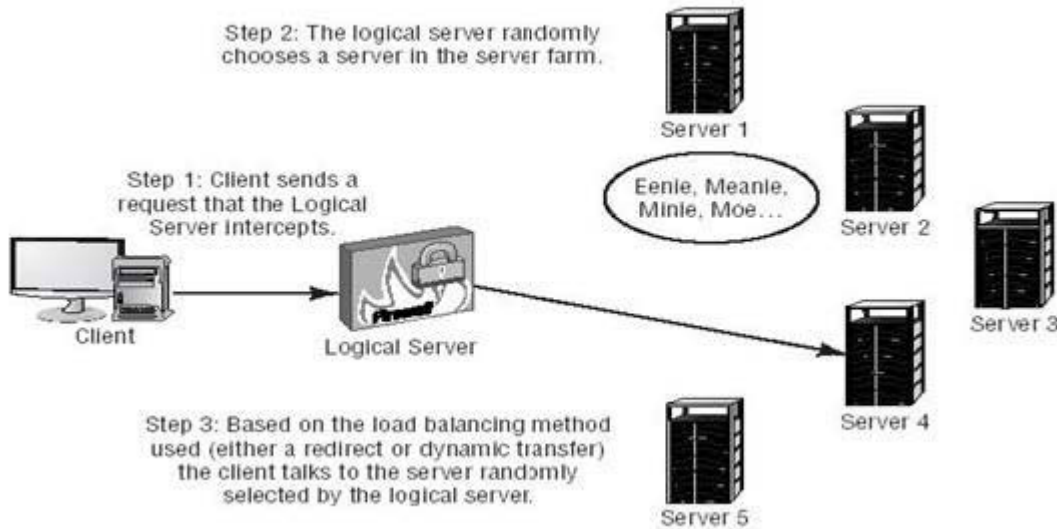
3. The round robin algorithm, shown in Figure below, is not very intelligent. This algorithm begins with the first server in the server farm and gives it the first connection. The second connection goes to the second server in the server farm, the third goes to the third, and so on. When the algorithm reaches the bottom of the list, it starts over.

Round robin algorithm



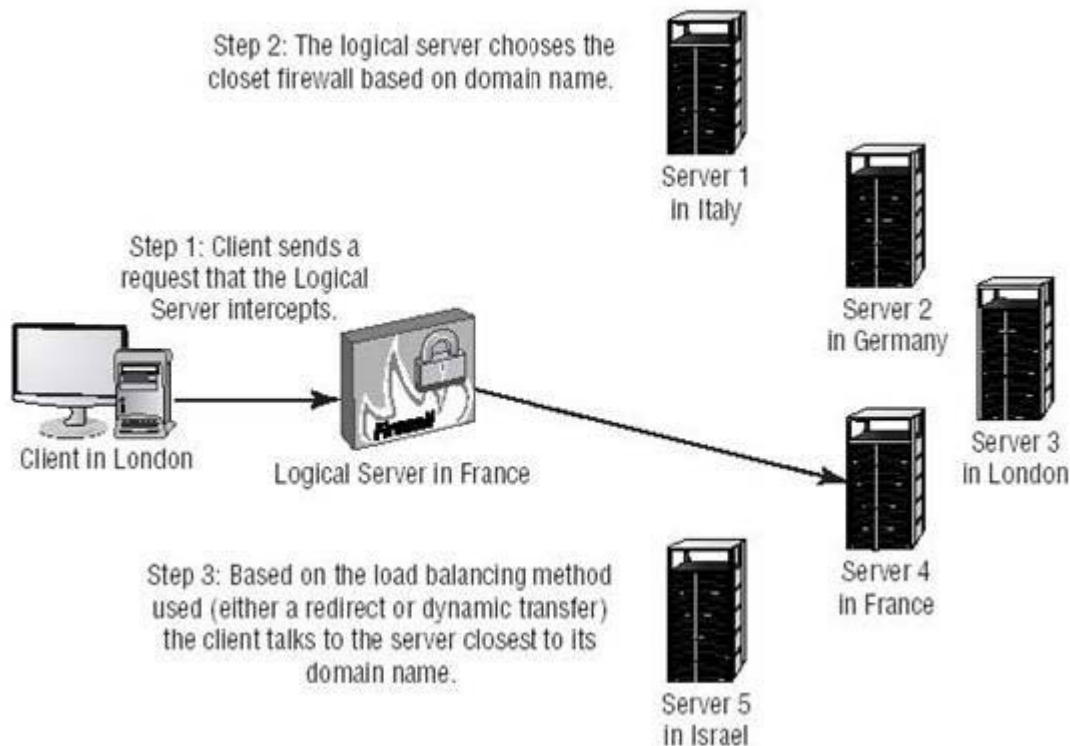
4. Next in the list of load balancing algorithms is random. Do you remember the method you used to choose teams when you were a kid? Eenie, Meanie, Minie, Mo! That is the same method the firewall uses. The random algorithm is illustrated in Figure below.

Random algorithm



5. Last is the domain algorithm. With this algorithm, the firewall chooses the closest server based on domain names. Figure below shows an illustration of the domain algorithm in action. There is an issue with the domain algorithm. Check Point doesn't recommend using it, because it creates a noticeable delay for requests due to the required reverse DNS lookups. In today's e-business environment, any delay experienced by users accessing your website could be disastrous. This algorithm was originally designed for clients in Europe and the rest of the world, where they use country names at the end of their URLs (such as `www.company.uk`). For example, in Figure below, if a client in the U.K. is trying to connect to a website for a global company based in France, the initial connection goes to the logical server in France. At this point, the closest server is in France, and it would be "logical" to send the connection to the server in France. Unfortunately, the domain algorithm will send packets back to the client in the U.K. and redirect them to the server located in the U.K., wasting precious time in the connection setup. This is an effective method only if all your servers are located in Europe and the client is also located in Europe.

Domain algorithm



To sum up, Check Point offers five algorithms-but in our opinion, only one is a true load balancing method. The server load algorithm is the only method that takes into account the actual load on each server. The rest of the algorithms don't consider how busy each server is in the server farm. As the administrator, you should check out all methods of load balancing (both Check Point and non-Check Point) before deciding which one is best for your situation.

QUESTION 81:

Which of the following encryption algorithms is a symmetric-key encryption method that uses a 168-bit key?

- A. CAST Cipher
- B. DES
- C. AES (Rijndael)
- D. 3DES
- E. Blowfish

Answer: D

3DES uses 168 bits. AES uses 128 - 256 bits

Explanation:

Encryption Standards Support by IKE and VPN-1

Algorithm	Description
DES	Data Encryption Standard (standard in the U.S. for the last 20 years). A symmetric key encryption method that uses 56-bit keys.
Triple DES	A variation on DES that addresses the problem of short, easily breakable keys. Encrypts with three different DES keys in succession, which increases the effective key strength to 168 bits.

Algorithm	Description
CAST	Named for its inventors, Carlisle Adams and Stafford Tavares. Similar to DES and supports variable key lengths from 40–128 bits.
AES	Advanced Encryption Standard. The new Federal Information Processing Standard (FIPS) standard. Also known as Rijndael (pronounced “rhine-doll”) for its inventors, Vincent Rihmen and Joan Daemen.

QUESTION 82:

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Certificate-based encryption
- B. Static encryption
- C. Asymmetric encryption
- D. Dynamic encryption
- E. Symmetric encryption

Answer: E

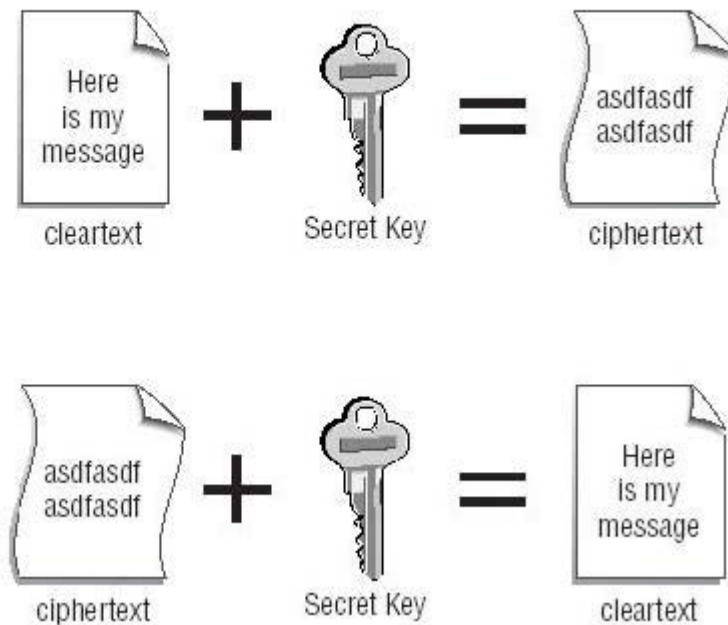
Explanation:

Symmetric Encryption

Symmetric encryption

is best described graphically, as shown in Figure below:

Symmetric encryption



The original message shown in Figure 6.1 is referred to as being in cleartext

because it's readable. When this original message is combined with the secret key the result is the encrypted message (referred to as ciphertext

). The message

can only be decrypted by someone who holds the same secret key. When the process is reversed, the encrypted message together with the secret key will produce the original cleartext message.

The process is relatively simple and very quick, but it has some drawbacks; the most basic is that the same key used to encrypt is also used to decrypt. The secret key must be created and then securely delivered to the person with whom you want to share encrypted messages. The safest way is to put it on a floppy disk and physically carry it to the person, but it is not always possible to do so. It's not secure to send this key via e-mail, because anyone could intercept it and read all of your encrypted messages. Even if you're able to physically get the key to the person, it is good security practice to change the key on a regular basis. When you're exchanging messages with one person, this is not a big deal-but with multiple people, it would be a daunting task. With symmetric encryption you should have a separate key for each person with whom you want to share encrypted information. If you used the same key for everyone, then everyone would be able to read all the

messages sent. So you need to generate one key for every person with whom you wish to encrypt. As the number of keys grows, key management becomes an issue.

We're not saying that symmetric encryption doesn't have a place in a VPN. However, you'll have to address the problem of key management. This leads us to asymmetric encryption

QUESTION 83:

You are setting up an IKE VPN between two VPN-1/FireWall-1 Enforcement Modules protecting two networks. One network is using an RFC 1918 compliant address range of 10.15.0.0. The other network is using an RFC 1918 compliant address range of 192.168.9.0. Which method of address translation would you use?

- A. Dynamic Source
- B. Dynamic
- C. Static Source
- D. None
- E. Static Destination

Answer: D

QUESTION 84:

Dr bill is using VPN-1/FireWall-1 to provide load balancing for his Web servers. When a client initiates a session with one of Dr bill's Web servers it must be able to retain its connection with the same server for the entire session. Which load-balancing mode is MOST appropriate for Dr bill's environment?

- A. Standby Server
- B. Relay Server
- C. Continuous Server
- D. Active Server
- E. Persistent Server

Answer: E

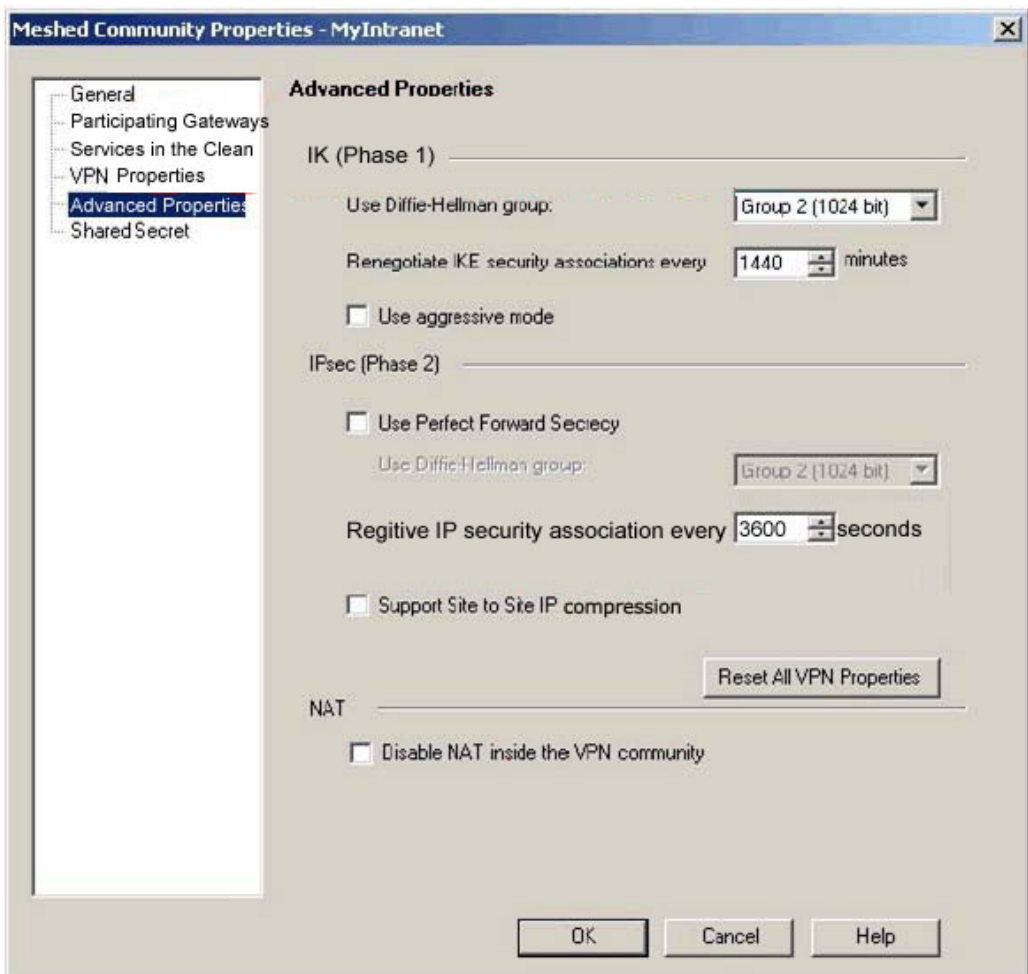
Explanation:

Persistent Server Mode should always be turned on. This option is the "superglue" of the logical server: It makes the connection stay with the same server or service for a time frame specified by you in the Global Properties. Persistent Server Mode is helpful with services such as FTP , which involve an active connection. You want the connection to stay with the same server

throughout the duration of the session. That way, if there is a break in the session, you will be able to get back to that specific server to complete the download. With Persistent Server Mode turned on (it is on by default), two persistency options are available: You can choose to make the connection persistent based on either the service being used (HTTP, FTP, and so on) or the server selected by the algorithm.

QUESTION 85:

Exhibit:



Dr. Bill is senior Security Administrator who supervises and trains junior Security Administrators. Dr. Bill must explain VPN-1/FireWall-1's Diffie-Hellman settings to the junior Security Administrator. Which of the following explanations is MOST correct?

- A. Diffie-Hellman key settings are in the Advanced Properties for a reason. Incorrect Diffie-Hellman key settings can stop and Enforcement Module from passing any traffic at all. Incorrect Diffie-Hellman key settings usually require a complete reinstallation.
- B. Diffie-Hellman groups exist for backward compatibility. When establishing VPN

tunnels between BG with Application Intelligence and older versions of VPN-1/FireWall-1, Diffie-Hellman groups allow Security Administrators to accommodate older encryption algorithms.

C. Diffie-Hellman key exchange is an encryption algorithm, which transforms clear text into ciphertext. Diffie-Hellman is vulnerable to man-in-the-middle attacks.

Diffie-Hellman groups with higher numbers use stronger keys, but have no impact on performance.

D. Diffie-Hellman key exchange is a cryptographic protocol, which allows two communicators to agree on a secret key over an insecure communication channel.

Diffie-Hellman groups with higher numbers use stronger keys. But have a negative impact on performance.

E. Diffie-Hellman keys are applied only when established Check Point-to-other-vendor VPNs. When creating VPN tunnels between different vendor's software, Diffie-Hellman keys automatically negotiate IKE and IPSEC parameters.

Answer: D

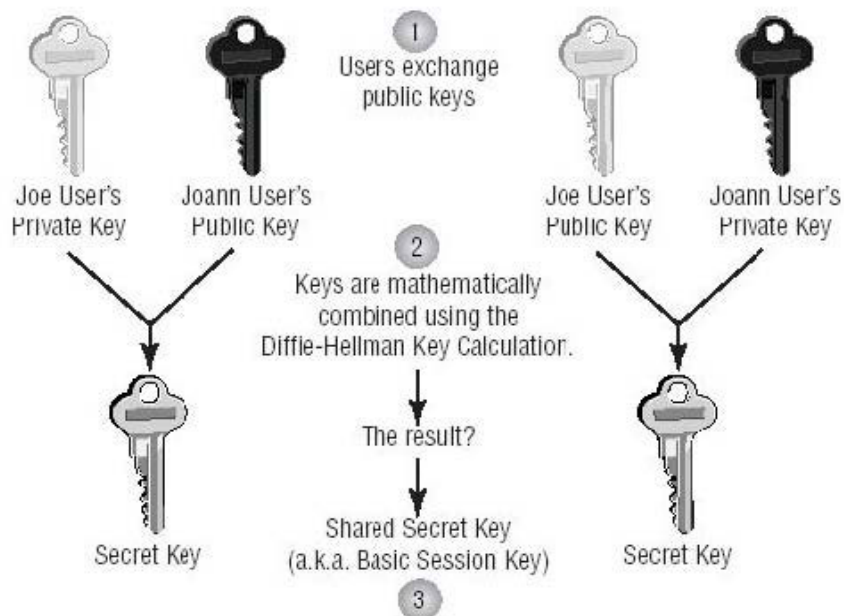
Explanation:

Diffie-Hellman Key Exchange Mechanism

The Diffie-Hellman

key exchange uses the public/private key pair to generate a secret key. This process is illustrated in Figure below.

Diffie-Hellman key exchange



In step 1, users exchange public keys. When you're using asymmetric encryption, the exchange of public keys is all that is required to begin encrypting. But Diffie-Hellman combines asymmetric and symmetric processes. Each user's private key is combined with their encrypting partners'

public key using the Diffie-Hellman key calculation, as shown in step 2. As we stated earlier, the public and private keys that each user creates are mathematically

related; that's how the users can exchange keys, apply the Diffie-Hellman key calculation, and both end up (in step 3) with mathematically identical keys.

Different mathematical groups can be used to generate the identical keys. The Diffie-Hellman standard supports three groups: DH groups 1, 2, and 5. The larger the group number, the larger the prime number used to generate the key pair. The larger groups are more secure but require more CPU cycles to generate the keys. Check Point also gives you the ability to expand the database of groups by adding custom groups.

The process depicted in Figure above solves two problems. First, you have generated the secret key necessary to perform symmetric encryption without having to physically exchange the secret key with your encrypting partner. Second, you can use that key to symmetrically encrypt data much more quickly than you can using asymmetric encryption alone. The best aspects of both encryption techniques are combined to yield a process that's better than each individual technique. The encryption processes we've described fill out the P in PAIN, but they are useless unless you get the correct key from your encrypting partner. The next section addresses how to verify that the key is from the correct source and explains the AIN in PAIN

QUESTION 86:

Which of the following conditions will cause Secure Client Verification to report that a SecureClient machine is NOT considered secured? (Choose three)

- A. The local.svc file is either corrupt or misconfigured.
- B. The SecureClient machine cannot contact the SmartCenter Server.
- C. The user has selected Disable from the SecureClient Policy menu.
- D. There are expired cookies in the machines TMP directory.
- E. There is no SCV policy on the SecureClient machine.

Answer: A, C, E

QUESTION 87:

Which component of VPN-1/FireWall-1 is used for Content Security to prevent end-user access to specific URLs?

- A. UFP Server
- B. TACACS Server

- C. URI Server
- D. CVP Server
- E. DEFENDER Server

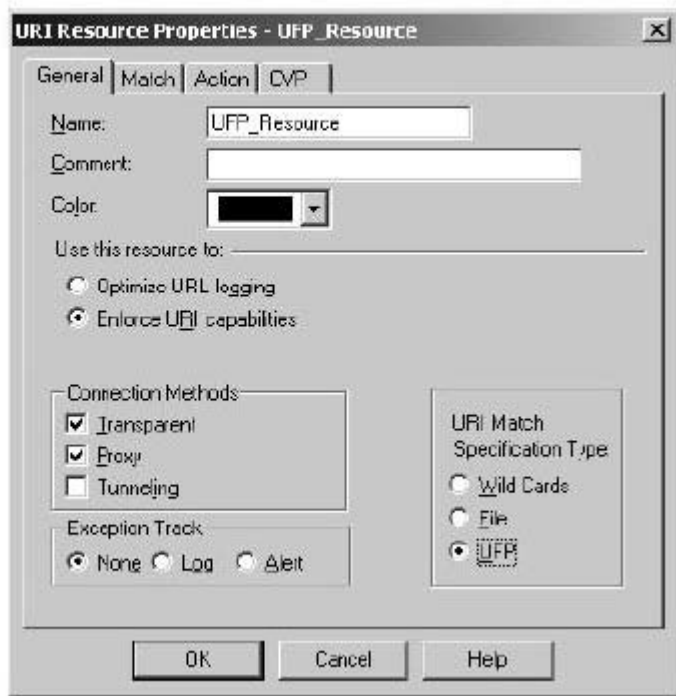
Answer: A

Explanation:

Filtering with a UFP Server

The UFP URI Match Specification Type allows firewall administrators to use an OPSEC server to keep track of sites they wish to block or filter. Before you create the resource object, you must create a Host Node object and pull it into an OPSEC application object as described in the section "Creating CVP and UFP Objects in FireWall-1" earlier in this chapter. Then, you can create a resource and select the UFP radio button under the URI Match Specification Type in the General tab of the URI Resource Properties, as shown in Figure below.

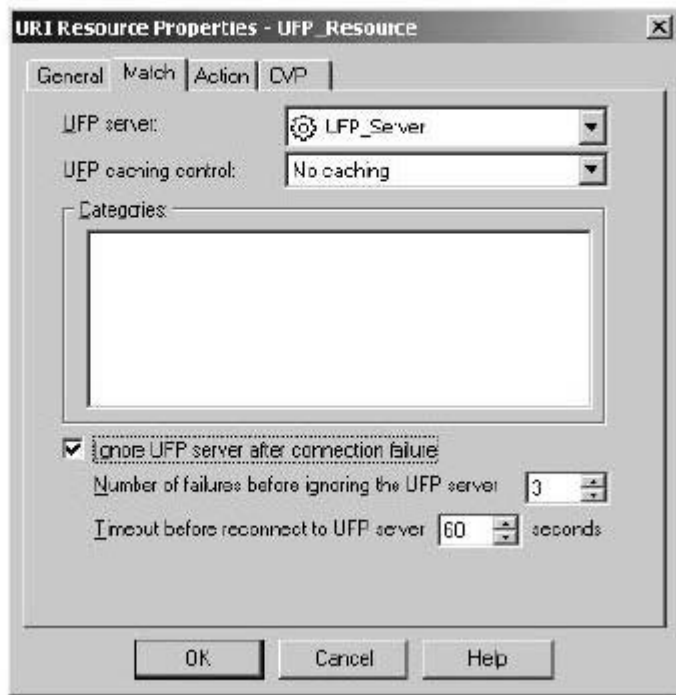
Filtering with UFP



With UFP selected, the Match tab appears as shown in Figure below.

The OPSEC server is pulled into the UFP Server field, and the categories you wish to filter/block are listed in the Categories field. You have caching options to speed up web browsing. The choices are No Caching, UFP Server, and VPN-1 & FireWall-1(one or two requests). Because the investment has

Match tab when the UFP URI Match Specification Type is selected



been made for a UFP server, it makes sense to use this caching feature on the UFP server to speed up web browsing for users.

There is one more option under the Match tab-Ignore UFP Server After Connection Failure-but we consider this option useless. You can define the number of failures and the timeout for reconnection; if the firewall still cannot contact the UFP server after that time period, then the firewall will ignore the UFP server and allow the traffic to proceed unfiltered.

QUESTION 88:

Which of the following actions does Secure Configuration Verification perform? (Choose three)
Secure Configuration Verification confirms that the:

- A. Desktop Policy is installed on all client interfaces.
- B. TCP/IP is enabled on the desktop.
- C. User name and password cached on the desktop are correct.
- D. Client's operating system has the appropriate patch level.
- E. IP address of the client is correct for entrance into the VPN Domain.

Answer: A, B, C

Explanation:

Secure Configuration Verification (SCV)

Secure Configuration Verification (SCV)

is a mechanism that determines whether the SecureClient machine is securely configured (clean) or not securely configured (dirty). SCV makes sure SecureClient machines that are attempting to VPN with the firewall are protected by the Policy Server's policy and their security is not being compromised.

The SCV process is done with an

SCV Manager

component running on

the Policy Server. The SCV Manager is responsible for configuration and maintenance of the SCV state from all

SCV plug-ins

. SCV plug-ins are DLLs

Manager of the DLL's state. When the SCV Manager wants SCV status, it queries all registered SCV plug-ins about the SCV state for which they are responsible. If all SCV plug-ins indicate that the machine is securely configured, the SCV Manager sets the general SCV state to "securely configured."

Otherwise, it considers the SecureClient machine to be not secure. One of the files that carries the SCV information is

local.scv

SecureClient machine with its other configuration files.

Future versions of SCV will support Check Point NG and third-party SCV plug-ins such as Open Platform for Security (OPSEC) products. Administrators will be able to configure both the SCV plug-ins and the SCV checks.

