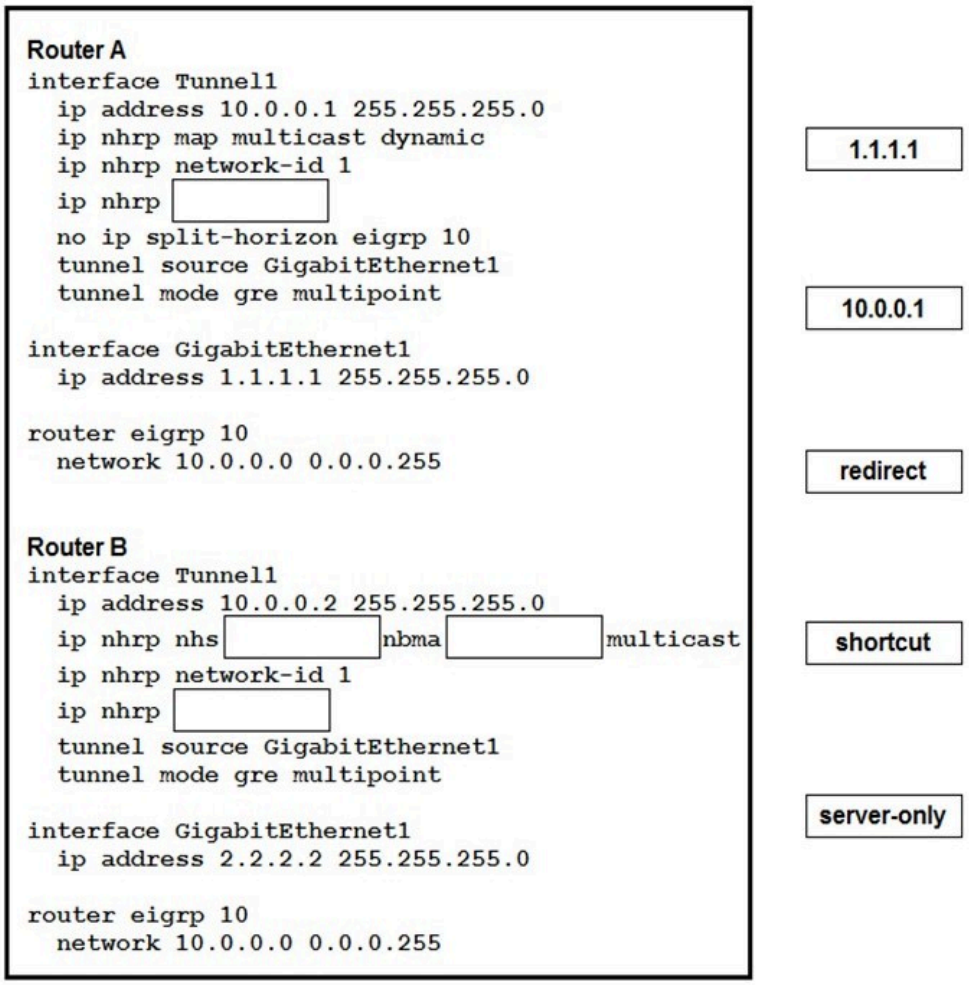
Implementing Secure Solutions with Virtual Private Networks (SVPN 300-730)

1. DRAG DROP (Drag and Drop is not supported)
Drag and drop the correct commands from the right onto the blanks within the code on the left to implement a design that allow for dynamic spoke-to-spoke communication. Not all commands are used.
Select and Place:

Answer Area



A. See Explanation section for answer.

Answer(s): A

---

2. A second set of traffic selectors is negotiated between two peers using IKEv2. Which IKEv2 packet will contain details of the exchange?

A. IKEv2 IKE_SA_INIT

B. IKEv2 INFORMATIONAL

C. IKEv2 CREATE_CHILD_SA

D. IKEv2 IKE_AUTH

Answer(s): B

---

3. Refer to the exhibit.

```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:02:09, expire 00:00:01
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:13:25, 01:46:34
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 3.3.3.1
```

The DMVPN tunnel is dropping randomly and no tunnel protection is configured. Which spoke configuration mitigates tunnel drops?

A.

B.

C.

D.

Answer(s): D

---

4. On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

A. interface virtual-access

B. ip nhrp redirect

C. interface tunnel

D. interface virtual-template

Answer(s): C

---

5. Which statement about GETVPN is true?

A. The configuration that defines which traffic to encrypt originates from the key server.

B. TEK rekeys can be load-balanced between two key servers operating in COOP.

C. The pseudotime that is used for replay checking is synchronized via NTP.

D. Group members must acknowledge all KEK and TEK rekeys, regardless of configuration.

Answer(s): A

---

6. Refer to the exhibit. Which two tunnel types produce the show crypto ipsec sa output seen in the exhibit? (Choose two.)

