300-730 Q&As

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/300-730.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
Dst             src             state          conn-id        slot     status
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0      ACTIVE
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0      ACTIVE (deleted)
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0      ACTIVE
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0      ACTIVE (deleted)


Router#debug crypto isakmp

01:12:45.250: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
01:12:45.250: ISAKMP:(0): beginning Main Mode exchange
01:12:45.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:45.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:12:55.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
01:12:55.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:55.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

VPN tunnels between a spoke and two DMVPN hubs are not coming up. The network administrator has verified that the encryption, hashing, and DH group proposals for Phase 1 and Phase 2 match on both ends. What is the solution to this issue?

A. Ensure bidirectional UDP 500/4500 traffic.

B. Increase the isakmp phase 1 lifetime.

C. Add NAT statements for VPN traffic.

D. Enable shared tunnel protection.

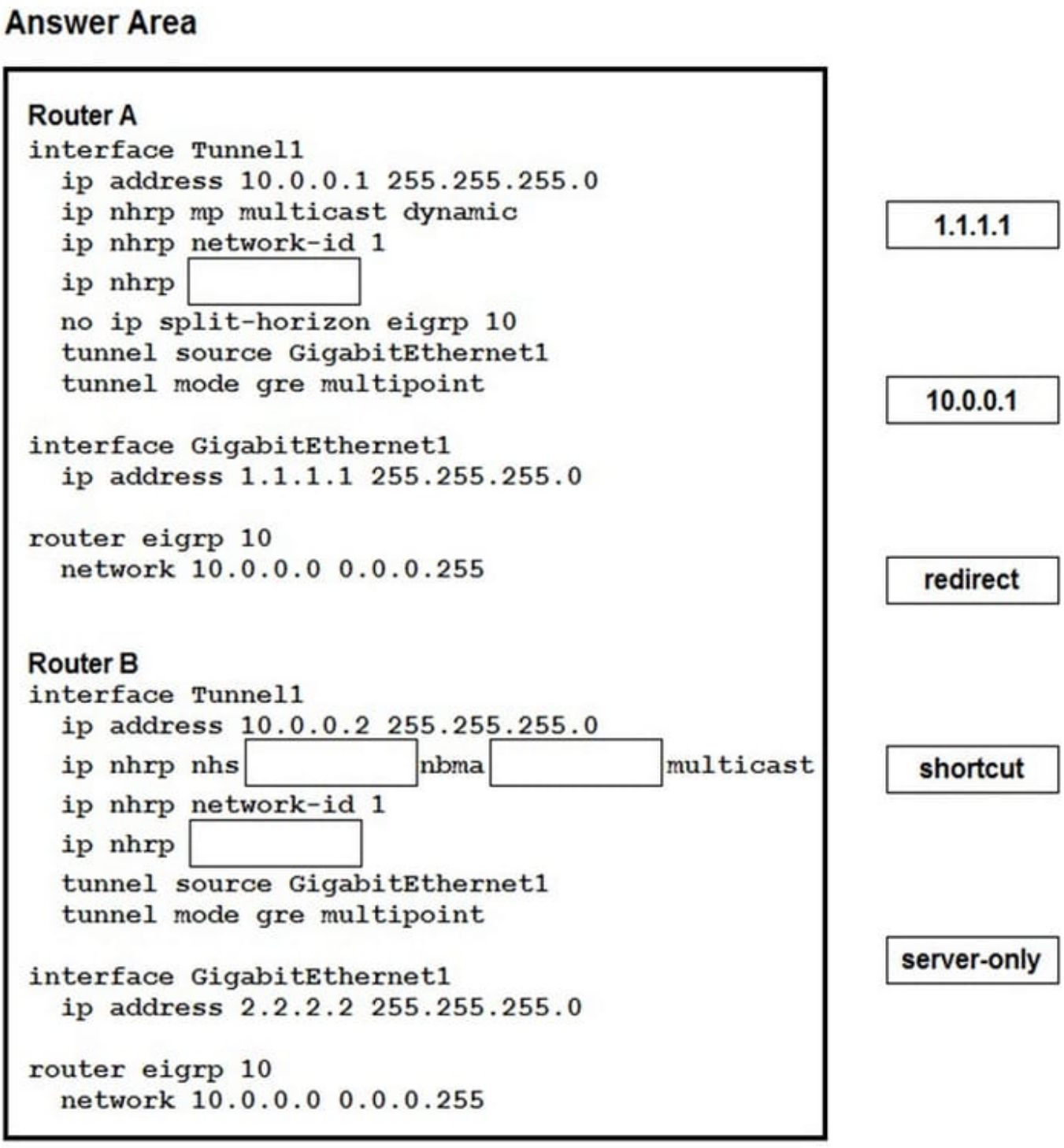
Correct Answer: A

QUESTION 2

DRAG DROP

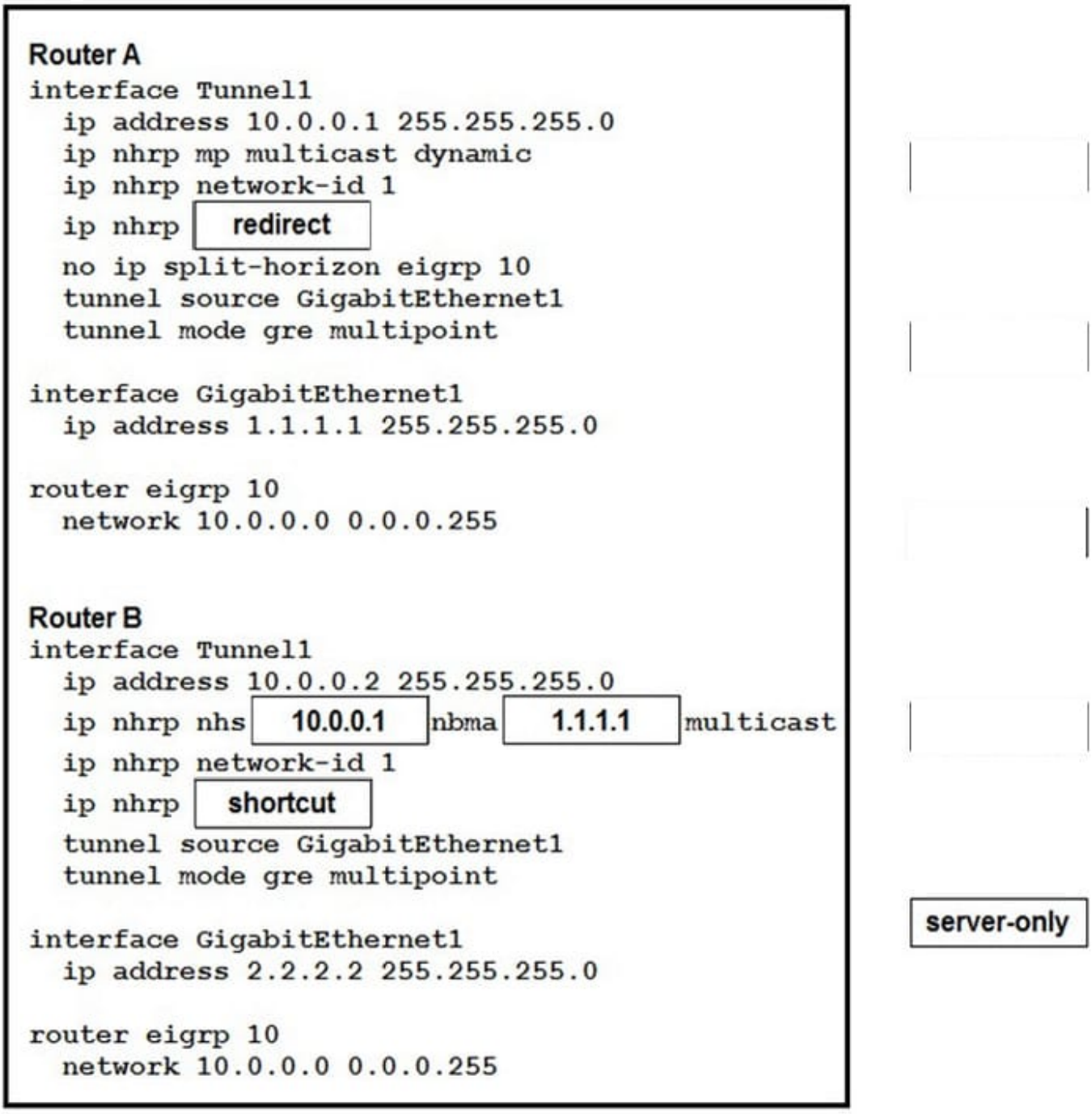
Drag and drop the correct commands from the night onto the blanks within the code on the left to implement a design that allow for dynamic spoke-to-spoke communication. Not all comments are used.

Select and Place:



Correct Answer:

Answer Area



Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-summ-maps.html

QUESTION 3

Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?

A. DMVPN with ISAKMP

B. GETVPN with ISAKMP

C. DMVPN with NHRP

D. GETVPN with NHRP

Correct Answer: C

QUESTION 4

Refer to the exhibit.

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):       encryption AES-CBC
ISAKMP: (0):       keylength of 256
ISAKMP: (0):       hash SHA256
ISAKMP: (0):       default group 14
ISAKMP: (0):       auth pre-share
ISAKMP: (0):       life type in seconds
ISAKMP: (0):       life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

A. An authentication failure occurs on the remote peer.

B. A certificate fragmentation issue occurs between both sides.

C. UDP 4500 traffic from the peer does not reach the router.

D. An authentication failure occurs on the router.

Correct Answer: C

QUESTION 5

A network engineer is implementing a FlexVPN tunnel between two Cisco IOS routers. The FlexVPN tunnels will terminate on encrypted traffic on an interface configured with an IP MTU of 1500, and the company has a security policy to drop fragmented traffic coming into or leaving the network. The tunnel will be used to transfer TFTP data between users and internal servers. When the TFTP traffic is not traversing a VPN, it can have a maximum IP packet size of 1500. Assuming the encrypted payload will add 90 bytes, which configuration allows TFTP traffic to traverse the FlexVPN tunnel without being dropped?

A. Set the tunnel IP MTU to 1500.

B. Set the tunnel tcp adjust-mss to 1460.

C. Set the tunnel IP MTU to 1400.

D. Set the tunnel tcp adjust-mss to 1360.

Correct Answer: C

tcp adjust-mss is for tcp traffic only. TFTP is UDP. The only answer can be C.