Doing so will help the administrator customize the SCV operation and gain more control over the SecureClient machine.

NOTE: The next section discusses SecureClient, its deployment, and the Secure-Client Packaging Tool.

QUESTION 89:

Dr. Bill is his organization's Chief Technology Officer. He is seeking a solution to control the impact of unauthorized software on his corporate network. Dr. Bill has established the following guidelines for any solution implemented:

1. Required objective: The solution must not allow access to corporate resources if user's virus-protection software is not current.
 2. Desired objective: The solution should be able to control protocols enabled on the user's computers.
 3. Desired objective: The solution should prevent users snooping traffic across internal segments of the corporate network, from acquiring useful information.
- Dr. Bill's Security Administrator proposes SecureClient with Policy Servers, internal Enforcement Modules, and Desktop policies as a solution. Based on the information, which of the following is the BEST answer?

A. The proposed solution does not meet the required objective.

- B. The proposed solution meets the required objective, but does not meet the desired objectives.
- C. The proposed solution meets the required objective, and only one desired objective.
- D. The proposed solution meets the requires objective and both desired objectives.

Answer: A

Only an OPSEC CVP server can virus check.

QUESTION 90:

Which of the following are TRUE about SecureClient? (Choose three)

- A. SecureClient cannot use Hybrid IKE for its encryption method.
- B. When SecureClient and Enforcement Module exchange keys, the user will be re-authenticated if the password has been erased.
- C. Before you attempt to download a Security Policy, you must first define a site in which a Policy Server is contained.
- D. SecureClient syntax checking can be used to monitor userc.C file parameters. This checking is used to prevent errors causing the site to which it belongs from being deleted.
- E. SecureClient supports Desktop Policies issued by a Policy Server.

Answer: B, D, E

Explanation:

Understanding SecureClient

SecureClient is the same software as SecuRemote, with added functionality.

Just as with SecuRemote, the client-to-site VPNs created with SecureClient use IPSec-based encryption. The major difference in using the SecureClient graphical interface (shown in Figure below) is the Policy menu, which helps users interact with the Policy Server. Most of the other menu options are the same as in SecuRemote and are defined in Chapter 9.

The only difference is the selection of the default

SecureClient with desktop security, instead of SecuRemote. However, despite the similarity in the GUI interface and the installation, SecureClient provides greater functionality than SecuRemote with its desktop security.

SecureClient Policy menu



As you can see in Figure above, an option in the Policy menu lets you log on to a Policy Server. When you choose the Logon to Policy Server option, a list of the installed Policy Servers is displayed as a submenu; you can then choose a Policy Server to log on to. When the SecureClient user logs on to the Policy Server, the Desktop policy is downloaded to the SecureClient machine.

The logon occurs as either an implicit logon or an explicit logon

. During an implicit logon, a Desktop policy is automatically installed on the SecureClient machine when the client authenticates. During an explicit logon, you click the Update button to update the Desktop policy. The logon is considered explicit because you initiate the download and are prompted to specify whether you would like to download a Desktop policy. The policy is downloaded only when you add or update a site that contains a Policy Server.

The Policy menu lets you disable a Desktop policy. If a Desktop policy is required by a Policy Server and you disable the policy, you will not be able to VPN with the firewall until you log on again and a new policy is issued to the client. If you disable the policy while participating in a VPN, the VPN will continue, and the change will take effect after you restart SecureClient. SecureClient does not support IP forwarding. IP forwarding may be enabled to forward packets to another NIC on a machine. When IP forwarding is detected, a warning message is shown to the user. If you are implementing SecureClient, be sure you off turn IP forwarding.

QUESTION 91:

The Check Point SecureClient Packaging Tool allows System Administrators to: (Choose three)

- A. Install a package on a client machine.
- B. Create customized SecuRemote/SecureClient installation packages to distribute to users.
- C. Customize the flow of end-user installation processed, before SecuRemote/SecureClient is installed.
- D. Configure Secu/Remote properties for users, before installation.
- E. Automatically update SecureClient installation at regular intervals.

Answer: B, C, D

p409 Check Point Mgmt II Student Manual

QUESTION 92:

Which VPN-1/FireWall-1 Security Server can hide real user names by rewriting information in the From field, while maintaining connectivity by restoring correct addresses in the response?

- A. RLOGIN
- B. SMTP
- C. FTP
- D. TELNET
- E. HTTP

Answer: B

QUESTION 93:

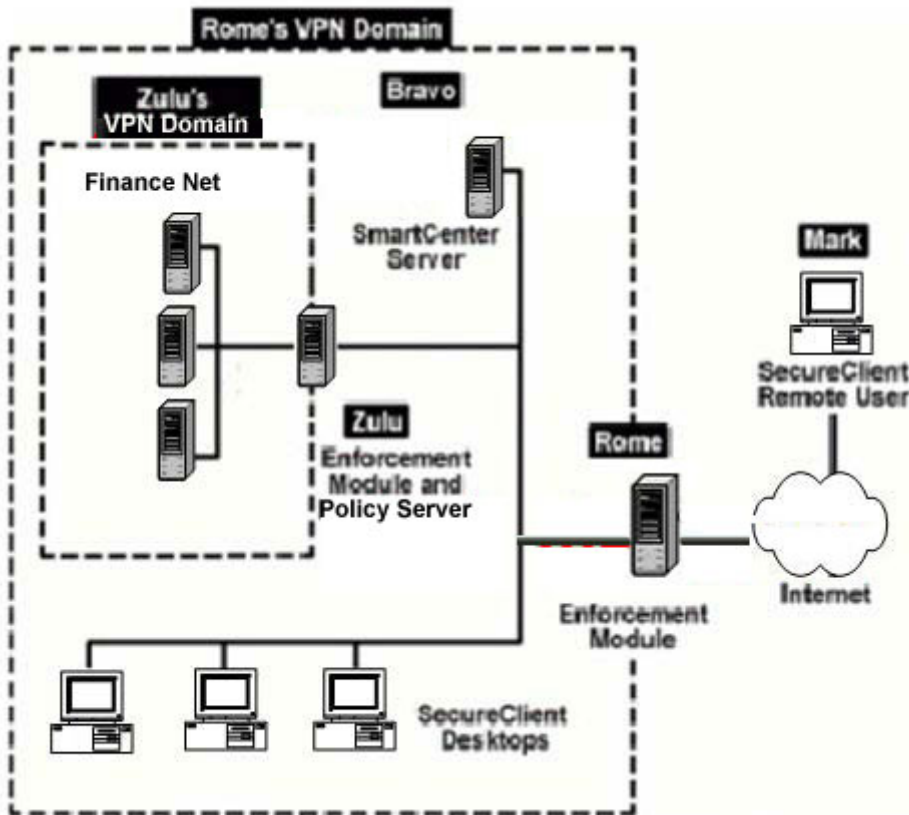
If a resource is specified in the Services field of a Rule Base, which of the following occurs?

- A. Users attempting to connect to the object defined in the Destination column of the rule will be required to authenticate.
- B. All packets matching the resource service will be analyzed based on resource properties.
- C. All packets that match the resource will be dropped.
- D. SecureClient users attempting to connect to the object defined in the Destination column of the rule will receive a new Desktop Policy from the resource.
- E. All packets matching that rule are either encrypted or decrypted by the defined resource.

Answer: B

QUESTION 94:

Exhibit



In the exhibit, SecureClient can be used inside and outside the LAN. To reach Finance.net, SecureClient users must pass through the Zulu Policy Server. When this connection is made, Zulu will attempt to load its Desktop Policy on the SecureClient remote user, and:

- A. Zulu will not allow an improperly configured SecureClient machine to reach its internal VPN Domain.
- B. Zulu will pass SecureClient users through the FinanceNet Servers to reach their internal VPN Domains.
- C. Zulu will pass SecureClient users through the FinanceNet Servers to reach their external VPN Domains.
- D. Zulu will pass SecureClient users through the Remote Enforcement Module to reach Mark.
- E. Zulu will allow an improperly configured SecureClient machine to reach its internal VPN Domain, if the traffic is accepted by the Rome Enforcement Module.

Answer: A
p51 CCSE Study Guide

QUESTION 95:

Which VPN-1/FireWall-1 Security Servers provide Content Security? (Choose three)

- A. HTTP
- B. NTP
- C. SMTP

- D. TELNET
- E. FTP

Answer: A, C, E

Explanation:

Security Servers Overview

The way Security Servers operate has changed from previous versions of FireWall-1. Previously, there was a separate service for each Security Server. In the NG version of Check Point FireWall-1, the fwssd

executable is in

charge of all Security Server functions.

Changing the architecture so that only one executable is in charge of a function or set of functions offers an advantage: It increases performance and eases debugging and troubleshooting (you no longer need to kill daemons or stop the firewall to debug and troubleshoot).

There are five Security Servers. Some are responsible for Content Security and some for User Authentication, and some fulfill both roles. Table 4.1 lists the Security Servers and their roles in User Authentication and Content Security.

Security Servers and Their Roles

Security Server	User Authentication	Content Security
telnet	Yes	No
rlogin	Yes	No
HTTP	Yes	Yes
FTP	Yes	Yes
SMTP	No	Yes

QUESTION 96:

In VPN-1/FireWall-1, Security Administrators can define URI Resource Properties to strip which of the following from HTML? (Choose three)

- A. Java applets

- B. Invalid mime types
- C. Java scripts
- D. ActiveX code
- E. Any content of a Web page

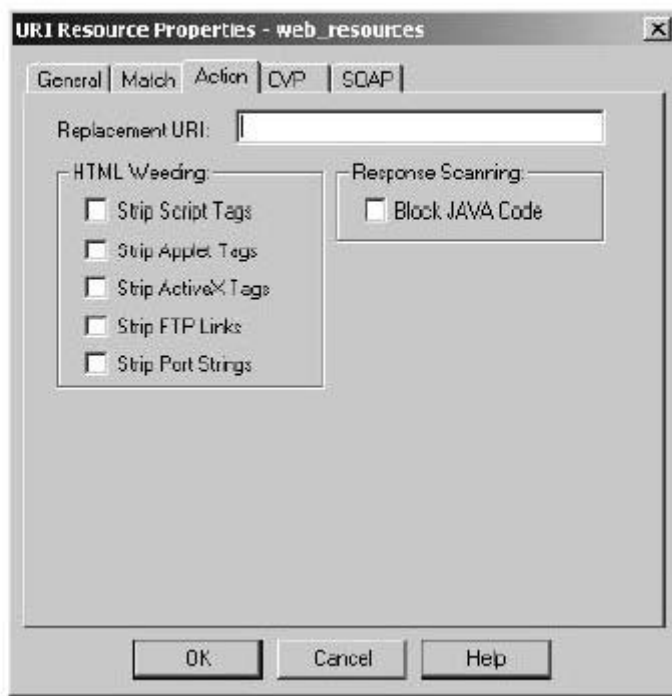
Answer: A, C, D

Explanation:

Action Tab Options

In the Action tab of the URI Resource dialog box, shown in Figure below, you define what happens to the traffic if it matches your specifications. The Replacement URI field is our favorite feature for HTTP scanning. If this value is defined and the Action of the rule that incorporates this resource is Drop or Reject, then this URI is given to the user instead of the URI they requested. For example, if a user tried to visit pornographic sites during work hours, you could redirect them to a custom web page that outlines the Human Resources policies that prohibit this kind of activity.

URI resource Action tab



If a UFP server, defined on this URI resource, sends a URL for redirection, it will override this replacement URI.

HTML Weeding options allow you to strip specified code from an HTML page. The user will not be aware that the code has been stripped (Java applets already in the cache are not affected by this option).

QUESTION 97:

Which VPN-1/FireWall-1 Security Server does NOT perform authentication?

- A. SMTP
- B. FTP
- C. RLOGIN
- D. TELNET
- E. HTTP

Answer: A

QUESTION 98:

Encryption is the transformation of readable data into an unreadable form called:

- A. One Way Hash
- B. Keyed Text
- C. Secret Text
- D. Ciphertext
- E. Cleartext

Answer: D

QUESTION 99:

Choose three. The Check Point SecureClient Packaging Tool allows System Administrators to:

- A. Install a package on a client machine.
- B. Create customized SecuRemote/SeucreClient installation packages to distribute to users.
- C. Customize the flow of end-user installation processes, before SecureRemote/SecureClient is installed.
- D. Configure SecuRemote properties for users, before installation.
- E. Automatically update SecureClient installation at regular intervals.

Answer: B, C, D

QUESTION 100:

Which of the following is TRUE of the relationship between the RemoteAccess VPN Community and the Security Policy Rule Base?

- A. The RemoteAccess VPN Community defines VPN connection parameters for SecuRemote connections. The Security Policy Rule Base is used to allow access to protected resources.
- B. The RemoteAccess VPN Community is used to allow access to protected resources. The Security Policy Rule Base is used to define VPN connection parameters for SecuRemote connections.
- C. The Security Policy Rule Base is used to define VPN connection parameters for SecuRemote connections and is used to allow access to protected resources. The RemoteAccess VPN Community applies only SecureClient.
- D. The RemoteAccess VPN Community defines VPN connection parameters for SecuRemote connections and is used to allow access to protected resources. Security Policy Rules are not defined for SecuRemote.

Answer: A

QUESTION 101:

Which of the following statements, about Hybrid Ike, are FALSE? Choose two.

- A. The final packet size is increased after it is encrypted
- B. Only pre-shared secrets or certificates may be used.
- C. SecureClient and Hybrid Ike are incompatible
- D. TCP/IP headers are encrypted along with the payload.
- E. Any authentication mechanism supported by VPN-1/Firewall-1 is supported.

Answer: B, C

QUESTION 102:

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

- A. True
- B. False

Answer: A

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

QUESTION 103:

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

- A. True
- B. False

Answer: A

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

QUESTION 104:

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

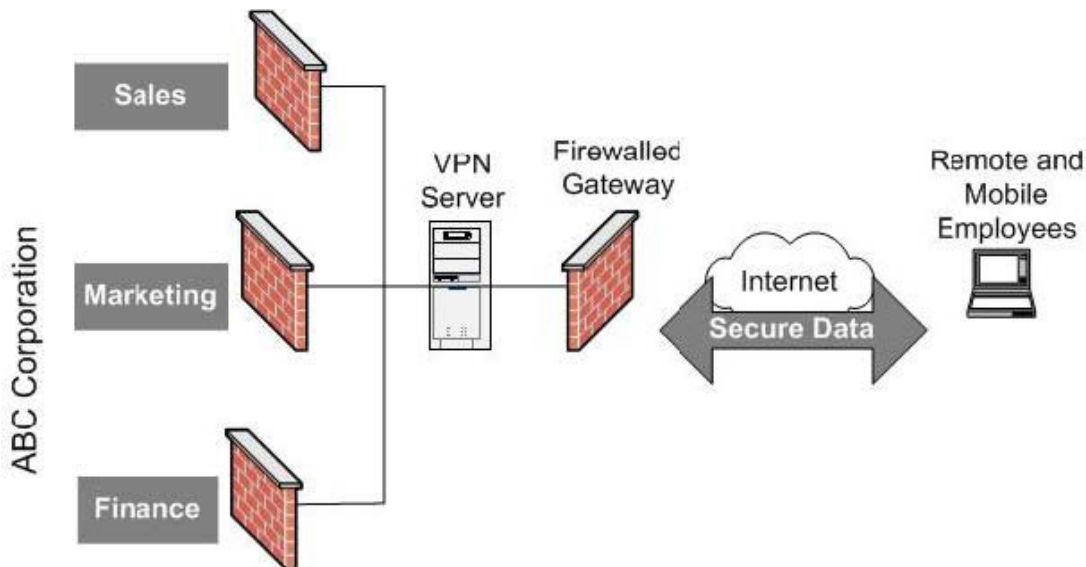
- A. A host IP address, license expiration date, product feature string and license key.
- B. A host IP address, license purchase date, product feature string and license key.
- C. A host IP address, license expiration date, product feature string and Certificate Authority Key.
- D. A host IP address,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

Answer: A

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

QUESTION 105:

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



The type of VPN you would choose is the:

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

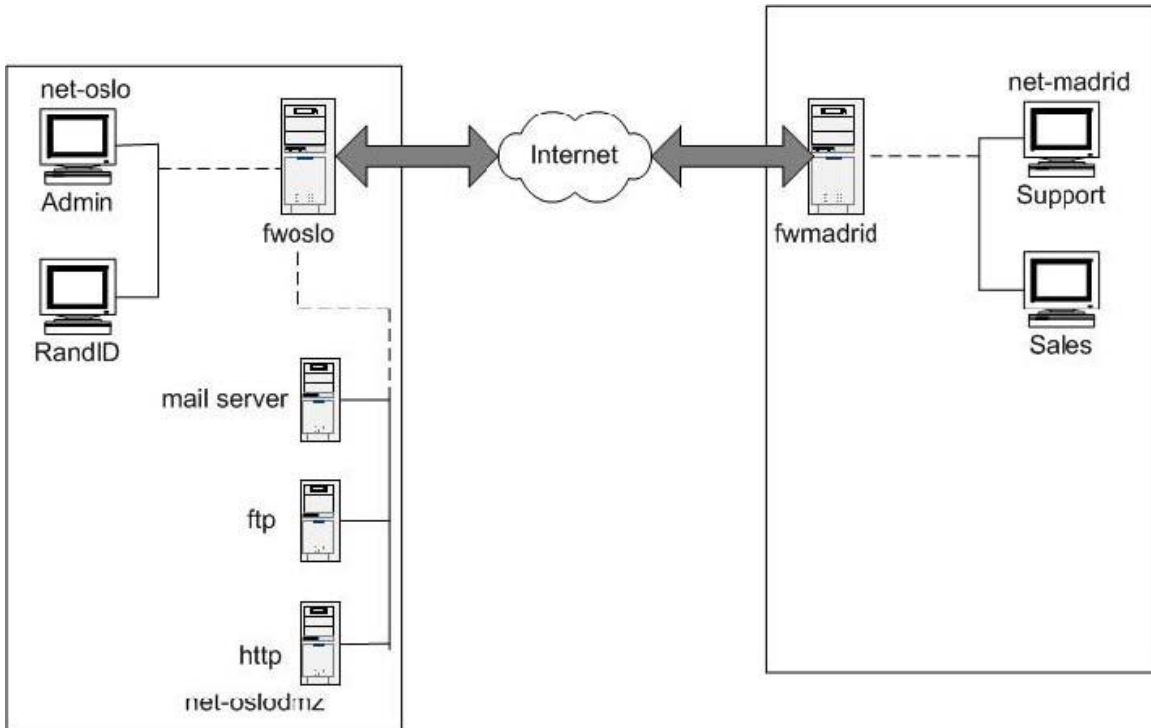
Answer: C

Explanations:

Not B: B is completely inappropriate as an extrant vpn would not satisfy any of the requirements.

QUESTION 106:

You are setting up an IKE VPN between the VPN-1/Firewall-1 modules protecting two networks. One network is using a RFC 1918 compliant address range of 10.15.0.0 and the other network is using a RFC1 818 compliant address range 192.168.9.0. What method of address translation would you use?



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

Answer: E

Explanations: NAT is not required in a IKE VPN unless the two networks are sharing the same address range.

QUESTION 107:

Secure Client supports desktop policies.

- A. True
- B. False

Answer: A

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

QUESTION 108:

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

Portability Standard

Key Management Automatic, external PKI

Session Keys Change at configured times during a connection's life time

Which encryption scheme do you choose?

- A. Rj indal
- B. FWZ
- C. IKE
- D. IKE
- E. Triple DES.
- F. Manual IPSec.

Answer: C

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

QUESTION 109:

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

- A. True
- B. False

Answer: A

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

QUESTION 110:

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

- A. True
- B. False

Answer: B

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

QUESTION 111:

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

- A. True
- B. False

Answer: B

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

QUESTION 112:

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

- A. True
- B. False

Answer: A

Explanations: For each connection that is established through VPN1/Firewall1 Security Server, the administrator controls specific access through the use of Resources from the specified Server. A Resource specification defines a set of entities which can be accessed by a specified protocol, you can define resources based on HTTP, FTP and SMTP. When you specify a resource, the security server will transfer the connection to a VCP or UFP server. See Page 5.4 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 113:

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

- A. True
- B. False

Answer: A

Explanations:

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

QUESTION 114:

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

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

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

Answer: C

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

QUESTION 115:

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

- A. 256-bit.
- B. 168 and 256-bit.

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

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

QUESTION 116:

The Check Point Secure Client packaging tool enables system administrators:

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

Answer: E

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

QUESTION 117:

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

- A. True
- B. False

Answer: B

Explanations: You cannot reinstall the Firewall adapters from a SecureClient by selecting re-bind adapters from the tools menu, you can only re-bind the SecureClients adapters.

QUESTION 118:

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

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

Answer: D

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

QUESTION 119:

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

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

Answer: A

Explanations:

to make this feature available you have to make a registry change in the client machine running secure client. The key is "EnableLogging" and the values are: 1 (Logging enabled) and 0 (Logging disabled). The default is 0 (Disabled).

See "Windows Registry changes" inside the official checkpoint documentation.

QUESTION 120:

The encryption key for SecuRemote connections, for two phase exchange, remains valid by default for _____.

- A. About 15 minutes.
- B. About 30 minutes.

- C. About 45 minutes.
- D. About 60 minutes.
- E. The entire remote user operating session.

Answer: D

Explanations: Phase 1 key exchange happens by default every 1440 minutes (24 hrs) and Phase 2 every 3600 seconds (1 hr).

QUESTION 121:

What is the purpose of HTML weeding when a defining a URI resource?

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

Answer: B

Explanations: As we can see in the "Action" tab of URI Resources Properties of an HTTP scheme, we can use HTML weeding to Strip Script Tags, Strip Applet tags, Strip ActiveX Tags, Strip FTP links and Strip Port Strings. We also have an option to "Block Java Code", it let us strip Java code and block Java applets. We can see this in Figure 10, Page L7.8 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 122:

When using IKE in a Firewall-to-Firewall VPN, _____ is used to manage session keys, encryption method and data integrity.

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

Answer: A

Explanations: RDP was used for FWZ not IKE which uses UDP to manage session keys. FWZ is no longer supported by NG (since FP1).

QUESTION 123:

Before installing VPN-1/Firewall-1 on Windows NT, you MUST confirm that:

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

Answer: A

Explanations: This has always been one of the "must" recommendations from Checkpoint engineers, here is what they say in the official CCSE courseware: "Before installing VPN1/FW1, make sure that your network is properly configured, with special emphasis on routing. Ensure that each of the internal gateways can see each other. See Page 1.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 124:

CRL lookups from VPN-1/Firewall-1 modules, or the SecuRemote Server, to the LDAP Server. When problems occur with CRL verification, how would you verify that the IP addresses and port numbers are correctly referencing the CA and LDAP Servers?

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

Answer: B

Explanations: since we want to see why we can't communicate and obtain the CRL verifications, we need to see if we are making the CRL verifications in the right place, we can check the CA object to see if we are referencing the correct IP address and port number. The CA.INI file will not be helpful in this situation. This is not usually a timeout problem. The CPConfig is not related to CRL configuration, we have to see inside the CA object.

QUESTION 125:

What are the disadvantages of Shared Secret Key encryption?

- A. A secure channel is required by which correspondents can agree on a key before their first encrypted communication.
- B. Correspondents may have to agree on a key by some other fairly secure method, such as by mail or

telephone.

C. The number of keys required can quickly become unmanageable since there must be a different key pair for each pair of possible correspondents.

D. B and C.

E. A, B and C.

Answer: D

Explanations: Since Shared Secret Encryption (Symmetric) only has one key for encrypt-decrypt, you need to use an alternative way to pass the shared secret, in our days, it's usually done by telephone or some secure methods that not involve the channel you are trying to secure. Also, since you need one different key to encrypt-decrypt every connection, the number of keys gets huge in a little time, for example, if we have 10 users trying to communicate between themselves, we have 100 different encryption keys to manage. There is an advantage for this, the encryption is very fast, about 1000 times faster than asymmetric encryption.

QUESTION 126:

An external UFP server, can perform which of the following?

A. Find out java, JavaScript, Active X.

B. Deny or allow access to URLs using categories.

C. Integrate Firewall-1 with an external user database.

D. Check for viruses and malicious contents.

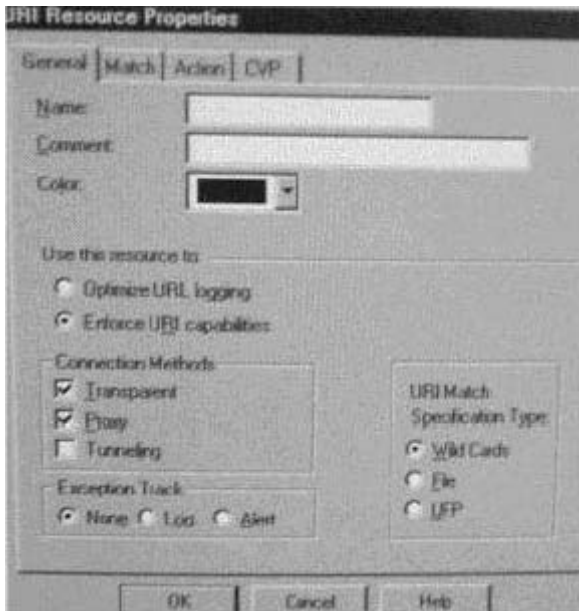
E. All of the above.

