



300-730^{Q&As}

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/300-730.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

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 of 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 of each FlexVPN server.

Correct Answer: A

QUESTION 2

What are two functions of ECDH and ECDSA? (Choose two.)

- A. nonrepudiation
- B. revocation
- C. digital signature
- D. key exchange
- E. encryption

Correct Answer: CD

Reference: https://tools.cisco.com/security/center/resources/next_generation_cryptography

QUESTION 3

Which method dynamically installs the network routes for remote tunnel endpoints?

- A. policy-based routing
- B. CEF
- C. reverse route injection
- D. route filtering



Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn-availability-12-4t-book/sec-rev-rte-inject.html

QUESTION 4

Which VPN does VPN load balancing on the ASA support?

- A. VTI
- B. IPsec site-to-site tunnels
- C. L2TP over IPsec
- D. Cisco AnyConnect

Correct Answer: D

QUESTION 5

Which two features are valid backup options for an IOS FlexVPN client? (Choose two.)

- A. HSRP stateless failover
- B. DNS-based hub resolution
- C. reactivate primary peer
- D. tunnel pivot E. need distractor

Correct Answer: BC

QUESTION 6

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 defined under the Employee tunnel-group this setting will be inherited from the DfltGrpPolicy And only ss-clientless is allowed in DfltGrpPolicy.

QUESTION 7

Which two commands help determine why the NHRP registration process is not being completed even after the IPsec tunnel is up? (Choose two.)



- A. show crypto isakmp sa
- B. show ip traffic
- C. show crypto ipsec sa
- D. show ip nhrp traffic
- E. show dmvpn detail

Correct Answer: AD

<https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html>

QUESTION 8

Refer to the exhibit.

```
router# show crypto ipsec sa

interface: GigabitEthernet0/1
  Crypto map tag: test, local addr. 209.165.200.225
  local ident (addr/mask/prot/port): (209.165.201.0/255.255.255.224/0/0)
  remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 209.165.200.226
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 918, #pkts encrypt: 918, #pkts digest 918
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0,
    #send errors 1, #recv errors 0

  local crypto endpt.: 209.165.200.225 , remote crypto endpt.: 209.165.200.226
  path mtu 1500, media mtu 1500
  current outbound spi: 3D3

inbound esp sas:
```

A TCP based application that should be accessible over the VPN tunnel is not working. Pings to the appropriate IP address are failing. Based on the output, what is a fix for this issue?

- A. Add a route on the remote peer for 209.165.201.0/27.



- B. Add a route on the local peer for 10.1.1.0/24.
- C. Add a permit for TCP traffic going to 10.1.1.0/24.
- D. Add a permit for TCP traffic going to 209.165.201.0/27.

Correct Answer: A

QUESTION 9

Refer to the exhibit.

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page. ⓘ

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

➕ Add ✎ Edit 🗑 Delete Find: 🔍 ☑ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPGROUP	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
Clientless	<input type="checkbox"/>	<input type="checkbox"/>	Clientless	AAA(LOCAL)	Clientless
AnyConnect	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AnyConnect	AAA(LOCAL)	GroupPolicy_AnyConnect

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Based on this ASDM output, which remote access technologies are allowed on the ASA?

- A. SSLAnyConnect VPN
- B. IKEv2 and SSL AnyConnect VPN
- C. SSL clientless VPN
- D. IKEv2 AnyConnect VPN

Correct Answer: B



QUESTION 10

Which technology is used to send multicast traffic over a site-to-site VPN?

- A. GRE over IPsec on IOS router
- B. GRE over IPsec on FTD
- C. IPsec tunnel on FTD
- D. GRE tunnel on ASA

Correct Answer: A

GRE is not supported in FTD, so A is correct <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/216276-configure-route-based-site-to-site-vpn-t.html#anc6>

QUESTION 11

Which two tasks must be performed to implement a clientless VPN on the Cisco ASA? (Choose two.)

- A. Configure a connection profile
- B. Upload an AnyConnect Package.
- C. Install an enrolled X.509 Certificate.
- D. Configure a language translation file.
- E. Configure a portal customization.

Correct Answer: AC

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html>

QUESTION 12

Refer to the exhibit.

**HUB configuration:**

```
crypto ikev2 profile default
  match identity remote fqdn domain cisco.com
  identity local fqdn hub.cisco.com
  authentication local rsa-sig
  authentication remote pre-shared-key cisco
  pki trustpoint CA
  aaa authorization group cert list default default
  virtual-template 1
```

SPOKE 1 configuration:

```
crypto ikev2 profile default
  match identity remote fqdn domain cisco.com
  identity local fqdn spoke.cisco.com
  authentication local rsa-sig
  authentication remote pre-shared-key cisco
  pki trustpoint CA
  aaa authorization group cert list default default
  virtual-template 1
```

SPOKE 2 configuration:

```
crypto ikev2 profile default
  match identity remote fqdn domain cisco.com
  identity local fqdn spoke2.cisco.com
  authentication local pre-shared-key flexvpn
  authentication remote rsa-sig
  pki trustpoint CA
  aaa authorization group cert list default default
  virtual-template 1
```

What is a result of this configuration?



- A. Spoke 1 fails the authentication because the authentication methods are incorrect.
- B. Spoke 2 passes the authentication to the hub and successfully proceeds to phase 2.
- C. Spoke 2 fails the authentication because the remote authentication method is incorrect.
- D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Correct Answer: A

QUESTION 13

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 14

Refer to the exhibit.



```
Hub-Router#show crypto isakmp sa
dst          src          state   conn-id  slot  status
172.16.0.1  10.10.10.1  QM_IDLE 1085     0     ACTIVE

Router#show crypto IPSEC sa
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/47/0)
#pkts encaps: 349, #pkts encrypt: 349, #pkts digest: 349
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)

!--- Output is truncated ---!

Spoke-Router#show ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.16.0.1 E req-sent 0 req-failed 31 repl-recvd 0
Pending Registration Requests:
Registration Requests:Reqid 4751, Ret 64 NHS 172.16.0.1

!--- Output is truncated ---!
```

The network security engineer identified that the hub router cannot send traffic to the spoke router. Based on the provided output, which action resolves the issue?

- A. Permit UDP ports 500 and 4500 between the hub and spoke.
- B. Correct the next hop server IP address on the spoke router.
- C. Ensure the preshared key on the hub-and-spoke router matches.
- D. Adjust the ip nhrp network-id command on the hub router.

Correct Answer: B

QUESTION 15

An engineer must configure remote desktop connectivity for offsite admins via clientless SSL VPN, configured on a Cisco ASA to Windows Vista workstations. Which two configurations provide the requested access? (Choose two.)

- A. Telnet bookmark via the Telnet plugin
- B. RDP2 bookmark via the RDP2 plugin



- C. VNC bookmark via the VNC plugin
- D. Citrix bookmark via the ICA plugin
- E. SSH bookmark via the SSH plugin

Correct Answer: BC

[Latest 300-730 Dumps](#)

[300-730 PDF Dumps](#)

[300-730 Study Guide](#)