Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

NEW QUESTION 1
A second set of traffic selectors is negotiated between two peers using IKEv2. Which IKEv2 packet will contain details of the exchange?

A. IKEv2 IKE_SA_INIT
B. IKEv2 INFORMATIONAL
C. IKEv2 CREATE_CHILD_SA
D. IKEv2 IKE_AUTH

Answer: B

NEW QUESTION 2
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 3
Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?

A. auto-upgrade
B. auto-connect
C. auto-start
D. auto-run

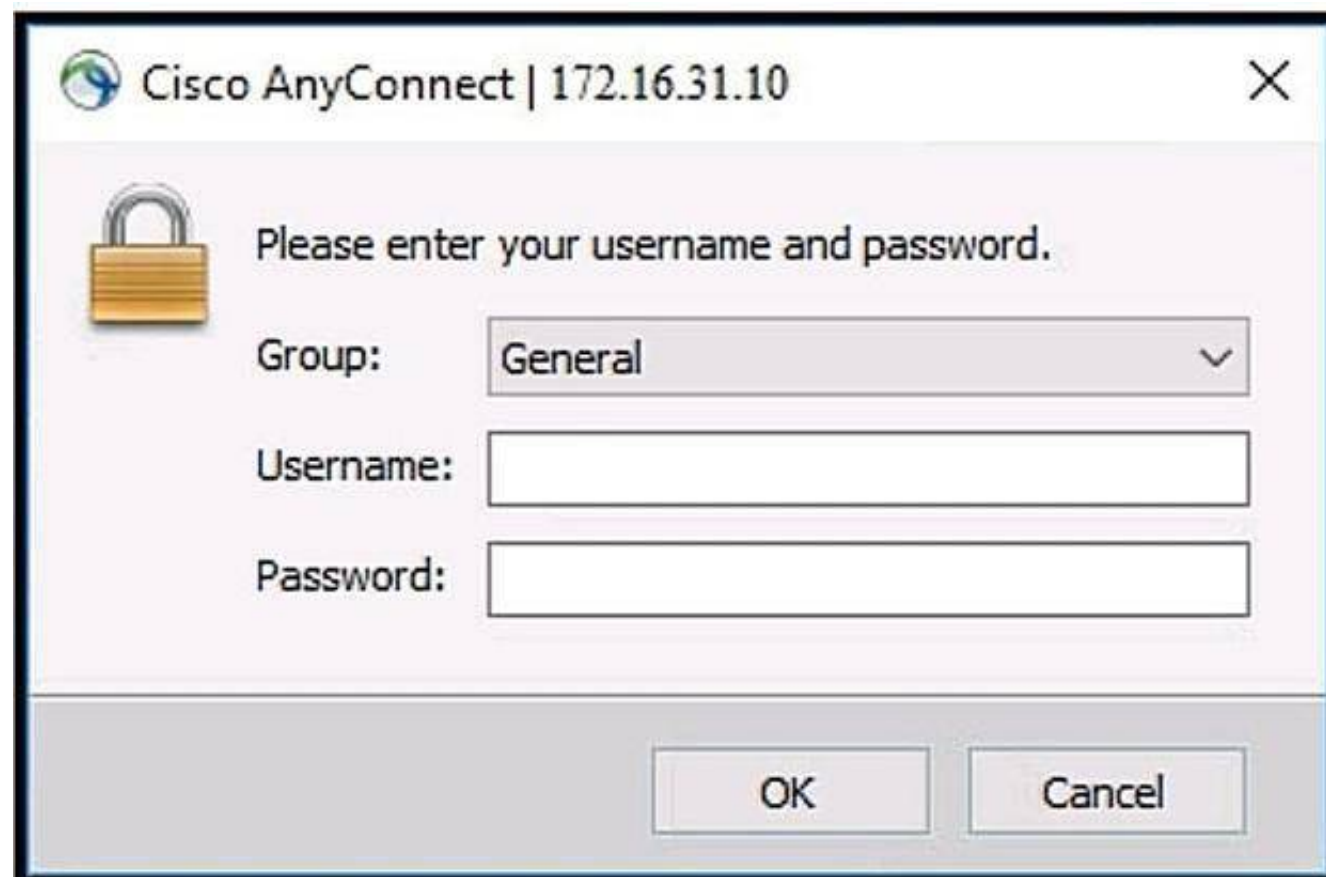**Answer:** C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

NEW QUESTION 4
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

Answer: BE

NEW QUESTION 5
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. *$DfltlkeIdentityS*

Answer: B

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

NEW QUESTION 6
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-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-summ-maps.pdf

NEW QUESTION 7
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 8
Refer to the exhibit.

```
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


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

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?

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:
Reference: https://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891

NEW QUESTION 9
Refer to the exhibit.

```
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
```

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.

Answer: C

NEW QUESTION 10
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 10
Refer to the exhibit.