Answer: B

Explanations: an UFP external server (URI Filter) it's an OPSEC certified application used for passing data between VPN1/FW1 and a third-party server for URI classification. You can use products like WebSense to achieve the URL filtering functionality through categories. For example you can define that your users cannot go to any sport sites beginning with the letter "B" or that kind of things. See page 318 of Syngress Book "Check Point NG - Next Generation Security Administration".

QUESTION 127:

Which of the following statements best describe the purpose of the Transparent Connection method shown below in the URI Resources Properties window?



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

Answer: A

Explanations: This is what's achieved in the question, if the traffic is not in tunneling or proxy mode, transparent connection will have a match, here is an explanation of them. The connection method options define what mode FW1 will use to analyze traffic, if "tunneling" mode is used you will not have access to CVP tab and you could not use UFP servers. Transparent is used when the user browser does not contain proxy information, in this configuration, the firewall must be your network gateway that handles internet traffic, the firewall will send the traffic to be analyzed in the UFP server. In proxy mode the firewall must be specified in the proxy settings of the user browser.

QUESTION 128:

When SecuRemote Client and Server key exchange occurs, the user will NOT be re-authenticated even if the Password Expires After timer on the SecuRemote Server has not expired.

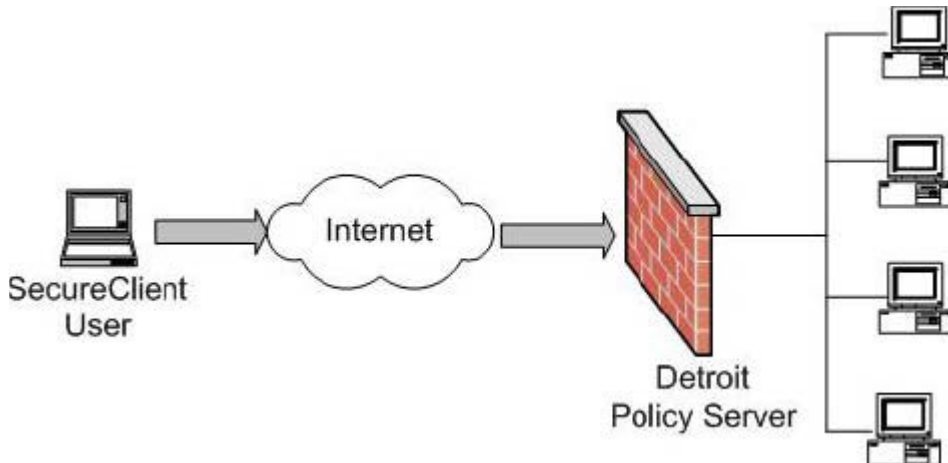
- A. True
- B. False

Answer: A

Explanations: This is true, if the Password expires timer has not expired in the SecuRemote Server, the user doesn't need to be re-authenticated. In the case that the password has expired, re-authentication will be necessary. See Checkpoint Online documentation on "Securemote Key Exchange".

QUESTION 129:

In the following graphic, the remote Secure Client machine does not have an installed Desktop Policy. The Secure Client user tries to connect to a host in Detroit's domain. Because Detroit is a Policy Server.



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

Answer: B
 Explanations: the implicit login occurs when a secure client does not have a security policy installed and tries to communicate through a policy server. The policy server will attempt to install a policy on the desktop. This is initiated by the policy server. See Page 12.19 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1). See also "Figure 9" on the same domain.

QUESTION 130:

In the event that an unauthorized user attempts to compromise a valid Secure Client connection, the Secure Client machine can remain protected by?

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

Answer: B

Explanations: Since we are using Secure Client, we can have a Desktop security policy installed if we have a Policy Server available to download one from. The security policy is installed when a user performs an implicit or explicit login to the policy server from the Secure Client machines.

In case someone tries to compromise a connection, the secure client with a desktop policy installed can block all incoming connections to the host, to keep security in place.

QUESTION 131:

How do determine what version of firewall kernel a customer is using?

- A. Fw ver.
- B. Cp kernel.
- C. Fw ver -k.
- D. Fw kernel -v.
- E. Cp cu -v.

Answer: C

Explanations: the command "fw ver" returns the version of FW1 currently running. By adding the "-k" option you can learn the kernel build as well. See Page 385 from Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 132:

When you select the Pre-Shared Secret check box in the IKE Properties window:

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

Answer: C

Explanations: That's true, Pre-Shared Secret is used when both ends of the VPN lacks access to a compatible certificate server. Once you have defined all the endpoints in your VPN, you can establish a password that is used to authenticate the other end of the connection. (Both ends of the connection must be configured with the same password). See page 323 of "Essential Checkpoint Firewall 1" Book.

QUESTION 133:

What is the Check Point recommended sequence for performing the following operations?

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

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

Answer: B

Explanations: 13452 - Checkpoint recommend that you finish hardening the operating system last so as not to interfere with the installation of the firewall.

QUESTION 134:

To reduce the effectiveness of traffic sniffing inside the LAN, internal users should have the _____ installed in their desktop.

- A. Management
- B. Real Secure.
- C. Enforcement
- D. Policy Server.
- E. Secure Client

Answer: E

Explanations: Since the Secure Client supports a desktop security policy in the host, we reduce traffic sniffing inside the LAN because every Secure Client host can enforce a desktop security policy checking for sniffing activity with counter-measures when necessary. The desktop policies are also very helpful because they provide distributed security in our environment (In the host and in the FW modules).

QUESTION 135:

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

- A. Encryption, inspection, routing.
- B. NAT, traffic control, topology.

- C. Static addressing, cryptosystems, spoofing.
- D. Encryption, authentication, integrity.
- E. DHCP, quality of service, IP pools.

Answer: D

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

QUESTION 136:

If you wish to move any Secure Client files to another directory.

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

Answer: A

Explanations: If you wish to move any Secure Client files to another directory, uninstall, and then reinstall secure client. When the choose destination location screen appears, change the default destination folder to a destination of your choosing. Here is the process: first backup your files, second, uninstall SC, third, reinstall SC, and then, Restore the original files. See Page 12.35 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 137:

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

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

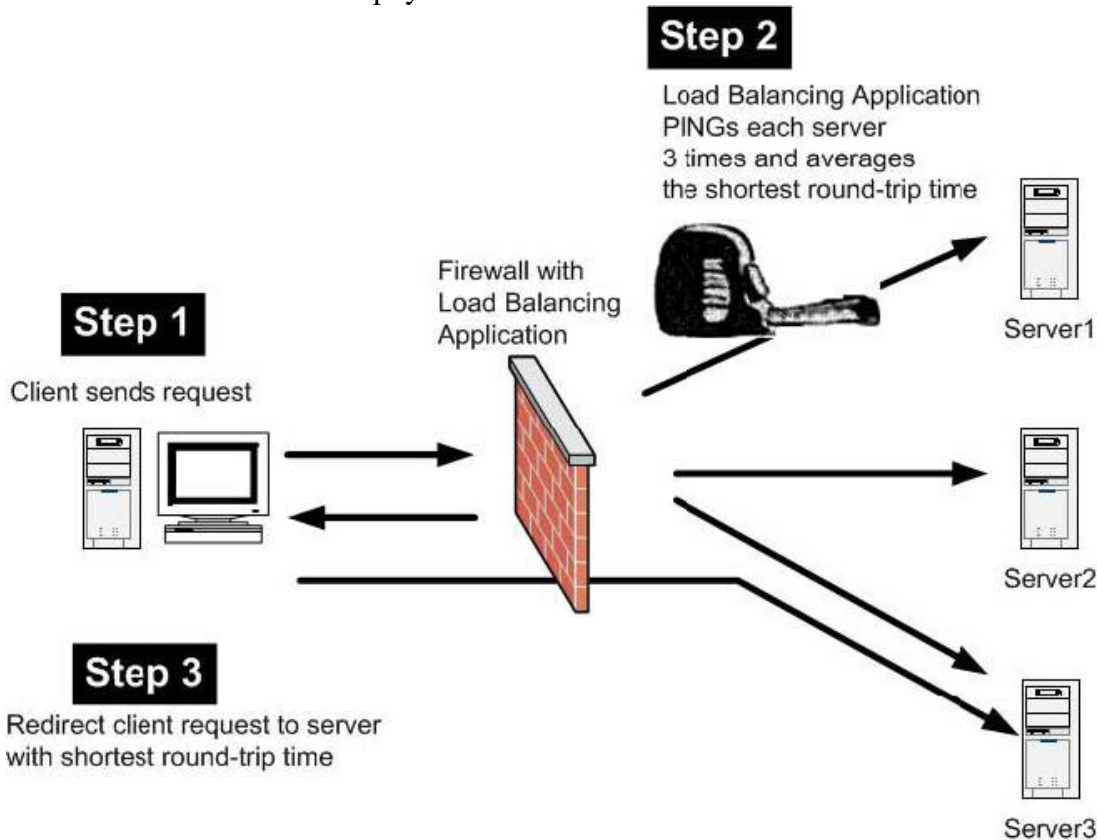
- A. Enterprise Primary Management.
- B. Enterprise Security Management.
- C. Enforcement Module & Primary Management.
- D. Enforcement Module.

Answer: A

Explanations: Since we only want this machine to install policies in the enforcement modules, we have to make it only a management server selecting the option "Enterprise Primary Management". In the case that we would also liked this machine to enforce a security policy, we would had selected "Enforcement Module and Primary Management".

QUESTION 138:

The _____ load balancing algorithm uses ICMP to determine the shortest time to and from the firewall and each individual physical server. It then chooses the server with the shortest time.



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

Answer: C

Explanations: This is one of the load balancing methods provided by Checkpoint, the others are "Server load", "Round Robin", "Random" and "Domain". Here is an example of the process of "Round Trip" load balancing. First, a client send an HTTP communication request the VPN1/FW1 module, then the load balancing application pings all the logical servers that belong to the HTTP service averaging the round trip, and finally,

the application notifies the firewall module which server has the lowest round trip time. The firewall module then send the request to the appropriate physical service. See Page 4.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 139:

Patrick has been hired to devise a security solution for a company that provides in-home care. Visiting Nurses use Internet connections to transmit confidential patient data to a database server located at the corporate office.

The visiting Nurses at the remote locations must have a secure connection to the database server to protect patient confidentiality. The database server itself must also be protected from external threats. The human resources department would like to have access to information about their Nurses access the database server. Accounting would like to offer Nurses the option of submitting their time sheets from remote locations, provided this can be accomplished in a secure manner.

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

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

Answer: B

Explanations: With the Patrick's proposal you can achieve the security of the database server because it is behind the VPN1/FW1 that is in the perimeter in the LAN, the remote communication of the nurses is secure, because they have Secure Client installed on their laptops. The only objective that is not met is the Human Resources department track of the database use, this is because Patrick recommends no logging in the enforcement module.

QUESTION 140:

When using the Load Measuring Agent, you can add a new server without stopping and starting anything. Review the steps listed below and select the response demonstrating the correct order for adding a new server for Load Measuring.

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

- A. 1, 2, 3.

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

Answer: A

Explanations: This is the correct order according to Checkpoint, you should always Install the load measuring agent first, once that is done, you need to add the object to the new server in the existing rule of the rule base, the last step is to reinstall the Security Policy to make your changes effective. If you do not reinstall the policy, the changes do not take effect. The "Load measuring agent" is the FW1 Load balancing component, it's a service running in a configurable port that returns information about the server load. You can see "Load Measuring Agent" in the Online Documentation of NG.

QUESTION 141:

What is the purpose of cplic check?

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

Answer: D

Explanations: The "cplic check" command is a shortcut of "Checkpoint Licensing Check" and its used to validate features on a license, like the VPN capability, the encryption algorithms supported and other capabilities that are obtained through the Key String that comes in the .LIC file. See "cplic check " in the Checkpoint NG online documentation.

QUESTION 142:

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

- A. True
- B. False

Answer: B

Explanations: If you have modified your network configuration by removing the FW1 Adapters, you can reinstall these adapters, without reinstalling secure client, by selecting Re-bind adapters from the tools menu. FW1 can be bound to more than one adapter, in Windows 98 the binding is static and takes place when Secure

Client is installed, in Windows NT / 2000, the binding is dynamic and takes place upon reboot. See Page 12.35 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 143:

Hector is a security administrator for a large, global enterprise that is preparing to implement VPN-1/Firewall-1. In the first phase of the rollout all Enforcement Modules will be installed at a central warehouse before being shipped to the final sites and final set-up. Site-specific information is not available to the warehouse installer. What are the MINIMUM elements Hector must configure to complete Enforcement Module installation?

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

Answer: A

Explanations: as a minimum for the enforcement module installation, you need to have the management server IP address because its necessary to retrieve the configurations and for policy installation, the management module IP address is also necessary to establish a SIC relationship for communications. Your management server is your certification authority, you only need its IP. You don't need passwords, shared secret keys or Security server at this time.

QUESTION 144:

Which of the following statements is FALSE?

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

Answer: C

Explanations: This is false, the policy server itself does not support all the platforms, only the server ones, you can't run a policy server in a Windows NT Workstation or a Windows 9x. Also remember, the policy server is limited to the platform compatibility of the VPN1/FW1 modules. As checkpoint states, the NG components

other than the GUI client, are not supported on client platforms. However a Policy Server supports Secure Clients running on Windows Client Platforms.

QUESTION 145:

Content Vectoring Protocol (CVP), by default uses which TCP? port 10101, and:

- A. 80
- B. 141
- C. 10101
- D. 18181

Answer: D

QUESTION 146:

Paul will be installing all of the components of VPN-1/Firewall-1 on a single machine. Company growth will require moving to a distributed environment as additional Enforcement Modules are added over the next six months. While installing, which option should Paul select to facilitate the transition six months from now?

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

Answer: C

Explanations: at this time, his option is to install both, the management server and the firewall module in the same machine because he will install all the firewall components in one place before the moving to the distributed environment in 6 months, so, at this time, he has to select "Enforcement Module & Primary Management". In the future he should distribute the additional enforcement modules as standalone components to provide the distributed environment.

QUESTION 147:

In the IKE properties window, you can use the Data Integrity drop-down menu to select:

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

- D. The CA checksum method to be used for ensuring data integrity.
- E. The shared-secret checksum method to be used for ensuring data integrity.

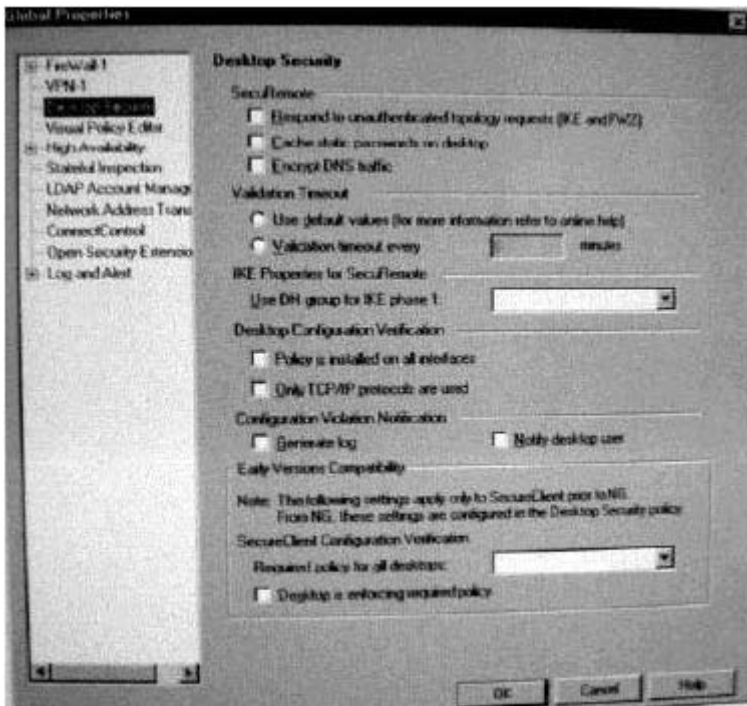
Answer: A

Explanations: This is true, from this drop menu at the properties of IKE you can select how do you want to ensure the data integrity, the integrity is one of the pillars of network security, it provides a guarantee that the information has not changed or tampered with from the source to the final destination. Integrity is usually achieved with digital signatures and algorithms. In IKE VPN's we can use two algorithms MD5 (Message Digest 5) and SHA1 (Secure Hashing Algorithm 1).

QUESTION 148:

You must configure your firewall for Hybrid IKE Secure Client connections. Which of the following fields **MUST** be selected to allow backward compatibility with earlier version of the Secure Client?

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



Answer: E

Explanations: "Respond to unauthenticated topology request", this future enables backwards-compatibility with early versions of Secure Client. The "Require policy for all desktops" option allows system administrators to specify a desktop policy for VPN1/FW1 4.1 clients, the clients will obtain the desktop policy during the key

exchange. The option "Desktop is enforcing required Security Policy" enables only desktops enforcing the Security Policy in Required policy for all desktops to be considered as SCV (Securely Configured). See Page 12.11 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 149:

Your Manager has requested that you implement a policy that prevents users on the network from transferring confidential files out of the intranet using FTP. You also want to check for virus signatures on those files entering the intranet. You setup an FTP resource and add it to the Service field of a rule. You have only redefined the FTP resource and selected the Get option under the Match tab. Does this meet all of the requirements of your manager?

- A. Yes
- B. No

Answer: B

Explanations: this actions do not comply with all the requirements of the question because you want to analyze the FTP traffic for Virus, to achieve this functionality you need to use the CVP protocol in combination with an OPSEC certified Virus Signature Scanning application. Checkpoint NG does not provide Virus Scanning capabilities by default.

QUESTION 150:

Secure Client syntax checking can be used to monitor usersc.C file parameters. The checking is used to prevent errors causing the site, to which it belongs from being deleted.

- A. True
- B. False

Answer: A

Explanations: This is true, as the official CCSE documentation says: "Secure Client performs minimal syntax checking for the usersc.c file. If a parameter is entered incorrectly, the site, to which it belongs, is deleted. No error messages will be displayed". See Page 12.29 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 151:

The Service drop-down menu in the OPSEC Definition Properties window allows you to select a service for communication with a server from the drop-down list.

The service contains the port number to watch the filer server listens. For UFP Server, the service is:

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

Answer: A
Explanations: This can be checked at the Figure 4 "OPSEC Application Properties" of the CCSE NG documentation, Page 9.3, as we can see here, the service to communicate with an external UPF server is "FW1_ufp", at the OPSEC application properties, you also have the option to set backward compatibility options. See Page L9.3 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 152:

You are concerned that an electronically transmitted message may be intercepted and manipulated as if it came from you. This would compromise the accuracy of the communications. To secure the validity of the original message sent, you attach a _____.

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

Answer: E

Explanations: In this case we need a feature of network security known as "Integrity", we need to be sure that the data has not changed from the source to the destination, this could be achieved through the use of digital signatures, Checkpoint provides support for the following algorithms: MD5 and SHA-1. Those can provide the desired functionality.

QUESTION 153:

When designing your company's content security solution, where should you place the CVP anti-virus server for the best performance?

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

Answer: D

Explanations: This is one of the best practices recommended by checkpoint engineers for CVP Certified OPSEC solutions. Since we want the traffic to be analyzed for Virus, we have to transmit much traffic between the servers, if we have a dedicated network just for the firewall and the CVP server, we can have much more throughput, the best practice is to use a crossover cable from the firewall NIC to the UFP server NIC. This method greatly increases performance.

QUESTION 154:

You are using Hybrid IKE. The certificate is not created in the Certificates tab of the VPN-1/Firewall-1 network object; even after "Internal CA created successfully" is displayed "fw internalca create" is displayed as having been issued. Which if the following lists the most likely cause of the problem, and the appropriate remedy?

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

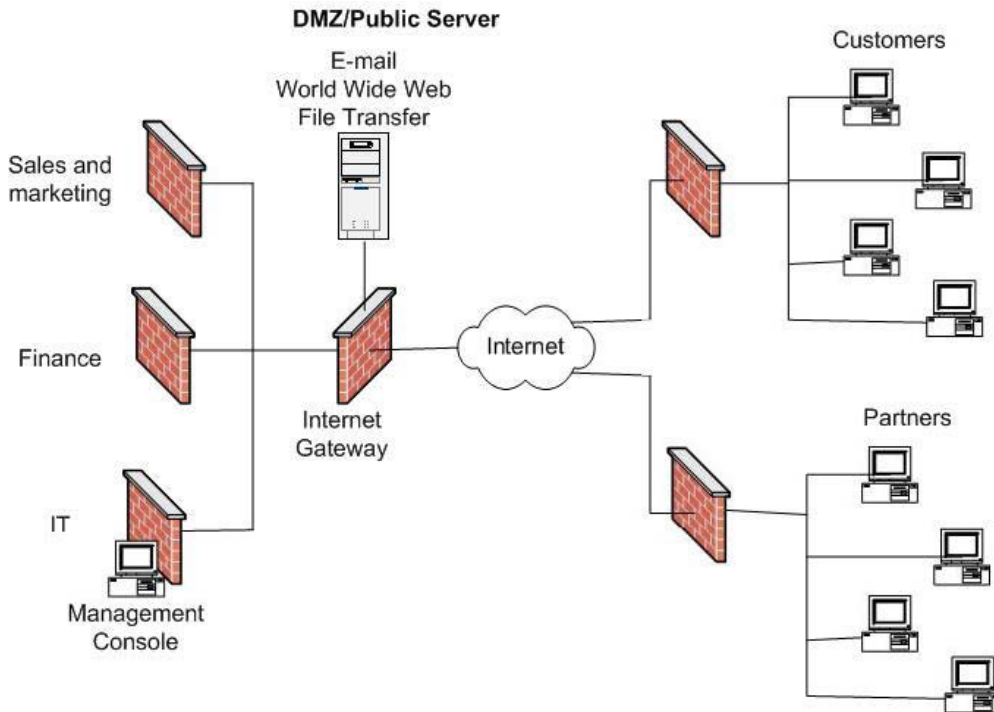
Answer: E

Explanations:

Sadly, the command "fw internalca X" have a length limitation, this could cause some errors, to provide a solution you can stop the firewall services and make some file moving from the \$FWDIR/Conf directory, the exact files are detailed in the documentation, once done, you can run the "fw internalca X" commands with the "-force" option. Check "Troubleshooting CA" in the Checkpoint NG online documentation.

QUESTION 155:

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



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

Answer: B

Explanations: Extranet VPN - Extranet VPNs are designed for Customers and Corporate Partners who manage their own secure firewalls.

QUESTION 156:

TCP services must have a rule in the Policy Editor Rule Base to be used by TCP resources.

- A. True
- B. False

Answer: A

Explanations: Since a TCP resource is a subset of a service running under TCP, we need those TCP services to have a rule entry in the rule base inside the Policy editor. This will allow the TCP resources to use those TCP services. You can check this in "TCP Resource Fundamentals" at the online NG documentation.

QUESTION 157:

User groups need NOT be defined to configure SecuRemote, but are required for the configuration of a Policy Server.

- A. True
- B. False

Answer: A

Explanations:

When we install a policy server, in the workstation properties box, after we have selected the "Policy Server" checkbox in the General tab, we need to configure the policy server, in the authentication tab, we have to select the user at the Policy Server part, we can only select a Group from here, not individual users, this is because the Policy server works exclusively with groups. There is another limitation, you can only select one group. When you define the rules for the policy server, you also have to do it referencing groups. "Each rule must be assigned to one or many user groups", not individual users See Page 12.14 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 158:

SYNDefender Gateway sends a FIN/ACK packet in immediate response to a server's SYN/ACK packet.

- A. True
- B. False

Answer: B

Explanations: This is false, when a SYNDefender Gateway configuration takes place in a checkpoint implementation it will automatically reply "SYN/ACK" packets from clients with an "ACK" packet. When the server receives the ACK packet from the gateway, the connection is moved out of the backlog queue, and becomes an open connection as far as the server is concerned. If the SYNDefender replies with a Fin/ACK as the question states, there will not be any connection, because a FIN/ACK ends TCP sessions. See Page 6.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 159:

What are the two types of HTTP Security Server authentication methods that may be used?

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

Answer: B

Explanations: .The connection method options define what mode FW1 will use to analyze / authenticate traffic, there are 3 methods, Transparent is used when the user browser does not contain proxy information, in this configuration, the firewall must be your network gateway that handles internet traffic, the firewall will send the traffic to be analyzed in the UFP server. In proxy mode the firewall must be specified in the proxy settings of the user browser. The other one is "Tunneling".

QUESTION 160:

You are implementing load-balancing to your Web Server using the Connect Control module. What type of logical server would you specify, if you need to load balance between servers that may not be behind the same firewall?

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

Answer: B

Explanations: the server type to implement should be "Other" because we have the servers behind different firewalls, when we check the option "Persistent Sever Mode" we are forcing that a user session always send all the flow of traffic to the same server, this is necessary in this situation because if the client send data traffic to servers behind different firewalls, the firewall will not expect the connection and will drop it. For load balancing between servers behind different firewalls "Other with Persistent Service mode" is the best option. See Page 4.17 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 161:

Below is the Log and Alert Page of the Global Properties window.

Exhibit missing

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

- A. If they have the same source address, source port, destination port and the same service was used.
- B. If they have the same source port, destination address, destination port and the same service was used.
- C. If they have the same source address, source port, destination port and any service was used.
- D. If they have the same destination address, source address, destination port, and the same service was used.
- E. None of the above answers are correct.

Answer: E

QUESTION 162:

Which position of a URL is sent to a UFP server when using a TCP resource?

