

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **300-730**

Title : Implementing Secure
Solutions with Virtual
Private Networks (SVPN)

Version : DEMO

1.DRAG DROP

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 comments are used.

Answer Area

Router A	
<code>interface Tunnell</code>	
<code>ip address 10.0.0.1 255.255.255.0</code>	<input type="text" value="1.1.1.1"/>
<code>ip nhrp mp multicast dynamic</code>	
<code>ip nhrp network-id 1</code>	
<code>ip nhrp <input type="text"/></code>	<input type="text" value="10.0.0.1"/>
<code>no ip split-horizon eigrp 10</code>	
<code>tunnel source GigabitEthernet1</code>	
<code>tunnel mode gre multipoint</code>	
<code>interface GigabitEthernet1</code>	
<code>ip address 1.1.1.1 255.255.255.0</code>	
<code>router eigrp 10</code>	
<code>network 10.0.0.0 0.0.0.255</code>	<input type="text" value="redirect"/>
Router B	
<code>interface Tunnell</code>	
<code>ip address 10.0.0.2 255.255.255.0</code>	
<code>ip nhrp nhs <input type="text"/> nbma <input type="text"/> multicast</code>	<input type="text" value="shortcut"/>
<code>ip nhrp network-id 1</code>	
<code>ip nhrp <input type="text"/></code>	
<code>tunnel source GigabitEthernet1</code>	
<code>tunnel mode gre multipoint</code>	
<code>interface GigabitEthernet1</code>	
<code>ip address 2.2.2.2 255.255.255.0</code>	<input type="text" value="server-only"/>
<code>router eigrp 10</code>	
<code>network 10.0.0.0 0.0.0.255</code>	

Answer:

Answer Area

Router A

```
interface Tunnell
  ip address 10.0.0.1 255.255.255.0
  ip nhrp mp multicast dynamic
  ip nhrp network-id 1
  ip nhrp redirect
  no ip split-horizon eigrp 10
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint
```

1.1.1.1

```
interface GigabitEthernet1
  ip address 1.1.1.1 255.255.255.0
```

10.0.0.1

```
router eigrp 10
  network 10.0.0.0 0.0.0.255
```

redirect

Router B

```
interface Tunnell
  ip address 10.0.0.2 255.255.255.0
  ip nhrp nhs 10.0.0.1 nbma 1.1.1.1 multicast
  ip nhrp network-id 1
  ip nhrp shortcut
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint
```

shortcut

```
interface GigabitEthernet1
  ip address 2.2.2.2 255.255.255.0
```

server-only

```
router eigrp 10
  network 10.0.0.0 0.0.0.255
```

Explanation:

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

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: C**Explanation:**

The IKEv2 CREATE_CHILD_SA packet is used to establish a new security association (SA) between two peers. This packet contains the details of the exchange, including the traffic selectors, the cryptographic algorithms and keys to be used, and any other relevant information

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)

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

B)


```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

C)

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 20
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

D)

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

<https://www.globalknowledge.com/us-en/resources/resource-library/articles/understanding-next-hop-resolution-protocol-commands/>

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: D

Explanation:

On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, the command that is needed for the hub to be able to terminate FlexVPN tunnels is interface virtual-template. The interface virtual-template command is used to configure a virtual template interface which provides a secure tunnel for FlexVPN connections. The other commands listed - interface virtual-access, ip nhrp redirect, and interface tunnel - are not related to FlexVPN and are not used to terminate FlexVPN tunnels.

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: A

Explanation:

KS (key server) is 'caretaker' of the GM group. Group registrations and authentication of GMs is taken care of by KS server. Any GM who wants to join the group is required to be successfully authenticated in the group and sends encryption keys and policy to be used within the group.

<https://ipwithease.com/introduction-to-getvpn/>