DUMPSBOSS.COM

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Cisco 300-730

Version Demo

Total Demo Questions: 10

Total Premium Questions: 149

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	51
Topic 2, Site-to-site Virtual Private Networks on Routers and Firewalls	10
Topic 3, Remote access VPNs	18
Topic 4, Troubleshooting using ASDM and CLI	12
Topic 5, Secure Communications Architectures	20
Topic 6, Mixed Questions	38
Total	149

QUESTION NO: 1

```
aaa authentication login default local
aaa authorization network Flex_AAA local

crypto ikev2 authorization policy Flex_Auth
 route set remote ipv4 10.0.0.0 255.255.255.0

crypto ikev2 proposal Crypto_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Crypto_Policy
 proposal Crypto_Proposal

crypto ikev2 keyring FlexKey
 peer any
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !

crypto ikev2 profile IKEv2_Profile
 match identity remote address 192.168.0.12 255.255.255.255
 authentication local pre-share
 authentication remote pre-share
 keyring local FlexKey
 aaa authorization group cert list Flex_AAA Flex_Auth

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile FlexVPN_Ipsec
 set transform-set TS
 set ikev2-profile IKEv2_Profile

interface Tunnel1
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 192.168.0.12
 tunnel protection ipsec profile FlexVPN_Ipsec
```

Refer to the exhibit. The VPN tunnel between the FlexVPN spoke and FlexVPN hub 192.168.0.12 is failing. What should be done to correct this issue?

A. Add the address 192.168.0.12 255.255.255.255 command to the keyring configuration.

B. Add the match fvrf any command to the IKEv2 policy.

C. Add the aaa authorization group psk list Flex_AAA Flex_Auth command to the IKEv2 profile configuration.

D. Add the tunnel mode gre ip command to the tunnel configuration.

ANSWER: C

QUESTION NO: 2

A network engineer is configuring a server. The router will terminate encrypted VPN connections on g0/0, which is in the VRF "Internet". The clear-text traffic that must be encrypted before being sent out traverses g0/1, which is in the VRF "Internal". Which two VRF-specific configurations allow VPN traffic to traverse the VRF-aware interfaces? (Choose two.)

A. Under the IKEv2 profile, add the ivrf Internal command.

B. Under the virtual-template interface, add the ip vrf forwarding Internet command.

C. Under the IKEv2 profile, add the match fvrf Internal command.

D. Under the IKEv2 profile, add the match fvrf Internet command.

E. Under the virtual-template interface, add the tunnel vrf Internet command.

ANSWER: B D

QUESTION NO: 3

Which two types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose two.)

A. SAML

B. NTLM

C. Kerberos

D. OAuth 2.0

E. HTTP Basic

ANSWER: B E

QUESTION NO: 4

```
tunnel-group client general-attributes
address-pool MYPOOL
authentication-server-group RADIUS
tunnel-group client ipsec-attributes
pre-shared-key test123
```

Refer to the exhibit. Which type of VPN is used?

A. GETVPN

B. clientless SSL VPN

C. Cisco Easy VPN

D. Cisco AnyConnect SSL VPN

ANSWER: C

QUESTION NO: 5

A network engineer must design a clientless VPN solution for a company. VPN users must be able to access several internal web servers. When reachability to those web servers was tested, it was found that one website is not being rewritten correctly by the ASA. What is a potential solution for this issue while still allowing it to be a clientless VPN setup?

A. Set up a smart tunnel with the IP address of the web server.

B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.

C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.

