PassQueen
a.k.a dumpsqueen.com

H12-841_V1.5HCIP-Datacom-Campus Network Planning and Deployment V1.5

Huawei h12-841_v1.5

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Campus Network Planning and Design	4
Topic 2, Campus Network Deployment	18
Topic 3, Campus Network O&M	1
Total	23

QUESTION NO: 1 - (SIMULATION)

(As shown in the following figure, R1 and R2 establish an IPsec VPN in ISAKMP mode for communication. For IPsec proposals on R1 and R2, ESP is used, the encapsulation mode is set to tunnel mode, SHA1 is configured as the authentication algorithm, and AES-256 is configured as the encryption algorithm. In addition, IKEv1 is configured for IKE peers, the main mode is configured for IKEv1 negotiation phase 1, and the PSK Huawei@123 is configured for PSK authentication between IKE peers. For IKE proposals on R1 and R2, SHA1 is configured as the authentication algorithm, AES-256 is configured as the encryption algorithm, and DH group 1 is configured for IKE negotiation. Based on these configurations on R1 and R2, drag the configuration items on the left to the correct locations on the right.)

ANSWER: See the explanation for the answer

Explanation:

Correct drag-and-drop mapping:

1 → `dh group1`
2 → `main`
3 → `esp`
4 → `tunnel`

Reasoning:

In the IKE proposal, `dh group1` configures the DH group used for IKEv1 Phase 1 key exchange.
In the IKE peer configuration, `exchange-mode main` selects IKEv1 main mode for Phase 1 negotiation.
In the IPsec proposal, `transform esp` specifies ESP as the IPsec protection protocol.
`encapsulation-mode tunnel` configures IPsec tunnel encapsulation mode.

```
IKE proposal:     dh group1
IKE peer:         exchange-mode main
IPsec proposal:   transform esp
IPsec proposal:   encapsulation-mode tunnel
```

QUESTION NO: 2

(A department occupies two buildings connected by redundant Layer 2 links. The links form a ring, and the enterprise requires sub-50-ms protection switching when a single ring link fails. Which Layer 2 protection technology is most suitable for this requirement?)

A. RSTP

B. ERPS

C. VRRP

D. LACP

ANSWER: B

Explanation:

ERPS is correct because Ethernet Ring Protection Switching is designed for Ethernet ring networks and provides rapid protection switching after a ring failure. It blocks the ring under normal conditions and unblocks the required protection path when a failure is detected.

RSTP can prevent loops but is not the ring-specific protection mechanism intended for the stated fast protection objective. VRRP protects Layer 3 gateways, whereas LACP bundles parallel links rather than protecting a multi-node Ethernet ring.