HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

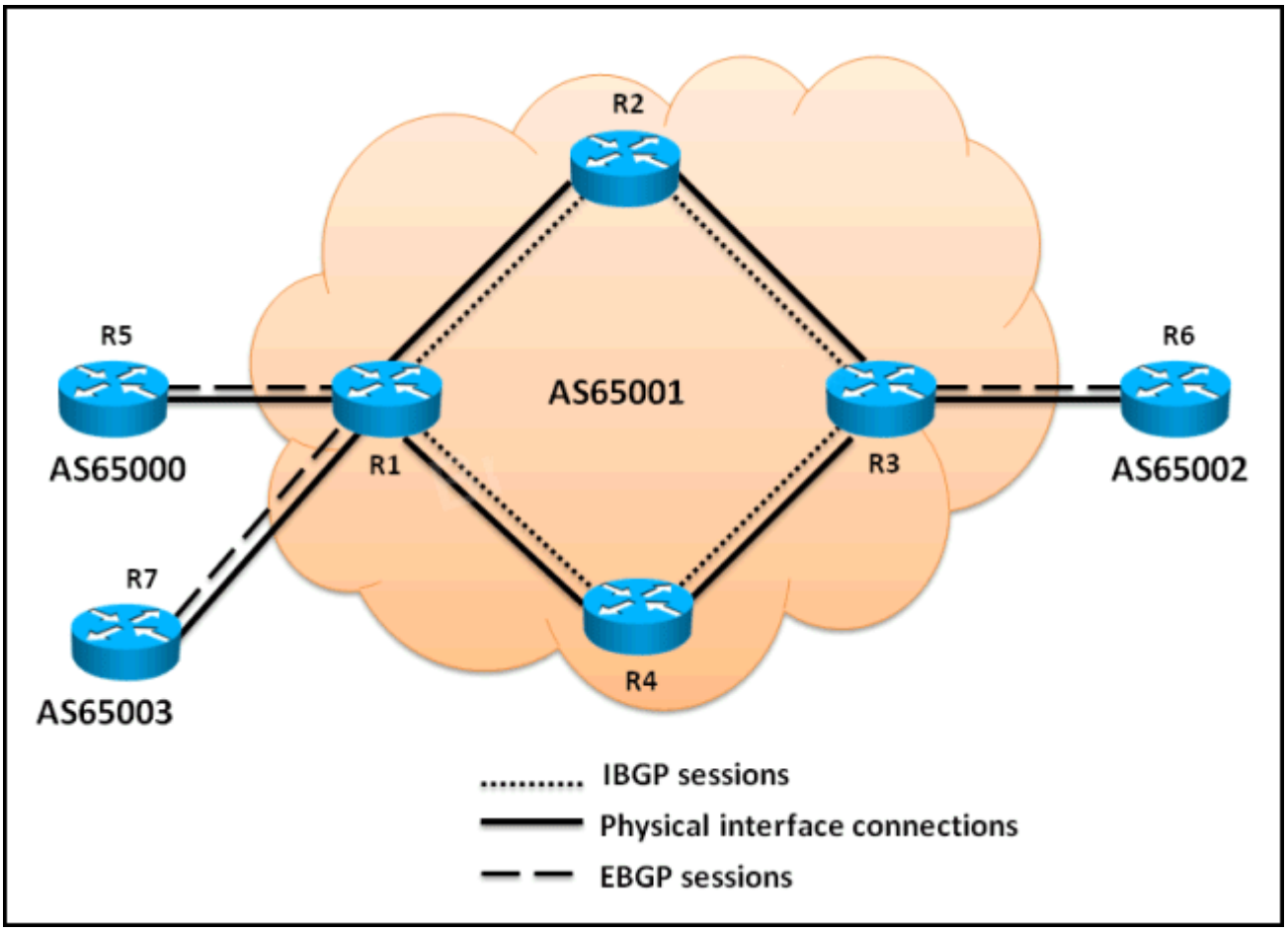
https://www.certtree.com

Exam : **642-885**

Title : Deploying Cisco Service Provider Advanced Network Routing

Version : DEMO

1.Referring to the topology diagram show in the exhibit,



Which three statements are correct regarding the BGP routing updates? (Choose three.)
A. The EBGP routing updates received by R1 from R5 will be propagated to the R2, R4, and R7 routers
B. The EBGP routing updates received by R3 from R6 will be propagated to the R2 and R4 routers
C. The EBGP routing updates received by R1 from R5 will be propagated to the R2 and R4 routers
D. The IBGP routing updates received by R3 from R2 will be propagated to the R6 router
E. The IBGP routing updates received by R2 from R1 will be propagated to the R3 router
F. The IBGP routing updates received by R1 from R4 will be propagated to the R5, R7, and R2 routers
Answer: A,B,D

2.When a BGP route reflector receives an IBGP update from a non-client IBGP peer, the route reflector will then forward the IBGP updates to which other router(s)?
A. To the other clients only
B. To the EBGP peers only
C. To the EBGP peers and other clients only
D. To the EBGP peers and other clients and non-clients
Answer: C

3.Which two BGP mechanisms are used to prevent routing loops when using a design with redundant route reflectors? (Choose two.)
A. Cluster-list

B. AS-Path
C. Originator ID
D. Community
E. Origin
Answer: A,C
Explanation:
As the iBGP learned routes are reflected, routing information may loop.
The route reflector model has the following mechanisms to avoid routing loops:
- Originator ID is an optional, nontransitive BGP attribute. It is a 4-byte attributed created by a route reflector.
The attribute carries the router ID of the originator of the route in the local autonomous system. Therefore, if amisconfiguration causes routing information to come back to the originator, the information is ignored.
- Cluster-list is an optional, nontransitive BGP attribute. It is a sequence of cluster IDs that the route haspassed. When a route reflector reflects a route from its clients to nonclient peers, and vice versa, it appendsthe local cluster ID to the cluster-list. If the cluster-list is empty, a new cluster-list is created. Using this attribute, a route reflector can identify if routing information is looped back to the same cluster due to misconfiguration. If the local cluster ID is found in the cluster-list, the advertisement is ignored.