D. Set up a WebACL to permit the IP address of the web server.

ANSWER: A

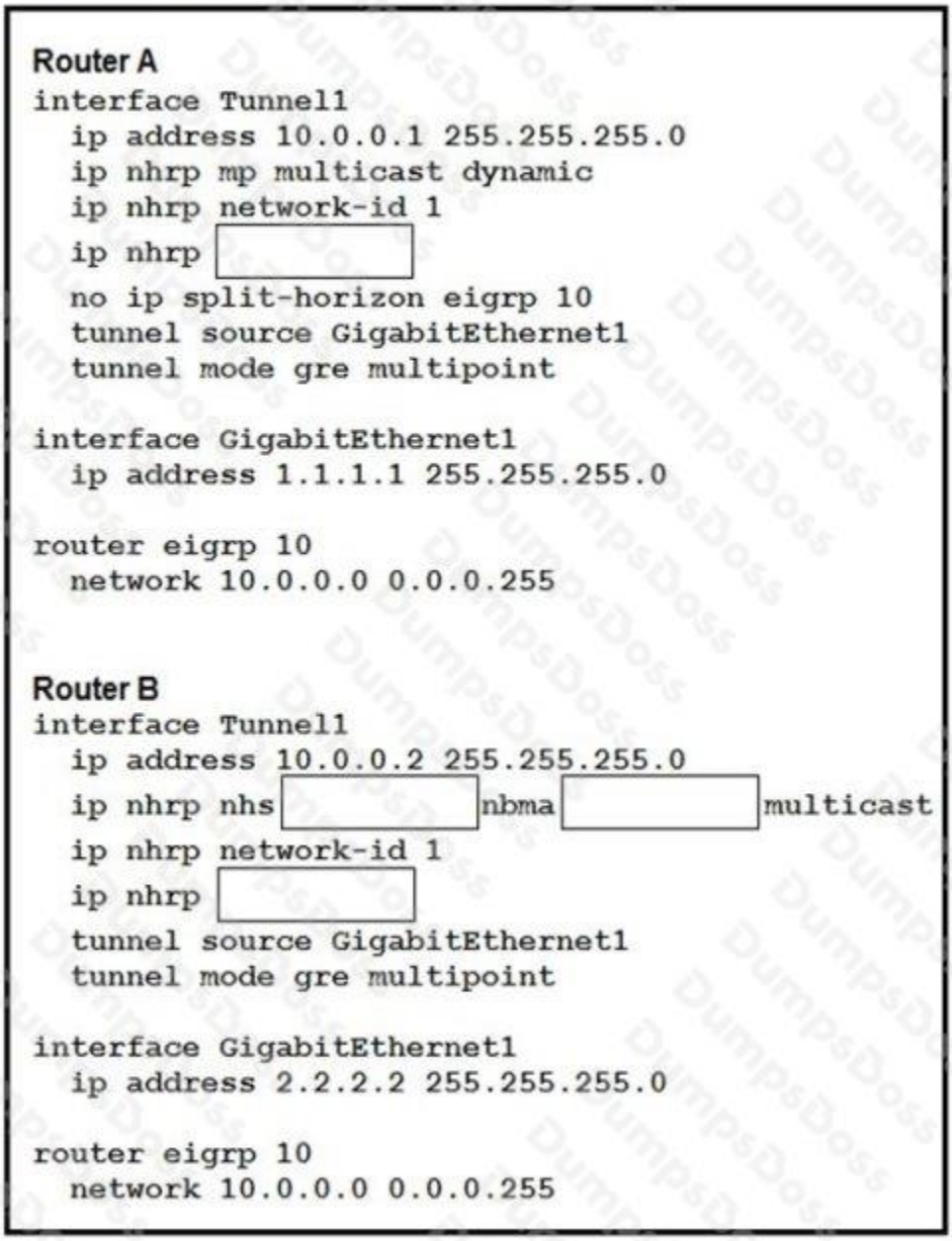
QUESTION NO: 6 - (DRAG DROP)

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:

