350-401 Q&As

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) & CCIE Enterprise Infrastructure & CCIE Enterprise Wireless

Pass Cisco 350-401 Exam with 100% Guarantee

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

https://www.leads4pass.com/350-401.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

How do the RIB and the FIB differ?

A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.

B. RIB contains the interface for a destination, and the FIB contains the next hop information.

C. FIB is derived from the control plane, and the RIB is derived from the data plane.

D. RIB is derived from the control plane, and the FIB is derived from the RIB.

Correct Answer: D

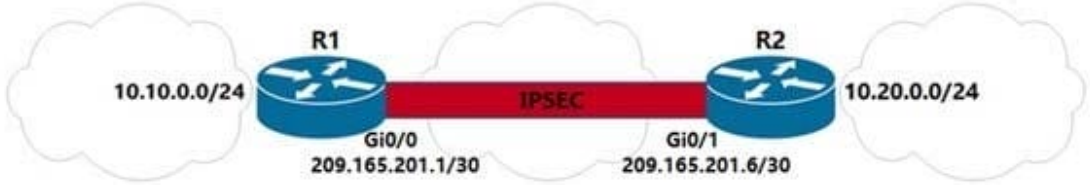
QUESTION 2

Refer to the exhibit.

A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two).

```
access-list 100 permit gre host 209.165.201.1 host 209.165.201.6

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3r address 209.165.201.6

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.6
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/0
description outside_interface
 no switchport
 ip address 209.165.201.1 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.1 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/0
tunnel destination 209.165.201.6

ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100
```

```
access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

crypto isakmp policy 5
authentication pre-share
hash sha256
encryption aes
group 14

crypto isakmp key D@t@c3nt3 address 209.165.201.1

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.1
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/1
description outside_interface
 no switchport
 ip address 209.165.201.6 255.255.255.252
 crypto map MAP

interface Tunnel100
ip address 192.168.100.2 255.255.255.0
ip mtu 1400
tunnel source GigabitEthernet0/1
tunnel destination 209.165.201.1

ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```



A. Create an IPsec profile, associate the transform-set ACL, and apply the profile to the tunnel interface.

B. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4.

C. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL.

D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface.

E. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24.

Correct Answer: CD

A is wrong, you don\\'t use a "transform-set ACL"

B is wrong. question states use IPsec profiles. Crypto maps was the old way of doing ipsec tunnels before profiles.

C is correct, need to remove crypto map config or it will cause some confusion if the tunnel profile is applied. Didn\\'t lab it up, but book references this. D is correct, all you need to do is create a profile and associate the transform-set to this

profile, then apply it to the tunnel. If no transform set was created you would have to create one. E is wrong, i believe removing crypto map would cause the traffic to flow unencrypted over the tunnel. acl in this case is to match the interesting

traffic to be encrypted. it\\'s denying it.

QUESTION 3

Which feature is supported by EIGRP but is not supported by OSPF?

A. equal-cost load balancing

B. route filtering

C. unequal-cost load balancing

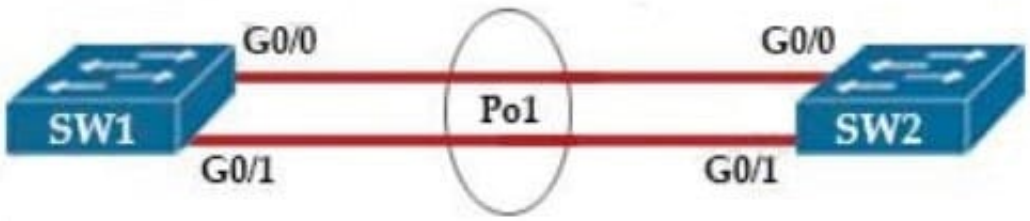
D. route summarization

Correct Answer: C

EIGRP support unequal-cost load balancing via the "variance ..." while OSPF only supports equalcost load balancing.

QUESTION 4

Refer to the exhibit.




```
SW1# show etherchannel summary

! output omitted

Group    Port-channel    Protocol    Ports
--------+---------------+-----------+-----
1        Po1 (SD)            -
```

After an engineer configures an EtherChannel between switch SW1 and switch SW2, this error message is logged on switch SW2.

```
SW2#
08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection on Gi0/0, putting
Gi0/0 in err-disable state
08:33:23: %PM-4-ERR_DISABLE: channel-misconfig error detection on Gi0/1, putting
Gi0/1 in err-disable state
```

Based on the output from SW1 and the log message received on Switch SW2, what action should the engineer take to resolve this issue?

A. Configure the same protocol on the EtherChannel on switch SW1 and SW2.

B. Connect the configuration error on interface Gi0/1 on switch SW1.

C. Define the correct port members on the EtherChannel on switch SW1.

D. Correct the configuration error on interface Gi0/0 switch SW1.

Correct Answer: A

In this case, we are using your EtherChannel without a negotiation protocol. As a result, if the opposite switch is not also configured for EtherChannel operation on the respective ports, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occuring by disabling all the ports bundled in the EtherChannel.

QUESTION 5

Refer to the exhibit.

```
*Jun19 11:12: BGP(4):10.1.1.2 rcvd UPDATE w/ attr:nexthop 10.1.1.2, origin ?,
localpref 100,metric 0,extended community RT:999:999
*Jun19 11:12: BGP(4):10.1.1.2 rcvd 999:999:192.168.1.99/32,label 29–DENIED due to:
extended community not supported
```

You have just created a new VRF on PE3. You have enabled debug ip bgp vpnv4 unicast updates on PE1, and you can see the route in the debug, but not in the BGP VPNv4 table. Which two statements are true? (Choose two)

A. After you configure route-target import 999:999 for a VRF on PE1, the route will be accepted

B. VPNv4 is not configured between PE1 and PE3

C. address-family ipv4 vrf is not configured on PE3

D. PE1 will reject the route due to automatic route filtering

E. After you configure route-target import 999:999 for a VRF on PE3, the route will be accepted

Correct Answer: AD

Because some PE routers might receive routing information they do not require, a basic requirement is to be able to filter the MP-iBGP updates at the ingress to the PE router so that the router does not need to keep this information in

memory. The Automatic Route Filtering feature fulfills this filtering requirement. This feature is available by default on all PE routers, and no additional configuration is necessary to enable it. Its function is to filter automatically VPN-IPv4 routes

that contain a route target extended community that does not match any of the PE\\'s configured VRFs. This effectively discards any unwanted VPN-IPv4 routes silently, thus reducing the amount of information that the PE has to store in

memory -> Answer \\'PE1 will reject the route due to automatic route filtering\\' is correct.

Reference: MPLS and VPN Architectures Book, Volume 1

The reason that PE1 dropped the route is there is no "route-target import 999:999" command on PE1 (so we see the "DENIED due to: extended community not supported" in the debug) so we need to type this command to accept this route ->

Answer \\'After you configure route-target import 999:999 for a VRF on PE1, the route will be accepted\\' is correct.