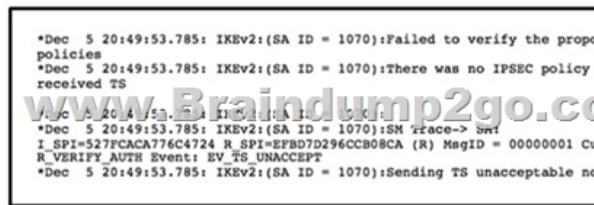


[2020-November-NewReal 300-730 Dumps PDF and VCE 300-730 70Q-Braindump2go[Q48-Q65

2020/November Latest Braindump2go 300-730 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 300-730 Real Exam Questions!QUESTION 48Refer 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> enableB. group-policy General internalC. authentication aaaD. authentication certificateE. group-alias General enableAnswer: BQUESTION 49Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)A. The VPN server must have a self-signed certificate.B. A SSL group pre-shared key must be configured on the server.C. Server side certificate is optional if using AAA for client authentication.D. The VPN IP address pool can overlap with the rest of the LAN networks.E. DTLS can be enabled for better performance.Answer: DEQUESTION 50An engineer is configuring IPsec VPN and wants to choose an authentication protocol that is reliable and supports ACK and sequence.Which protocol accomplishes this goal?A. IKEv1B. AES-192C. ESPD. AES-256Answer: CQUESTION 51Refer to the exhibit. What is the problem with the IKEv2 site-to-site VPN tunnel?



A. incorrect PSKB. crypto access list mismatchC. incorrect tunnel groupD. crypto policy mismatchE. incorrect certificateAnswer: BQUESTION 52Which requirement is needed to use local authentication for Cisco AnyConnect Secure Mobility Clients that connect to a FlexVPN server?A. use of certificates instead of username and passwordB. EAP-AnyConnectC. EAP query-identityD. AnyConnect profileAnswer: DExplanation:

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

QUESTION 53Which 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. *\$DfltKeldentity\$*

Answer: BExplanation:

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

QUESTION 54Refer to the exhibit. Which VPN technology is allowed for users connecting to the Employee tunnel group?

```
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 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
```

A. SSL AnyConnectB. IKEv2 AnyConnectC. crypto mapD. clientless
Answer: BQUESTION 55Refer to the exhibit. An engineer is troubleshooting a new GRE over IPsec tunnel. The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2. Which type of traffic is being blocked?

```
Spoke1#
local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
#pkts encaps: 200, #pkts encrypt: 200
#pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
inbound esp sas:
spi: 034832CA36 (1261619766)
outbound esp sas:
spi: 0x0601918E (1760427022)
Spoke2#
local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
#pkts encaps: 210, #pkts encrypt: 210,
#pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
inbound esp sas:
spi: 03D601918E (1760427022)
outbound esp sas:
spi: 034832CA36 (1261619766)
```

A. ESP packets from spoke2 to spoke1B. ISAKMP packets from spoke2 to spoke1C. ESP packets from spoke1 to spoke2D. ISAKMP packets from spoke1 to spoke2
Answer: AQUESTION 56Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

A. show crypto ikev2 saB. show crypto isakmp saC. show crypto gkmD. show crypto identity
Answer: AExplanation: <https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116413-configure-flexvpn-00.pdf>
QUESTION 57In 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: BExplanation: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-summ-maps.pdf

QUESTION 58An 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: BQUESTION 59What are two variables for configuring clientless SSL VPN single sign-on? (Choose two.)
A. CSCO_WEBVPN_OTP_PASSWORDB. CSCO_WEBVPN_INTERNAL_PASSWORDC. CSCO_WEBVPN_USERNAMED. CSCO_WEBVPN_RADIUS_USER

Answer: BCQUESTION 60Which two NHRP functions are specific to DMVPN Phase 3 implementation? (Choose two.)
A. registration requestB. registration replyC. resolution requestD. resolution replyE. redirect
Answer: DEQUESTION 61Refer to the exhibit. The customer can establish a Cisco AnyConnect connection without using an XML profile. When the host "ikev2" is selected in the AnyConnect drop down, the connection fails. What is the cause of this issue?

