300-730$^{Q\&As}$

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

QUESTION 1

A network engineer is setting up Cisco AnyConnect 4.9 on a Cisco ASA running ASA software 9.1. Cisco AnyConnect must connect to the Cisco ASA before the user logs on so that login scripts can work successfully. In addition, the VPN must connect without user intervention. Which two key steps accomplish this task? (Choose two.)

A. Create a Network Access Manager profile with a client policy set to connect before user logon.

B. Create a Cisco AnyConnect VPN profile with Start Before Logon set to true.

C. Issue an identity certificate to the trusted root CA folder in the machine store.

D. Create a Cisco AnyConnect VPN profile with Always On set to true.

E. Create a Cisco Anyconnect VPN Management Tunnel profile.

Correct Answer: BC

QUESTION 2

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

QUESTION 3

An engineer is implementing a failover solution for a FlexVPN client site where ESP traffic to the primary FlexVPN server is blocked intermittently after tunnel establishment. This issue causes users at the branch site to lose access to the corporate network. The solution must quickly establish a tunnel and send traffic to the secondary FlexVPN server only during a failover event. Which action must the engineer take to implement this solution?

A. Create one tunnel with peer statements to each server and use Dead Peer Detection to track the status or the primary server.

B. Create two tunnels for each FlexVPN server and use the tunnel keepalive command to track the status of each FlexVPN server.

C. Create one tunnel with peer statements to each server and use object tracking to track the status of the primary server.

D. Create two tunnels for each FlexVPN server and use a dynamic routing protocol to track the status or each FlexVPN server.

Correct Answer: A

QUESTION 4

An administrator is deciding which authentication protocol should be implemented for their upcoming Cisco AnyConnect deployment. A list of the security requirements from upper management are: the ability to force AnyConnect users to use complex passwords such as C1$c0451035084!, warn users a few days before their password expires, and allow users to change their password during a remote access session. Which authentication protocol must be used to meet these requirements?

A. LDAPS

B. RADIUS

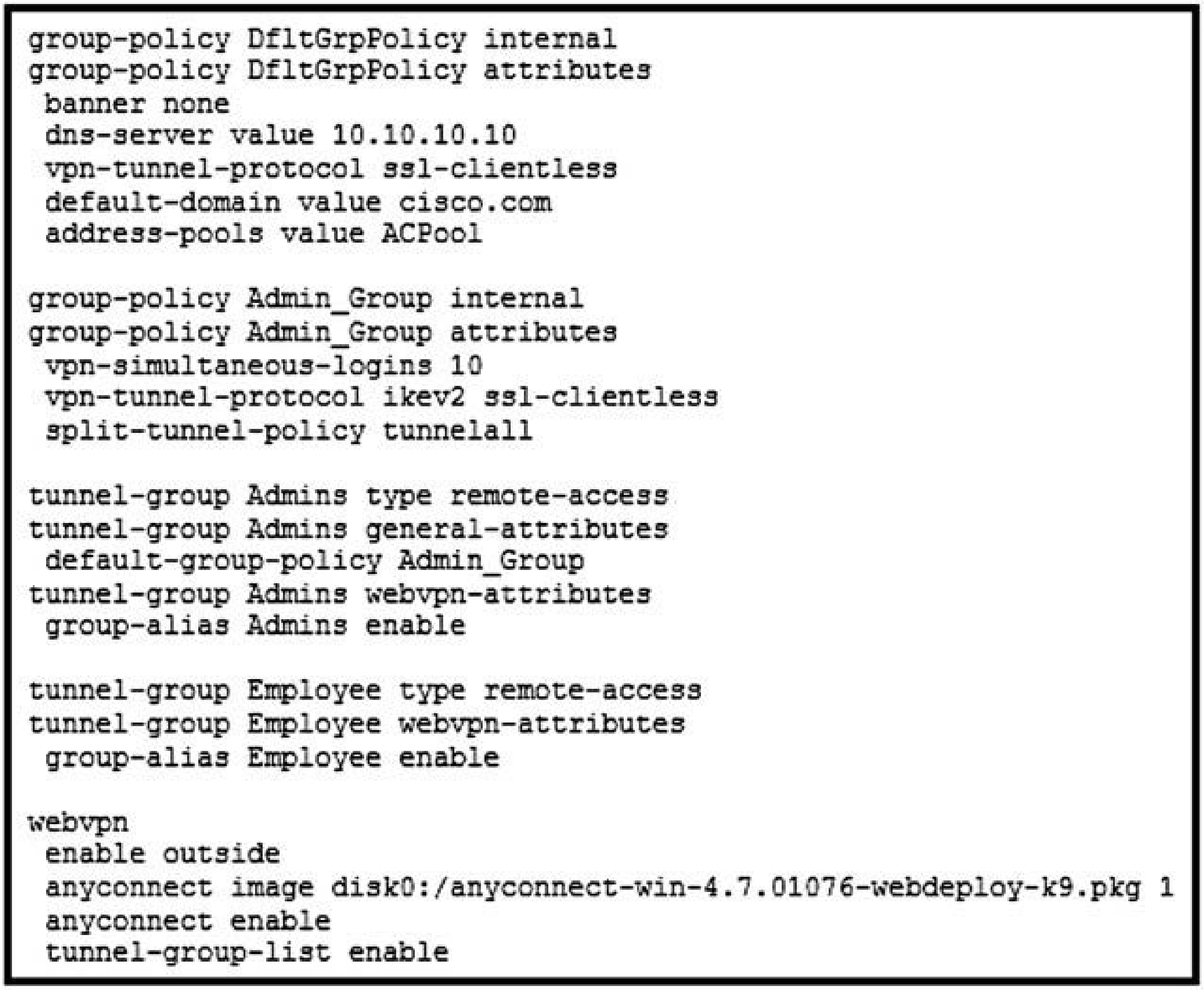
C. Kerberos

D. TACACS+

Correct Answer: B

QUESTION 5

Refer to the exhibit.



```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-clientless
 split-tunnel-policy tunnelall

tunnel-group Admins type remote-access
tunnel-group Admins general-attributes
 default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes
 group-alias Admins enable

tunnel-group Employee type remote-access
tunnel-group Employee webvpn-attributes
 group-alias Employee enable

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

Which VPN technology is allowed for users connecting to the Employee tunnel group?

A. SSL AnyConnect

B. IKEv2 AnyConnect

C. crypto map

D. clientless

Correct Answer: D

Since there is no vpn-tunnel-protocol defnied under the Employee tunnel-group this setting will be inherited from the DfltGrpPolicy And only ss-clientless is allowed in DfltGrpPolicy.