

H12-721

HCNP-Security-CISN (Huawei Certified
Network Professional - Constructing
Infrastructure of Security Network)

DEMO

<https://www.islever.com/h12-721.html>

<https://www.islever.com/huawei.html>

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

The main method of caching servers DNS Request Flood defense is the use of DNS source authentication.

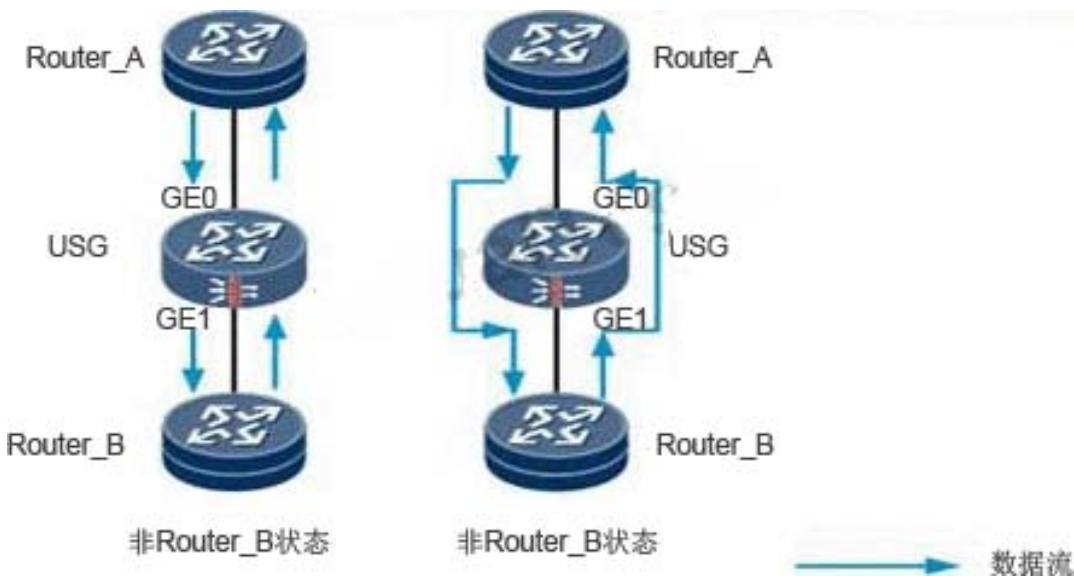
- A. TRUE
- B. FALSE

Answer: A

Explanation:

QUESTION NO: 2

Refer to the following diagram in regards to Bypass mode.



Which of the following statements is correct a few? (Choose two answers)

- A. When the interface is operating in a non-Bypass state, the flow from the inflow of USG Router_A interfaces from GE0, GE1 after USG treatment from the interface flow Router_B.
- B. When the Interface works in Bypass state, traffic flow from the interface by the Router_A GE0 USG, USG without any treatment, flows directly Router_B flows from the GE1 interfaces.
- C. When there are firewall requirements to achieve security policies, while working at the interface Bypass state to operate without interruption. Therefore, the device can be maintained in the Bypass state job.
- D. Power Bypass interface can work in bridge mode, and can work with the bypass circuit.

Answer: A,B

Explanation:

QUESTION NO: 3

With the Huawei abnormal flow cleaning solution, deployed at the scene of a bypass, drainage schemes can be used to have? (Choose three answers)

- A. Dynamic routing drainage
- B. Static routing strategy drainage
- C. Static routing drainage
- D. MPLS VPN cited

Answer: A,B,C

Explanation:

QUESTION NO: 4

Regarding IKE main mode and aggressive modes, which of the following statements is correct?

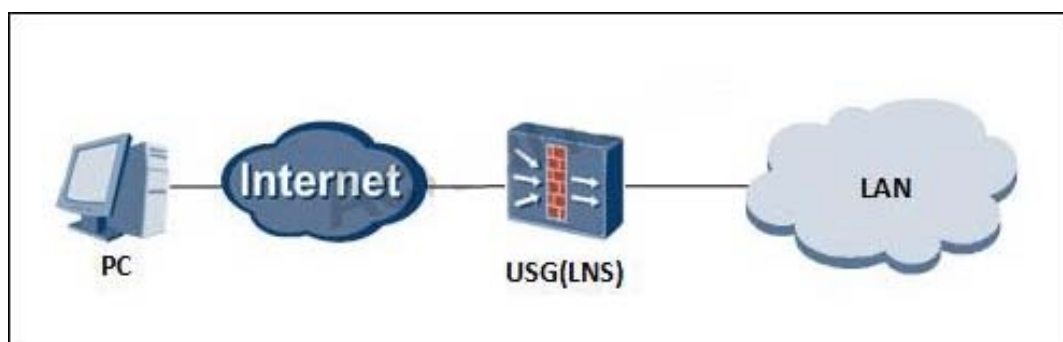
- A. In savage mode with the the first phase of negotiation, all packets are encrypted
- B. All main mode packts under the first phase of negotiation are encrypted
- C. The DH algorithm is used in aggressive mode
- D. Whether the negotiation is successful or not, IKE will enter into fast mode

Answer: C

Explanation:

QUESTION NO: 5

A network is shown below.



A dial customer cannot establish a connection via a VPN client PC and USG (LNS) l2tp vpn. What are valid reasons for this failure? (Choose three answers)

- A. LNS tunnel name change is inconsistent with the client name.
- B. L2TP tunnel authentication failed.
- C. PPP authentication fails, PPP authentication mode set on the client PC and LNS inconsistent.
- D. Client PC can not obtain an IP address assigned to it from the LNS.

Answer: B,C,D

Explanation:

QUESTION NO: 6

From the branch offices, servers are accessed from the Headquarters via IPsec VPN. An IPSEC tunnel can be established at this time, but communication to the servers fails. What are the possible reasons? (Choose three answers)

- A. Packet fragmentation, the fragmented packets are discarded on the link.
- B. Presence of dual-link load balancing, where the path back and forth may be inconsistent.
- C. Route flapping.
- D. Both ends of the DPD detection parameters are inconsistent.

Answer: A,B,C

Explanation:

QUESTION NO: 7

A user has been successfully authenticated using an SSL VPN. However, users can not access the Web-link resources through the Web server.

netstat -anp tcp

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9594	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9595	0.0.0.0:0	LISTENING