

SectionA: 65 Questions

SectionB: 64 Questions

SectionC: 64 Questions

### SectionA

1. Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs are only supported on Nokia IPSO
- B. VTIs are assigned only local addresses, not remote addresses
- C. VTIs can use an already existing physical-interface IP address
- D. VTIs may share an IP address

Answer: D

2. Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs cannot use an already existing physical-interface IP address
- B. VTIs are assigned only local addresses, not remote addresses
- C. VTIs are only supported on Nokia IPSO
- D. VTIs cannot share IP addresses

Answer: A

3. Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs are assigned only local addresses, not remote addresses
- B. VTIs can use an already existing physical-interface IP address
- C. VTIs are supported on SecurePlatform
- D. VTIs cannot share IP addresses

Answer: C

4. When configuring VPN High Availability (HA) with MEP, which of the following is correct?

- A. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues.
- B. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
- C. MEP VPN Gateways cannot be geographically separated machines.
- D. MEP Gateways must be managed by the same SmartCenter Server.

Answer: B

5. When configuring site-to-site VPN High Availability (HA) with MEP, which of the following is correct?

- A. If one MEP Security Gateway fails, the connection is lost and the backup Gateway picks up the next connection.
- B. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.
- C. MEP Gateways cannot be geographically separated machines.
- D. MEP Gateways must be managed by the same SmartCenter Server.

Answer: A

6. Control connections between the SmartCenter Server and the Gateway are not encrypted by the VPN Community. How are these connections secured?

- A. They are not secured.
- B. They are not encrypted, but are authenticated by the Gateway
- C. They are encrypted and authenticated using SIC.
- D. They are secured by PPTP

