Free Questions for H12-721 by vceexamstest

Shared by Cash on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following configurations is mandatory when the IKE peer needs to be referenced to the IPSec policy template in the divquarters-branch-based IPSec VPN network (pre-shared key + traversal NAT)?

Options:

A- ipsec proposal

B- exchang-mode aggressive

C- pre-shared-key

D- remote-address

Answer:

A, C

Question 2

Question Type: MultipleChoice

The SSL VPN authentication is successful, but the Web-link resources cannot be accessed. What is the correct one?

Options:

A- server does not open web service

B- policy restricts user access

C- device and intranet server are unreachable

D- SSL VPN users reach the maximum limit

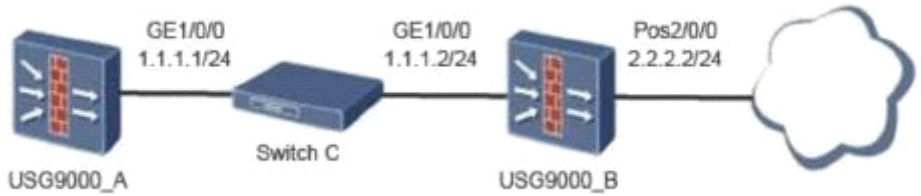
Answer:

A, B, C

Question 3

Question Type: **MultipleChoice**

The topology of the BFD-bound static route is as follows: The administrator has configured the following on firewall A: [USG9000_A] bfd [USG9000_A-bfd] quit [USG9000_A] bfd aa bind peer-ip 1.1.1.2 [USG9000_A- Bfd session-aa] discriminator local 10 [USG9000_A-bfd session-aa] discriminator remote 20 Which of the following configurations can be added to the firewall to implement BFD-bound static routes?



Options:

A- [USG9000_A-bfd session-aa] commit

B- [USG9000_A]bfd aa bind local-ip 1.1.1.1

C- [USG9000_A]ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa

D- [USG9000_A] ip route-static 0.0.0.0 0 1.1.1.2 bfd-session aa

Answer:

A, C

Question 4

Question Type: MultipleChoice

Which of the following technologies can enhance the security of mobile users accessing the company's intranet VPN solution?

Options:

A- SSL

B- PPPoE

C- GRE

D- L2TP

Answer:

A

Question 5

Question Type: **MultipleChoice**

Avoid DHCP server spoofing attacks. DHCP snooping is usually enabled. What is the correct statement?

Options:

A- connected user's firewall interface is configured in trusted mode

B- The firewall interface connected to the DHCP server is configured as untrusted mode.

C- DHCP relay packets received on the interface in the untrusted mode are discarded.

D- The DHCP relay packet received in the D trusted mode and passed the DHCP snooping check.

Answer:

C

Explanation:

Note: DHCP snooping is a DHCP security feature that filters DHCP messages that do not contain information through MAC address restriction, DHCP snooping security binding, IP+MAC binding, and Option 82 features. DHCP DoS attack, DHCP server spoofing attack, ARP man-in-the-middle attack, and IP/MAC Snooping attack. DHCP snooping is enabled on all interfaces of the DHCP client. If the user-side interface is not configured with the Trusted mode, the interface is enabled with the Snooping feature. The default interface mode is Untrusted. This prevents the DHCP server from being attacked by the bogus. To prevent the attack from being attacked by the DHCP server, you can configure the DHCP snooping function on the device to configure the interface on the user side as Untrusted and the interface on the DHCP server as Trusted. All received from the Untrusted interface. DHCP relay packets are discarded. DHCP snooping is configured on the firewall. The DHCP snooping binding function is used to forward packets only if the received packets are the same as those in the binding table. Otherwise, the packets are discarded.

Question 6

Question Type: MultipleChoice

Which attack method is CC attack?

Options:

A- denial of service attack

B- scan snooping attack

C- malformed packet attack

D- System-based vulnerability attacks

Answer:

A