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

Answer: B

Explanations: The TCP resource supports all TCP services. This resource allows URL screening via a UFP server. If enabled, the UFP server can provide URL verification without a security server. The full URL is not sent to the UFP server, only the IP address of the remote server. This allows faster transactions to occur since name to IP resolution does not have to take place. See Page 5.22 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 163:

For standard RFC (Request for Comments) compliant IKE VPN's, a user's authentication method should be defined where?

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

Answer: C

Explanations: Since we are talking about RFC compliant IKE VPN's we have to define the authentication at the encryption tab of both, the user and the firewall. This is the practice recommended when talking about RFC compliant IKE (Internet Key Exchange) VPN's. See "RFC compliant VPN" at the online documentation.

QUESTION 164:

When you install the Management Module and GUI Client on a Windows NT Server:

- A. The Windows NT Server in which you install becomes the Management Module and Authentication GUI for the Enforcement Module.
- B. The Administration GUI resides on the Enforcement Module and the Management Module resides on its

own machine.

- C. The Windows NT Server on which you install becomes the Enforcement Module.
- D. The Administration GUI only resided on the Management Module.
- E. The Administration GUI communicated with the Management Module on port 257.

Answer: D

Explanations: This is true, by default, you have to install every single GUI client throughout your network manually, so if you install a management module on an NT, and you install a GUI client in the same machine, the administrator GUI only resides on that machine. In the question and the answers, you never touched another host, so there are not other GUI clients through your network.

QUESTION 165:

The following steps correctly list the actions taken by a Certificate Authority (CA)

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

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

- A. True
- B. False

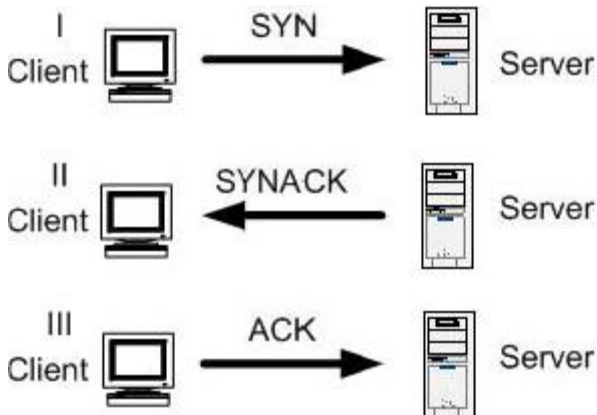
Answer: A

Explanations: You can verify this process in page 8.7 of the Checkpoint CCSE NG Courseware. The sender need to send his/her public keys, they are signed with the private key of the CA (here is the security), this creates a public key for the C

A. With this key and the private ones, the CA creates a certificate. This certificate can validate the sender's public key against the receiver. See Page 8.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 166:

This picture shows a normal three-way TCP/IP handshake.



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

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

Answer: D

Explanations:

This is true, since the 3 way normal handshake process is SYN, SYN/ACK, ACK, the client needs to complete this step to establish the TCP connection. If the user never send this ACK, the gateway running SYNDefender will reset the connection with a RST packet, this is because SYNDefender is not going to leave the connection in waiting state for more than the configured time, if SYNDefender does not reset the connection, your network is vulnerable to the Denial of Service Attack "SYN Flood".

QUESTION 167:

With Secure Client, if you have more than one network adapter: (Choose all that apply)

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

Answer: A, C

Explanations: Here is what the official documentation says "If you have more than one adapter, FW1 can bound to all of them. In Windows 98, the binding is static, and takes place when secure client is installed. On NT/2000, the binding is dynamic, and takes place upon reboot. See Page 12.35 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 168:

Which load-balancing method chooses the physical server closest to the client, based on DNS?

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

Answer: E

Explanations:

With the domain load balancing algorithm, VPN1-FW1 chooses the closest server, based on domain names, This algorithm is useful outside a network, such as when a domain name identifies the location of a remote device. This method is not recommended because it creates a noticeable delay to HTTP requests because of the reverse DNS lookups required. See Page 4.13 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 169:

On which the following operating systems does Check Point support installation of the VPN-1/Firewall-1 Management Server?

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

Answer: A

Explanations: Solaris 2.7 & 2.8 are no longer supported Nor is Red Hat Linux 7.1.

QUESTION 170:

SYN flood attacks are used in the Denial-of-Service (Dos) attacks, or in conjunction with other exploits to block access to a server network.

- A. True
- B. False

Answer: A

Explanations: This is true, the SYN flood attack never completes the third step of the 3 way TCP handshake, it never sends the ACK, this makes the attacked server to allocate memory to connections that will never be completed, with thousands of this uncompleted connections the protocol stack at the server gets and overflow and crash the O.S. The SYN Flood is considered a DoS attack, it can be used in conjunction of other attacks like IP spoofing.

QUESTION 171:

Which of the following statements is FALSE?

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

Answer: D

Explanations: This is wrong, alerts are executed by the "alertrd" process running where the log files are written. The default machine is the management server, but the logs can be directed to other machines, this also makes the answer "D" wrong. If logs are directed to more than one machine, then the "alertrd" process will execute the alert command in every machine containing the logs. See Page 3.6 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 172:

Which command is used to export a group of users from VPN-1/Firewall?

- A. Fw dbexport.
- B. Ldapmodify
- C. Ldabsearch
- D. Ldap export.
- E. fwm dbimport

Answer: E

Explanations: The fw dbimport and fw dbexport commands have been replaced by the fwm dbimport and fwm dbexport commands.

QUESTION 173:

You are using Hybrid IKE. SecuRemote produces the error "Certificate is badly signed". Which of the following lists the most likely cause of the problem, and the appropriate remedy?

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

Answer: D

Explanations: This is a well-known problem with SecuRemote, if you are using Hybrid IKE, you need to upgrade your SecuRemote software at east to 4.1 with SP1, this will make the problem disappear. The problem is caused by the way previous versions of SecuRemote manage the certificate validation and multiple definitions of certificate standards that are provided by the Hybrid Authentication scheme.

QUESTION 174:

The "Man in the Middle" threat consists of the possibility of a third party intercepting the private keys of you and another correspondent, even though you think you're communicating directly with each other.

- A. True
- B. False

Answer: A

Explanations: Yes, when you are suffering a "Man in the middle attack" everything seems to be right with your communication, the problem is that you have an agent in the middle of the communication capturing your information (data, encryption keys). The difference between a "man in the middle" attack and a Session Hijacking is that the first is passive. The "Man in the middle" attack is very difficult to detect.

QUESTION 175:

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

- A. True
- B. False

Answer: AExplanations: Here is the message you get at the installation of VPN1-FW1 in Solaris at the "Configuring Groups" Screen: "Usually, a VPN1 & FW1 module is given group permissions for access

and execution. You may now name such a group or instruct the installation procedure to give no group permissions to the VPN1 & FW1 module. In the latter case, only the Super-user will be able to access and execute the VPN1 & FW1 module.

QUESTION 176:

When you conduct a distributed installation of VPN-1/Firewall-1:

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

Answer: A

Explanations: this is true, here is what the official courseware says: "Checkpoint SVN Foundations NG" is the Checkpoint Operating System that is silently installed with every Checkpoint product. SVN provides a true Secure Virtual Network architecture that provides an integrated framework for deploying and managing an Internet security implementation. See Pages 1.2 and 1.19 of CCSA NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 177:

If the Persistent Server mode check box is selected in the Logical Server Properties window, which of the following is TRUE?

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

Answer: A

Explanations: If selected, "Persistent Server mode" allows some fine-tuning of the load balancing process. When enabled, you can enforce connection persistence, meaning you can force packets from an established flow to continue to a single destination. You can select to 2 modes: "Persistent by service" and "Persistent by server". The relation is client to server, so its the client the one that keeps connecting to the same server. See page 155 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 178:

Which of the following statements is FALSE?

- A. A SYN flood attack is an attack against a service designed to make a server unavailable.
- B. A SYN flood attack exploits the limitations of the TCP/IP protocol.
- C. During SYN flood attack, a client sends a SYN/NACK to a server and data exchange begins.
- D. During a SYN flood attack, a server replies with a SYN/ACK identified by the source IP address in an IP header.

Answer: C

Explanations: This is false, during the attack, the client send "SYN/ACK" packets, if the attacker sends "SYN/NACK" the server will drop the connection and the SYN FLOOD attack wouldn't be successful. Remember that a NACK its a "Not acknowledge", so this cant establish a valid TCP connection.

QUESTION 179:

When a user leaves an organization or when a key is compromised, a certificate must be revoked. The Certificate Authority does this by using and distributing a:

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

Answer: D

Explanations: Here is the information obtained in the CCSE official courseware: "When a user leaves an organization, or when a key is compromised, the certificate must be revoked. The certification authority does this by issuing and distributing a Certificate Revocation List (CRL). Before accepting a certificate, the CRL should be checked to confirm that the certificate has not been revoked. The CRL distribution point is usually a Web Server. See Page 8.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 180:

The internal program, know as alertf, allows an operator to define how many events with in a defined number of seconds before the script is executed.

- A. True
- B. False

Answer: A

Explanations: Alertf is a program that acts as a wrapper for user-defined scripts. It simplifies the process of launching your user defined event by allowing some specific criteria. It does this by enabling you to specify a threshold that must be met in order for your user-defined script to be executed. See Page 400 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 181:

When you connect to a site referenced in your database SecuRemote:

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

- A. True
- B. False

Answer: B

Explanations:

This is false, before step 3, the firewall challenges the user to authenticate him or herself, then the client initiates a key exchange protocol with the VPN1-FW1 module, and finally, SecuRemote encrypts the first packet and transmits it. After this happen, all the from the SecuRemote client to the firewall module encryption domain is encrypted. See Page 11.14 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 182:

You are the VPN-1/Firewall-1 administrator for a company WAN. You want all users to communicate across WAN securely. You must use an encryption scheme that does not change packet size, to allow for better network performance. You must also be able to define the Certificate Authority from your local VPN-1/Firewall-1 Management Module. Which encryption scheme do you choose?

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

Answer: B

Explanations: FWZ support in-place encryption, encrypting the payload portion (data) of the packet and leaving the original TCP/IP headers intact. Because packet size is not increased, in-place encryption allows for better network performance than the provided by IKE encryption. FWZ encryption gets certified

Diffie-Hellman public keys from a trusted certificate authority, the CP Management server. See Page 7.16 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

Note: FWZ is and has not been supported by checkpoint since NGFP1.

QUESTION 183:

SecuRemote operates between the _____ and the _____.

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

Answer: A

Explanations: as stated in the official CCSE courseware: "The SecuRemote client is made up of a kernel module and a daemon. The kernel module is an NDIS driver that is installed between the TCP/IP stack and the adapter in use, and filters all TCP/IP communication passing through the PC. See Page 11.14 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 184:

By default where does VPN-1/Firewall-1 look for a user-defined tracking script?

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

Answer: C

Explanations: As stated in the official CCSE Courseware "The user defined tracking scripts must be placed in the \$FWDIR/BIN folder on the management station. With user defined tracking scripts you can allow the following: custom log filter programs to log screen entries generated by a specific rule, alerts when a complex condition is met, a single rule to generate different types of alarms for different conditions. See Page 3.3 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 185:

Which parameter, of TRUE, will automatically initiate an RDP status query with a gateway to check if it

is still alive?

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

Answer: C

Explanations: if true, secure client will automatically initiate an RDP status query with a gateway to see if it is still alive. If false, secure Client will postpone sending the query until that information is actually needed - in which case the user may experience some delay. See Page 12.28 of CCSE NG Official Courseware.

(VPN1-FW1 Management II NG FP-1).

QUESTION 186:

The Secure Client packaging tool installation generates a self-extracting auto-running executable file by saving SecuRemote properties on the Management Server and applying the properties to and open (unzipped) SecuRemote installation folder.

- A. True
- B. False

Answer: A

Explanations: As stated in the official CCSE Courseware, the SecuRemote properties are saved on the management server, and are then applied to an open SecuRemote installation folder, generating a self-extracting, auto running executable file. Customizing SecuRemote installations simplifies and standardizes the installation of SecuRemote, and makes the process user-friendly. See Page 12.41 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 187:

You are a firewall administrator using SecuRemote. You are providing digital signatures to achieve both data integrity checking and verification of sender. Certificates are possible when using _____.

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

Answer: B

Explanations: if we need to use certificates, we will have to use IKE, as the name says "Internet Key Exchange"

will be the vehicle to obtain the certificates, because IKE is the one in charge of changing the different keys provided to use and validate certificates. See IKE definition in the Checkpoint Online documentation.

QUESTION 188:

Some VPN-1/Firewall-1 tracking options generate log entries and trigger executables. These executables take the form of:

- A. User-defined executables in \$FWDIR/local.
- B. SNMP traps, or other functions defined by security engineers, EXCEPT socket-based applications.
- C. SNMP traps, alert emails, or other functions defined by security engineers.
- D. User-defined JAVA scripts in \$FWDIR/bin
- E. SMS traps, alert emails, or other functions defined by security engineers.

Answer: C

Explanations: Tracking is the process of creating definitions in which the parameters of an alert or log are established. Tracking occurs when an option is defined in the track column of a rule in the rule base, as well as when an object is defined. Certain tracking options will just generate a log entry, viewable in the log viewer, while other tracking options will generate a log entry and trigger an executable. These executables can take the form of an SNMP trap, sending an alert e-mail, or any other function that a security engineer can define. See Page 3.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 189:

You are using a 56-bit encryption key called DES. Your client is concerned that this is insufficient security. You reconfigure the VPN to use the strongest encryption used by the VPN-1/Firewall-1 software. Which of the following would you use?

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

Answer: A

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

QUESTION 190:

The functionality of the VPN-1/Firewall-1 architecture can be divided between which workstations?

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

Answer: C

Explanations: Those are the 3 principal components, we use the policy editor as an interface to our security policy and a centralized configuration point, the management server, that stores and provides the security policies, user databases, logging & tracking functions, and finally the enforcement modules, that contain the inspect engines, where all the traffic is analyzed and forced to comply with the enterprise security policy.

QUESTION 191:

Respond to unauthenticated topology requests (IKE and FWI) on the Desktop Security screen in Global Properties allow backward compatibility with earlier versions of the SecuRemote /Secure Client.

- A. True
- B. False

Answer: A

COMMENT: This setting instructs the firewall to respond to topology requests from remote workstations running SecuRemote / Secure Client, even if the requested does not come over an encrypted connection. Only previous versions of SecuRemote and Secure Client require this option, is you have actual clients, better disable it for stronger security. See page 458 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 192:

You are working with a Windows NT server running the Check Point VPN-1/Firewall-1 software. Which if the following radio button options would you select from the Server Setup Properties window to configure the connect memory strategy for this configuration?

- A. Minimize memory used.
- B. Balance
- C. Maximize Throughput File Sharing.

- D. Maximize Throughput for Network Applications.
- E. Make Browser Broadcast to LAN Manager 2.x Clients.

Answer: D

Explanations: This is an operating system configuration, since we are going to run a Checkpoint firewall in this Windows NT server, the best option for the memory management and priorities is "Maximize throughput for Network Applications" because it will provide priority for the firewall software over the File/Print sharing capabilities of Windows NT. This will greatly increase performance.

QUESTION 193:

The Solaris command to install the Enforcement Module software without using the Installation Wrapper is:

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

Answer: B

Explanations: To install an enforcement module without the wrapper in a Solaris environment you have to use the command "pkgadd -d" to begin the installation. You must install the SVN foundation package prior to installing any other modules in the system. However, you can install Management clients without the SVN foundation. See Page 96 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 194:

When installing the Secure Client packaging tool, users must define their VPN-1/Firewall-1 sties.

- A. True
- B. False

Answer: B

Explanations: As stated in the official CCSE Courseware, "Customizing SecuRemote installations simplifies and standardize the installation of SecuRemote, and makes the process user-friendly. The SecuRemote user only has to install the package they are given, and then reboot. They do not have to define the NG site, and they are prompted fro authentication if needed. See Page 12.41 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 195:

The following URL specification blocks access to the /warez/illegal.html
204.32.38.254/warez/illegal.html 1

- A. True
- B. False

Answer: B

Explanations: This is false, this is not the syntax used to make the URL screening by file. You cannot put the site and the path together in your definition, you have to separate the site, the path and the hex character with a tab like this.

Example: 204.32.38.254 /warez/illegal.html 1

See Page L8.1 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 196:

In a fully overlapping encryption domain with two gateways serving the domain which one will a SecuRemote client connect to?

- A. It is preconfigured
- B. The first to reply
- C. They are chosen alternately
- D. The nearest

Answer: B

Explanations: This is a not very basic situation, in the case you have 2 gateways with 2 overlapping encryption domains, the SecuRemote Client connects to the first firewall to reply to it. You can check this looking at "Overlapping encryption domains & SecuRemote issues" in the NG online documentation. You can also have a look at the "SecuRemote" chapter of the official CCSE NG Courseware.

QUESTION 197:

What is the default port for a standard LDAP connection?

- A. 389
- B. 636
- C. 1024
- D. 23

Answer: A

Explanations: The "Lightweight Directory Access Protocol" is used for a bevy of purposes. With regards to Firewall-1, this server object is used for the purposes of user management. You can verify that the LDAP port is 389 at the properties of the LDAP Accounting Unit in Policy Editor (You have to see the "port" field in the general tab). To create a LDAP account unit in policy editor, go to "Manage | Servers | New | LDAP". See page 291 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 198:

What is an incorrect minimum requirement for a SecuRemote PC running Windows 2000?

- A. 6 Mbytes spare disk space
- B. 24 Mbytes memory
- C. Microsoft TCP/IP support
- D. 32 Mbytes memory

Answer: B

Explanations: This can be checked at the Microsoft Website, you need a very minimum of 32Mb of memory running in your PC to run Windows 2000, Checkpoint and Microsoft recommend 64MB as a minimum. Remember, 32MB of RAM is the very minimum amount to run Windows 2000, just to load the OS and something else. Windows 2000 won't run in a PC with 24MB, or at least Microsoft engineers says it won't.

QUESTION 199:

In which tab of an SMTP definition screen would you specify the maximum size of an email to be allowed through when using content security?

- A. General
- B. Match
- C. Action 1
- D. Action 2

Answer: D

Explanations: As stated in the official CCSE Courseware, you can configure an option called "Do not send mail larger than XX KB" in the "Action 2" tab of the SMTP Resource Properties. From this tab, you can also strip mime types and certain attachment from the message by name. You can check this in Figure 11 at page 10.8 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 200:

How many attack types can be monitored by CPMAD?

- A. 6
- B. 7
- C. 8
- D. 9

Answer: C

Explanations: "Check Point Malicious Activity Detection" (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities across a range of firewall modules. It can be used to detect 8 types of attacks, they are: syn attacks, anti spoofing, successive alerts, port scanning, blocked connections port scanning, login failure, successive multiple connections, land attack. See page 406-407 of Syngress

Book "Checkpoint NG - Next Generation Security Administration".

Note: CPMAD has been replaced by SmartDefense which currently protects against many more than 8 types of attack.

QUESTION 201:

Which load balancing algorithm uses pings to determine the best server to use?

- A. Server load
- B. Domain
- C. Round trip
- D. Round robin
- E. Random

Answer: C

Explanations: This is one of the load balancing methods provided by Checkpoint, the others are "Server load", "Round Robin", "Random" and "Domain". Here is an example of the process of "Round Trip" load balancing. First, a client send an HTTP communication request the VPN1/FW1 module, then the load balancing application pings all the logical servers that belong to the HTTP service averaging the round trip, and finally, the application notifies the firewall module which server has the lowest round trip time. The firewall module then send the request to the appropriate physical service. See Page 4.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 202:

How would a Secure Client user log onto the policy server? (Choose all that apply)

- A. Click on the shortcut icon.
- B. Pull down the file menu and click on login.
- C. Pull down sites menu left click on policy server.
- D. Pull down the policy menu and select "login to policy server".

Answer: A, D

Explanations: You can login to a policy server from two places, the first is the icon in the far right of the Toolbar (Login to Policy Server), and the second is in the policy menu of Secure client, the option is "Login to policy server".
See Page 12.23 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 203:

Which is NOT an icon present on the top left SecuRemote desktop screen?

- A. Sites/make new
- B. Sites/connect
- C. Sites/delete
- D. Sites/properties

Answer: B

Explanations: this is the only invalid option, if you go to the SecuRemote GUI and pass your cursor through the different icons you will see that we have "make new site", "delete site", "site properties", what we don't have is "Connect to Site". You can also check this in the online NG documentation, see "SecuRemote GUI".

QUESTION 204:

Which is NOT a valid parameter in the userc.C options section?

- A. keepalive
- B. fwm_encrypt
- C. encrypt_resolver
- D. encrypt_db
- E. resolver_ttl

Answer: C

Explanations: from the above list this is the only invalid parameter, the "keepalive" specifies whatever the VPN

modules maintain session key information for Secure Client, "fwm_encrypt" enables secure client encryption for GUI Client-Server communications, "encrypt_db" will obscure topology information in the secure client database and "resolver_ttl" defines the number of seconds Secure Client will wait for a reply on an RDP status query before concluding that the gateway is unavailable. See Page 12.28 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 205:

What does CPMAD stand for?

- A. Checkpoints multiple access denial
- B. Checkpoints malicious activity detection
- C. Checkpoints malicious attack denial
- D. Checkpoints memory attack detector

Answer: B

Explanations: "Check Point Malicious Activity Detection" (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities across a range of firewall modules. It can be used to detect 8 types of attacks. See page 406-407 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 206:

Which is NOT a valid content security function under the HTML weeding category in a URI definition action tab?

- A. Strip applet tags
- B. Strip script tags
- C. Block Java code
- D. Strip ActiveX tags

Answer: C

Explanations: The "Block Java code" option is not part of HTML weeding, it is part of "Response Scanning", You can see this the "Action" tab at the properties of an URI Resource. The HTML weeding options available are: "Strip Script Tags", "Strip applet tags", "Strip Active X tabs", "Strip FTP links" and "Strip Port Strings". See Figure 10 in Page L7.8 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 207:

Which of the following is classed as a strong encryption algorithm?

- A. DES
- B. FWZ-1
- C. 3DES
- D. CAST

Answer: C

Explanations: 3DES addresses the security concerns resulting from the relatively short 56-bit key used by DES. Triple DES encrypts under three different DES keys in succession equivalent to make the DES Key length 3 time larger to 168 bits. For this functionality 3DES is considered a "Strong" encryption algorithm. See Page 7.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 208:

Which CVP anti-virus options are available? (Choose all that apply)

- A. None
- B. Read only
- C. Read/write
- D. Write only

Answer: A, B, C

Explanations: "Write Only" its not a valid option, the 3 valid options are: "None" (no antivirus checking is performed), "Read only" (A retrieved file is checked for viruses. If the file contains a virus, it is not retrieved , and finally "Read/Write" (A retrieved file is checked for viruses. Detected viruses are removed and the file retrieval continues). See Page 5.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 209:

SecuRemote uses a site-to-site VPN type. True or false?

- A. True
- B. False

Answer: B

Explanations: This is absolutely false, since SecuRemote is engineered to provide Desktop secure connections from remote places, SecuRemote uses "Client-to-Site" VPN's, for example, a user traveling through the country with his laptop needing access to the corporate intranet. With SecuRemote, he can connect to Internet and create a VPN from his laptop to access his headquarters, what type of VPN?, a Client-to-Site one.

QUESTION 210:

What is NOT true about LDAP?

- A. The LDAP server is a module within Firewall 1.
- B. It is a standard protocol.
- C. FW1 uses AMC to configure accounts on an LDAP server.
- D. It is based on a client/server model.

Answer: A

Explanations: This is false, LDAP functionality is implemented in conjunction with an external server. What you create inside the policy editor is an "LDAP Account Unit", but the real server with user information is external, it's not within FW1. An example of external LDAP servers is a Microsoft Active Directory implementation, Active Directory is based in LDAP and it's accessed through port 389. In the properties of the LDAP Account Unit inside the Policy Editor, you can select the host, port, Login, password and your rights inside the external LDAP server.

QUESTION 211:

Reply packets to a SecuRemote client must be routed through the same encrypting gateway that received the incoming packets. True or false?

- A. True
- B. False

Answer: A

Explanations: This is true, this behavior is needed because the negotiation of the encryption keys was made with that gateway, so if you reply packets to the SecuRemote client through another gateway that is not the original one, it will not know how to encrypt the information to make it valid for the SecuRemote client. It's an encryption matter.

QUESTION 212:

When a Secure Client user logs on the password is remembered by the daemon. How long will the password be remembered?

- A. Until the next reboot.
- B. For ever.
- C. Until a new policy is loaded.
- D. Until a connection to another site is made.

Answer: A

Explanations: As stated in the official CCSE NG Documentation, "Because the passwords are stored in the secure client daemon, instead of being written to disk, they are erased when you reboot. There are two ways a user can set a password for a site, before attempting to make a connection, setting a password and enabling "Single sign on". See Page 12.31 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 213:

When configuring an ARP entry in an windows server running a FW1. Which is the correct method?

- A. Add an entry into \$FWDIR/state/local.arp of the form <IP address> <TAB> <External Mac address> and restart the server.
- B. Add an entry into \$FWDIR/state/local.arp of the form <External Mac address> <TAB> <IP address> and restart the server.
- C. Add an entry into \$FWDIR/state/arp.txt of the form <IP address> <TAB> <External Mac address> and restart the server.
- D. Add an entry into \$FWDIR/state/local.arp of the form <IP address> <TAB> <External Mac address>

Answer: A

Explanations: There are times where you will need to add static NAT entries, however, NT does not allow this via the arp command, and so you must edit the file \$FWDIR/Conf/Local.arp. In this file, a line is as follows:
Translated IP MAC Address.

