

Check Point CCSE NGX (Exam 156-315.1)

1

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.

2

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 gateway-to-gateway encryption? Choose two.

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

3

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

- Confirmed that the Network Interface Card, Ethernet cable, and router port are all functioning properly.
- 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.
- Used Ping to confirm connectivity with the default gateway and upstream router.
- Completed an FTP session to an Internet host.
- Tried to Telnet to a host in the VPN Domain; this attempt failed.

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

- A. Eric'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. Eric'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. Eric's methodology is valid, and his conclusion is correct. Because Eric has tested all seven layers of the OSI Model on the SecureClient machine, the problem must be malfunctioning SecureClient software.
- D. Eric'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. Eric's tests and conclusion are invalid. SecureClient operates between the Presentation and Session Layers of the OSI Model, and Eric only tested up to the Transport Layer.

4

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.

5

Tammi 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 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.

6

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.