PASSTCERT
QUESTION & ANSWER

Higher Quality
Better Service!

Exam : **156-310**

Title : Check Point CCSE NG

Version : Demo

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

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

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

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

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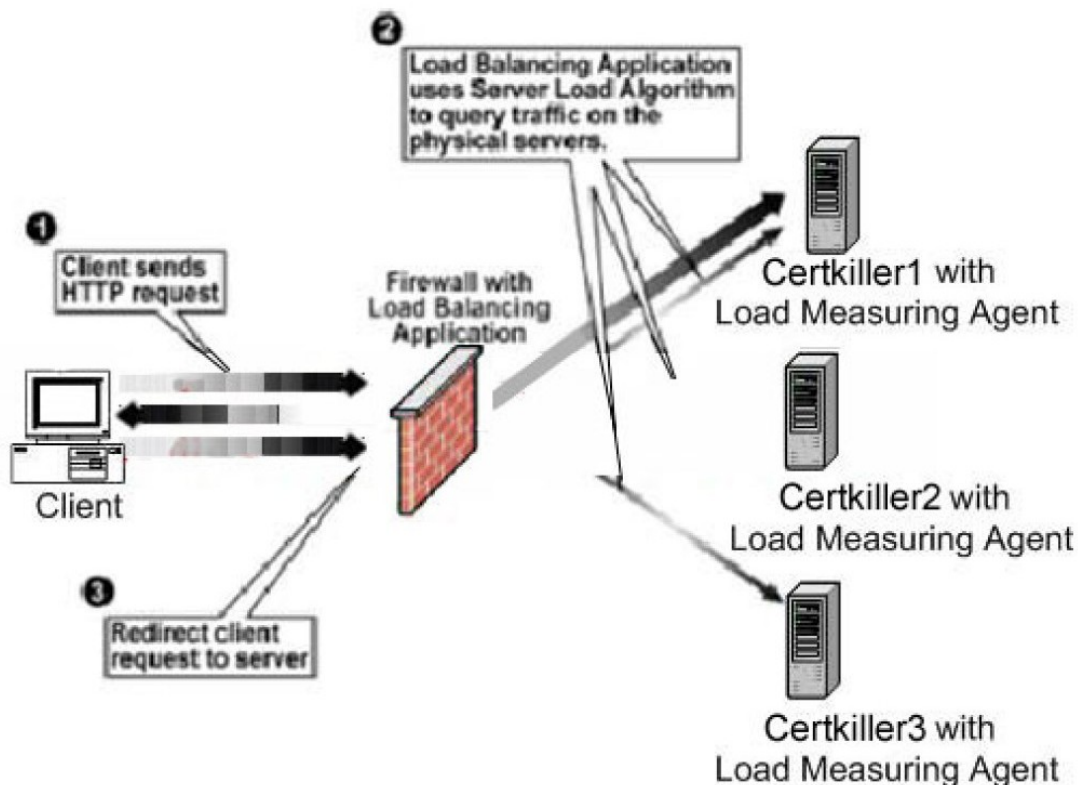files to external FTP Servers, while allowing users to retrieve files?

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

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

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

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

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

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

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.
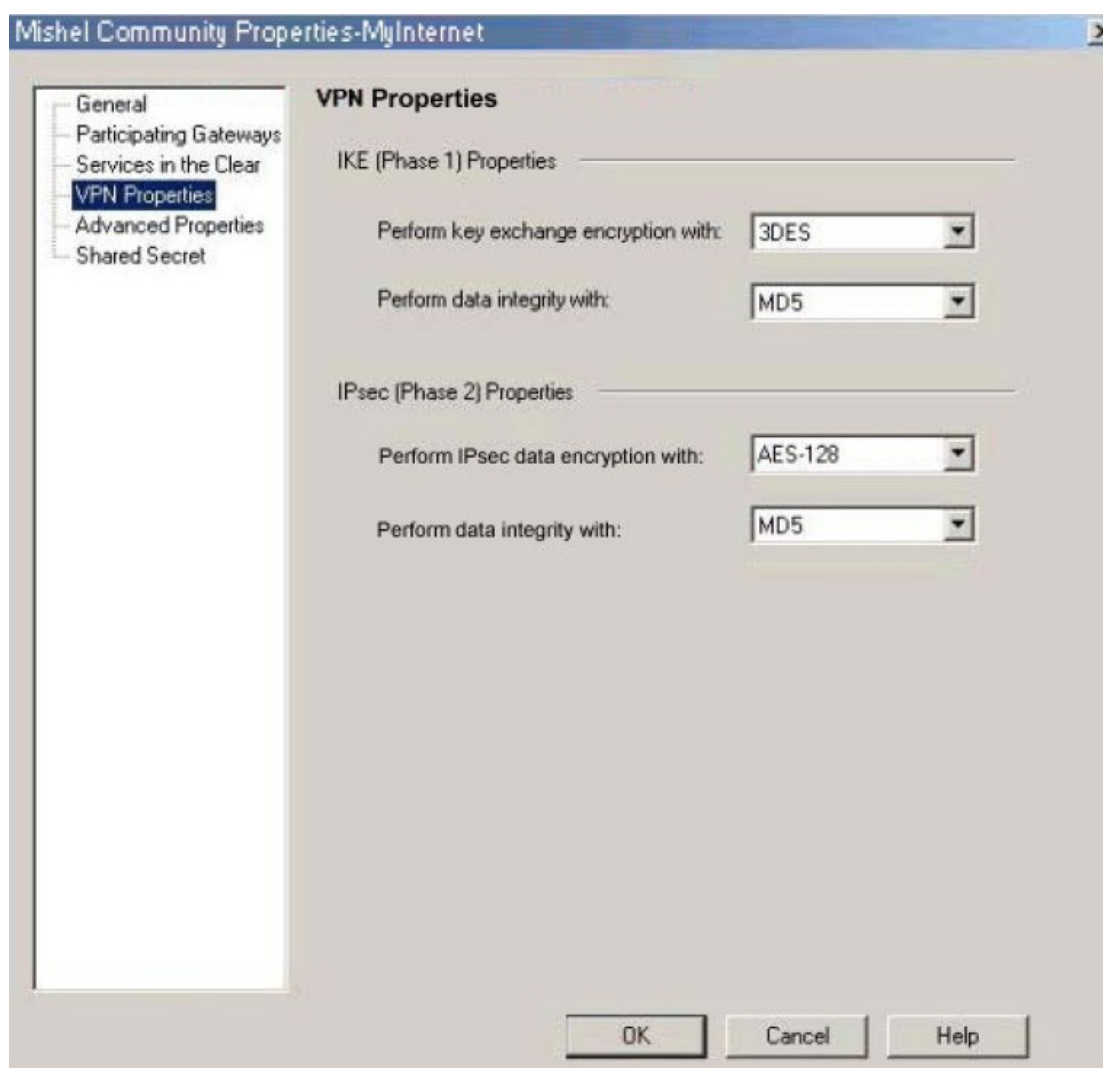The Security Policy Rule Base is used to define VPN connection parameters for

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

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

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

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 and 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 VPNSs.
C. VPN Domains are used in Microsoft environments, and allow VPN-1/FireWall1- 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

15.Ken us assisting a user whose SecurityClient 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 as 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

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

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

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

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

20.You are using Hybrid IKE for Client Authentication. SecureClient produces the error Certifcation 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

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

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

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

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

25.Diffie-Hellman uses which type of key exchange?

A. Static

B. Dynamic

C. Symmetric

D. Asymmetric

E. Adaptive

Answer: D

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

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

Results of ipconfig/all

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

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

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

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

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