On Windows and Solaris, you can display a list of current ARP entries by issuing the command "arp -a". See Page 235 of Syngress Book "Check Point NG - Next Generation Administration".

QUESTION 214:

Which logical server type hides the address of the real servers from the clients?

- A. HTTP redirect
- B. Other
- C. NAT redirect
- D. HTTP NAT

Answer: B

Explanations: neither A,C or D are valid types of servers used to hide addresses by clients. You can hide the real address of a server by using NAT (either Static or Dynamic), but there is no a "NAT redirect" server.

QUESTION 215:

When AMC initializes if there is a red X against the LDAP server (account server) what does this mean?

- A. It means that the account server is not functioning.
- B. It means that the account server is read only.
- C. It means that the account server has not been created in the AMC.
- D. It means that the account server is not accepting commands from this AMC.

Answer: C

Explanations: according to Checkpoint NG online documentation, this could happen when we have not the account created for the LDAP server in the AMC. This red X, is a clear indicator that your configuration is not complete. See "Troubleshooting AMC" at the online Checkpoint NG documentation.

QUESTION 216:

Before configuring a new user, group or organizational unit in an LDAP server which of the following should be done?

- A. Disable schema checking and restart the LDAP server and AMC.
- B. Enable schema checking and restart the LDAP server and AMC.
- C. Disable schema checking but do not restart the LDAP server and AMC.
- D. Enable schema checking but do not restart the LDAP server and AMC.

Answer: A

Explanations: in LDAP implementations, its always better to disable the schema checking of the directory

before adding objects to it. This is because the object creating can provide some "refresh" problems in the directory as a whole. For this reason, its better to disable the checking of the schema. Once you are done with the creation of the objects, you should restart the LDAP server and the AMC to make the new objects effective, and make the "refresh" process in a correct fashion.

QUESTION 217:

What does LDAP stand for?

- A. Long Distance Access Protocol
- B. Lightweight Directory Account Provisioning
- C. Limited Directory Account Protocol
- D. Lightweight Directory Access Protocol

Answer: D

Explanations: LDAP or "Lightweight Directory Access Protocol" are becoming popular in the midsize to large enterprise as a way to centrally store and manage information about people, place, things. FW1 allow you to utilize information stored in an LDAP server as well as store FW1 specific data there. See page 158 of Book "Essential Checkpoint Firewall 1" from Dameon Welch.

QUESTION 218:

MD5 is the only data integrity method applicable to the IKE scheme. True or false?

- A. True
- B. False

Answer: B

Explanations: In this case we need a feature of network security known as "Integrity", we need to be sure that the data has not changed from the source to the destination, this could be achieved through the use of digital signatures, Checkpoint provides support for the following algorithms in combination with IKE VPN's: MD5 and SHA-1. Those can provide data integrity. See the properties of you IKE VPN for the configuration of this options.

QUESTION 219:

What version of VPN1/FW1 introduced Secure Client?

- A. 2.1
- B. 3.1
- C. 4.1
- D. 5.1

Answer: C

Explanations: This is true, the first version of Secure Client was provided with VPN1/FW1 4.1. If you search the checkpoint web site about Secure

Client, you will see that you can't get a version earlier than the one that was provided with VPN1/FW1 4.1. You can also see that earlier compatibility is only provided for 4.1 version.

QUESTION 220:

Which is NOT a method to "hide" a rule in the rule base?

- A. Click on the rule to be hidden, select the EDIT pull down menu and click on "Hide rule".
- B. Right click on the rule and select "Hide rule".
- C. Click on the rule to be hidden, then from the RULES pull down menu select HIDE and check "hide".
- D. Click on the rule to be hidden, select the MANAGE pull down menu and click on "Hide rule".

Answer: D

Explanations: You can check this right in your policy editor application. With the manage menu you cannot disable rules, there is not option

available to achieve this. The other 3 method exposed in the question possible answers are valid. A hidden rule is replaced with a Thick, gray divider

line, giving you an easy visual indication that a hidden rule exists.

QUESTION 221:

Which encryption method(s) are supported by SecuRemote client pre-version 4.0?

- A. IKE
- B. FWZ
- C. SKIP
- D. CAST

Answer: B

Explanations: Since FWZ or "Firewall 1Encryption" is the proprietary Checkpoint encryption scheme, it was the first to be supported by

SecuRemote. In checkpoint NG, you can use FWZ with the FWZ1 (Checkpoint proprietary symmetric encryption algorithm, It uses a 40 bits key length) and DES encryption algorithms, and, as a Authentication algorithm, it can use MD5. See Page 7.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 222:

When you first connect to a certificate authority you get a warning message because the transaction to get the CA public key cannot be authenticated. What should you do?

- A. Your CA has been spoofed take appropriate action.
- B. Reject the key and try again, it will probably be OK next time.
- C. This is normal, you may want to verify the key over the phone.
- D. Reconfigure your firewall to correct the error.

Answer: C

Explanations: This is an absolutely normal behavior, since you are connecting for the first time to the certification authority it will display this kind of warning message, so you may want to verify the keys over another alternative communication method, this could be the phone, a FAX or something else. This warning message will not appear again the next time you connect to the certification authority.

QUESTION 223:

Which of the following protocols open back connections on another port to that which the initial connection is made as part of the normal progression of the connection? (Choose all that apply)

- A. FTP
- B. RSH
- C. Telnet
- D. SMTP

Answer: A, B

Explanations: A clear case of this behavior is the FTP protocol, because it uses 2 ports in parallel, it uses port 21 for the connection control on port TCP 21 and it use port TCP 20 for the actual data transfer. With FTP we begin the connection in port 20 TCP and with the progression of it, the port 20 TCP is also open as a back connection. This behavior is also true with the "RSH" protocol, obviously using other ports than FTP.

With telnet and SMTP, we only use 2 ports for the whole protocol functionality at all times. They are port 23 TCP for telnet and port 25 TCP for SMTP.

QUESTION 224:

What parameters are available on the SYNDefender screen of global properties to tune SYNDefender operation? (Choose all that apply)

- A. Maximum retries
- B. Maximum sessions
- C. Time out
- D. Block source

Answer: B, C

Explanations: This are the 2 configurable options in the global properties relating to SynDefender. "Timeout for SYN attack identification"

specified how long VPN1/FW1 NG waits for an acknowledge from the client, before terminating the connection. "Maximum protected sessions"

specifies the maximum number of protected sessions from one connection. The maximum sessions allowed are the number of pending sessions

VPN1/FW1 NG allows outside the network.

See Page 6.12 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 225:

Which of the following is NOT true about a SEP VPN?

- A. All gateways must be on the same platform.
- B. All gateways must be running the same software version.
- C. All gateways must have the same hardware configuration.
- D. The management server cannot be on the same host as a gateway.

Answer: C

Explanations: "Single Entry point" VPN's enable your enterprise to deploy a solution that protects critical elements of the network. Before you go about configuring SEP VPN solutions, you need to make sure that gateway clusters are enabled on the management server, remember that this will be a cluster. There is a limitation for the creation of SEP VPN's, it's the Hardware configuration, it must be the same. See page 488 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 226:

Secure Client requires that the client is a remote access workstation. True or false?

- A. True
- B. False

Answer: B

Explanations: Here is what the official CCSE NG documentation says, "Checkpoint VPN1 Secure Client extends security to the desktop by enabling the enforcement of a security policy in computer desktops both inside and outside the local area network. Secure Client and the Policy server protects servers and desktops from both external and internal attackers with enforceable security policies to the desktop. See Page 12.1 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 227:

Which port does CPMAD use for communication to an LEA server?

- A. 18181
- B. 18182
- C. 18183
- D. 18184

Answer: D

Explanations: This can be checked in the Checkpoint NG online documentation, CPMAD is a piece of software that allows the NG logs to be analyzed in the search of patterns of some well-known network attacks. CPMAD establish communication with the LEA through port 18183 TCP. LEA means "Log export API", it allows applications to access information contained in the Checkpoint NG logs, CPMAD needs this for the analysis.

QUESTION 228:

What are valid advantages of binding a Secure Client user id to an IP address? (Choose all that apply)

- A. It prevents spoofing.
- B. It ensures that the user does not have more than one session active.

- C. When a user connects from a different IP address than last time then it forces re-authentication.
- D. The same user can connect from more than one workstation.

Answer: C, D

Explanations: With the binding of a user ID to an IP address, you can force re-authentication when a user connects from another machine, this is because the binding will not match, this feature can increase security. Another benefit is that the user can connect from different workstation in a secure fashion because the binding functionality provides re-authentication as stated above. See "Secure Client Binding" in the Secure Client Documentation.

QUESTION 229:

What is a trusted third party from which a public key can be reliably obtained?

- A. Key repository
- B. Certificate authority
- C. Key store
- D. Certificate database

Answer: B

Explanations: A certificate Authority, or CA, is a trusted third party from whom a public key can be obtained reliably, even via the Internet. The CA certifies a public key by generating a certificate. A digital signature acts as a proof of the sender's identity. The certificates security is based on: the access difficulty of the physical machine that stores the certificate and the secrecy of the access password. See Page 8.1 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 230:

Which of the following is NOT a CPMAD global configuration parameter, ie is specific to a particular alert?

- A. MAD_system_mode
- B. MAD_successive_alerts_mode
- C. MAD_memory
- D. MAD_clean_interval
- E. MAD_number_of_connection_attempts
- F. MAD_interval_between_connection_attempts

Answer: B

Explanations: Option B is not a global configuration parameter for CPMAD, the global configuration is changed through "cpmad_confir.conf" file,

all the other parameter are valid in this file. The "MAD_system_mode" enables and disables CPMAD, "MAD_memory" is the amount of memory in bytes allocated to the MAD process. "MAD_clean_interval" define the amount of time that old attacks will be stores in MAD memory tables. "MAD_number_of_connection_attempts" define the number of times MAD will try to reconnect either to the LEA or ELA server, and "MAD_interval_between_connection_attempts" defines the wait period between those reconnection attempts. See Page 408-409 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 231:

Which port does UFP use?

- A. 18182
- B. 18181
- C. 389
- D. 636

Answer: A

Explanations: As stated in appendix C, in the page C.4 of the CCSA NG Official documentation (Course Management I NG FP-1) the port used for UFP is the TCP port 18182. UFP is the "Uri Filtering Protocol" used to provide content security and URL address classification with the use of external UFP OPSEC applications.

QUESTION 232:

Which encryption algorithm is NOT supported by VPN1/FW1?

- A. FWZ
- B. DES
- C. Triple DES
- D. AES
- E. CAST

Answer: A

Explanations: FWZ is not an encryption algorithm, FWZ is one of the 2 Checkpoint NG encryption schemes, an encryption scheme uses encryption algorithms, FWZ supports DES and FWZ-1 as encryption algorithms. Checkpoint NG supports the following encryption algorithms with IKE and FWZ in combination: DES, 3DES, AES, CAST, FWZ-1. See Page 7.10 of CCSE NG Official Courseware.

(VPN1-FW1
Management II NG FP-1).

QUESTION 233:

If you want to set up a virus scanner for FTP files in firewall-1 how would you do it?

- A. In the match tab of the FTP resource definition.
- B. In the action tab of the FTP resource definition.
- C. In the CVP tab of the FTP resource definition.
- D. In the general tab of the FTP resource definition.

Answer: C

Explanations: You have to use the "CVP tab" in the properties of the resource, from there you can select the option "Use Content Vectoring

Protocol" and specify a CVP server. You can also specify if the CVP server is allowed to modify the content and how is the reply order going to be managed. You do not specify the CVP use neither in the match, action or general tab of the resource. See Figure 12 in Page L10.9 of

CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 234:

What is NOT a function of RDP in the FWZ encryption scheme?

- A. Transporting the encrypted data
- B. Out of band session
- C. Negotiating session keys
- D. Agreeing encryption algorithms
- E. Negotiating MD5 usage
- F. Recovering dropped UDP packets

Answer: A

Explanations: RDP or "Reliable Datagram protocol" is used to manage VPN session keys (Negotiating session keys, Out of band sessions), encryption method (Agreeing encryption methods) and data integrity (Negotiating MD5 usage, recovering UDP dropped packets). RDP is not in

charge of the actual transfer of the encrypted data. See Page 7.16 of CCSE NG Official Courseware. (VPN1-FW1
Management II NG FP-1).

QUESTION 235:

What is the name given to a denial of service attack that consumes resources on a device by creating too many unacknowledged TCP sessions?

- A. Syn flooding
- B. TCP flooding
- C. Ack flooding
- D. Ack attack

Answer: A

Explanations: This is an attack against a service designed to make the server unavailable. The attack exploits the limitations of the TCP/IP protocol.

A client initiates a TCP connection to a server via a request with the SYN flag set in the TCP header, the server tries to contact the source with a

SYN/ACK but the real host is unavailable, this makes the 3 way handshake process incomplete. When multiple Syn attacks floods a server, the

server will spend all of its time trying to acknowledge these connections, and be unavailable to process legitimate requests. See Page 6.4 of

CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 236:

Which port does CVP use?

- A. 18182
- B. 18181
- C. 389
- D. 636

Answer: B

Explanations: As stated in appendix C, in the page C.4 of the CCSA NG Official documentation (Course Management I NG FP-1) the port used for

CVP is the TCP port 18182. CVP is the "Content Vectoring Protocol" used to provide content security and scanning of content with the use of

external CVP OPSEC applications. Its most common use is virus scanning.

QUESTION 237:

Which form of overlapping encryption domain is described as one gateways' encryption domain being fully

contained within another gateways' encryption domain?

- A. Full overlap
- B. Partial overlap
- C. Proper subset

Answer: C

Explanations: This is the proper term for this situation, a VPN encryption domain is a group of networks or hosts behind a firewalled gateway that participate in a VPN. Any traffic coming from one VPN domain and going to another will be encrypting outbound, and then decrypted inbound at the other end. We can have "Full overlap" and "Proper Subset" of overlapping in the VPN encryption domains.

QUESTION 238:

When using FW1 load balancing where does the logical server exist?

- A. As a dummy server on the "DMZ".
- B. As a dummy server on the "outside".
- C. As a dummy server on the "inside".
- D. As a dummy server in the firewall.

Answer: D

Explanations: Load balancing allows several servers to share and distribute network load. The VPN/FW1 Suite allows this by creating a Logical Server on the firewall. The logical server has a unique IP address through which packets are routed for load balancing. Traffic that is directed to this logical server is then load shared among the physical servers in a logical server group. See Page 4.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 239:

A hash function is a one-way mathematical function that maps variable values into smaller values of a fixed length. True or false?

- A. True
- B. False

Answer: A

Explanations: As stated in the official CCSE NG Courseware: "A hash function is a one-way mathematical function that maps variable values into smaller values of a fixed length" The size of the message is made smaller in order to ensure maximum network

performance. The shorter the message, the less computation required, and the better the performance. See Page 7.7 of CCSE NG Official Courseware.
(VPN1-FW1 Management II NG FP-1).

QUESTION 240:

What is the name given to an extension of SecuRemote that allows users to install a security policy on the desktop?

- A. Secure Client
- B. Policy Client
- C. SecuClient
- D. SecureDesktop

Answer: A

Explanations: Secure Client is an extension to SecuRemote that allows desktop user to download Desktop Policies from Policy servers. Once a secureremote user downloads a Desktop policy from a Policy Server, the secure Client software is enabled. SecuRemote is currently free of charge, while Secure Client is licensed and priced per client. See Page 12.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 241:

Which load balancing algorithm chooses the server closest to the client?

- A. Server load
- B. Domain
- C. Round trip
- D. Round robin
- E. Random

Answer: B

Explanations: With the domain load balancing algorithm, VPN1-FW1 chooses the closest server to the client, based on domain names. This algorithm is useful outside a network, such as when a domain name identifies the location of a remote device. This method is not recommended because it creates a noticeable delay to HTTP requests because of the reverse DNS lookups required. See Page 4.13 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 242:

Checkpoint Firewall 1 licenses are based on which IP address?

- A. An outside IP address.
- B. An inside IP address.
- C. An DMZ IP address.
- D. An IP address that is not allocated to any interface but is.

Answer: A

Explanations: All checkpoint management server and enforcement module licenses is based in the IP address of the Outside (routable, valid) interface. Its not a good practice to license your enforcement modules of management station with the address at the inside of your network. This is a checkpoint license guideline. See "Licensing FW1" at the Checkpoint online documentation.

QUESTION 243:

When configuring a new user with AMC which options are available to restrict the times at which the user is allowed to connect? (Choose all that apply)

- A. Day of week
- B. Month of year
- C. Start and end time of day
- D. Year

Answer: A, C

Explanations: When you configure a user through AMC, you can restrict the times the user is allowed to connect. Remember, the restriction are made in a time and day fashion. You cannot set the restrictions in a monthly or yearly fashion. For example, you can restrict a user to connect only on Fridays from 3:00PM to 9:00PM.

QUESTION 244:

In a SEP VPN when a gateway fails, a backup will take its place but all client connections will have to be remade.

True or false?

- A. True
- B. False

Answer: B

Explanations: This is false, the clients will not have to make the connections again because all the session state information is saved in the Ng suite, so, when a gateway fails in a SEP VPN configuration, the process of fail over is transparent for the user. Also remember that the traffic enters only from one side, it's a "Single Entry Point" VPN.

QUESTION 245:

What are the two modes for phase 1 of the ISAKMP scheme? (Choose two)

- A. Aggressive mode
- B. Simple mode
- C. Main mode
- D. Extended mode

Answer: A, C

Explanations:

VPN1/FW1 supports 2 modes, "aggressive mode" (the default), in which three packets are exchanged, and "main mode", in which six packets are exchanged. In phase 1, the peers negotiate security associations that will be used for encrypting and authenticating Phase 2 exchanges. Phase 1 involves long and CPU intensive computations, so is executed infrequently. See Page 7.13 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 246:

Which encryption algorithm as supported by VPN1/WF1 uses a key length between 112-168 bits?

- A. FWZ-1
- B. DES
- C. CAST
- D. Triple DES

Answer: D

Explanations: "CAST Cipher" is similar to DES. While the NG implementation of CAST uses a 40 bit key length, the CAST algorithm supports variable key length anywhere from 40 to 128 bits. CAST has a 64 bit block size, which is the same as DES. CAST is not as strong as DES, using comparable key lengths. See Page 7.11 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 247:

When using a proper subset encryption domain, which gateway is used for the Secure Client connection?

- A. The nearest gateway to the destination host.
- B. The first gateway in the path.
- C. All the gateways in the path.
- D. A gateway specified by the administrator.

Answer: A

Explanations: This is true, the client always connect to the nearest server based in the DNS domain information. This works like the "domain" load balancing fashion, the client creates connections based on the Domain info. You can check this at the Checkpoint NG online documentation, see "Proper Subset encryption".

QUESTION 248:

If a web user has requested a URL that contains unsuitable material it is possible, with content security, to specify a replacement URI that will warn the user. Where is that replacement URI specified?

- A. In the match tab of the URI resource definition.
- B. In the action tab of the FTP resource definition.
- C. In the general tab of the URI resource definition.
- D. In the action tab of the URI resource definition.

Answer: D

Explanations: You can achieve this functionality at the "Replacement URI" field in the "Action" tab at the properties of the URI resource. This field will replace the matching address with the one specified in the field. This is very useful for people getting into restricted sites, you can give them a really nice warning. See Figure 10 in page L9.8 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 249:

When the "generate log" option is checked for desktop security which is NOT a valid log message that can be reported?

- A. Lost policy
- B. No policy

- C. Corrupt policy
- D. Wrong policy

Answer: C

Explanations: "Corrupt policy" is not a valid message inside the logs, when the "generate log" option is checked in the "Configuration Violation Notification" part of the Desktop Security global properties. You can get the "lost policy" message when the violation comes from a machine that loses a policy, "No policy" when the machine has no policy at all or "Wrong Policy", when the machine has a policy installed, but the one it should. You can check this in the logs.

QUESTION 250:

Where would you define encryption for a firewall?

- A. General screen of workstation properties for the firewall.
- B. Certificates screen of workstation properties for the firewall.
- C. VPN screen of workstation properties for the firewall.
- D. Encryption screen of workstation properties for the firewall.

Answer: C

Explanations: This can be checked at the properties of a firewall object, you can set the "encryption scheme" for the firewall at the VPN tab. The possible options are: "IKE" and "FWZ". From this tab you can also add, edit and remove certificates and edit the configuration of the encryption schemes. See Figure 2 on Page L13.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 251:

It is possible to configure in the rule base an event such as a log or to run an executable when the entry in the rule base is triggered. What is this function called?

- A. Tracking
- B. Monitoring
- C. Reporting
- D. Triggering

Answer: A

Explanations: Tracking occurs when an option is defined in the Track column of a rule in the rule base, as well as when an object is defined. Certain

tracking options will generate just a log entry, viewable in log viewer, while other tracking options will generate a log entry and trigger an executable. See Page 3.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 252:

What is the name given to the ability of SecuRemote gateways to provide redundancy?

- A. High uptime
- B. Low downtime
- C. High availability
- D. High recovery

Answer: C

Explanations: Relating to Checkpoint Technologies, "High availability" enables enforcement modules to participate in CPHA (Check Point High Availability) configuration with one or more other enforcement modules to provide redundancy. See page 86 of Syngress Book "Checkpoint NGNext Generation Security Administration".

QUESTION 253:

Which is NOT a valid policy for a Secure Client desktop?

- A. Allow all
- B. Allow incoming only
- C. Allow outgoing only
- D. Allow encrypted only
- E. Allow outgoing and encrypted

Answer: B

Explanations: "Allow incoming only" is not a valid Secure Client Desktop policy, you have "Allow Outgoing & Encrypted" that will allow connections by "allow outgoing only" and "allow encrypted only" functionality allowed. "Allow outgoing only" will allow outgoing connections, the return of ICMP packets and the Session Authentication agent (port 261). "Allow encrypted only" will allow only encrypted connections, incoming and outgoing. See Page 12.11 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 254:

What is the name of the program that can be used to carry out a predefined function if an alert is triggered a number of times within a set period?

- A. fwalert
- B. alertf
- C. fwtrigger
- D. alertfw

Answer: B

Explanations:

Alertf is a program that acts as a wrapper for user-defined scripts. It simplifies the process of launching your user-defined events by allowing some specific criteria. It does this by enabling you to specify a threshold that must be met in order for your user-defined script to be executed. See Page 400 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 255:

What is the purpose of the "respond to unauthenticated topology requests" in relation to a SecuRemote client?

- A. It allows OEM products to act as SecuRemote clients.
- B. It is a useful tool for debugging.
- C. It is more efficient and handles more users, but is less secure.
- D. It enables backward compatibility with earlier versions.

Answer: D

Explanations: "Respond to unauthenticated topology request", this feature enables backwards-compatibility with

early versions of SecuRemote, for Secure Client, this option does not need to be selected.. See Page 12.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 256:

What is another name for asymmetric encryption?

- A. Shared key encryption
- B. Public/private key encryption
- C. Unbalanced encryption

Answer: B

Explanations: as stated in the official CCSE Courseware, "Asymmetric Encryption is also called public/private key encryption, because the

encryption scheme uses 2 keys, one private and one public. These keys are created using the Diffie Hellman key scheme, where one firewall's public key, and another firewall's private key, creates a shared secret key. See Page 7.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 257:

What is not a valid load-balancing algorithm in FW1?

- A. Server load
- B. Bandwidth
- C. Round trip
- D. Round robin
- E. Random
- F. Domain

Answer: B

Explanation: "Bandwidth" is not a valid load-balancing algorithm in FW1, the valid ones are: Server load (that needs an agent installed in the servers to provide load information), Round Trip (that uses ICMP to calculate the best server), Round Robin (that selects the destination server in order from a list), Random (that sends the request in a random fashion) and Domain (that uses the user location based on DNS).

QUESTION 258:

The four policies that can be applied to a Secure Client desktop are known collectively as a what?

- A. Trivial policy
- B. Remote policy
- C. Non-trivial policy
- D. Policy subset

Answer: C

Explanation: This can be checked in the Checkpoint NG online documentation, "Non-trivial policy" is the combination of all the policies that can be applied to a Secure Client desktop, the four policies are "Allow Outgoing & Encrypted", Allow outgoing only", "Allow encrypted only" and "No policy". See "Non-trivial Policy".

QUESTION 259:

SecuRemote requires the use of network driver interface specification (NDIS) in order to work. True or false?

- A. True
- B. False

Answer: A

Explanations: The SecuRemote module is made up of a kernel module and a daemon. The kernel module is an NDIS driver that is installed between the TCP/IP stack and adapter in use, that filters all the TCP/IP communication passing through the PC. Since SecuRemote needs its Kernel, it needs NDIS to work. See Page 11.14 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 260:

Which load balancing algorithm uses a load measuring agent?

- A. Server load
- B. Domain
- C. Round trip
- D. Round robin
- E. Random

Answer: A

Explanations: The "Server load" algorithm queries all servers in a logical server group to determine which is best able to handle a communication request. A load measuring agent must be installed in each physical server. The "Load measuring agent" is the FW1 Load balancing component, its a service running in a configurable port that returns information about the server load. You can see "Load Measuring Agent". See Page 4.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 261:

CPMAD can be configured to monitor successive multiple connections. What is it trying to prevent when it does this?