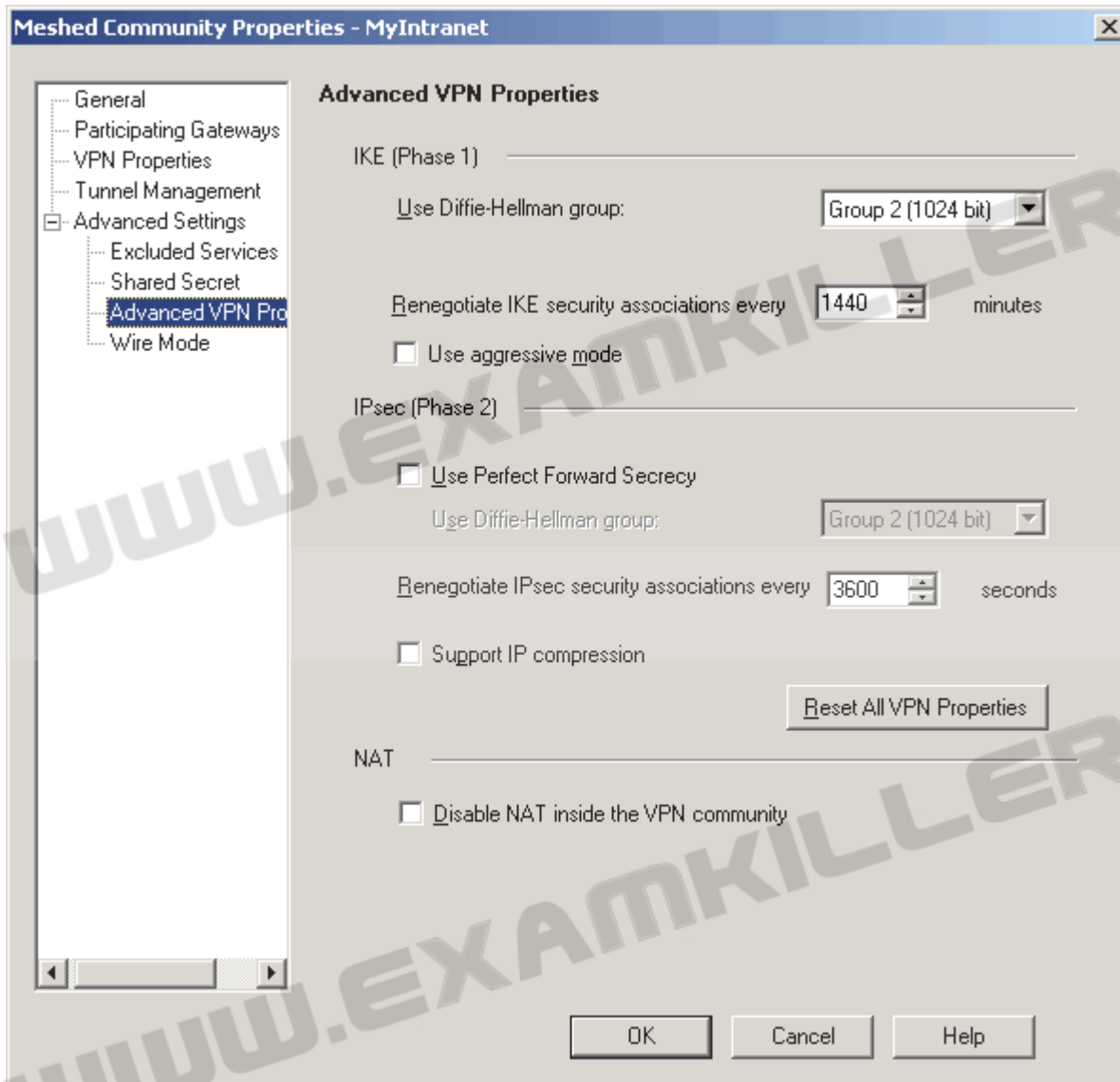
Answer: C

7. Multi-Corp wants to implement IKE DoS protection to prevent a denial-of-service (DoS) attack from paralyzing its VPN Communities. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations would BEST enable this new protection with minimal impact to the organization?

- A. Set both "Support IKE DoS protection from identified source", and "Support IKE DoS protection from unidentified source" to "Stateless".
- B. Set both "Support IKE Dos protection from identified source", and "Support IKE DoS protection from unidentified source" to "Puzzles".
- C. Set "Support IKE DoS protection from identified source" to "Puzzles", and "Support IKE DoS protection from unidentified source" to "Stateless".
- D. Set "Support IKE DoS protection from identified source" to "Stateless", and "Support IKE DoS protection from unidentified source" to "None".

Answer: A

8. Look at the Advanced Properties screen exhibit. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?



- A. Change the setting "Use Diffie-Hellman group:" to "Group 5 (1536 bit)"
- B. Change the "Renegotiate IPsec security associations every 3600 seconds" to 7200
- C. Check the box "Use Perfect Forward Secrecy"
- D. Check the box "Use aggressive mode"

Answer: B

9. Which of the following is TRUE concerning control connections between the SmartCenter Server and the Gateway in a VPN Community?

- A. Control Connections are encrypted using SIC and re-encrypted again by the Community regardless of

VPN domain configuration

- B. Control Connections are encrypted using SIC and re-encrypted again by the Community but only if the Gateway is also included in the VPN domain configuration
- C. Control Connections are encrypted by the Community (redundant SIC encryption is bypassed)
- D. Control Connections are not encrypted, only authenticated

Answer: B

10. Which of the following is TRUE concerning control connections between the SmartCenter Server and the Gateway in a VPN Community?

- A. Control Connections are encrypted using SIC and re-encrypted again by the Community regardless of VPN domain configuration
- B. Control Connections are not encrypted, only authenticated
- C. Control Connections are encrypted by the Community
- D. Control Connections are encrypted using SIC

Answer: D

11. You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting "All IP Addresses behind Gateway based on Topology information."

You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPsec tunnels instead of the routed VTI tunnels.

What is the problem and how do you make the VPN to use the VTI tunnels?

- A. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, use an empty group object as each Gateway's VPN Domain
- B. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community
- C. Route-based VTI takes precedence over the Domain VPN. To make the VPN go through VTI, use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes