

## 300-730 Dumps

# Implementing Secure Solutions with Virtual Private Networks (SVPN)

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



## NEW QUESTION 1

Refer to the exhibit.

```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
    Tunnel0 created 00:02:09, expire 00:00:01
    Type: dynamic, Flags: unique registered used nhop
    NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
    Tunnel0 created 00:13:25, 01:46:34
    Type: dynamic, Flags: unique registered used nhop
    NBMA address: 3.3.3.1
```

The DMVPN tunnel is dropping randomly and no tunnel protection is configured. Which spoke configuration mitigates tunnel drops?

A.

```
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
no ip redirects
ip nhrp map 10.0.0.1 1.1.1.1
ip nhrp map multicast 1.1.1.1
ip nhrp network-id 1
ip nhrp holdtime 20
ip nhrp nhs 10.0.0.1
ip nhrp registration timeout 120
ip nhrp shortcut
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
end
```

A. interface Tunnel0

```
ip address 10.0.0.2 255.255.255.0
no ip redirects
ip nhrp map 10.0.0.1 1.1.1.1
ip nhrp map multicast 1.1.1.1
ip nhrp network-id 1
ip nhrp holdtime 120
ip nhrp nhs 10.0.0.1
ip nhrp registration timeout 120
ip nhrp shortcut
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
end
```

B. interface Tunnel0

```
ip address 10.0.0.2 255.255.255.0
no ip redirects
ip nhrp map 10.0.0.1 1.1.1.1
ip nhrp map multicast 1.1.1.1
ip nhrp network-id 1
ip nhrp holdtime 120
ip nhrp nhs 10.0.0.1
ip nhrp registration timeout 20
ip nhrp shortcut
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
end
```

D.

```
interface Tunnel0
  ip address 10.0.0.2 255.255.255.0
  no ip redirects
  ip nhrp map 10.0.0.1 1.1.1.1
  ip nhrp map multicast 1.1.1.1
  ip nhrp network-id 1
  ip nhrp holdtime 120
  ip nhrp nhs 10.0.0.1
  ip nhrp registration timeout 150
  ip nhrp shortcut
  tunnel source GigabitEthernet0/1
  tunnel mode gre multipoint
end
```

**Answer:** D

#### NEW QUESTION 2

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 3

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 4

Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

- A. Add NHRP shortcuts on the hub.
- B. Add NHRP redirects on the spoke.
- C. Disable EIGRP next-hop-self on the hub.
- D. Enable EIGRP next-hop-self on the hub.
- E. Add NHRP redirects on the hub.

**Answer:** CE

#### NEW QUESTION 5

Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

- A. group-alias
- B. certificate map
- C. optimal gateway selection
- D. group-url
- E. AnyConnect client version

**Answer:** BD

#### NEW QUESTION 6

Refer to the exhibit.



```
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
```

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

**Answer:** A

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/xs-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-clnt.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xs-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-clnt.html)

#### NEW QUESTION 7

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 8**

Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

- A. The XML profile is not configured correctly for the affected users.
- B. The new client image does not use the same major release as the current one.
- C. Client services are not enabled.
- D. Client software updates are not supported with IKEv2.

**Answer: C**

**NEW QUESTION 9**

Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

- A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the client uses the local DNS to perform FQDN resolution.
- B. The rewriter enable command under the global webvpn configuration enables the rewriter functionality because that feature is disabled by default.
- C. A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.
- D. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution.
- E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

**Answer: CD**

**NEW QUESTION 10**

Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

- A. single sign-on
- B. Smart Tunnel
- C. WebType ACL
- D. plug-ins

**Answer: B**

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa\\_90\\_cli\\_config/vpn\\_clientless\\_ssl.html#29951](https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_clientless_ssl.html#29951)

**NEW QUESTION 10**

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](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 13**

