

## Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

<https://www.2passeasy.com/dumps/300-730/>



#### NEW QUESTION 1

On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

- A. interface virtual-access
- B. ip nhrp redirect
- C. interface tunnel
- D. interface virtual-template

**Answer: D**

#### NEW QUESTION 2

Which statement about GETVPN is true?

- A. The configuration that defines which traffic to encrypt originates from the key server.
- B. TEK rekeys can be load-balanced between two key servers operating in COOP.
- C. The pseudotime that is used for replay checking is synchronized via NTP.
- D. Group members must acknowledge all KEK and TEK rekeys, regardless of configuration.

**Answer: A**

#### NEW QUESTION 3

Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

- A. Reduce the maximum SA limit on the local Cisco ASA.
- B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.
- C. Remove the maximum SA limit on the remote Cisco ASA.
- D. Correct the crypto access list on both Cisco ASA devices.

**Answer: B**

#### NEW QUESTION 4

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

**Answer: DE**

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/webvpn-configure-gateway.html>

#### NEW QUESTION 5

Which configuration construct must be used in a FlexVPN tunnel?

- A. EAP configuration
- B. multipoint GRE tunnel interface
- C. IKEv1 policy
- D. IKEv2 profile

**Answer: D**

#### NEW QUESTION 6

Which two features provide headend resiliency for Cisco AnyConnect clients? (Choose two.)

- A. AnyConnect Auto Reconnect
- B. AnyConnect Network Access Manager
- C. AnyConnect Backup Servers
- D. ASA failover
- E. AnyConnect Always On

**Answer: CD**

**NEW QUESTION 7**

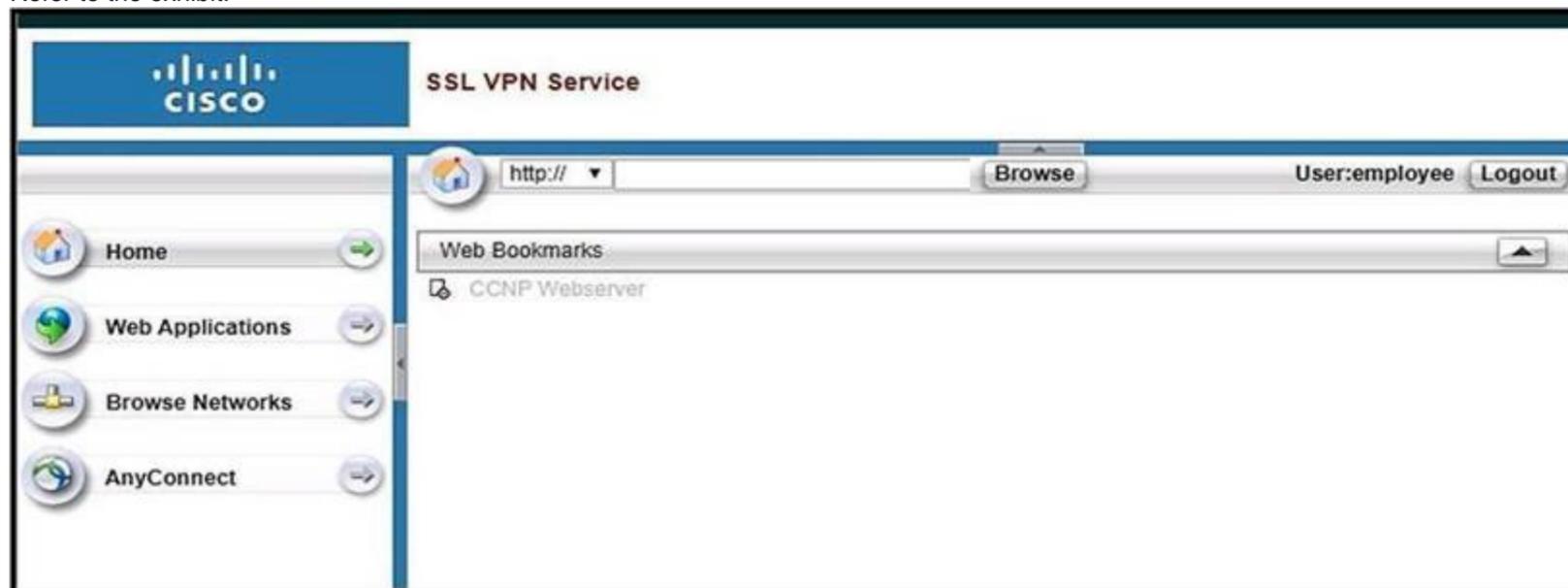
Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

- A. tunnel-group (general-attributes)
- B. tunnel-group (webvpn-attributes)
- C. webvpn (group-policy)
- D. webvpn (global configuration)

**Answer: D**

**NEW QUESTION 8**

Refer to the exhibit.



