300-730 Q&As

Implementing Secure Solutions with Virtual Private Networks (SVPN)

QUESTION 1

Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

A. HTTP

B. ICA (Citrix)

C. VNC

D. RDP

E. CIFS

Correct Answer: AE

"NOTE You will not see an option of RDP, VNC, SSH, and/or Telnet unless the appropriate client/server plug-in has been installed first. " Leaves only HTTP and CIFS as your options.

QUESTION 2

Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

A. sequence numbers that enable scalable replay checking

B. enabled use of ESP or AH

C. design for use over public or private WAN

D. no requirement for an overlay routing protocol

Correct Answer: D

QUESTION 3

Why must a network engineer avoid usage of the default X.509 certificate when implementing clientless SSLVPN on an ASA?

A. The certificate must be managed by the local CA.

B. The certificate is regenerated at each reboot.

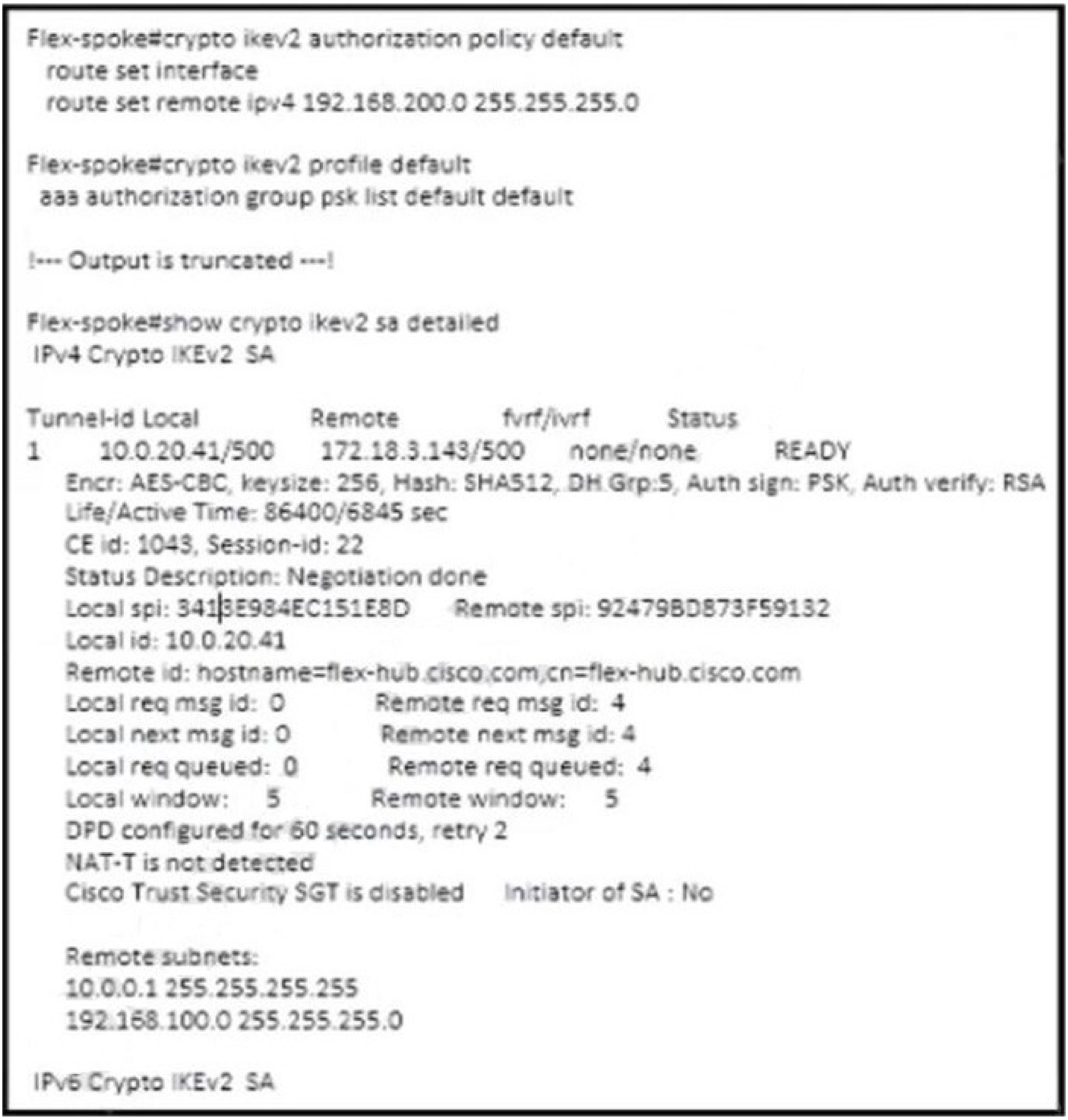
C. The default X.509 certificate is not supported for SSLVPN.