4.Which two statements correctly describe the BGP ttl-security feature? (Choose two.)
A. This feature protects the BGP processes from CPU utilization-based attacks from EBGP neighbors which can be multiple hops away
B. This feature prevents IBGP sessions with non-directly connected IBGP neighbors
C. This feature will cause the EBGP updates from the router to be sent using a TTL of 1
D. This feature needs to be configured on each participating BGP router
E. This feature is used together with the ebgp-multihop command
Answer: A,D

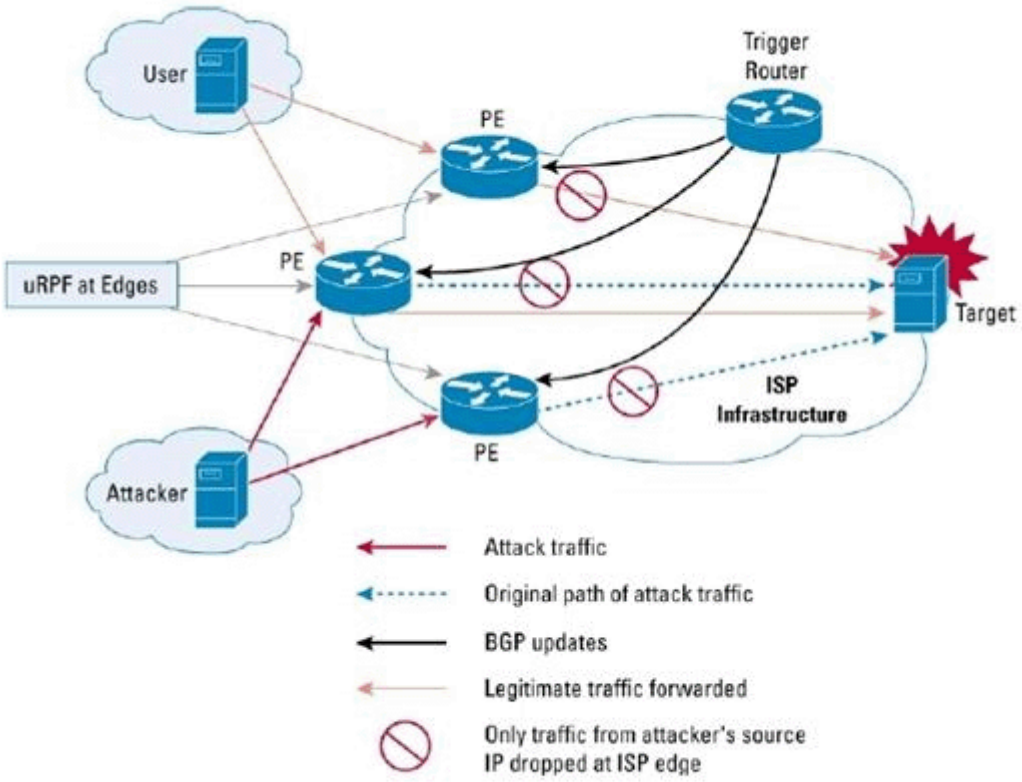
5.When implementing source-based remote-triggered black hole filtering, which two configurations are required on the edge routers that are not the signaling router? (Choose two.)
A. A static route to a prefix that is not used in the network with a next hop set to the Null0 interface
B. A static route pointing to the IP address of the attacker
C. uRPF on all external facing interfaces at the edge routers
D. Redistribution into BGP of the static route that points to the IP address of the attacker
E. A route policy to set the redistributed static routes with the no-export BGP community
Answer: A,C
Explanation:
Source-Based RTBH Filtering
With destination-based black holing, all traffic to a specific destination is dropped after the black hole has beenactivated, regardless of where it is coming from. Obviously, this could include legitimate traffic destined for the target. Source-based black holes provide the ability to drop traffic at the network edge based on a specificsource address or range of source addresses.
If the source address (or range of addresses) of the attack can be identified (spoofed or not), it would be betterto drop all traffic at the edge based on the source address, regardless of the destination address. This wouldpermit legitimate traffic from other sources to reach the target.

Implementation of source-based black holefiltering depends on Unicast Reverse Path Forwarding (uRPF), most often loose mode uRPF.

Loose mode uRPF checks the packet and forwards it if there is a route entry for the source IP of the incomingpacket in the router forwarding information base (FIB). If the router does not have an FIB entry for the source IP address, or if the entry points to a null interface, the Reverse Path Forwarding (RPF) check fails and thepacket is dropped, as shown in Figure 2. Because uRPF validates a source IP address against its FIB entry, dropping traffic from specific source addresses is accomplished by configuring loose mode uRPF on the external interface and ensuring the RPF check fails by inserting a route to the source with a next hop of Null0.

This can be done by using a trigger device to send IBGP updates. These updates set the next hop for the source IP to an unused IP address that has a static entry at the edge, setting it to null as shown in Figure 2.

Figure 2. Source-Based Black Hole Filtering



In this way, traffic that is entering the edge network sourced from a host that has a route pointing to null will result in a uRPF drop.