DUMPSBOSS.

Fortinet NSE 6LAN Edge 7.6 Architect

Fortinet FCSS_LED_AR-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

DHCP snooping is enabled on a FortiSwitch to prevent unauthorized DHCP servers from assigning addresses to endpoint devices. A legitimate DHCP server is located upstream of the FortiSwitch, and its DHCP Offer and DHCP ACK messages enter the FortiSwitch through an uplink.

How should the uplink be configured?

A. Mark the uplink as a trusted DHCP snooping interface.

B. Disable DHCP snooping on the uplink and leave all other interfaces untrusted.

C. Enable DHCP relay on the uplink interface.

D. Configure the uplink as an access port in the client VLAN.

ANSWER: A

Explanation:

The uplink toward the legitimate DHCP server, or toward the path on which legitimate DHCP server replies arrive, must be trusted for DHCP snooping. DHCP snooping blocks server-originated DHCP messages received on untrusted interfaces. Client-facing access ports should normally remain untrusted so that an endpoint cannot send rogue Offer or ACK messages.

Disabling DHCP snooping on the uplink removes protection unnecessarily. Enabling a DHCP relay does not make the interface trusted for DHCP snooping, and configuring the uplink as an access port does not determine whether DHCP server messages are accepted.

QUESTION NO: 2

A company deploys EAP-TLS authentication for wired users. FortiAuthenticator is configured as the RADIUS server, and the client certificates were issued by an internal certification authority. Client devices trust the internal certification authority, but FortiAuthenticator rejects every EAP-TLS authentication attempt with a certificate validation error.

What configuration change is required on FortiAuthenticator?

A. Import and trust the certification authority certificate that issued the client certificates.

B. Replace the FortiGate certificate with the certificate used by the internal certification authority.

C. Configure the same RADIUS shared secret on every client device.

D. Disable client certificate validation in the EAP-TLS authentication policy.

ANSWER: A

Explanation:

FortiAuthenticator must trust the certification authority that issued the client certificates. During EAP-TLS authentication, the RADIUS server validates the certificate presented by the supplicant. The client trusting the issuing CA is necessary for validating the server certificate, but it does not cause FortiAuthenticator to trust client certificates.

Replacing the FortiGate certificate does not establish trust for the client certificate chain. A RADIUS shared secret secures communication between network devices and FortiAuthenticator; it is not used to validate EAP-TLS client certificates. Disabling certificate validation would defeat the purpose of certificate-based authentication.