```
*Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D5684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
*Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
 VID Next payload: IDr, reserved: 0x0, length: 20
 IDr Next payload: AUTH, reserved: 0x0, length: 12
   Id type: IPv4 address, Reserved: 0x0 0x0
 AUTH Next payload: SA, reserved: 0x0, length: 28
   Auth method PSK, reserved: 0x0, reserved: 0x0
 SA Next payload: TSi, reserved: 0x0, length: 40
   last proposal: 0x0, reserved: 0x0, length: 35
   Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
     type: 1, reserved: 0x0, id: 3DES
     last transform: 0x3, reserved: 0x0: length: 8
     type: 3, reserved: 0x0, id: SHA96
     last transform: 0x0, reserved: 0x0: length: 8
     type: 5, reserved: 0x0, id: Don't use ESN
 TSi 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
   start port: 0, end port: 65535
   start addr: 30.30.30.0, end addr: 30.30.30.255
 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: 20.20.20.0, end addr: 20.20.20.255
 NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
   Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
 NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
 NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
```
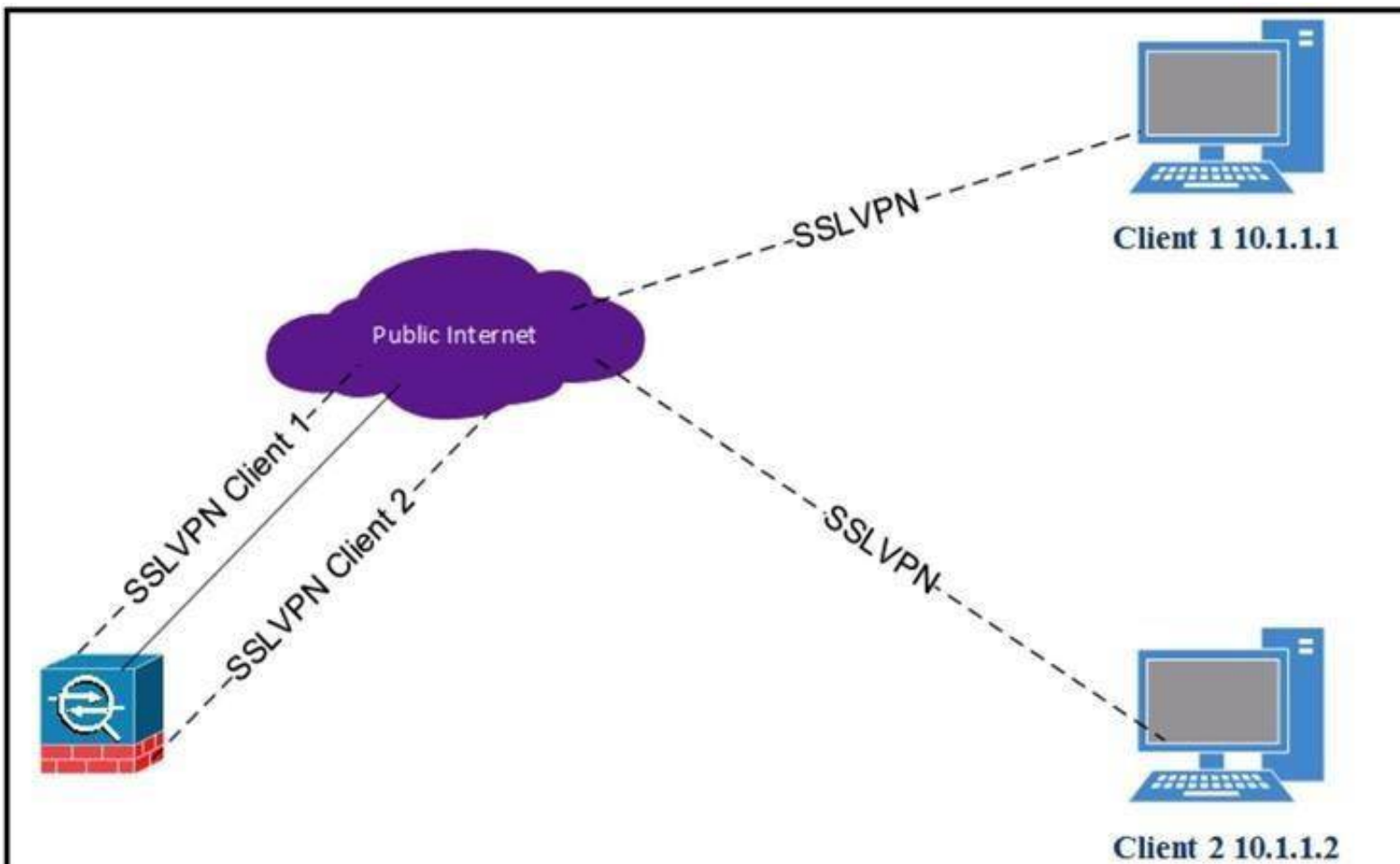
The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch is the problem?

A. preshared key
B. peer identity
C. transform set
D. ikev2 proposal

Answer: B

NEW QUESTION 12
Refer to the exhibit.

Client 1 cannot communicate with client 2. Both clients are using Cisco AnyConnect and have established a successful SSL VPN connection to the hub ASA.

Which command on the ASA is missing?

A. dns-server value 10.1.1.2
B. same-security-traffic permit intra-interface
C. same-security-traffic permit inter-interface
D. dns-server value 10.1.1.3

Answer: B

NEW QUESTION 15
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

NEW QUESTION 18
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

NEW QUESTION 23
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 Tunnel1
  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_vpnips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

NEW QUESTION 24
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

Answer: D

NEW QUESTION 27
Which parameter is initially used to elect the primary key server from a group of key servers?

A. code version
B. highest IP address
C. highest-priority value
D. lowest IP address

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

NEW QUESTION 31
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 34
Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

A. sequence numbers that enable scalable replay checking
B. enabled use of ESP or AH
C. design for use over public or private WAN
D. no requirement for an overlay routing protocol

Answer: D

NEW QUESTION 39
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The 300-730 Practice Test Here](https://www.surepassexam.com/300-730-exam-dumps.html)