Answer Area



1.1.1.1

10.0.0.1

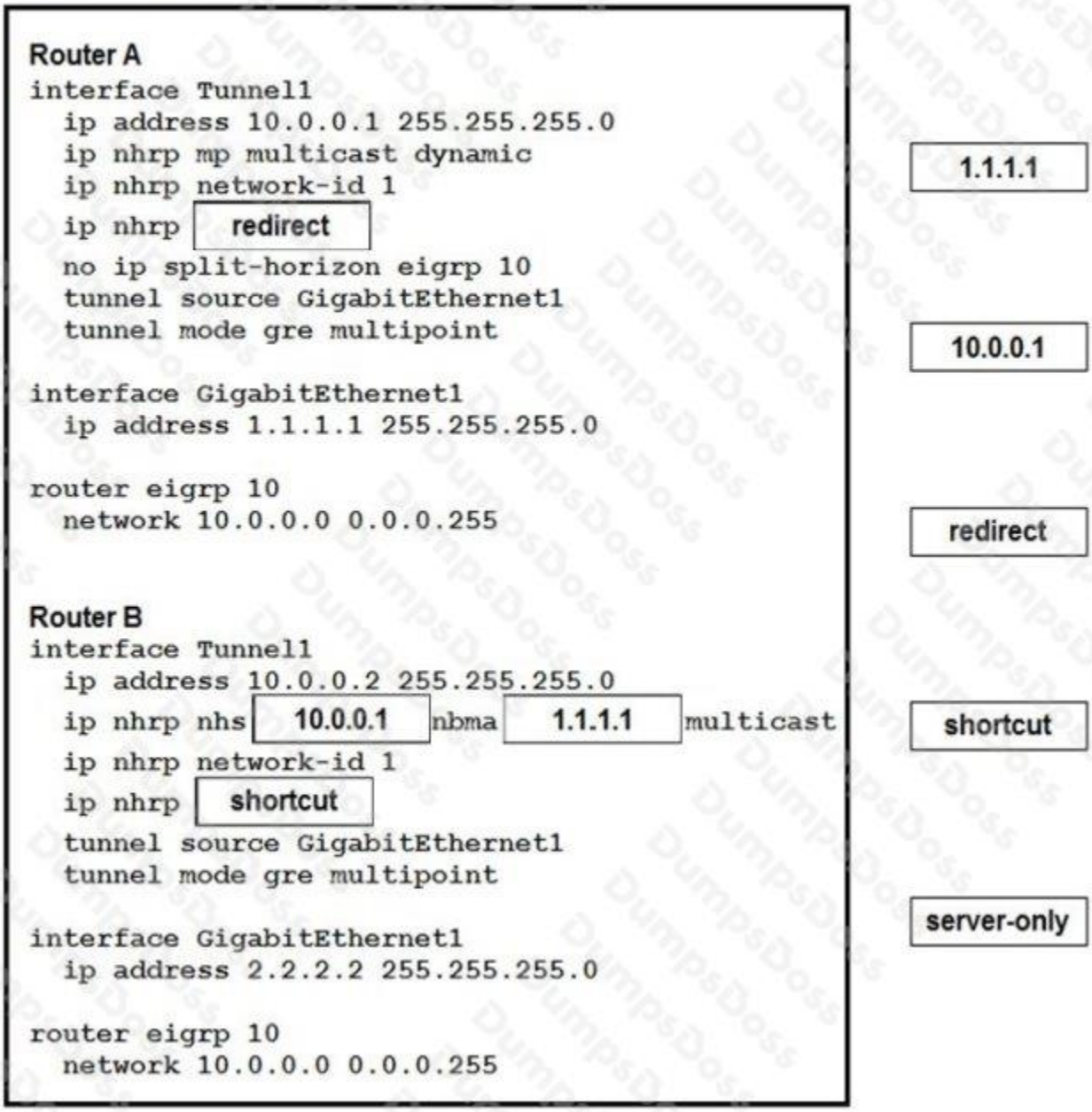
redirect

shortcut

server-only

ANSWER:

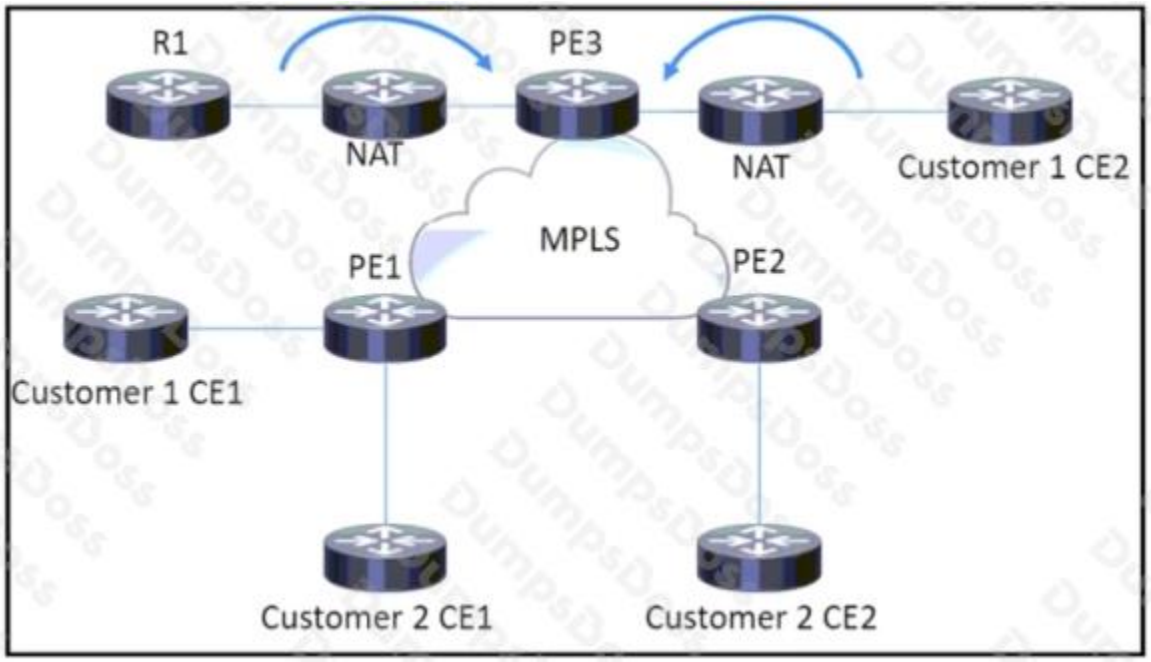
Answer Area



Explanation:

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 NO: 7



Which component must be configured on routers for a GETVPN deployment work properly?

A. PE3: Key Server – Customer 2 CEs: Group Members

B. Customer 1 CE1: Key Server – R1 and Customer 1 CE2: Group Members

C. R1: Key Server – Customer 1 CEs: Group Members

D. PE3: Key Server – all CEs: Group Members

ANSWER: A

QUESTION NO: 8

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
    500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
    failed its sanity check or is malformed
```

Refer to the exhibit. Which type of mismatch is causing the problem with the IPsec VPN tunnel?

A. crypto access list

B. Phase 1 policy

C. transform set

D. preshared key

ANSWER: D

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409ipsec-debug-00.html#ike

QUESTION NO: 9

What are two functions of ECDH and ECDSA? (Choose two.)

A. nonrepudiation

B. revocation

C. digital signature

D. key exchange

E. encryption

ANSWER: C D

Explanation:

Reference: https://tools.cisco.com/security/center/resources/next_generation_cryptography

QUESTION NO: 10

Which two components are required in a Cisco IOS GETVPN key server configuration? (Choose two.)

A. RSA key

B. IKE policy

C. SSL cipher

D. GRE tunnel

E. L2TP protocol

ANSWER: A B