

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.certbus.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

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1 New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):      encryption AES-CBC
ISAKMP: (0):      keylength of 256
ISAKMP: (0):      hash SHA256
ISAKMP: (0):      default group 14
ISAKMP: (0):      auth pre-share
ISAKMP: (0):      life type in seconds
ISAKMP: (0):      life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2 New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3 New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4 New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4 New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

Refer to the exhibit. A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

- A. An authentication failure occurs on the remote peer.
- B. A certificate fragmentation issue occurs between both sides.
- C. UDP 4500 traffic from the peer does not reach the router.
- D. An authentication failure occurs on the router.

Correct Answer: C

QUESTION 2

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. *\$DfltIkeIdentityS*

Correct Answer: B

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

QUESTION 3

An organization wants to distribute remote access VPN load across 12 VPN headend locations supporting 25,000 simultaneous users. Which load balancing method meets this requirement?

A. one VPN profile per site

B. DNS-based load balancing

C. AnyConnect native load balancing

D. equal cost, multipath load balancing

Correct Answer: B

QUESTION 4

```
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
```

Refer to the exhibit. 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

Correct Answer: A

TS unacceptable:

The IPsec SA setup has failed due to a mismatch in the policy rule definition between the gateways for the tunnel configuration.

Check the local and remote network configuration on both gateways.

QUESTION 5

Which parameter in IPsec VPN tunnel configurations is optional?

- A. hash
- B. lifetime
- C. encryption
- D. Perfect Forward Secrecy

Correct Answer: D

QUESTION 6

An engineer is configuring clientless SSL VPN. The finance department has a database server that only they should access, but the sales department can currently access it. The finance and the sales departments are configured as separate group-policies. What must be added to the configuration to make sure the users in the sales department cannot access the finance department server?

- A. tunnel group lock
- B. smart tunnel
- C. port forwarding
- D. webtype ACL

Correct Answer: A

Reference <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/acl->

webtype.pdf

QUESTION 7

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

QUESTION 8

Which configuration allows a Cisco ASA to receive an IPsec connection from a peer with an unknown IP address?

- A. dynamic crypto map
- B. dynamic tunnel group
- C. dynamic AAA attributes
- D. dynamic access policy

Correct Answer: A

QUESTION 9

Refer to the exhibit.

```
interface Tunnel119
 ip address 172.20.58.7 255.255.0.0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel destination 128.17.64.8
 tunnel protection ipsec profile DMVPN_profile
end
```

Which type of VPN tunnel is configured?

- A. Multipoint GRE
- B. DMVPN
- C. FlexVPN
- D. GRE over IPsec

Correct Answer: D

QUESTION 10

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 11

An administrator is setting up Cisco AnyConnect on a Cisco ASA with the requirement that AnyConnect automatically establishes a VPN when a company-owned laptop is connected to the internet outside of the corporate network. Which configuration meets these requirements?

- A. SBL with user certificate authentication
- B. TND with machine certificate authentication
- C. SBL with machine certificate authentication
- D. TND with user certificate authentication