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
address-pool split
default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
group-alias ikev2 enable

www.Braindump2go.com

-<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

A. The HostName is incorrect. B. The IP address is incorrect. C. Primary protocol should be SSL. D. UserGroup must match connection profile. Answer: D Explanation:

<https://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891> QUESTION 62 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?

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my
ISAKMP-PAK: (0):received packet from 192.168.0.8
ISAKMP: (0):Old State = IKE_I_MM1 New State = I
ISAKMP: (0):found peer pre-shared key matching 1
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against
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
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my
ISAKMP-PAK: (0):received packet from 192.168.0.8
ISAKMP: (0):Old State = IKE_I_MM1 New State = I
ISAKMP: (0):found peer pre-shared key matching 1
ISAKMP: (1005):Old State = IKE_I_MM4 New State =
ISAKMP: (1005):pre-shared key authentication using
ISAKMP-PAK: (1005):sending packet to 192.168.0.8
ISAKMP: (1005):received packet from 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4 New State =
ISAKMP: (1005):retransmitting due to retransmit
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH
ISAKMP: (1005):: incrementing error counter on s
ISAKMP-PAK: (1005):sending packet to 192.168.0.8
ISAKMP: (1005):received packet from 192.168.0.8
ISAKMP: (1005):phase 1 packet is a duplicate of
ISAKMP: (1005):retransmitting due to retransmit
```

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. Answer: C QUESTION 63

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

```
IKEV2:(SESSION ID = 17, SA ID = 1):Processing
IKEV2:IPsec policy validate request sent fr
IKEV2:(SA ID = 1):[IPsec -> IKEV2] Callbac
IKEV2-ERROR:(SESSION ID = 17, SA ID = 1)::
IKEV2:(SESSION ID = 17, SA ID = 1):Sending
IKEV2:(SESSION ID = 17, SA ID = 1):Get my au
IKEV2:(SESSION ID = 17, SA ID = 1):My auther
IKEV2:(SESSION ID = 17, SA ID = 1):Get peer
IKEV2:(SESSION ID = 17, SA ID = 1):Generate
IKEV2:(SESSION ID = 17, SA ID = 1):Use presh
IKEV2:(SESSION ID = 17, SA ID = 1):Use presh
IKEV2:(SESSION ID = 17, SA ID = 1):Get my au
IKEV2:(SESSION ID = 17, SA ID = 1):My auther
IKEV2:(SESSION ID = 17, SA ID = 1):Generatin
IKEV2:(SESSION ID = 17, SA ID = 1):Construct
IKEV2:(SESSION ID = 17, SA ID = 1):Building
Payload contents:
VID IDr AUTH NOTIFY(TS_UNACCEPTABLE)
IKEV2:(SESSION ID = 17, SA ID = 1):Sending
Initiator SPI : 3D527B1D500BEEF4 - Responde
IKEV2 IKE_AUTH Exchange RESPONSE
Payload contents:
ENCR
```

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. QUESTION 64 Refer to the exhibit. The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch is the problem?