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
```

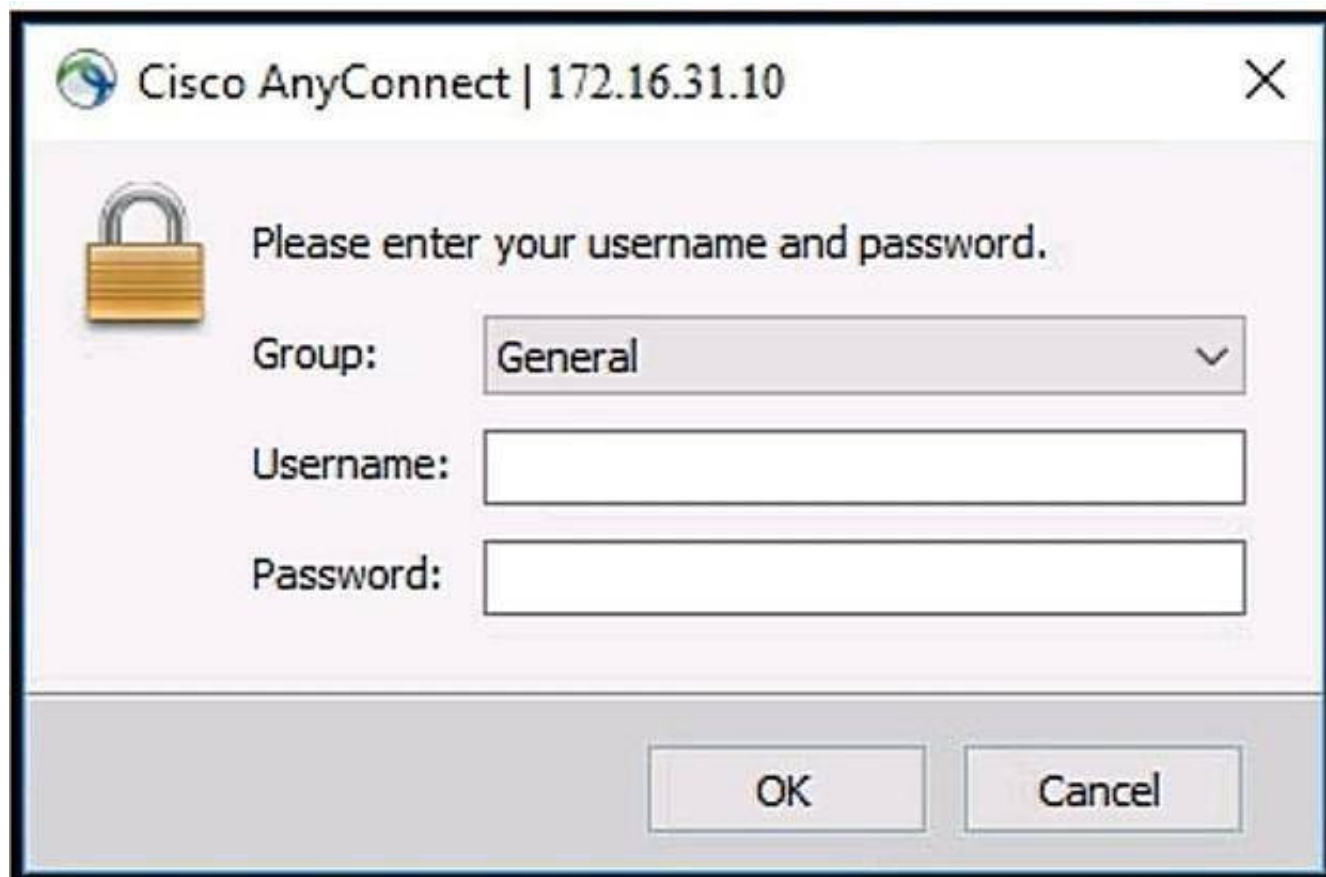
**Answer:** C

**Explanation:**

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

**NEW QUESTION 15**

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 17**

Which 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 password
- B. EAP-AnyConnect
- C. EAP query-identity
- D. AnyConnect profile

**Answer:** D

**Explanation:**

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

**NEW QUESTION 21**

Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

- A. show crypto ikev2 sa
- B. show crypto isakmp sa
- C. show crypto gkm
- D. show crypto identity

**Answer:** A

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116413-configure-flexvpn-00.pdf>



**NEW QUESTION 26**

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 28**

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 29**

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 32

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 34

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 37

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 41**

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 45**

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 47**

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\\_vpnips/configuration/zZ-Archive/IPsec\\_Virtual\\_Tunnel\\_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91](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 49**

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 54**

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 vpnsession-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 56**

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 57**

What is a requirement for smart tunnels to function properly?

- A. Java or ActiveX must be enabled on the client machine.
- B. Applications must be UDP.
- C. Stateful failover must not be configured.
- D. The user on the client machine must have admin access.

**Answer:** A

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00.html>

**NEW QUESTION 60**

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 65**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 300-730 Exam with Our Prep Materials Via below:**

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