- A. A land attack

- B. A possible denial of service attack
- C. Port scanning
- D. Spoofing

Answer: B

Explanations: When CPMAD (Checkpoint Malicious Activity Detector) monitor multiple successive connections, its obviously trying to prevent a

DoS attack, this is because DoS attacks usually come with a great number of connections to the server being attacked, we can take the example of a

SynFlood that in the attack never completes the third step of the 3 way TCP handshake, it never sends the ACK, this

makes the attacked server to allocate memory to connections that will never be completed, with thousands of this uncompleted connections the protocol stack at the server gets an overflow and crash the O.S.

QUESTION 262:

Which are valid SYNDefender options. (Choose all that apply)

- A. SYNDefender gateway
- B. SYNDefender server
- C. SYNDefender transparent
- D. SYNDefender passive gateway

Answer: A, D

Explanations: We have 2 options in here, when "SYNDefender Gateway" configuration takes place in a checkpoint implementation it will automatically reply "SYN/ACK" packets from clients with an "ACK" packet. When the server receives the ACK packet from the gateway, the connection is moved out of the backlog queue, and becomes an open connection as far as the server is concerned. The second option

"Passive SynDefender Gateway" is the same as the first with the difference that FW1 does not simulate the client ACK to the server, instead, it waits for the client ACK, before passing it to the server. See Pages 6.8-6.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 263:

Having configured a content security resource how would you use it in a rule base entry?

- A. Left click the service column and select "add with resource", then select the required resource.
- B. Right click the service column and select "add", then select the required resource.
- C. Right click the action column and select "add with resource", then select the required resource.
- D. Right click the service column and select "add with resource", then select the required resource.

Answer: D

Explanations: Here is what the official CCSE documentation says, "From the Checkpoint Policy editor, select the specific rule, complete the source, destination, action, track and install on field of it. Right click the service column of the select rule, select the "Add with resource" option from the service menu, select the service, then, select the pre-configured resource. See Page L7.9 of CCSE NG Official Courseware.
(VPN1-FW1 Management II NG FP-1).

QUESTION 264:

The AMC does not allow deletion of an organizational unit from an account server (LDAP server) database. The deletion has to be done from the server itself or another LDAP editor. True or false?

- A. True
- B. False

Answer: A

Explanations: This is true, if you see AMC features, you will see that you can't delete an OU from there. You need to have access to the LDAP server itself or a LDAP editor, like an ADSI modified version that is used very commonly in Microsoft implementations, specially with Active Directory, that is based in LDAP. See "AMC features" in the Checkpoint NG online documentation.

QUESTION 265:

Which two of the following CPMAD parameter types combine to specify the rate of occurrence of an attack before action is taken?
(Choose all that apply)

- A. Repetitions
- B. Resolution
- C. Time_interval
- D. Clean_interval
- E. Interval_between_connection_attempts
- F. Number_of_connection_attempts

Answer: A, C

Explanations: The "MAD_syn_attack_repetitions" CPMAD parameter list the number of unique events that must be recorded within interval seconds in order for the action specified to be taken. The "MAD_syn_attack_time_interval" is the amount of time, in seconds, that attack information is stored within the internal MAD memory tables. The combination of both parameters specify the occurrence

of an attack before an action is taken.

See Page 410 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 266:

Where would you configure desktop security for Secure Clients?

- A. On the global properties setup screen select security servers.
- B. On the global properties setup screen select services.
- C. On the global properties setup screen select security policy.
- D. On the global properties screen select desktop security.

Answer: D

Explanations: When you enter to the global properties, you have the "Desktop Security" tab. From there you can configure SecuRemote and Secure

Client Validation Timeouts, IKE properties for SecuRemote and Secure Client, Desktop Configuration verification, Configuration Violation

Verification and Early version verification. See Page 12.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 267:

How would you configure an MEP VPN on the global properties setup screen?

- A. On the high availability screen select "enable backup gateway".
- B. On the high availability screen select "enable gateway clusters".
- C. On the desktop security screen select "enable backup gateway".
- D. On the connect control screen select "enable gateway clusters".

Answer: A

Explanations: Multiple entry point VPNs (MEPs) deployment make use of the VPN1/FW1 "Backup Gateway Feature". You should remember that

MEP is primary used to support providing automatic backup gateways to SecuRemote clients. You can make this configuration at the "Gateway

High availability" tab in the properties of the Gateway object. Under the "High availability options" select "Enable backup gateway" to provide high

availability in a multiple entry point configuration. See page 496 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 268:

SYNDefender configuration is common to all gateways and hosts. There is no way to specify SYNDefender gateway for one host and SYNDefender passive gateway for another. True or false?

- A. True
- B. False

Answer: A

Explanations: This is true, when we talk about SYNDefender settings, we are talking about global settings (Configured at the Global Properties of the implementation), they apply to all the enforcement modules, there is no way to change that, the SynDefender settings are implementation wide.
You can only use one SynDefender Gateway method a time.

QUESTION 269:

Secure Client adds a new pull down menu option to the SecuRemote desktop screen. What is this called?

- A. Security
- B. Policy
- C. Certificates
- D. Secure Client

Answer: B

Explanations: As stated in the official CCSE Courseware, "The secure client GUI is basically the same as the SecuRemote GUI, but with 2 differences, a new toolbar icon, and a new menu option. Secure Client's new menu option is the "Policy" Menu. Remember, Secure Client supports desktop policies, SecuRemote not, this is the main difference between the two clients. See Page 12.24 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 270:

If there is NAT in the path of a Secure Client connection it will still operate as normal. True or false?

- A. True
- B. False

Answer: B

Explanations: If a firewall, along the path connecting the Secure Client and the policy server, translates the

secure clients IP address, so that the Policy server does not see the Secure Clients true IP address, Secure Client will not function properly, unless UDP encapsulation is used. See Page 12.21 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 271:

What is the result of a hash function known as?

- A. Message summary
- B. Message précis
- C. Message compound
- D. Message digest

Answer: D

Explanations: As stated in the official CCSE Courseware, "A hash function is a one-way mathematical function that maps variable values into smaller values of a fixed length" The size of the message is made smaller in order to ensure maximum network performance. The shorter the message, the less computation required, and the better the performance. The result of the hash function, known as a message digest, is much smaller than the original message, but unique to it. If any changes to a message occur, the message digest will be different, indicating that the message has been altered. See Page 7.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 272:

Which type of encryption encapsulates the entire packet including the headers inside a packet with its own set of headers?

- A. In place encryption
- B. Tunneling mode encryption

Answer: B

Explanations: IKE uses "Tunneling mode" encryption, which works by encapsulating the entire packet, and then adding its own encryption protocol header to the encrypted packet. A drawback of using tunneling mode encryption is that the packet size has been increased. This increase in the packet size degrades network performance, however, the security of the packet is increased. See Page 7.15 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 273:

When configuring a URI definition what is NOT a valid URI match specification type?

- A. CVP
- B. Wild cards
- C. File
- D. UFP

Answer: A

Explanations: NG suite supports 3 "URI match specification types" they are "Wild Cards", "File" and "UFP". This can be configured in the "General" tab in the properties of the URI resource. We don't have a "CVP option". The URI Match specification type radio group tells VPN1/FW1 how you want to inspect the URI's matched by this object. See page 321 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 274:

Which form of overlapping encryption domain is NOT supported by VPN-1/FW-?

- A. Full overlap
- B. Partial overlap
- C. Proper subset

Answer: B

Explanations: A VPN encryption domain is a group of networks or hosts behind a firewalled gateway that participate in a VPN. Any traffic coming from one VPN domain and going to another will be encrypting outbound, and then decrypted inbound at the other end. We can have "Full overlap" and "Proper Subset" of overlapping in the VPN encryption domains supported by the NG suite. Partial overlap is not supported by VPN1/FW1.

QUESTION 275:

What is the default port for a secure socket layer (SSL) LDAP connection?

- A. 389
- B. 636

- C. 1024
- D. 23

Answer: B

Explanations: The normal port for LDAP servers is port 389 TCP but in the case that we want to use the LDAP services through a Secure Sockets Layer connection (SSL), the default port is 636 TCP. Your LDAP server must support connections through SSL to enable this type of connection. As a benefit, it increases security. You can check this in the online NG documentation, see "SSL + LDAP".

QUESTION 276:

Which encryption algorithms are supported by IKE? (Choose all that apply)

- A. DES
- B. CAST
- C. FWZ-1
- D. 3DES
- E. AES-256

Answer: A, B, D, E

Explanations: IKE (Internet Key Exchange) encryption scheme can be used with the following encryption algorithms: DES, 3DES, AES and CAST, for integrity it can use MD5 or SHA-1. You cant use FWZ-1 as an encryption algorithm with IKE because it's Checkpoint's proprietary an is only supported by the FWZ encryption scheme. See Page 7.13 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 277:

Which function handles load balancing in a FW1?

- A. Desktop security
- B. Connect control
- C. Inspect engine
- D. Daemon

Answer: B

Explanations: VPN1/FW1 can add the connection control module that incorporates advanced traffic control functionality to ensure the highest degree of network connectivity and optimal server response times. With Connect control, a single server

providing services can be replaced with a logical pool of server sharing a common IP address. See Page 4.2 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 278:

Which options are available on the "match" tab of a URI definition when using a URI match specification of "file"? (Choose all that apply)

- A. Import
- B. Export
- C. Schemes
- D. Methods

Answer: A, B

Explanations: this can be checked in the match tab, in the properties of an URI resource with a "file" matching specification or in the online NG documentation, the options are "Import" to make some import of data if you get a match, or "export" to get some export of data if you get a match. "Schemes" and "Methods" are not valid options.

QUESTION 279:

What is NOT true about single signon?

- A. It is useful for users who have network drives mapped behind a policy server.
- B. It correlates NT and SecuRemote user names and passwords.
- C. It is available for password authentication only.
- D. It is suitable for clients with multiple sites defined.

Answer: D

Explanations: By using "single sign on", users can save their Secure Client username and password, so they do not have to entered manually in the future. Single sign on is available for password authentication only, and is suitable for Secure Client hosts with only one site defined. See Page 12.31 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 280:

How would you configure a SEP VPN from the global properties setup screen?

- A. On the high availability screen select "enable gateway clusters", you can then configure the cluster members under manage> network objects.
- B. On the services screen select "enable gateway clusters", you can then configure the cluster members under manage> network objects.
- C. On the security policy screen select "enable gateway clusters", you can then configure the cluster members under manage> network objects.
- D. On the high availability screen select "enable backup gateway".

Answer: A

Explanations: "Single Entry point" VPN's enable your enterprise to deploy a solution that protects critical elements of the network. Before you go about configuring SEP VPN solutions, you need to make sure that "gateway clusters" are enabled on the management server at the high availability screen, remember that this will be a cluster. There is a limitation for the creation of SEP VPN's, it's the Hardware configuration, it must be the same. See page 488 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 281:

What is the name of the FW1 facility that scans the log file and alerts the system administrator that a prespecified suspicious event has occurred?

- A. SYNDefender
- B. CVP
- C. alertf
- D. CPMAD

Answer: D

Explanations: "Check Point Malicious Activity Detection" (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities across a range of firewall modules, it can notify administrators about special conditions. It can be used to detect 8 types of attacks, they are: syn attacks, anti spoofing, successive alerts, port scanning, blocked connections port scanning, login failure, successive multiple connections, land attack. See page 406-407 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 282:

Which encryptions schemes are supported by VPN1/FW1? (Choose all that apply)

- A. FWZ

- B. DES
- C. IKE
- D. SKIP

Answer: A, C

Explanations: The checkpoint Ng suite supports two encryption schemes, "IKE" and "Fwz". Those encryption schemes consist of "Key management protocol" for generating and exchanging keys, "Encryption algorithm" for encrypting messages, and "Authentication algorithm" for ensuring integrity. IKE is an industry standard protocol for VPN key management while FW is a proprietary VPN1/Firewall1 encryption scheme.

See Page 7.10 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 283:

If there are two gateways and two encryption domains which are fully overlapped, in which of the domains will the gateways belong?

- A. The gateways will be outside the domains.
- B. There will be one gateway in each domain.
- C. They will both be in both domains.
- D. There can only be one gateway for full overlap encryption domains.

Answer: C

Explanations: Since the domains are fully overlapped, the gateways will belong to both of them, remember that a VPN encryption domain is a group of networks or hosts behind a firewalled gateway that participate in a VPN. Any traffic coming from one VPN domain and going to another will be encrypting outbound, and then decrypted inbound at the other end. Also, This kind of VPN domains is very handy when dealing with critical connections. When a SecuRemote client tries to communicate with a server residing in this overlapping domain, it will try to connect to all of the gateways and will complete the connection with the first gateway to respond. There are some problems with this, to resolve them you can use IP

Pools to assign a previously configured IP address to the SecuRemote client. You can also use NAT to hide the connection passing through the gateway behind the gateway. See page 498 of Syngress Book "Checkpoint NG - Next Generation Security Administration". You can check this at the online NG documentation.

QUESTION 284:

What is NOT true about the FWZ-1 encryption algorithm?

- A. It uses in-place encryption.
- B. It uses RDP to manage VPN session keys.
- C. It encrypts all data including the headers.
- D. Supports a 40-56 bit encryption key.

Answer: C

Explanations: FWZ uses in place encryption, encrypting the payload portion (data) of the packet and leaving the original TCP/IP headers intact. Because packet size is not increased, in place encryption allows for better network performance than the provided by IKE encryption. A drawback of using in-place encryption is that the headers remain intact, indicating the origin IP address and destination IP address See Page 7.16 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 285:

Which two of the following CPMAD parameter types combine to control the action taken if the connection to a LEA or ELA server is lost?

(Choose all that apply)

- A. Repetitions
- B. Resolution
- C. Time_interval
- D. Clean_interval
- E. Interval_between_connection_attempts
- F. Number_of_connection_attempts

Answer: E, F

Explanations: "MAD_number_of_connection_attempts" define the number of times MAD will try to reconnect either to the LEA or ELA server, and "MAD_interval_between_connection_attempts" defines the wait period between those reconnection attempts. Both parameters together defines the action taken if the connection to a LEA or ELA server is lost. See Page 408-409 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 286:

Which of the following CPMAD parameter types controls the amount of time old events stay in the CPMAD tables?

- A. Repetitions

- B. Resolution
- C. Time_interval
- D. Clean_interval
- E. Interval_between_connection_attempts
- F. Number_of_connection_attempts

Answer: D

Explanations: "MAD_clean_interval" define the amount of time that old attacks will be stores in MAD memory tables. Just to remember, "Check

Point Malicious Activity Detection" (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities

across a range of firewall modules. It can be used to detect 8 types of attacks, they are: syn attacks, anti spoofing, successive alerts, port scanning,

blocked connections port scanning, login failure, successive multiple connections, land attack. See Page 408-409 of Syngress Book "Checkpoint NG

- Next Generation Security Administration".

QUESTION 287:

When configuring match parameters for content security resources it is possible to use a wild card character to represent anything. What is that character?

- A. *
- B. #
- C. !
- D. %

Answer: A

Explanations: You can use the "*" (Asterisk) symbol to represent anything and provide a match. You can use the asterisk in the "match" tab at the

properties of an URI Resource, for example, you can complete the "Host", "path" and "query" fields of the match tab with an asterisk to always

match those fields. You can see this illustrated in Figure 9 at Page L7.7 of CCSE NG Official

Courseware.(VPN1-FW1

Management II NG FP-1).

QUESTION 288:

Put the following LDAP distinguished name entities in hierarchical order starting from the root.

- 1 - c
- 2 - cn
- 3 - o

4 - ou

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

Answer: D

Explanations: This is the correct order, if we have to go through an LDAP hierarchy from the root, we first go from the container (it could be your country for example), then the "O" (Object, as an example, it could be your company), then optionally you have the "OU" (Organizational unit for logical organization purposes) and for the end, you have the CN that provides the name of the object inside the hierarchy (For example it could be your name and last name). Like this: cn=joe bloggs, o=company inc, c=us

QUESTION 289:

If the HTTP security server is defined as a proxy for a web browser. What connection method should be used in the general tab of the URI resource definition when configuring HTTP content security.

- A. Proxy
- B. Transparent
- C. Tunneling
- D. None

Answer: C

Explanations: The connection methods options defines what modes FW1 will use to examine traffic. If tunneling mode is elected, you will not have access to the CVP tab and will not be able to use any URI filtering or UFP servers, since tunneling only allows the security server to inspect the port and IP address information, not the URI. This achieve our requirements See page 321 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 290:

How would you configure a rule for a Secure Client user?

- A. Choose client encrypt under the service column, right click and check "Apply rule only if desktop configurations are verified".
- B. Choose client encrypt under the action column, right click and check "Apply rule only if desktop

configurations are verified".

C. Choose client encrypt under the action column, right click and check "Apply desktop policy".

D. Choose client encrypt under the service column, right click and check "Apply desktop policy".

Answer: B

Explanations:

As stated in the CCSE official courseware, "By applying a rule whose action is "Client encrypt", you protect the enterprise network from attack by

someone in control of an unprotected SecuRemote machine. In the client encrypt rule user encryption action properties windows, check "Apply rule

only if desktop configuration options are verified". To display this window, double-click on the client encrypt action rule. See Page 12.12 of

CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 291:

If you want to backup your security policy you need to make a copy of the following files:

\$FWDIR/conf/objects_5_0.C

\$FWDIR/conf/*.W

\$FWDIR/conf/rulebases.fws

\$FWDIR/database/fwauth.NDB*

True or false?

A. True

B. False

Answer: A

Explanations: The objects_5_0.C was formerly called users.c in earlier versions of FW-1, the purpose of this file is to contain network objects,

properties and configuration information from the management server. The .W files are created after you create a rule base in a new policy upon

saving or installing the policy, it contains the information displayed graphically in the GUI regarding the rule base. The rulebases.fws file also

contains part of the security policy information and fwauth.NDB contain the users. You need all of this files to make a complete backup of your security policy.

QUESTION 292:

Which security server or service provides protection by: hiding IP addresses from outgoing email, strips Mime attachment types, drops

large messages, and perform mail filtering?

- A. HTTP security server
- B. SMTP security server
- C. FTP security server
- D. Java and active X stripping

Answer: B

Explanations:

VPN1-Firewall1 NG offers an SMTP security server that provides highly granular control over smtp connections. A new pool dequeuer mechanism provides more efficient spool scanning by performing FIFO, which enables mail to be put in the mail dequeuer and give priority to new mail over underivable old mail. The smtp server allows to hide outgoing e-mail, perform mail filtering, strip mime attachments, drop mails above a given size and many features more. See Page 5.15 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 293:

Which of the following desktop policies can be modified by the Secure Client user?

- A. Allow all.
- B. Allow outgoing only.
- C. Allow encrypted.
- D. Allow outgoing and encrypted.
- E. None of them.

Answer: E

Explanations: Users cannot modify any of the desktop policies, this policies are defined by administrators, and there is nothing a user can do to change it once its installed an running in its Secure Client. Remember that the secure desktop policies are downloaded from a Policy server, and that SecuRemote does not support them, this is the great difference between SecuRemote and Secure Client.

QUESTION 294:

What parameter in userc.C allows you to set the port for topology download?

- A. gettop_port
- B. topology_port
- C. top_port
- D. port_gettop

Answer: A

Explanations: The "gettop_port (x)" parameter specifies the port for topology download. If unsuccessful after 30 seconds, Secure Client will try again in port 264 by default. The other parameters listed as answers are not valid ones. Remember that Secure Client performs minimal syntax checking for the users.c file. If a parameter is entered incorrectly, the site, to which it belongs is deleted. No error messages are displayed. See Page 12.28 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 295:

Which is NOT a viewing option on the log viewer screen?

- A. Log
- B. Audit
- C. Account
- D. Active

Answer: C

Explanations: The log viewer has three different predefined selection views. These view models can be modified and saved. Selection of the log mode is done through the mode drop-down list on the toolbar. The 3 modes are: "log mode" that is the one by default, "active mode" that shows currently open connections and "Audit mode" used to display only audit entries in the Log Viewer. See Page 4.6 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 296:

If a certificate appears in the CRL what does this mean?

- A. The certificate authority has revoked the certificate and it is no longer valid.
- B. The certificate is valid and certified.
- C. The certificate supercedes a previous certificate.
- D. The certificate is in use by another device.

Answer: A

Explanations: Here is the information contained in the CCSE official courseware: "When a user leaves an organization, or when a key is compromised, the certificate must be revoked. The certification authority does this by issuing and distributing a Certificate Revocation List (CRL). Before accepting a certificate, the CRL should be checked to confirm that the certificate has not been revoked. The CRL distribution point is usually a

Web Server. When a certificate appears in a CRL it is no longer valid, it has been revoked. See Page 8.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 297:

Which of the following uses an external certificate authority in a VPN1/FW1 implementation?

- A. IKE
- B. FWZ
- C. SKIP

Answer: A

Explanations: with IKE, you can set the key management either automatic or with an external PKI. IKE uses tunneling mode encryption, it provides encryption of the original IP and TCP headers, and can be used in VPN's that use reserved IP addresses without needing address translation or proxying. FWZ only supports automatic key management through the management server, it cannot use an external PKI solution. See Page 7.17 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 298:

What is the name given to an attack that is characterized by: attempts to find an unblocked port by sequentially trying each port in turn for a particular IP address?

- A. Port hopping
- B. Port scanning
- C. Port popping
- D. Port hacking

Answer: B

Explanations: the Port scanning attack is one of the most used and easiest to perform in the hacking arena, there are many easy to use executables that make the job, one of the most famous is "NMAP". In a port scan attack, the attacker tries to make a connection to a range of ports through a range of IP address to see what ports are open and what service are running. With this information the attacker can use exploits on the particular services running in those ports that were found open.

QUESTION 299:

What is the name given to a globally unique entity within an LDAP server?

- A. Specific name
- B. Unique name
- C. Designated name
- D. Distinguished name

Answer: D

Explanations: As stated in the online NG documentation, LDAP uses a DN (Distinguished name) to provide a unique entity within an LDAP server, this entity is unique through the LDAP directory. When we define an LDAP account unit we must provide a "Login DN" at the general tab of the LDAP account unit properties. This will be used to bind to the account unit. See Page 291 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 300:

What is true about proper subset encryption domains?

- A. Only one domain can be fully contained within another domain.
- B. There can multiple levels of domains contained within a domain.
- C. Devices in the internal encryption domain are excluded from the domain of the outer gateway.
- D. No special steps need be taken to allow the connection through the outer gateway.

Answer: B

Explanations: This is a feature of proper subset encryption domains, inside a domain, you can have multiple levels contained within it. This could not happen in a fully overlapped VPN domain. You can check this feature in the Online NG documentation. See "proper subset features".

QUESTION 301:

When configuring network objects from the "manage" pull down menu which is NOT an option on the "Network objects" screen?

- A. New
- B. Remove
- C. Copy
- D. Edit

Answer: C

Explanations: This is true, you cannot copy the definition of a network object from the "manage" menu in the network objects screen, however you can create a new network object, remove a network object or edit an existent one. You can check this inside the policy editor in the "Manage" pull down menu at the network objects screen.

QUESTION 302:

Which operating software will not support a SecuRemote client? (Choose all that apply)

- A. Windows NT
- B. Windows 2000
- C. HP-UX
- D. Windows 98
- E. AIX

Answer: C, E

Explanations: Since SecuRemote was created for client operating systems, it doesn't provide support for UNIX server operating systems like IBM AIX and HP-UX, SecuRemote and Secure Client are designed for Windows platforms, The most current versions support Windows 9x, Windows NT, Windows 2000 and Windows XP. The key here is that SecuRemote and Secure Client are not designed to run in server operating systems other than Microsoft ones. There is also another limitation, the SecuRemote software is composed of a Win32 daemon that runs as a service, UNIX does not run Win32 services.

QUESTION 303:

What is the name given to encrypted data?

- A. Cleartext
- B. Ciphertext
- C. Code
- D. Cryptext

Answer: B

Explanations: This is a well-known term used in cryptography, when we talk about "Cipher Text" we are talking about a text that has been modified by a mathematical function that was applied some kind of key of a certain length, in other words, a text that has been encrypted. To make Cipher text

we take "Clear text" and we apply to it the mathematical function and the associated key. In symmetric encryption we only use one key to go from clear to cipher and cipher to clear text. In asymmetric or public key encryption, we have to use 2 keys, one for encrypt and one for decrypt.

QUESTION 304:

MEP VPN's support both SecuRemote and Secure Client connections. True or false?

- A. True
- B. False

Answer: B

Explanations: This is false, when we talk about Multiple entry point VPN's we can provide support for SecuRemote clients, but there is no support currently available for Secure Client and the desktop security policy feature. This can be checked in the online NG documentation.

QUESTION 305:

In a fully overlapping encryption domain with multiple gateways, the gateway that the SecuRemote client connects to remains valid for a set period of time. How long is that?

- A. 30 secs
- B. 1 minute
- C. 5 minutes
- D. 1 hour

Answer: B

Explanations: There is not too much to comment in here, this is the default, when you connect with secureremote to a fully overlapping domain with multiple gateways, the gateway that received your connection will only make the session valid for a period of 1 minute. In my opinion, this is a very short time, but its like that, 1 minute by default. You can check this at the NG documentation, see "Fully overlapping domain timeout".

QUESTION 306:

In relation to load balancing which are valid logical server types? (Choose all that apply)

- A. HTTP
- B. SNMP redirect
- C. non HTTP
- D. Other

Answer: A, C, D

Explanations: As stated in the official CCSE NG Courseware, there are 3 types of logical server, "HTTP" used for HTTP server load balancing, "Other Load Balancing" that allows a server IP address to be a logical server address, from a firewall to a client, and a physical server IP address from a server to the firewall. Each HTTP connection is then handled separately, and connections may be redirected to different servers. The last one is "NON HTTP", is used when a non HTTP service request is detected, for example FTP. See Page 4.5 and 4.6 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 307:

When using an "other" load balancing server type it uses NAT to convert the logical server address to a real server address. The NAT rules have to be configured manually. True or false?