D. The certificate is too weak to provide adequate security.

Correct Answer: B

QUESTION 4

Refer to the exhibit.



```
Flex-spoke#crypto ikev2 authorization policy default
  route set interface
  route set remote ipv4 192.168.200.0 255.255.255.0

Flex-spoke#crypto ikev2 profile default
 aaa authorization group psk list default default

!--- Output is truncated ---!

Flex-spoke#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local            Remote            fvrf/ivrf         Status
1       10.0.20.41/500      172.18.3.143/500     none/none          READY
    Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: RSA
    Life/Active Time: 86400/6845 sec
    CE id: 1043, Session-id: 22
    Status Description: Negotiation done
    Local spi: 3413E984EC151E8D     Remote spi: 92479BD873F59132
    Local id: 10.0.20.41
    Remote id: hostname=flex-hub.cisco.com,cn=flex-hub.cisco.com
    Local req msg id:  0           Remote req msg id:  4
    Local next msg id: 0           Remote next msg id: 4
    Local req queued:  0           Remote req queued:  4
    Local window:      5           Remote window:      5
    DPD configured for 60 seconds, retry 2
    NAT-T is not detected
    Cisco Trust Security SGT is disabled     Initiator of SA : No

    Remote subnets:
    10.0.0.1 255.255.255.255
    192.168.100.0 255.255.255.0

 IPv6 Crypto IKEv2  SA
```

An engineer has configured a spoke to connect to a FlexVPN hub. The tunnel is up, but pings fail when the engineer attempts to reach host 192.168.200.10 behind the spoke, and traffic is sourced from host 192.168.100.3, which is behind the FlexVPN server. Based on packet captures, the engineer discovers that host 192.168.200.10 receives the icmp echo and sends an icmp reply that makes it to the inside interface of the spoke. Based on the output in the exhibit captured on the spoke by the engineer, which action resolves this issue?

A. Add the aaa authorization group cert list default default command to the spoke ikev2 profile.

B. Add the route set remote ipv4 192.168.200.0 255.255.255.0 command to the hub authorization policy.

C. Add the aaa authorization group cert list default default command to the hub ikev2 profile.

D. Add the route set remote ipv4 192.168.100.0 255.255.255.0 command to the spoke authorization policy.

Correct Answer: D

QUESTION 5

A network engineer must expand a company\\'s Cisco AnyConnect solution. Currently, a Cisco ASA is set up in North America and another will be installed in Europe with a different IP address. Users should connect to the ASA that has the lowest Round Trip Time from their network location as measured by the AnyConnect client. Which solution must be implemented to meet this requirement?

A. VPN Load Balancing

B. IP SLA

C. DNS Load Balancing

D. Optimal Gateway Selection

Correct Answer: D

Optimal Gateway Selection (OGS) is a feature that can be used for determining which gateway has the lowest RTT and connect to that gateway. Using the Optimal Gateway Selection (OGS) feature, administrators can minimize latency for Internet traffic without user intervention. With OGS, AnyConnect identifies and selects which secure gateway is best for connection or reconnection. OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection

Latest 300-730 Dumps 300-730 Practice Test 300-730 Study Guide