```
*Nov 26 08:52:28.882: DEX(2):(SESSION ID = 1, SA ID = 1):Received Packet (From 19.19.19.1:500/To 19.19.19.2:500/Off 0h-0s)
Initiator SPI : 056440240291656 - Responder SPI : 254234029165644 Message id: 1
DEX(2) DEX_AUTH Exchange RESPONSE
*Nov 26 08:52:28.882: DEX(2)-PM:(SESSION ID = 1, SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: DEX_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 204
Payload contents:
V2D Next payload: IDr, reserved: 0x0, length: 20
IDr Next payload: AUTH, reserved: 0x0, length: 12
ID type: IPv4 address, reserved: 0x0
AUTH Next payload: SA, reserved: 0x0, length: 28
Auth method PFX, reserved: 0x0, reserved: 0x0
SA Next payload: TSr, reserved: 0x0, length: 40
Last proposal: 0x0, reserved: 0x0, length: 35
Proposal: 1, Protocol id: ESP, SPI size: 4, Nrans: 3 last transform: 0x0, reserved: 0x0, length: 8
Type: 1, reserved: 0x0, id: 0003
Last transform: 0x0, reserved: 0x0, length: 8
Type: 3, reserved: 0x0, id: 5000
Last transform: 0x0, reserved: 0x0, length: 8
Type: 5, reserved: 0x0, id: Don't use ESP
TSr Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved: 0x0, reserved: 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
TS: 19.19.19.1/24, reserved: 0x0, reserved: 0x0
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
Num of TSs: 1, reserved: 0x0, reserved: 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 19.19.19.0, end addr: 19.19.19.255
NOTIFY(SET_KIDNOV_SIZES) Next payload: NOTIFY, reserved: 0x0, length: 12
Security protocol id: Unknown - 0, spi size: 0, type: SET_KIDNOV_SIZES
NOTIFY(ESP_TFC_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_SUPPORT
NOTIFY(NON_FINAL_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: NON_FINAL_FRAGS
*Nov 26 08:52:28.883: DEX(2):(SESSION ID = 1, SA ID = 1):Process auth response notify
*Nov 26 08:52:28.883: DEX(2):(SESSION ID = 1, SA ID = 1):Searching policy based on peer's identity '19.19.19.1' of type 'IPv4 address'
*Nov 26 08:52:28.884: DEX(2)-SRR:(SESSION ID = 1, SA ID = 1):Failed to locate an item in the database
*Nov 26 08:52:28.884: DEX(2):(SESSION ID = 1, SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 08:52:28.884: DEX(2):(SESSION ID = 1, SA ID = 1):Auth exchange failed
*Nov 26 08:52:28.884: DEX(2)-SRR:(SESSION ID = 1, SA ID = 1):Auth exchange failed
Restart
*Nov 26 08:52:28.884: DEX(2):(SESSION ID = 1, SA ID = 1):Abort exchange
*Nov 26 08:52:28.884: DEX(2):(SESSION ID = 1, SA ID = 1):Setting SA
```

A. preshared key B. peer identity C. transform set D. ikev2 proposal
Answer: B
Refer to the exhibit. Which type of mismatch is causing the problem with the IPsec VPN tunnel?

```
*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: Ikev2: Error: Invalid payload:
*Jul 16 20:21:25.317: CRYPTO-4-IPSEC_BAD_MESSAGE: IKE message from 192.168.0.2 failed its sanity check or is malformed
```

A. crypto access list B. Phase 1 policy C. transform set D. preshared key
Answer: D
Explanation:
<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike>
Resources
From: 1.2020 Latest Braindump2go 300-730 Exam Dumps (PDF & VCE) Free Share:
<https://www.braindump2go.com/300-730.html>
2.2020 Latest Braindump2go 300-730 PDF and 300-730 VCE Dumps Free Share:
https://drive.google.com/drive/folders/1zBS7xcmszvPHrS_IPaM4uUF1VvomE4a?usp=sharing
3.2020 Free Braindump2go 300-730 PDF Download:
[https://www.braindump2go.com/free-online-pdf/300-730-Dumps\(38-48\).pdf](https://www.braindump2go.com/free-online-pdf/300-730-Dumps(38-48).pdf)
[https://www.braindump2go.com/free-online-pdf/300-730-PDF\(27-37\).pdf](https://www.braindump2go.com/free-online-pdf/300-730-PDF(27-37).pdf)
[https://www.braindump2go.com/free-online-pdf/300-730-PDF-Dumps\(1-15\).pdf](https://www.braindump2go.com/free-online-pdf/300-730-PDF-Dumps(1-15).pdf)
[https://www.braindump2go.com/free-online-pdf/300-730-VCE\(16-26\).pdf](https://www.braindump2go.com/free-online-pdf/300-730-VCE(16-26).pdf)
[https://www.braindump2go.com/free-online-pdf/300-730-VCE-Dumps\(49-60\).pdf](https://www.braindump2go.com/free-online-pdf/300-730-VCE-Dumps(49-60).pdf)
Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!