Based on the exhibit, why are users unable to access CCNP Webservers bookmark?

- A. The URL is being blocked by a WebACL.
- B. The ASA cannot resolve the URL.
- C. The bookmark has been disabled.
- D. The user cannot access the URL.

**Answer: C**

**NEW QUESTION 9**

Refer to the exhibit.



The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?

- A. `crypto vpn anyconnect profile Profile 1 flash:RDP.xml`  
`webvpn context Context1`  
`svc platform win seq 1`  
`policy group PolicyGroup1`  
`functions svc-enabled`
- B. `crypto vpn anyconnect profile Profile 1 flash:RDP.xml`  
`webvpn context Context1`  
`browser-attribute import flash:RDP.xml`
- C. `crypto vpn anyconnect profile Profile 1 flash:RDP.xml`  
`webvpn context Context1`  
`policy group PolicyGroup1`  
`svc profile Profile1`
- D. `crypto vpn anyconnect profile Profile 1 flash:RDP.xml`  
`webvpn context Context1`  
`policy group PolicyGroup1`  
`svc module RDP`

**Answer: C**

**Explanation:**

Reference: <https://community.cisco.com/t5/vpn/starting-anyconnect-vpn-through-rdp-session-on-cisco-891/td-p/2128284>

**NEW QUESTION 10**

Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

- A. \*\$SecureMobilityClient\$\*
- B. \*\$AnyConnectClient\$\*
- C. \*\$RemoteAccessVpnClient\$\*
- D. \*\$DfltIkeIdentity\$\*

**Answer:** B

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html>

**NEW QUESTION 10**

In a FlexVPN deployment, the spokes successfully connect to the hub, but spoke-to-spoke tunnels do not form. Which troubleshooting step solves the issue?

- A. Verify the spoke configuration to check if the NHRP redirect is enabled.
- B. Verify that the spoke receives redirect messages and sends resolution requests.
- C. Verify the hub configuration to check if the NHRP shortcut is enabled.
- D. Verify that the tunnel interface is contained within a VRF.

**Answer:** B

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dmvpn/configuration/15-ml/sec-conn-dmvpn-15-ml-book/sec-conn-dmvpn-summaps.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-ml/sec-conn-dmvpn-15-ml-book/sec-conn-dmvpn-summaps.pdf)

**NEW QUESTION 11**

An engineer is troubleshooting a new DMVPN setup on a Cisco IOS router. After the show crypto isakmp sa command is issued, a response is returned of "MM\_NO\_STATE." Why does this failure occur?

- A. The ISAKMP policy priority values are invalid.
- B. ESP traffic is being dropped.
- C. The Phase 1 policy does not match on both devices.
- D. Tunnel protection is not applied to the DMVPN tunnel.

**Answer:** B

**NEW QUESTION 15**

Refer to the exhibit.

```
IKEv2:(SESSION ID = 17,SA ID = 1):Processing IKE_AUTH message
IKEv2:IPsec policy validate request sent for profile CloudOne with psh index 1.

IKEv2:(SESSION ID = 17,SA ID = 1):
IKEv2:(SA ID = 1):[IPsec -> IKEv2] Callback received for the validate proposal - FAILED.

IKEv2-ERROR:(SESSION ID = 17,SA ID = 1):: There was no IPSEC policy found for received TS
IKEv2:(SESSION ID = 17,SA ID = 1):Sending TS unacceptable notify
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Get peer's preshared key for 68.72.250.251
IKEv2:(SESSION ID = 17,SA ID = 1):Generate my authentication data
IKEv2:(SESSION ID = 17,SA ID = 1):Use preshared key for id 68.72.250.250, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Generating IKE_AUTH message
IKEv2:(SESSION ID = 17,SA ID = 1):Constructing IDr payload: '68.72.250.250' of type 'IPv4 address'
IKEv2:(SESSION ID = 17,SA ID = 1):Building packet for encryption.
Payload contents:
VID IDr AUTH NOTIFY(TS_UNACCEPTABLE)

IKEv2:(SESSION ID = 17,SA ID = 1):Sending Packet [To 68.72.250.251:500/From 68.72.250.250:500/VRF i0:f0]
Initiator SPI : 3D527B1D50DBEEF4 - Responder SPI : 8C693F77F2656636 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
ENCR
```

Based on the debug output, which type of mismatch is preventing the VPN from coming up?

- A. interesting traffic
- B. lifetime
- C. preshared key
- D. PFS

**Answer:** B

**Explanation:**

If the responder's policy does not allow it to accept any part of the proposed Traffic Selectors, it responds with a TS\_UNACCEPTABLE Notify message.

**NEW QUESTION 19**

Refer to the exhibit.

