Checkpoint

Exam 156-310

Check Point NG with Application Intelligence - Management II

Version: 3.0

[Total Questions: 398]

Topic break down

Topic	No. of Questions
Topic 1: Main Questions 4	101
Topic 2: Practice Questions 99	297

Topic 1, Main Questions 4

Question No : 1 - (Topic 1)

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 No : 2 - (Topic 1)

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 No : 3 - (Topic 1)

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

Dr BillMUST:

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 No : 4 - (Topic 1)

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

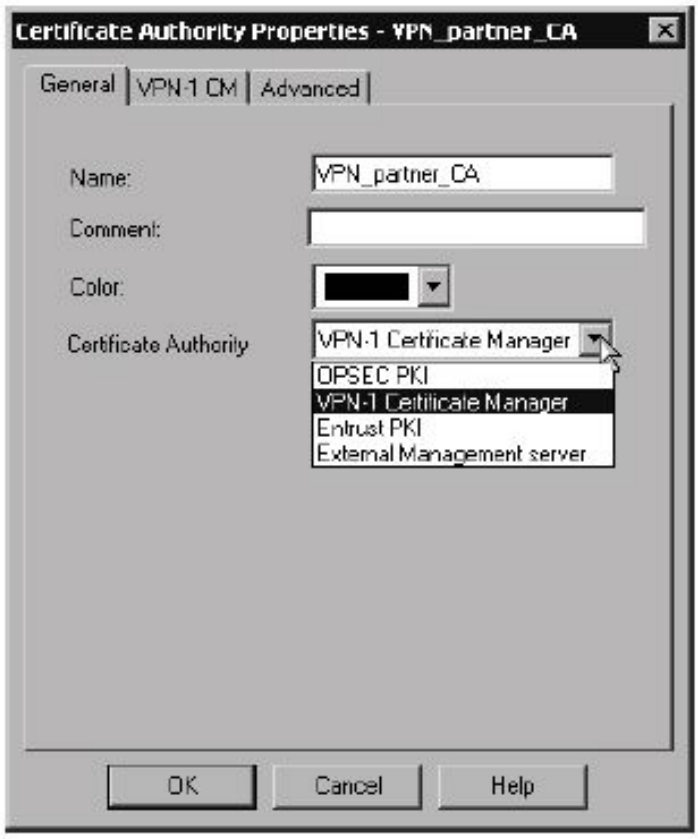
Answer: E

Explanation: p208 Check Point Mgmt II Student Manual

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.comfor 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



9

Question No : 5 - (Topic 1)

Dr Billis 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 King. 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 Billto 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 King.Dr Billneeds physicalto the SecuRemote machine to load the certificate.
D. Dr Billmust 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

Explanation: p271 Check Point Mgmt II Student Manual

Question No : 6 - (Topic 1)

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 No : 7 - (Topic 1)

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.

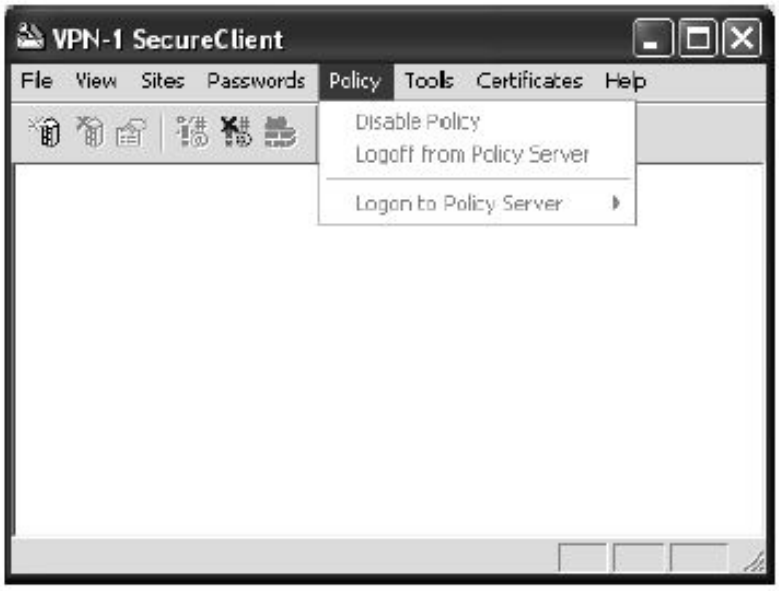
Answer: B,D,E

Explanation:

Understanding SecureClient

SecureClient is the same software as SecuRemote, with added functionality. Just as with SecuRemote, the client-to-site VPNs created with Secure-Client 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



9

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 Secure-Client 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 No : 8 - (Topic 1)

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 No : 9 - (Topic 1)

Dr Billis using VPN-1/FireWall-1 to provide load balancing for his Web servers. When a client initiates a session with one of Dr King'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 King'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 No : 10 - (Topic 1)

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 No : 11 - (Topic 1)

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.