

Cisco

300-730 Exam

Implementing Secure Solutions with Virtual Private Networks

Questions & Answers

Demo

Version: 5.0

Topic 1, Site-to-site Virtual Private Networks on Routers and Firewall

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

interface GigabitEthernet1
 ip address 1.1.1.1 255.255.255.0

router eigrp 10
 network 10.0.0.0 0.0.0.255

Router B
interface Tunnell
 ip address 10.0.0.2 255.255.255.0
 ip nhrp nhs [ ] nbma [ ] multicast
 ip nhrp network-id 1
 ip nhrp [ ]
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint

interface GigabitEthernet1
 ip address 2.2.2.2 255.255.255.0

router eigrp 10
 network 10.0.0.0 0.0.0.255
    
```

1.1.1.1

10.0.0.1

redirect

shortcut

server-only

Answer:

Explanation:

Answer Area

Router A	
interface Tunnel1	
ip address 10.0.0.1 255.255.255.0	
ip nhrp mp multicast dynamic	
ip nhrp network-id 1	
ip nhrp <input type="text" value="redirect"/>	<input type="text" value="1.1.1.1"/>
no ip split-horizon eigrp 10	
tunnel source GigabitEthernet1	
tunnel mode gre multipoint	<input type="text" value="10.0.0.1"/>
interface GigabitEthernet1	
ip address 1.1.1.1 255.255.255.0	
router eigrp 10	
network 10.0.0.0 0.0.0.255	<input type="text" value="redirect"/>
Router B	
interface Tunnel1	
ip address 10.0.0.2 255.255.255.0	
ip nhrp nhs <input type="text" value="10.0.0.1"/> nbma <input type="text" value="1.1.1.1"/> multicast	<input type="text" value="shortcut"/>
ip nhrp network-id 1	
ip nhrp <input type="text" value="shortcut"/>	
tunnel source GigabitEthernet1	
tunnel mode gre multipoint	
interface GigabitEthernet1	
ip address 2.2.2.2 255.255.255.0	
router eigrp 10	
network 10.0.0.0 0.0.0.255	<input type="text" value="server-only"/>

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

Question: 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: B

Question: 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: D

Question: 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

Question: 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
