Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

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
Refer to the exhibit.

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 192.168.0.2 port 500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

    local crypto endpt.: 192.168.0.1, remote crypto endpt.: 192.168.0.2
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
    current outbound spi: 0x3D05D003(1023791107)
    PFS (Y/N): N, DH group: none
```

Which two tunnel types produce the show crypto ipsec sa output seen in the exhibit? (Choose two.)

A. crypto map
B. DMVPN
C. GRE
D. FlexVPN
E. VTI

Answer: BE

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
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/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-clnt.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
A Cisco AnyConnect client establishes a SSL VPN connection with an ASA at the corporate office. An engineer must ensure that the client computer meets the enterprise security policy. Which feature can update the client to meet an enterprise security policy?

A. Endpoint Assessment
B. Cisco Secure Desktop
C. Basic Host Scan
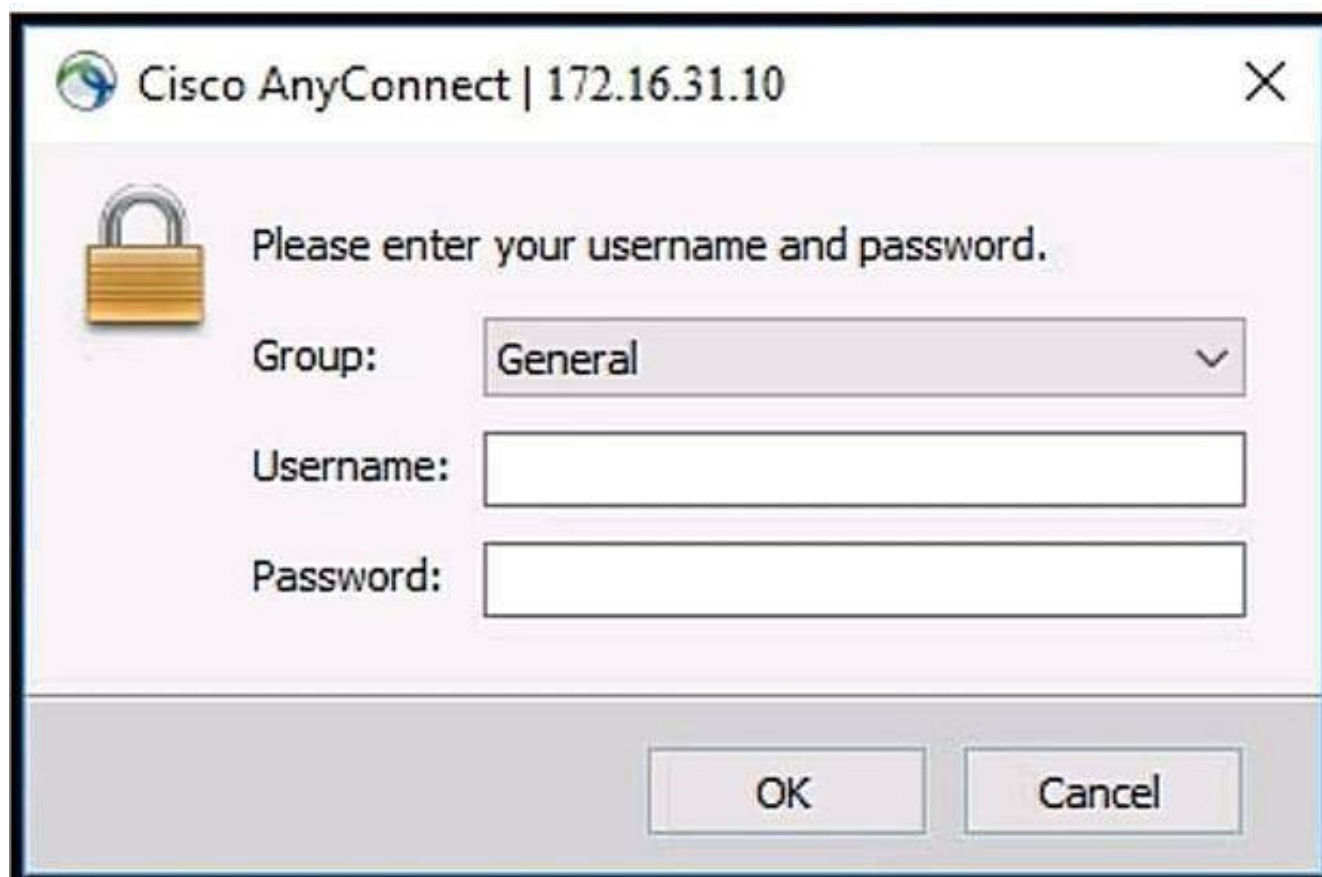D. Advanced Endpoint Assessment

Answer: D

NEW QUESTION 7
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 8
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 9
Refer to the exhibit.

```
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 type remote-access
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
```

Which VPN technology is allowed for users connecting to the Employee tunnel group?

A. SSL AnyConnect
B. IKEv2 AnyConnect
C. crypto map
D. clientless

Answer: B

NEW QUESTION 10
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 10
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 14
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 16
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 20
......

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