- A. True
- B. False

Answer: B

Explanations: Other load balancing place entries in the VPN1-FW1 NG address translation tables for a connection. , "Other Load Balancing" allows a server IP address to be a logical server address, from a firewall to a client, and a physical server IP address from a server to the firewall. Each HTTP connection is then handled separately, and connections may be redirected to different servers. This may cause problems in some case, for example, in an application where a user fills a number of HTTP forms and a single server is expected to process all the data. You don't have to define any manual NAT rules. See Page 4.6 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 308:

What is the name given to a code that can be attached to a message that uniquely identifies the message and verifies that it hasn't been tampered with?

- A. Digital authentication

- B. Digital signature
- C. Digital lock
- D. Digital affirmation

Answer: B

Explanations: As stated in the official CCSE NG courseware, "A digital signature is a code that can be attached to an electronically transmitted message that uniquely identifies the sender, and verifies that the message hasn't been tampered with in transit. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message is really who claims to be. Digital signatures use public key cryptography". See Page 7.8 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 309:

Asymmetric encryption is around 10 times slower than symmetric encryption True or false?

- A. True
- B. False

Answer: B

Explanations: As stated in the official CCSE NG courseware, "Due to performance issues, asymmetric encryption is 1000 times slower than symmetric cryptography. Asymmetric cryptography is typically used to encrypt small amount of data, such as keys, for symmetric cryptography. See Page 7.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 310:

Secure Client encryption does not take place under some circumstances. Which is NOT one of these circumstances?

- A. A key is being exchanged.
- B. A new site is being added or updated.
- C. The data is intended for an SMTP server.
- D. The source and destination are both in the same encryption domain.

Answer: C

Explanations: According to the official CCSE NG documentation, these are the circumstances when Secure Client encryption will not take place, "a new site is added, or when updating an existing site", "a key is exchanged", "DNS information is exchanged", "ftp, Real audio and VDOlive are

exchanged" and when secure client is on the local network. Send data to a SMTP server is not one of the exceptions. See Page 12.22 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 311:

Which product is NOT under the "mobile/desktop components" section of the Checkpoint product installation menu?

- A. VPN-1 SecuRemote
- B. VPN-1 Secure client
- C. Floodgate-1 modules
- D. Session authentication agent

Answer: C

Explanations: At the product menu we have 2 sections, "Server/gateway components" composed of: VPN1-FW1, FloodGate1, MetaIP, Management clients, User Authority, Policy Server, Reporting module and Real Time monitor. Under "Mobile/Desktop Components" we have the following products: VPN1 SecuRemote, VPN1 Secure Client and Session authentication agent. See Figure 3 at page L1.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 312:

What is the name of the VPN1/FW1 facility that extends security to the desktop?

- A. Security server
- B. Policy server
- C. SecuRemote
- D. Policy client

Answer: B

Explanations: As stated in the official CCSE NG Courseware, "Policy server extends security to the desktop by allowing administrators to enforce a security policy on desktops - both inside the LAN and connecting from the Internet, this prevent unauthorized connections from being compromised. See page 12.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 313:

Which of the following CPMAD parameters types specified a period during which multiple log entries for the same occurrence are classed as one entry?

- A. Repetitions
- B. Resolution
- C. Time_interval
- D. Clean_interval
- E. Interval_between_connection_attempts
- F. Number_of_connection_attempts

Answer: B

Explanations: The "MAD_syn_attack_resolution = X" sets the resolution for this attack. Conceptually, a timer is started when the first matching event is recorded. All subsequent matching events within resolution seconds will be counted as part of the first event and will not count towards repetitions for logging purposes only. See page 409 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 314:

What is NOT true about in-place encryption?

- A. It only supports the FWZ-1 algorithm.
- B. It does not encrypt the IP and TCP headers.
- C. It does not increase the packet size.
- D. It can be used with VPN's that use reserved IP addresses.

Answer: D

Explanations: FWZ uses in place encryption, encrypting the payload portion (data) of the packet and leaving the original TCP/IP headers intact. Because packet size is not increased, in place encryption allows for better network performance than the provided by IKE encryption. A drawback of using in-place encryption is that the headers remain intact, indicating the origin IP address and destination IP address this prevents the use of reserved IP addresses with the VPN's. See Page 7.16 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 315:

Where would you configure a user defined alert command?

- A. In global properties select the "Open security extensions" page.
- B. In global properties select the "log" page.
- C. In global properties select the "log and alert" page.
- D. Use the policy pull down menu, choose properties, select "log and alert" tab.

Answer: C

Explanations: As stated in the official CCSE NG documentation, "To set up user defined tracking, modify the "Logs and alerts page" and the "Alerts" command page in the global properties window. Remember, you can replace any of the executable in the command fields of the log and alerts tab with custom scripts. See Page 3.4 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 316:

When using HTTP redirect what is the minimum number of rules required?

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

Answer: B

Explanations: This is the minimum number of rules in required for this functionality, remember that you are making a redirection of the HTTP protocol, so you will not have enough with only one rule. You can check "HTTP redirect rules" in the Online NG documentation.

QUESTION 317:

Which programming language cannot be used for writing user defined applications?

- A. C/C++
- B. Cobol
- C. Perl
- D. Bourne Shell
- E. C-Shell

Answer: B

Explanations: This language is not supported for user defined applications, this can be checked in the Online NG documentation. C++, Perl, Bourne Shell and C-Shell are all supported languages, but Cobol is not a supported one. See "User defined application development" in the NG online help.

QUESTION 318:

Which security server or service provides protection by blocking undesirable web pages?

- A. HTTP security server
- B. SMTP security server
- C. FTP security server
- D. Java and active X stripping

Answer: A

Explanations: The HTTP security server protects against specific URL destinations in the Internet through the use of UFP (URI Filtering Protocol).

This security server can determine user rights including the ability to visit a particular website, or download certain file types. This capability is

integrated into VPN1-FW1 NG and does not require additional software. However, it has limits, it does not scale well, it should be used for less than

50 URL restrictions, if you want more its better to use a UFP certified OPSEC application for URL filtering.

See Page 5.5 of CCSE NG

Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 319:

What is the name given to an attack that masks the attackers true source IP address by using an address borrowed from a device on a trusted network?

- A. Land attack
- B. Denial of service
- C. SYN attack
- D. Spoofing

Answer: D

Explanations: This kind of attack is called spoofing, a spoof attack consist of an attacker using an IP address that its not its real one, the used

address is usually an address considered as trusted in the network being attacked. There are many free programs in the web that lets you use the spoof functionality.

QUESTION 320:

What is the correct protocol sequence when opening a TCP session?

- A. SYN - ACK - SYN ACK - DATA

- B. SYN - SYN ACK - ACK - DATA
- C. SYN - SYN RPLY - ACK - ACK RPLY - DATA
- D. SYN - ACK - DATA

Answer: B

Explanations: This is the correct order of a TCP session, the user send a "SYN" packet to the server (ask the server for a connection), the server sends to the user a "SYN/ACK" packet (telling the client that he is going to open a port for the connection and giving his ACK), then the user send the server an ACK (to complete the negotiation of the session), once this 3 way handshake process is done, the two sides can begin the exchange of data.

QUESTION 321:

What is the filename of the file on a SecuRemote client that contains the topology of the site to which the client connects?

- A. user.C
- B. userclient.c
- C. userc.C
- D. userc.cfg

Answer: C

Explanations: The system administrator can create a userc.c file for SecuRemote users, pre-defining the sites for them. The userc.c file contains all of the network topology information of a site. By pre-configuring this file, System administrators can ensure that SecuRemote setup can be an easy process for end users. With the sites pre-defined the users do not need to download the topology of the sites to which they will connect. See Page 12.26 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 322:

Which operating system can NG FW1 NOT be used under? (Choose all that apply)

- A. HPUX 11.0
- B. Solaris 2.8
- C. AIX 4.1
- D. Windows 2000
- E. Red Hat Linux 6.2

Answer: A, C

Explanations: Here are the supported Operating Systems for FW1 as stated in the official CCSE NG courseware:

NT Server 4.0 (SP6a), Win2000 Server and Advanced Server (SP0 and SP1). Solaris 2.7 with patch 106327, Solaris 2.7 (32-bits mode only). Solaris 2.8 with patch 108434 and 108435. Red Hat Linux 6.2, 7.0 and 7.1. There is no support for HP-UX and AIX 4.1. See Page 1.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 323:

What happens if CPMAD runs out of memory?

- A. It exits but logs the cause.
- B. It issues a warning and carries on, but it may lose some data.
- C. It exits without notification.
- D. It automatically assigns some more memory and carries on.

Answer: C

Explanations: CPMAD, in common with any other piece of software written by us mere mortals, has some problems. One of the most glaring problem is the tendency of CPMAD to silently exit if insufficient memory resources are available, we hope that this gets a solution in the next revision. See page 410 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 324:

What is the VPN type that is between two firewalls?

- A. Site-to-site VPN
- B. Client-to-site VPN
- C. Internal VPN
- D. External VPN
- E. Remote access VPN

Answer: A

Explanations: When we talk about site-to-site VPN's, we are talking about VPN's between two firewall/Gateways, the most common configuration is 2 Checkpoint NG enforcement modules connected through the Internet to provide transparent access between locations, this kind of VPN does not provide support for mobile users needing access to the network. For this kind of remote functionality we need client-to-site VPN's that works with a gateway receiving VPN connections from remote clients.

QUESTION 325:

Which phase of the IKE process uses a previously negotiated security association (SA) to encrypt and authenticate?

- A. Phase 1
- B. Phase 2
- C. Phase 3

Answer: B

Explanations:

In phase 2, the SA (Security association) negotiated in phase 1 is used by the peers to negotiate an SA for encrypting the IPSEC traffic. Keys can be modified as often as required during a connection lifetime by performing phase 2. Phase 2 provides additional security by refreshing the keys to ensure the reliability of the SA's and prevent a man-in-the-middle-attack. See Page 7.14 of CCSE NG Official Courseware.
(VPN1-FW1 Management II NG FP-1).

QUESTION 326:

What is NOT true about a SEP VPN?

- A. A mechanism is needed for redirecting traffic around a failed gateway.
- B. Synchronization between gateways in a cluster must be maintained.
- C. They utilize IP pools.
- D. They use a distributed architecture where clustered gateways are managed by a separate management station.

Answer: C

Explanations: Since we are talking about SEP VPN's (Single entry point) you cannot consider using IP pools on them, its not a correct option.

Remember, a SEP VPN enable your enterprise to deploy a solution that protects critical elements of the network. Before you go about configuring SEP VPN solutions, you need to make sure that gateway clusters are enabled on the management server, remember that this will be a cluster. You can review the IP Pool concept at the Online NG documentation.

QUESTION 327:

Secure Client users cannot change the desktop policy but they can make some changes to the operation of the

desktop. Which is NOT one of these.

- A. Disabling the policy
- B. Selecting block all
- C. Uninstalling Secure Client
- D. Selecting block none

Answer: D

Explanations: This is part of what can a user make in relation to the desktop behavior, is perfectly possible that the user uninstalls Secure Client from the OS, the user could also disable the policy from Secure Client or select to block all the connections to the machine for security. What the user can't do is to have a security policy applied and running select not to block any connection, Secure Client will not allow this to the user. Try it yourself.

QUESTION 328:

Which is NOT a disadvantage of the symmetric encryption method?

- A. The same key is used for decrypt and encrypt, therefore if someone steals the key they can decode traffic in both directions.
- B. The keys must be delivered in a secure manner, by telephone or face to face.
- C. It is less efficient.
- D. It is not scalable for large numbers of keys.

Answer: C

Explanations: Since we are using only one key to encrypt and decrypt the data (Convert from clear-text to cipher-text), this method of encryption is like a thousand times more efficient than Asymmetric encryption that uses 2 keys, one for encrypting and the other for decrypting. However symmetric encryption is not very scalable for the number of different keys you need to manage, there is also a security weakness because you can use the same key to encrypt and decrypt the communications.

QUESTION 329:

What is the default timeout value for SYNDefender to wait for an ACK from a client?

- A. 5 secs
- B. 10 secs
- C. 30 secs

D. 60 secs

Answer: B

Explanations: The default time out for the "Timeout for SYN attack identification" is 10 seconds, this can be changed in the global properties of the firewall object, in the advanced section, at the SYNDefender tab. "Timeout for SYN attack identification" specifies how long VPN1-FW1 NG waits for the ACK from the client, before terminating the connection. See Page 6.12 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 330:

What is true about the Secure Client users ability to disable policy on the desktop? (Choose all that apply)

- A. The user can disable it by default.
- B. The user cannot disable it by default.
- C. The default state can be changed by configuring the "manual_slan_control" option in userc.c.
- D. The default state can be changed by configuring the "manual_slan_control" option in objects.c.

Answer: A, C

Explanations: As stated in the official CCSE NG courseware, "The disable policy menu option cancels the desktop policy that you receive, and its only available if the network administrator did not eliminate it, its enabled by default. The administrator can eliminate the "disable policy" option by editing the userc.c file setting the "manual_slan_control" to true. See Page 12.25 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 331:

Asymmetric routing is when a return packet is not routed through the same gateway that the incoming packet came through. What can be done to overcome this in a MEP VPN?

- A. Use SEP VPN's instead.
- B. Use IP pools.
- C. Reconfigure the SecuRemote clients.
- D. Nothing it is not a problem.

Answer: B

Explanations: Since we are using MEP VPN (Multiple entry point) we can use the functionality of the IP Pools to overcome the asymmetric routing

issues. The bad thing is that it's a tedious and complex configuration, you can see a walkthrough of it at the secure checkpoint website. Just to remember, Multiple entry point VPNs (MEPs) deployment make use of the VPN1/FW1 "Backup Gateway Feature". You should remember that MEP is primary used to support providing automatic backup gateways to SecuRemote and Secure client.

QUESTION 332:

Which Windows file contains the CPMAD configuration?

- A. \$FWDIR/cpmad/cpmad_config.conf
- B. \$FWDIR/cpmad/config.conf
- C. \$FWDIR/conf/cpmad_config.conf
- D. \$FWDIR/conf/cpmad.conf

Answer: C

Explanations: The main configuration file for CPMAD events is cpmad_config.conf. This file can be found in the \$FWDIR/conf directory. Its format is pretty standard. You can place comments in it with the "#" symbol. Just to remember, Check Point Malicious Activity Detection (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities across a range of firewall modules. It can be used to detect 8 types of attacks, they are: syn attacks, anti spoofing, successive alerts, port scanning, blocked connections port scanning, login failure, successive multiple connections, land attack. See page 406-407 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 333:

How many keys are used in asymmetric encryption?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Explanations: Talk about asymmetric encryption is the same as talk about Public / Private key encryption, in this method of encryption we use 2 keys, one to encrypt the data, and another to decrypt it. In this model of encryption, the users have a public and a private key, the public key is of free distribution and is usually published in a directory, while the private keys must be keep secure. This kind of

encryption is like a thousand times slower than symmetric one. Asymmetric encryption usually use certificates to validate the key.

QUESTION 334:

What does CRL stand for?

- A. Critical resource list
- B. Customer request label
- C. Certificate revocation list
- D. Common rule list

Answer: C

Explanations: Here is the information obtained in the CCSE official courseware: "When a user leaves an organization, or when a key is compromised, the certificate must be revoked. The certification authority does this by issuing and distributing a Certificate Revocation List (CRL). Before accepting a certificate, the CRL should be checked to confirm that the certificate has not been revoked. The CRL distribution point is usually a Web Server. See Page 8.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 335:

If you check the "cache static passwords on the desktop" option on the desktop security tab of properties setup. What does this mean for SecuRemote users?

- A. OS or VPN-1/FW-1 passwords will be cached on the desktop, no re-authentication is required for this session.
- B. Radius or TACACS passwords will be cached on the desktop, no re-authentication is required for this session.
- C. All passwords will be cached on the desktop, no re-authentication is required for this session.
- D. S/Key or SecurID passwords will be cached on the desktop, no re-authentication is required for this session.

Answer: A

Explanations: As stated in the official CCSE NG Courseware, "Allow cache static password on the desktop - if checked, static passwords (OS or VPN1-FW1 NG) will be cached on the desktop. SecuRemote / Secure Client user will not be required to re-authenticate if using the Operating system and VPN1/FW1 passwords, until the next login. See Page 12.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 336:

Which security server or service provides protection by: controlling get and puts, restricting file names and checking for virus's?

- A. HTTP security server
- B. SMTP security server
- C. FTP security server
- D. Java and active X stripping

Answer: C

Explanations: As stated in the official CCSE NG Courseware, "The FTP security server provides authentication services and content security based on FTP commands (Put and Get), file name restrictions, and anti-virus checking for files. You implement FTP security with an FTP resource." See Page 5.15 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 337:

What is AMC used for?

- A. Configuring FW1 load balancing.
- B. Configuring FW1 URI filtering.
- C. Configuring user accounts on an LDAP server.
- D. Configuring VPN's.

Answer: C

Explanations: The "AMC" is our primary tool that help us to configure user account inside an LDAP server. Of course, AMC is absolutely LDAP compliant. The AMC communicates by default in port 389 to establish communication with the LDAP server. You can get more on "AMC" in the Online NG documentation. See "AMC".

QUESTION 338:

A Management server can act as a certificate authority for which type of encryption scheme?

- A. FWZ
- B. IKE

Answer: A

Explanations: as stated in the official CCSE NG Courseware, "The FWZ scheme does the following, encrypts

all data behind the IP and TCP

headers, use RDP to manage session keys, Gets certified Diffie Hellman public keys from a trusted certificate authority, the CP Management server.

FWZ Schemes supports a 40-56 bit FWZ-1 encryption key. See Page 7.16 of CCSE NG Official Courseware. (VPN1-FW1

Management II NG FP-1).

QUESTION 339:

There are two John Doe's working for different departments of the same company in the US. How could they be distinguished in an LDAP DN?

- A. Use their middle names or some agreed variant of the name.
- B. Assign them to different organizational units.
- C. Do nothing, you are allowed to duplicate DN's.
- D. They cannot be entered into an LDAP server.

Answer: B

Explanations: When we talk about LDAP functionality we can use something known as an OU (Organizational unit) to organize our users or

objects inside the catalog in a very flexible way. If we have objects with the same name, you can put them in different OU's and they will not be the

same for the LDAP repository, this is because the LDAP DN name will be different between the 2 objects.

(That LDAP DN contains the location of the object inside the directory and also the name of it).

QUESTION 340:

Which of the following levels of encryption supports a key length of between 128 and 256 bits?

- A. AES
- B. 3DES
- C. FWZ-1
- D. CAST

Answer: A

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

QUESTION 341:

When configuring CPMAD which character precedes a comment?

- A. #
- B. ?
- C. *
- D. %

Answer: A

Explanations: The main configuration file for CPMAD events is cpmad_config.conf. This file can be found in the \$FWDIR/conf directory. Its format is pretty standard. You can place comments in it with the "#" symbol. Just to remember, Check Point Malicious Activity Detection (CPMAD) is a handy log analyzer. This feature aids in detection of unusual, potentially dangerous activities across a range of firewall modules. It can be used to detect 8 types of attacks, they are: syn attacks, anti spoofing, successive alerts, port scanning, blocked connections port scanning, login failure, successive multiple connections, land attack. See page 406-407 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 342:

Which of the following is NOT covered by FW1's content security?

- A. Viruses
- B. Syn flooding
- C. Java applets
- D. Active X code
- E. Undesirable web content

Answer: B

Explanations: Content Security does not address Syn flooding attacks, syn flooding attacks are a type of DoS attack, and its addressed with a component of Firewall 1 called "SYN Defender", Syn Defender can be configured in the advanced tab, at the properties of a firewall object. Content security can address things that involve layer 7 of the OSI model, like HTTP (URI filtering), FTP (Put, Get), SMTP (Mime striping, size limit), Java striping, Virus inspection inside the data and many more. See Page 5.4 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 343:

What is the name given to the load balancing mode that allows the same server to be used for the duration of the session?

- A. Consistent server mode
- B. Fixed server mode
- C. Permanent server mode
- D. Persistent server mode

Answer: D

Explanations:

If selected, "Persistent Server mode" allows some fine-tuning of the load balancing process. When enabled, you can enforce connection persistence, meaning you can force packets from an established flow to continue to a single destination. You can select to 2 modes: "Persistent by service" and "Persistent by server". The relation is client to server, so its the client the one that keeps connecting to the same server. See page 155 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 344:

What is NOT true about a SecuRemote VPN?

- A. It requires fixed IP addressing for the remote station.
- B. It encrypts data before it leaves a remote computer.
- C. It interfaces with any NDIS interface.
- D. It enables access for remote VPN users through the rule base.

Answer: A

Explanations: This statement is not true, SecuRemote clients are not required to have a fixed IP address, they can also work with a dynamic one, this can be achieved through an auto-configuration with DHCP or some kind of Bootp server. As stated in the official CCSE Courseware, "

SecuRemote includes support for dynamic IP addressing, necessary for dialup communications. See Page 11.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 345:

What is the default name for a user defined script or program?

- A. \$fwdir/bin/fwscript
- B. \$fwdir/bin/fwlog
- C. \$fwdir/bin/alert

D. \$fwdir/bin/alertf

Answer: C

Explanations: As stated in the official CCSE Courseware, "Popup Alert - the OS command (normally \$FWDIR/CONF/alert) to be executed in the firewalled machine when an alert is issued. It is recommended not to change this command; otherwise you may not become aware of the condition that caused the alert. See Page 3.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 346:

Secure Client only supports Microsoft TCP stacks. True or false?

- A. True
- B. False

Answer: A

Explanations: This is true, as you can see in the operating system compatibility of Secure Client, there is no support for any other operating system that is not from Microsoft, one of the reasons for this is because Secure Client does not support other TCP/IP stacks that are not the Microsoft one. This is why you don't see a Secure Client running on Linux right now.

QUESTION 347:

What term is used to describe a VPN where multiple gateways are not synchronized but still provide redundancy?

- A. SEP
- B. MEP
- C. SSO
- D. PFS

Answer: B

Explanations: This is the proper definition for MEP's, they provide redundancy, but are not synchronized. Just to remember, Multiple entry point VPNs (MEPs) deployment make use of the VPN1/FW1 "Backup Gateway Feature". You should remember that MEP is primary used to support providing automatic backup gateways to SecuRemote clients. You can make this configuration at the "Gateway High availability" tab in the properties of the Gateway object. Under the "High availability options" select "Enable backup gateway" to provide high availability in a multiple

entry point configuration. See page 496 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 348:

When configuring a tracking option for a particular rule. Which is NOT a valid option?

- A. Mail
- B. SNMPTrap
- C. Alert
- D. E-page
- E. Account

Answer: D

Explanations: According to official CCSA NG Courseware, this are the valid options for the Tracking field of a rule: none (no logging or alert), log (for logging), account (log in accounting format), alert (Issue an alert), snmp trap (issue an snmp trap), mail (send a mail alert) and User defined (Issue an user defined alert). There is no "E-Page" option available. See Page 2.14 of CCSA NG Official Courseware.(VPN1-FW1 Management I NG FP-1).

QUESTION 349:

Which encryption schemes are supported by SecuRemote? (Choose all that apply)

- A. FWZ
- B. IKE
- C. SKIP
- D. FWZ-1

Answer: A, B

Explanations: The latest version of Secure Remote supports all the encryption schemes provided by the Checkpoint NG suite, those schemes are FWZ and IKE. Those encryption schemes consist of "Key management protocol" for generating and exchanging keys, "Encryption algorithm" for encrypting messages, and "Authentication algorithm" for ensuring integrity. IKE is an industry standard protocol for VPN key management while FW is a proprietary VPN1/Firewall1 encryption scheme. See Page 7.10 of CCSE NG Official Courseware.(VPN1-FW1 Management II NG FP-1).

QUESTION 350:

Where would you configure a pre-shared secret for the IKE scheme?

- A. From the firewall workstation properties screen select the VPN screen and select IKE. edit to see the IKE properties screen. Configure pre-shared secret on the VPN tab.
- B. From the firewall workstation properties screen select the VPN screen and select IKE. edit to see the IKE properties screen. Configure pre-shared secret on the properties tab.
- C. From the firewall workstation properties screen select the VPN screen and select IKE. edit to see the IKE properties screen. Configure pre-shared secret on the key tab.
- D. From the firewall workstation properties screen select the VPN screen and select IKE. edit to see the IKE properties screen. Configure pre-shared secret on the general tab.

Answer: D

Explanations: This is the correct answer, you can configure "Pre-Shared Secret" under the "Support authentication methods" in the IKE properties.

To get to IKE properties you need to go to the VPN tab of the properties of the firewall object. Once in there you can edit IKE. Just to remember,

Pre-Shared Secret is used when both ends of the VPN lacks access to a compatible certificate server. Once you have defined all the endpoints in your VPN, you can establish a password that is used to authenticate the other end of the connection. (Both ends of the connection must be configured with the same password). See page 323 of "Essential Checkpoint Firewall 1" Book.

QUESTION 351:

What does AES stand for?

- A. Automated Encryption Services
- B. Augmented Encryption System
- C. Authorized Encryption Scheme
- D. Advanced Encryption Standard

Answer: D

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

QUESTION 352:

Which form of overlapping encryption domain is described as multiple gateways each having the same encryption domain?