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
  500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
  failed its sanity check or is malformed
```

Which type of mismatch is causing the problem with the IPsec VPN tunnel?

- A. crypto access list
- B. Phase 1 policy
- C. transform set
- D. preshared key

Answer: D

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike>

**NEW QUESTION 23**

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.

**Answer:** A

#### NEW QUESTION 28

Refer to the exhibit.

An SSL client is connecting to an ASA headend. The session fails with the message "Connection attempt has timed out. Please verify Internet connectivity."  
Based on how the packet is processed, which phase is causing the failure?

- A. phase 9: rpf-check
- B. phase 5: NAT
- C. phase 4: ACCESS-LIST
- D. phase 3: UN-NAT

**Answer:** D

#### NEW QUESTION 30

Which redundancy protocol must be implemented for IPsec stateless failover to work?

- A. SSO
- B. GLBP
- C. HSRP
- D. VRRP

**Answer:** C

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/vpn/ipsec-negotiation-ike-protocols/17826-ipsec-feat.html>

#### NEW QUESTION 34

Which technology works with IPsec stateful failover?

- A. GLBR
- B. HSRP
- C. GRE
- D. VRRP

**Answer:** B

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/ios/12\\_2/12\\_2y/12\\_2yx11/feature/guide/ft\\_vpnha.html#wp1122512](https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp1122512)

#### NEW QUESTION 35

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

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

**Answer:** CD

#### Explanation:

Reference: [https://tools.cisco.com/security/center/resources/next\\_generation\\_cryptography](https://tools.cisco.com/security/center/resources/next_generation_cryptography)

#### NEW QUESTION 37

What uses an Elliptic Curve key exchange algorithm?

- A. ECDSA
- B. ECDHE
- C. AES-GCM
- D. SHA

**Answer:** B

#### Explanation:

Reference: <https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>

#### NEW QUESTION 40

Which two remote access VPN solutions support SSL? (Choose two.)

- A. FlexVPN

- B. clientless
- C. EZVPN
- D. L2TP
- E. Cisco AnyConnect

**Answer:** BE

#### NEW QUESTION 43

Which VPN solution uses TBAR?

- A. GETVPN
- B. VTI
- C. DMVPN
- D. Cisco AnyConnect

**Answer:** A

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_getvpn/configuration/xs-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xs-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html)

#### NEW QUESTION 47

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

**Answer:** AD

#### NEW QUESTION 52

Cisco AnyConnect clients need to transfer large files over the VPN sessions. Which protocol provides the best throughput?

- A. SSL/TLS
- B. L2TP
- C. DTLS
- D. IPsec IKEv1

**Answer:** C

#### NEW QUESTION 54

Refer to the exhibit.

```
crypto isakmp policy 10
  encr aes 256
  hash sha256
  authentication pre-share
  group 14

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode transport

crypto ipsec profile CCNP
set transform-set TS

interface Tunnell
ip address 10.0.0.1 255.255.255.0
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 172.18.10.2
tunnel protection ipsec profile CCNP
```

Which VPN technology is used in the exhibit?

- A. DVTI
- B. VTI
- C. DMVPN
- D. GRE

**Answer:** B

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_vpniips/configuration/zZ-Archive/IPsec\\_Virtual\\_Tunnel\\_Interface.html#GUID-](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpniips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-)

EB8C433B-2394-42B9-997F-B40803E58A91

**NEW QUESTION 55**

A Cisco ASA is configured in active/standby mode. What is needed to ensure that Cisco AnyConnect users can connect after a failover event?

- A. AnyConnect images must be uploaded to both failover ASA devices.
- B. The vpn-session-db must be cleared manually.
- C. Configure a backup server in the XML profile.
- D. AnyConnect client must point to the standby IP address.

**Answer:** A

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa\\_90\\_cli\\_config/ha\\_active\\_standby.html](https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html)

**NEW QUESTION 60**

Which benefit of FlexVPN is a limitation of DMVPN using IKEv1?

- A. GRE encapsulation allows for forwarding of non-IP traffic.
- B. IKE implementation can install routes in routing table.
- C. NHRP authentication provides enhanced security.
- D. Dynamic routing protocols can be configured.

**Answer:** B

**NEW QUESTION 61**

Where is split tunneling defined for IKEv2 remote access clients on a Cisco router?

- A. IKEv2 authorization policy
- B. Group Policy
- C. virtual template
- D. webvpn context

**Answer:** B

**NEW QUESTION 64**

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

**Answer:** B

**NEW QUESTION 67**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-730 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-730 Product From:

<https://www.2passeasy.com/dumps/300-730/>

### Money Back Guarantee

#### **300-730 Practice Exam Features:**

- \* 300-730 Questions and Answers Updated Frequently
- \* 300-730 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-730 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 300-730 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year