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.1, remote crypto endpt.: 192.168.0.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0x3D05D003(1023791107)
     PFS (Y/N): N, DH group: none
```

- [ ] A. crypto map
- [ ] B. DMVPN
- [ ] C. GRE
- [ ] D. FlexVPN
- [ ] E. VTI

Answer(s): B E

---

7. Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

- [ ] A. Add NHRP shortcuts on the hub.
- [ ] B. Add NHRP redirects on the spoke.
- [ ] C. Disable EIGRP next-hop-self on the hub.
- [ ] D. Enable EIGRP next-hop-self on the hub.
- [ ] E. Add NHRP redirects on the hub.

Answer(s): C E

---

8. Refer to the exhibit. A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

- [ ] A. Reduce the maximum SA limit on the local Cisco AS

B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.

C. Remove the maximum SA limit on the remote Cisco ASA.

D. Correct the crypto access list on both Cisco ASA devices.

Answer(s): B

---

9. Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

- [ ] A. group-alias
- [ ] B. certificate map
- [ ] C. optimal gateway selection
- [ ] D. group-url
- [ ] E. AnyConnect client version

Answer(s): B D

---

10. Which method dynamically installs the network routes for remote tunnel endpoints?

A. policy-based routing

B. CEF

C. reverse route injection

D. route filtering

Answer(s): C

---

11. Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?

A. svc import profile SSL_profile flash:simos-profile.xml

B. anyconnect profile SSL_profile flash:simos-profile.xml

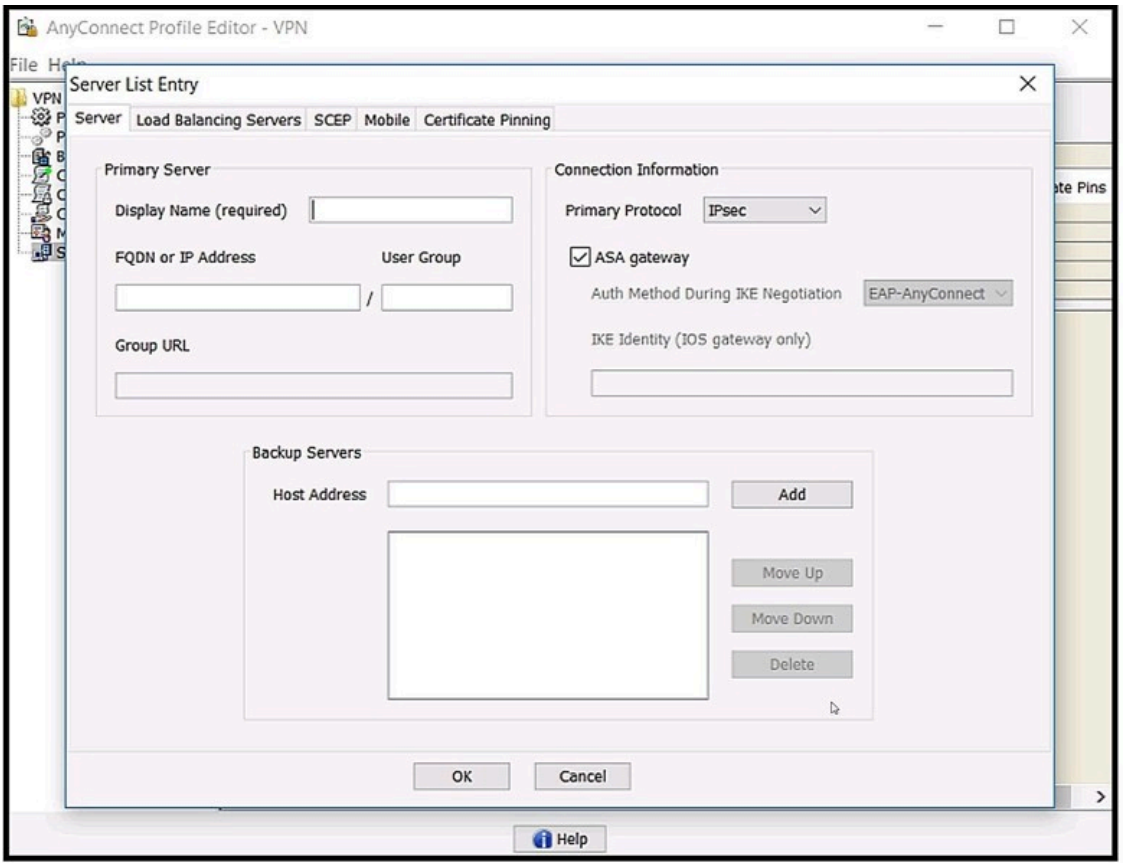
C. crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml

D. webvpn import profile SSL_profile flash:simos-profile.xml

Answer(s): C

---

12. Refer to the exhibit. Which value must be configured in the User Group field when the Cisco AnyConnect Profile is created to connect to an ASA headend with IPsec as the primary protocol?



A. address-pool

B. group-alias

C. group-policy

D. tunnel-group

Answer(s): D

---

13. Refer to the exhibit. What is configured as a result of this command set?

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list
author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
```