- A. Full overlap
- B. Partial overlap
- C. Proper subset

Answer: A

Explanations: This kind of VPN domains is very handy when dealing with critical connections. When a SecuRemote client tries to communicate with a server residing in this overlapping domain, it will try to connect to all of the gateways and will complete the connection with the first gateway to respond. There are some problems with this, to resolve them you can use IP Pools to assign a previously configured IP address to the SecuRemote client. You can also use NAT to hide the connection passing through the gateway behind the gateway. See page 498 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 353:

What is the name of the FW1 facility that can protect against SYN flood attacks?

- A. SYNProtector
- B. SYNGuard
- C. SYNDefender
- D. SYNPolice

Answer: C

Explanations: VPN1-FW1 NG's SynDefender stop SYN Flood attacks, it provides two defenses against it, a "SynDefender Gateway" and "SynDefender Passive Gateway", both of these are integrated with the Inspect module of the enforcement modules. Just to remember, the SYN flood attack never completes the third step of the 3 way TCP handshake, it never sends the ACK, this makes the attacked server to allocate memory to connections that will never be completed, with thousands of these uncompleted connections the protocol stack at the server gets overflow and crash the O.S. The SYN Flood is considered a DoS attack, it can be used in conjunction of other attacks like IP spoofing.

QUESTION 354:

What is the name given to the ability of a CVP manager to sequentially use the services of several CVP servers as part of a single request from a firewall?

- A. CVP load sharing
- B. CVP chaining
- C. CVP sequencing
- D. CVP forwarding

Answer: B

Explanations: The capability called "Chained", is useful when each of the CVP servers performs a different function. The chaining process connects servers for the purpose of stringing functionality. For example, you can invoke 3 CVP server, each with a different task, such as scanning for viruses, stripping mime tags or stopping large e-mail attachments. See Page 5.29 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 355:

Which VPN type is used by SecuRemote?

- A. Site-to-site
- B. Client-to-site
- C. Client-to-client

Answer: B

Explanations: Since SecuRemote was designed to provide secure communication for remote user through the use of VPN's, it uses client-to-site VPN's. This is because usually the SecuRemote users are usually not located in the LAN and need to establish a VPN with a gateway to access the resources behind it. For example, a vendor working from home that wants to access the corporate intranet.

QUESTION 356:

What is the name given to a server, which maintains a list of banned URL's?

- A. A UFP server
- B. A URI server
- C. A CRL server
- D. A CVP server

Answer: A

Explanations: An UFP external server (URI Filter) it's an OPSEC certified application used for passing data between VPN1/FW1 and a third-party application for URI classification. You can use products like WebSense to achieve the URL filtering functionality through categories. For example you can define that your users cannot go to any sport sites beginning with the letter "B" or that kind of things. See page 318 of Syngress Book "Check Point NG - Next Generation Security Administration".

QUESTION 357:

Which of the following is an encryption method that uses a different keys to decrypt and encrypt messages?

- A. Symmetric encryption
- B. Shared key encryption
- C. Asymmetric encryption

Answer: C

Explanations: As stated in the official CCSE Courseware, "Asymmetric Encryption is also called public/private key encryption, because the encryption scheme uses 2 keys, one private and one public. This keys are created using the Diffie Hellman key scheme, where one firewalls public key, and another firewalls private key, creates a shared secret key. See Page 7.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 358:

What name is given to the option of specifying that keys should be exchanged at intervals during phase 2 of the IKE (ISAKMP) process?

- A. Regular key exchange
- B. Perfect forward secrecy
- C. Perfect key secrecy
- D. Perfect forward exchange

Answer: B

Explanations: In phase 2, the SA (Security association) negotiated in phase 1 is used by the peers to negotiate an SA for encrypting the IPSEC traffic. Keys can be modified as often as required during a connection lifetime by performing phase 2. Phase 2 provides additional security by refreshing the keys to ensure the reliability of the SA's and prevent a man-in-the-middle-attack, this can be achieved by using the option "Perfect Forward secrecy" in the encryption properties of the VPN. See Page 7.14 of CCSE NG Official Courseware.

(VPN1-FW1
Management II NG FP-1).

QUESTION 359:

Which of the following is a Checkpoint proprietary encryption algorithm?

- A. DES
- B. FWZ-1
- C. 3DES
- D. CAST
- E. AES

Answer: B

Explanations: As stated in the official CCSE NG Courseware, "FWZ-1 is the Checkpoint's proprietary symmetric encryption algorithm, it uses a 40 bit key and is only supported by the FWZ encryptions scheme. FWZ support in-place encryption, encrypting the payload portion (data) of the packet and leaving the original TCP/IP headers intact. Because packet size is not increased, in-place encryption allows for better network performance than the provided by IKE encryption. See Page 7.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 360:

What is NOT true if you add a SecuRemote site and its encryption domain overlaps an already configured site?

- A. A warning is displayed.
- B. The existing conflicting site is disabled.
- C. A red X is placed over the new sites icon.
- D. The new site is disabled.

Answer: B

Explanations: As stated in the official CCSE NG Courseware documentation, "If you attempt to add a site whose encryption domain overlaps those already defined in your sites window, a warning is displayed, and a red X is placed on the conflicting new site. If one of your previous sites have been disabled, you can enable it through your sites menu. The existing conflicting sites are not disabled. See Page 12.29 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 361:

MD5 is the only data integrity method applicable to the FWZ scheme.

True or false?

- A. True
- B. False

Answer: A

Explanations:

This is true, in the case we use the FWZ encryption scheme we can only provide data integrity through the use of MD5 (Message Digest 5), in case that we use the IKE encryption scheme, we also have the option to use "SHA-1" (Secure Hashing Algorithm) to provide data integrity in the VPN's. So, IKE supports MD5 and SHA-1 and FWZ only supports MD5.

QUESTION 362:

What is the name given to a server giving anti virus protection for transferred files?

- A. A UFP server
- B. A URI server
- C. A CRL server
- D. A CVP server

Answer: D

Explanations: CVP Servers provide virus detection and cleanup capabilities, this functionality is achieved with the

CVP protocol that send data streams arriving to FW1 to OPSEC certified CVP (Content Vectoring Protocol) applications. Once the data streams are translated to the external CVP server, the OPSEC application check the data for virus patterns and then return the data flow to the FW1 server. The URL filtering capabilities are not achieved through CVP, they are achieved through UFP (URI Filtering Protocol).

QUESTION 363:

FW1 provides content security for which of the following resources? (Choose all that apply)

- A. HTTP
- B. FTP
- C. SMTP
- D. Telnet
- E. SNMP

Answer: A, B, C

Explanations: Content security extends the scope of data inspection to the highest level of a service protocol, achieving highly tuned access to the network resources. VPN1/FW1 NG provides content security for the following connections, using the VPN1/FW1 NG Security servers, and resource object specifications: HTTP, FTP, SMTP. There is no actual support for Telnet and SNMP. See Page 5.4 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 364:

The userc.C file contains information for SecuRemote and Secure Client desktops. It includes information about site topology. Under which heading would you find the topology information?

- A. :site
- B. :options
- C. :topology
- D. :gws

Answer: C

Explanations: You define the topology information under the ":topology" heading, there you can add a name for the server, a type (gateway for example), an IP address and an Ipmask for the different gateways that make part of your topology. Just to remember, Secure Client performs minimal syntax checking for the userc.c file. If a parameter is entered incorrectly, the site, to which it belong, is deleted. No error messages will be displayed. See Page 12.27 and 12.29 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 365:

Where is the default SMTP error-handling server configured?

- A. \$FWDIR/bin/smtp.conf
- B. \$FWDIR/conf/smtp.conf
- C. \$FWDIR/objects/smtp.conf
- D. \$FWDIR/conf/smtp.C

Answer: B

Explanations: Aside from using resources, the SMTP Security server has parameters that are configured in \$FWDIR/conf/smtp.conf. It has parameters like "timeout" (amount in seconds to spend in CVP scanning), "Scan_period" (amount of time to

check the spool directory for e-mail delivered, "resend_period" (Amount of time in seconds that a message that failed to be delivered will be resend from the SMTP security server. For a complete list, see Page 247 of Dameon Welch Book "Essential Checkpoint Firewall 1".

QUESTION 366:

When using a URI match specification type of "UFP" where would you specify the UFP server to be used?

- A. In the match tab
- B. In the action tab
- C. In the General tab

Answer: A

Explanations: This can be checked right in the properties of an URI resource, when you select "UFP" as the URI match type, you can select the UFP server from the "Match" tab, you can also define "UFP caching control" and list categories. There is also an option to ignore the UFP server after connection failure. See Figure 9 in Page L9.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 367:

Which command would you use the print out details of checkpoint licenses on a machine?

- A. cplic print
- B. licprint
- C. cplic check
- D. showlic

Answer: A

Explanations: As stated in the official CCSA Courseware, "Cplic print prints the details of the VPn1/FW1 licenses. The syntax for this command is: "cplic print(local management) (remote host)". See Page 12.38 of CCSA NG Official Courseware. (VPN1-FW1 Management I NG FP-1).

QUESTION 368:

Which of the following levels of encryption is used by financial institutions throughout the world and other

customers with special permits?

- A. VPN
- B. VPN+DES
- C. Strong

Answer: B

Explanations:

This is the correct answer, this kind of institutions need the integrity and authentication benefits of a VPN, and also the privacy provided by an encryption algorithm like DES, or 3DES in case that its necessary. With this answer we get three most important pillars of network security: Integrity (Through digital signatures), Privacy (through encryption) and Authenticity (through authentication).

QUESTION 369:

Which options are NOT available on the personal tab when configuring a new user using AMC? (Choose all that apply)

- A. Expiration date
- B. Users email address
- C. Users telephone number
- D. Comment
- E. Users location

Answer: B, E

Explanations: AMC does not provide a way to set the e-mail address and the user location in the personal tab when you are creating a new user, this can be checked just trying to create one in your NG deployment, however you can specify basic info like Expiration date, telephone and comments. Check your AMC personal tab screen.

QUESTION 370:

A Diffie-Hellman key engine is used in which of the following encryption methods?

- A. Symmetric encryption
- B. Shared key encryption
- C. Asymmetric encryption

Answer: C

Explanations: As stated in the official CCSE Courseware, "Asymmetric Encryption is also called public/private

key encryption, because the encryption scheme uses 2 keys, one private and one public. These keys are created using the Diffie Hellman key scheme, where one firewall's public key, and another firewall's private key, creates a shared secret key. See Page 7.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 371:

What is the term given to a number of VPN-1/FW-1 gateways that are synchronized together?

- A. Gateway group
- B. Gateway ring
- C. Gateway farm
- D. Gateway cluster

Answer: D

Explanation: A "Gateway Cluster" is a grouping of machines running VPN1/FW1 that is grouped together as a means of fail over support. To configure this you first have to visit the global properties and under the gateway high availability tab, place checkmarks enabling "gateway clusters". The next step is to create your workstation object. You can see more at page 156-157 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 372:

What are the two types of login for a Secure Client user? (Choose two)

- A. Auto login
- B. Explicit logon
- C. Implicit login
- D. Enforced login

Answer: B, C

Explanation: As stated in the official CCSE NG Courseware, "Policy server install Desktop policies in Secure Client machines when user performs implicit or explicit login. Explicit login occurs when a Secure Client user logs into a policy server to download a new or updated desktop policy, this is initiated by the desktop user. Implicit login occurs when a Secure Client user does not have an installed policy and tries to communicate through a policy server, the server will try to install a security policy, this is initiated by the policy server. See Page 12.19

of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 373:

Where do you enable an LDAP account unit?

- A. Global properties> Services page
- B. Global properties> LDAP account management page
- C. Global properties>Authentication page
- D. Global properties>Security servers page

Answer: B

Explanations: This is true, you need to enable the account unit, and that can be done in the global properties accessed through the Policy editor, once there, you go to the Account management page. You can check this in the global properties of your Checkpoint NG deployment.

QUESTION 374:

Which is NOT a valid scheme on the match tab of a wild card URI definition?

- A. http
- B. ftp
- C. gopher
- D. mailto
- E. news
- F. smtp

Answer: F

Explanations: If you see the Match tab in the properties of an URI resource that is working with "wild cards" matching, we can see the following schemes: HTTP, FTP, GOPHER, MAILTO, NEWS, WAIS and a option to specify "others". We don't have a checkbox to select SMTP. You can check this is Figure 9 at page L8.19 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 375:

Under which tab of a URI definition window would you specify a third party CVP server?

- A. General

- B. Match
- C. Action
- D. CVP

Answer: D

Explanations:

If you see the CVP tab in the properties of an URI resource we can see the following at the CVP tab: "Use CVP (Content Vectoring Protocol" and the possibility to select a CVP server from the drop down list. You can also specify if the CVP server is allowed to modify the content and the "reply order". You can check this in Figure 12 at page L10.9 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 376:

Which load balancing algorithm allocates the server based on the next physical server in the group?

- A. Server load
- B. Domain
- C. Round trip
- D. Round robin
- E. Random

Answer: D

Explanations: When using the Round Robin algorithm, the VPN1-FW1 application chooses the next server in the list. Round Robin is a sequential algorithm. The round robin algorithm assumes that all physical servers are equally capable of servicing connection requests, regardless of location or server load. Request are directed to server in sequential order. See page 4.11 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 377:

What is the name of the Secure Client facility that can create customized installation files for distribution to users?

- A. Secure Client Packaging Tool
- B. Secure Client Generation Wizard
- C. Secure Client Installation Wizard
- D. Secure Client Download Tool

Answer: A

Explanations: The "

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

QUESTION 378:

How would you apply encryption to a rule?

- A. For the rule concerned select encrypt under the action column.
- B. For the rule concerned select encrypt under the service column.
- C. For the rule concerned select VPN under the action column.
- D. For the rule concerned select VPN under the service column.

Answer: A

Explanations: As stated in the official CCSA NG Courseware, you have the following options in the "Action" field of a rule: Accept (accepts connections), drop (drop connections), reject (rejects the connection and notify the sender), user authentication (invokes user authentication), client authentication (invokes client authentication), session authentication (invokes session authentication), encrypt (encrypt outgoing packets, accept incoming encrypted packets) and client encrypt (accepts only SecuRemote communications, which allows remote). As you can see, our correct answer is A.

QUESTION 379:

Which of the following is NOT a valid CPMAD attack parameter?

- A. Mode
- B. Time interval
- C. Number of connection attempts
- D. Repetitions
- E. Resolution
- F. Action

Answer: C

Explanations: All of those are attack specific parameters of CPMAD configuration file, but "Number of connection attempts" is not an attack parameter, it's a global parameter. It defines the number of times CPMAD will try to connect to an ELA or LEA server. See Page 407 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

QUESTION 380:

Which are public key schemes supported by VPN1/FW1? (Choose all that apply)

- A. Diffie-Hellman
- B. FWZ
- C. RSA
- D. IKE

Answer: A, C

Explanations: As stated in the official CCSE NG Courseware, " RSA is the public key cryptosystem that NG suite uses to create and verify digital signatures. Any information encrypted with the RSA public key can only be decrypted with the matching RSA private key, and vice versa.

Asymmetric Encryption keys are created using the Diffie Hellman key scheme, where one firewalls public key, and another firewalls private key, creates a shared secret key. See Page 7.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 381:

When configuring an FTP resource for content security where would you specify that the security should be based on a file get or a file put command?

- A. General tab
- B. Match tab
- C. Action tab

Answer: B

Explanations: If you go to the properties of an FTP resource, you will see 3 tabs, "General", "Match" and "CVP". In the "General" tab you can specify a name, a comment, a color and the exception track. At the "Match" tab you can specify the "path", and the two possible methods, those methods are: "get" and "put".

See Figure 5 on Page L11.4 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 382:

If you wanted to use content security on an SMTP resource which parameter can be specified on the match tab of the SMTP definition

screen? (Choose all that apply)

- A. Sender
- B. Mail server
- C. Recipient
- D. Contents

Answer: A, C

Explanations: If you go to the properties of an SMTP resource, you will see 5 tabs, "General", "Match", "Action1", "Action2" and "CVP". At the "Match" tab you can specify 2 fields, "Sender" and "Recipient". "Mail Server" and "Content" are not valid options for the Match tab at the properties of an SMTP resource.

See Figure 9 on Page L10.7 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 383:

Which is NOT a valid term used in relation to the IKE encryption scheme?

- A. ISAKMP
- B. PKI
- C. SKIP
- D. Oakley

Answer: C

Explanations: SKIP is the no related term, we use "ISAKMP" (Internet Security Association and Key Management Protocol) as the framework for transferring keys and authenticating. "PKI" is a fundamental part of IKE functionality because it will provide the infrastructure to use digital certificates, commonly used by IKE for authentication. "Oakley" is the protocol used to establish strong cryptography based keys used for the encryption of data. See Page 7.12 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 384:

Which is a valid distinguished name for a LDAP database?

- A. o=joe bloggs, c=company inc, cn=us
- B. cn=joe bloggs, o=company inc, c=us
- C. cn=joe bloggs, o-company inc, c=us
- D. c=joe bloggs, cn=company inc, o=us

Answer: B

Explanations: Option B provides a valid Distinguished name, it begins with the canonical name (Usually your name and last name), then the object (usually your company) and the container at the root (usually your country). The use of an Ou (Organizational unit) is optional, we don't need an OU in here. Remember that you always need to have the "cn" in one corner and the "c" in the other corner.

QUESTION 385:

Which CPMAD attack is defined as a SYN packet with the source IP address the same as the destination IP address?

- A. LandAttack
- B. SYN attack
- C. Spoofing
- D. Loopback attack

Answer: A

Explanations: This is the behavior of a Land Attack, this kind of attack sends packets with the SYN flag on, with the same source and destination IP address. This can cause some old, unpatched TCP/IP stacks to crash the operating system they are running on, Land attack its considered a DoS type of attack. You can view the attack in action downloading a Free Land attack hacking utility from internet and capturing the packets generated by the tool in your LAN.

QUESTION 386:

What does VPN1/FW1 use to create and verify a digital signature?

- A. RSA
- B. CVP
- C. UFP
- D. IKE

Answer: A

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

QUESTION 387:

Which is NOT true about tunnel mode encryption?

- A. It supports all algorithms except FWZ-1.
- B. It encrypts IP and TCP headers.
- C. It does not increase the packet size.
- D. It can be used with VPN's that use reversed addresses.

Answer: C

Explanations: "Tunneling mode" encryption, works by encapsulating the entire packet, and adding its own encryption protocol header to the encrypted packet. A drawback of using tunneling mode encryption is that the packet size has been increased. This increase in the packet size degrades network performance, however, the security of the packet is increased. See Page 7.15 of CCSE NG Official Courseware.
(VPN1-FW1 Management II NG FP-1).

QUESTION 388:

Where would you select the load balancing server type for a group of servers?

- A. From the policy editor use Manage> Network objects> New> load balancing server.
- B. From the policy editor use Manage> Network objects> New> logical server.
- C. From the policy editor use Manage> Network objects> New> workstation.
- D. From the policy editor use Manage> Network objects> New> servers.

Answer: B

Explanations: This is the correct way to create a new logical "load balancing server". You can check this right in your policy editor. You use the manage menu, and in the network objects part you reference a new "load balancing server". This load balancing server will serve as a logical front end for other physical server providing the same services. You can apply a load balancing algorithm to this logical servers.

QUESTION 389:

Which encryption algorithms are supported by FWZ? (Choose all that apply)

- A. DES

- B. CAST
- C. FWZ-1
- D. 3DES
- E. RC2

Answer: A, C

Explanations: FWZ supports DES and FWZ-1 as encryption algorithms. Checkpoint NG supports the following encryption algorithms with IKE and FWZ in combination: DES, 3DES, AES, CAST and FWZ-1. See Page 7.10 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 390:

Which commands would you use to stop and start Firewall1?

- A. fwstop and fwrn
- B. fwstop and fwstart
- C. fwdown and fwrn
- D. fwstop and fwinit

Answer: B

Explanations: Those are well-known commands for any Checkpoint NG administrator, you can issue the command "Fwstop" to stop the firewall services from the gateway or make some changes made to take effect when you make a restart. You can issue the "fwstart" command, it starts the firewall services and upload the inspect engine to enforce the enterprise security policy. This is a must know for anyone trying work with Checkpoint Firewall technologies.

QUESTION 391:

What is the function of a VPN1 accelerator card?

- A. To increase the throughput of traffic being processed by the inspection engine.
- B. To offload encryption from software to hardware.
- C. To speed up the time taken for a Securemote user to log on.
- D. To increase the CPU cycle rate of the server to give an overall performance improvement.

Answer: B

Explanations:

A "VPN1 accelerator" card is a special hardware NIC provided by checkpoint with special built-in encryption

capabilities. The purpose of this card is to offload the encryption CPU intensive tasks from the processor of gateways that process many VPN connections at the same time. If you have more than 80 simultaneous VPN connections to your server, it is recommendable to have one of these cards. This card is very useful when you have many SecuRemote / secure Clients accessing to your headquarters in parallel. With the card, the encryption is processed by the hardware and not with the software.

QUESTION 392:

In which directory would you place a user defined alert application script?

- A. \$FWDIR/bin
- B. \$FWDIR/alerts
- C. \$FWDIR/user
- D. \$FWDIR/conf

Answer: A

Explanation: As stated in the official CCSE Courseware "The user defined tracking scripts must be placed in the \$FWDIR/BIN folder on the management station. With user defined tracking scripts you can allow the following: custom log filter programs to log screen entries generated by a specific rule, alerts when a complex condition is met, a single rule to generate different types of alarms for different conditions. See Page 3.3 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 393:

Secure Client can use Reliable Datagram Protocol (RDP) status queries to check that the gateway is still alive. Which parameters in userc.C control this action? (Choose all that apply)

- A. Keepalive
- B. Keep_alive_interval
- C. Active_resolver
- D. Resolver_session_timeout
- E. Resolver_ttl

Answer: C, D, E

Explanation: If "Active_resolver" is true, secure client will automatically initiate an RDP status query with a gateway to see if it is still alive. If false, secure Client will postpone sending the query until that information is actually needed - in which case the

user may experience some delay. "Resolver_session_interval" is the interval, in second, between RDP status queries. "Resolver_ttl" is the number of second Secure Client will wait for a reply on an RDP status query before concluding that the gateway is unavailable. The action is controller by this 3 parameters. See Page 12.28 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 394:

If you want to bind a Secure Client user id to an IP address then the following has to be added into which filename?

```
:props  
:userc_bind_user_to_IP (true)
```

- A. \$FWDIR/conf/conf.C
- B. \$FWDIR/conf/secureclient.c
- C. \$FWDIR/conf/objects.cnf
- D. \$FWDIR/conf/objects.C

Answer: D

Explanations: This configuration is made at the objects.C file, this file is located in the CONF directory at the \$FWDIR variable. With this code,

you can bind a Secure client ID to an IP address. Just to remember, with the binding of a user ID to an IP address, you can force

re-authentication when a user connects from another machine, this is because the binding will not match, this feature can increase security. Another benefit is that the user can connect from different workstations in a secure fashion because the binding functionality provides re-authentication as stated above. See "Secure Client Binding" in the Secure Client Documentation.

QUESTION 395:

What command string would you use to run the script "fwalert" if an alert occurs 5 times in 2 minutes?

- A. alertf 2 5 fwalert
- B. alertf 120 5 fwalert
- C. alertf 5 120 fwalert
- D. alertf 5 2 fwalert

Answer: B

Explanations: Here is the syntax for the command:

"alertf (Number of seconds) (number of alerts) (name of the program or script to run).

In this question, our script is "fwalert", the time is 120 seconds (2 minutes) for 5 times that the event occurs.

You can check this on Page 400 of

Syngress Book "Check Point NG - Next Generation Security Administration".

QUESTION 396:

How would you configure a rule to support SecuRemote?

- A. Under the action column for the rule select "client encrypt".
- B. Under the action column for the rule select "SecuRemote".
- C. Under the service column for the rule select "SecuRemote".
- D. Under the service column for the rule select "client encrypt".

Answer: A

Explanations: This is the correct way, since SecuRemote provides encryption functionality through VPN capabilities, we have to specify the "client encrypt" option in our action field of the rule to support SecuRemote. Remember that SecuRemote encrypts or decrypts depending on the direction of the communication. See Page 11.5 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 397:

A load balancing logical server does not really exist therefore you need to manually arrange for an ARP to be published by the firewall that can respond to an arp request for that logical server. True or false?

- A. True
- B. False

Answer: B

Explanations: The logical server exists, here is what the official CCSE NG courseware says, "Load balancing shares and distributes network load, this is done by creating a logical server on the firewall. The logical server has a unique IP address through which packets are routed for load balancing. Using address resolution protocol (ARP) the FW1 load balancing ensures packets destined to the IP address of the logical server are passed to the appropriate physical server. See Page 4.2 of CCSE NG Official Courseware. (VPN1-FW1 Management II NG FP-1).

QUESTION 398:

Which of the following happens if the user.C syntax is incorrect? (Choose all that apply)

- A. No error messages are displayed.
- B. An appropriate error message is displayed.
- C. The site to which the wrong parameter belongs is deleted.
- D. The desktop will be disabled.

Answer: A, C

Explanations: As stated in the official CCSE NG documentation, "Secure Client performs minimal syntax checking for the userc.c file. If a parameter is entered incorrectly, the site, to which it belong, is deleted. No error messages will be displayed. See Page 12.29 of CCSE NG

Official Courseware. (VPN1-FW1 Management II NG FP-1).