Correct Answer: D

QUESTION 12

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
  enrollment url http://192.168.3.1:80
  revocation-check crl
!
crypto pki certificate map certmap1 1
  subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
  ipv6 pool v6-pool
  ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
  ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
  match certificate certmap1
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint trustpoint1
  aaa authorization group cert list local-group-author-list
  author-policy1
  virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
  set transform-set trans transform1
  set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
  ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
  ipv6 unnumbered Ethernet0/0
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
  permit ipv6 host 2001:DB8:1::20 any
  permit ipv6 host 2001:DB8:1::30 any
```

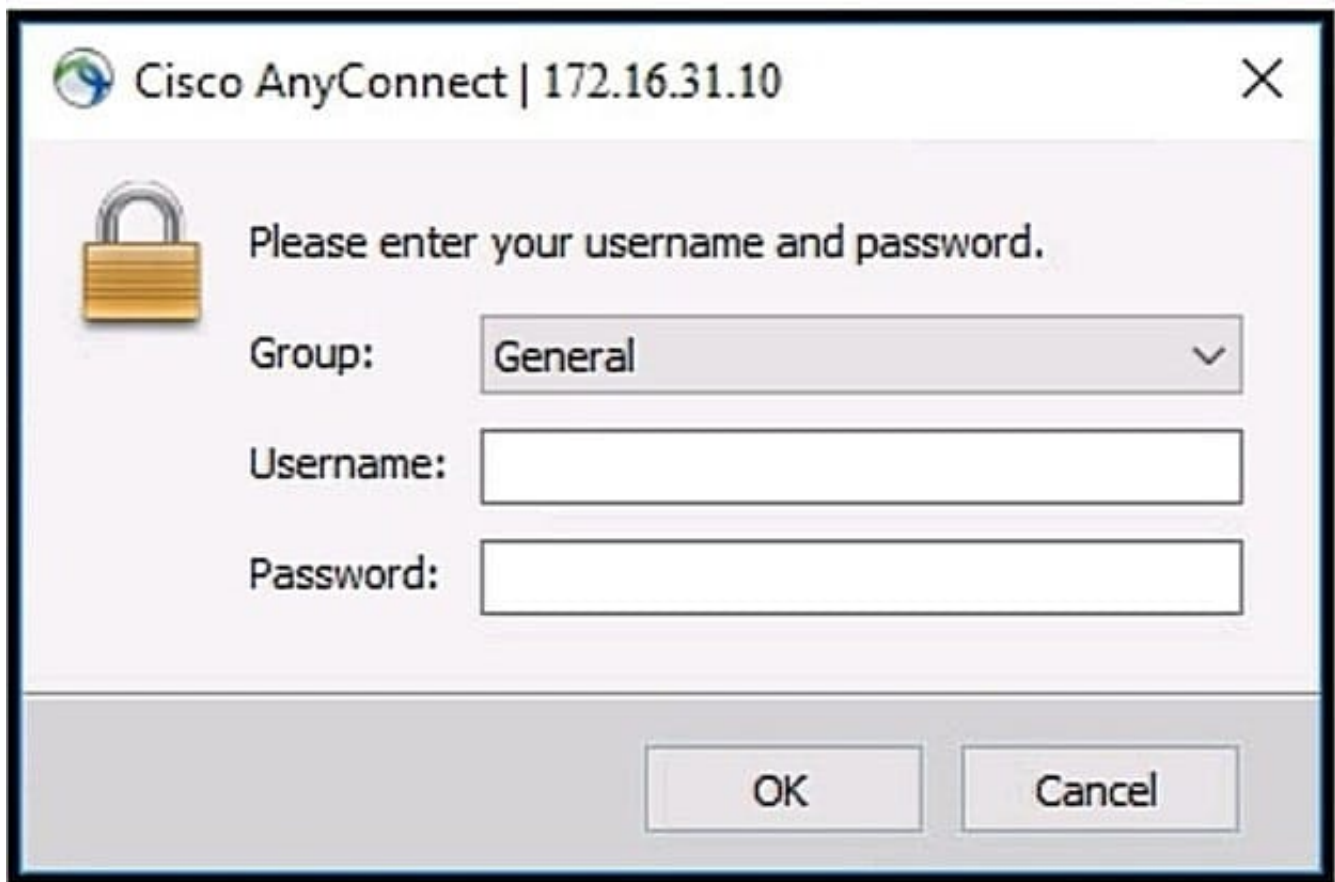

Refer to the exhibit. What is configured as a result of this command set?

- A. FlexVPN client profile for IPv6
- B. FlexVPN server to authorize groups by using an IPv6 external AAA
- C. FlexVPN server for an IPv6 dVTI session
- D. FlexVPN server to authenticate IPv6 peers by using EAP

Correct Answer: C

The configuration snippet is an identical match to the server configuration when you look it up. Not the client.

QUESTION 13



Refer to the exhibit. Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)

- A. group-url https://172.16.31.10/General enable
- B. group-policy General internal
- C. authentication aaa

D. authentication certificate

E. group-alias General enable

Correct Answer: CE

QUESTION 14

Refer to the exhibit.

```
group-policy My_GroupPolicy internal
group-policy My_GroupPolicy attributes
  vpn-tunnel-protocol l2tp-ipsec
!
webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
http server enable 8080
!
tunnel-group My_WebVPN general-attributes
  address-pool My_Pool
  default-group-policy My_GroupPolicy
```

Users cannot connect via AnyConnect SSLVPN. Which action resolves this issue?

A. Configure the ASA to act as a DHCP server.

- B. Configure the HTTP server to listen on port 443.
- C. Add an IPsec preshared key to the group policy.
- D. Add ssl-client to the allowed list of VPN protocols.

Correct Answer: D

QUESTION 15

A network engineer must design a clientless VPN solution for a company. VPN users must be able to access several internal web servers. When reachability to those web servers was tested, it was found that one website is not being rewritten correctly by the ASA. What is a potential solution for this issue while still allowing it to be a clientless VPN setup?

- A. Set up a smart tunnel with the IP address of the web server.
- B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.
- C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.
- D. Set up a WebACL to permit the IP address of the web server.

Correct Answer: B

[Latest 300-730 Dumps](#)

[300-730 PDF Dumps](#)

[300-730 Exam Questions](#)