A. FlexVPN client profile for IPv6

B. FlexVPN server to authorize groups by using an IPv6 external AAA

C. FlexVPN server for an IPv6 dVTI session

D. FlexVPN server to authenticate IPv6 peers by using EAP

Answer(s): C

---

14. Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

- [ ] A. HTTP
- [ ] B. ICA (Citrix)
- [ ] C. VNC

- [ ] D. RDP
- [ ] E. CIFS

Answer(s): D E

---

15. Which configuration construct must be used in a FlexVPN tunnel?

A. EAP configuration

B. multipoint GRE tunnel interface

C. IKEv1 policy

D. IKEv2 profile

Answer(s): D

---

16. A Cisco AnyConnect client establishes a SSL VPN connection with an ASA at the corporate office. An engineer must ensure that the client computer meets the enterprise security policy. Which feature can update the client to meet an enterprise security policy?

A. Endpoint Assessment

B. Cisco Secure Desktop

C. Basic Host Scan

D. Advanced Endpoint Assessment

Answer(s): D

---

17. Which two features provide headend resiliency for Cisco AnyConnect clients? (Choose two.)

- [ ] A. AnyConnect Auto Reconnect
- [ ] B. AnyConnect Network Access Manager
- [ ] C. AnyConnect Backup Servers
- [ ] D. ASA failover
- [ ] E. AnyConnect Always On

Answer(s): C D

---

18. Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

A. The XML profile is not configured correctly for the affected users.

B. The new client image does not use the same major release as the current one.

C. Client services are not enabled.

D. Client software updates are not supported with IKEv2.

Answer(s): C

---

19. Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

A. tunnel-group (general-attributes)

B. tunnel-group (webvpn-attributes)

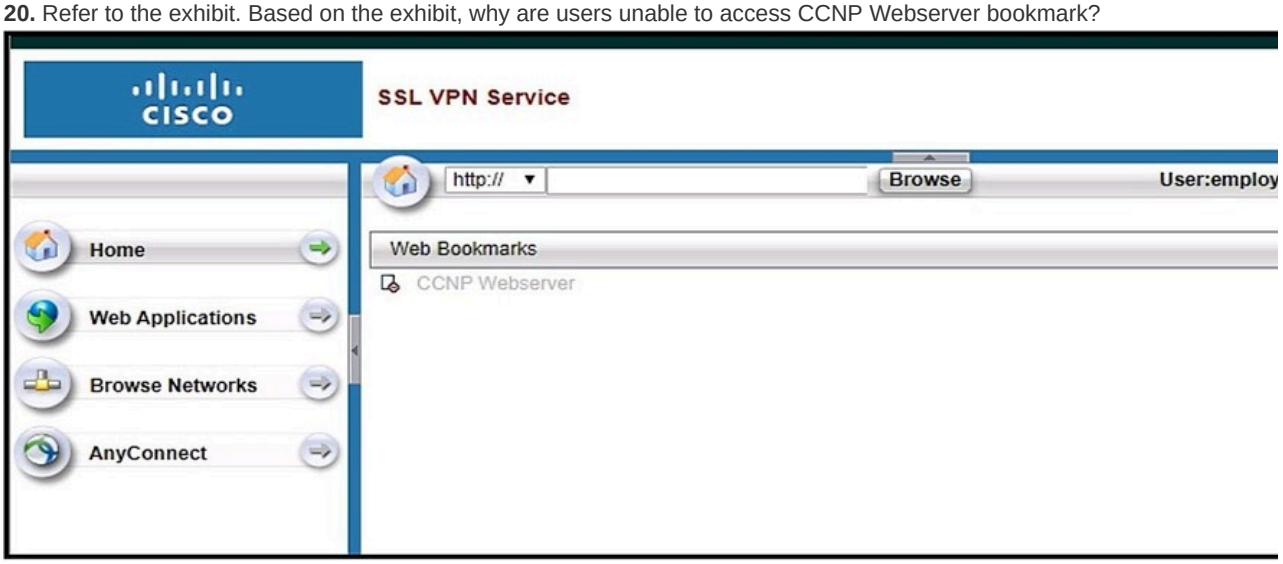
C. webvpn (group-policy)

D. webvpn (global configuration)

Answer(s): C

---

20. Refer to the exhibit. Based on the exhibit, why are users unable to access CCNP Webserver bookmark?



A. The URL is being blocked by a WebACL.

B. The ASA cannot resolve the URL.

C. The bookmark has been disabled.

D. The user cannot access the URL.

Answer(s): B
