

300-730.VCEplus.premium.exam.60q

Number: 300-730
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

300-730

Implementing Secure Solutions with Virtual Private Networks



Sections

1. Site-to-site Virtual Private Networks on Routers and Firewalls
2. Remote access VPNs
3. Troubleshooting using ASDM and CLI
4. Secure Communications Architectures

Exam A

QUESTION 1 DRAG
DROP

Drag and drop the correct commands from the right onto the blanks within the code on the left to implement a design that allow for dynamic spoke-to-spoke communication. Not all comments are used.

Select and Place:

Answer Area

```

Router A
interface Tunnell
 ip address 10.0.0.1 255.255.255.0
 ip nhrp mp multicast dynamic
 ip nhrp network-id 1
 ip nhrp [ ]
 no ip split-horizon eigrp 10
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint

interface GigabitEthernet1
 ip address 1.1.1.1 255.255.255.0

router eigrp 10
 network 10.0.0.0 0.0.0.255

Router B
interface Tunnell
 ip address 10.0.0.2 255.255.255.0
 ip nhrp nhs [ ] nbma [ ] multicast
 ip nhrp network-id 1
 ip nhrp [ ]
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint

interface GigabitEthernet1
 ip address 2.2.2.2 255.255.255.0

router eigrp 10
 network 10.0.0.0 0.0.0.255

```

1.1.1.1

10.0.0.1

redirect

shortcut

server-only

Correct Answer:

Answer Area

<pre> Router A interface Tunnell ip address 10.0.0.1 255.255.255.0 ip nhrp mp multicast dynamic ip nhrp network-id 1 ip nhrp redirect no ip split-horizon eigrp 10 tunnel source GigabitEthernet1 tunnel mode gre multipoint interface GigabitEthernet1 ip address 1.1.1.1 255.255.255.0 router eigrp 10 network 10.0.0.0 0.0.0.255 </pre>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">1.1.1.1</div>
	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">10.0.0.1</div>
	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">redirect</div>
<pre> Router B interface Tunnell ip address 10.0.0.2 255.255.255.0 ip nhrp nhs 10.0.0.1 nbma 1.1.1.1 multicast ip nhrp network-id 1 ip nhrp shortcut tunnel source GigabitEthernet1 tunnel mode gre multipoint interface GigabitEthernet1 ip address 2.2.2.2 255.255.255.0 router eigrp 10 network 10.0.0.0 0.0.0.255 </pre>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">shortcut</div>
	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;">server-only</div>

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xr-16/sec-conn-dmvpn-xr-16-book/sec-conn-dmvpn-summm-maps.html

QUESTION 2

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

Correct Answer: B

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 3

```
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
```

Refer to the exhibit. 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
```



```
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
```

```
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
```

```
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
```



B. C.

D.

Correct Answer: D Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 4

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**



Correct Answer: D

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 5

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.

Correct Answer: A

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 6

```
interface: Tunnell
  Crypto map tag: Tunnell-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
```

Refer to the exhibit. 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



Correct Answer: BE

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 7 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.

Correct Answer: CE

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 8

```
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
```

Refer to the exhibit. 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.

Correct Answer: B

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 9 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



Correct Answer: BD

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

QUESTION 10 Which method dynamically installs the network routes for remote tunnel endpoints?

- A. policy-based routing
- B. CEF
- C. reverse route injection
- D. route filtering

Correct Answer: C

Section: Site-to-site Virtual Private Networks on Routers and Firewalls Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn-availability-12-4t-book/sec-rev-rte-inject.html

QUESTION 11 Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?

- A. **svc import profile SSL_profile flash:simos-profile.xml**
- B. **anyconnect profile SSL_profile flash:simos-profile.xml**
- C. **crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml**
- D. **webvpn import profile SSL_profile flash:simos-profile.xml**

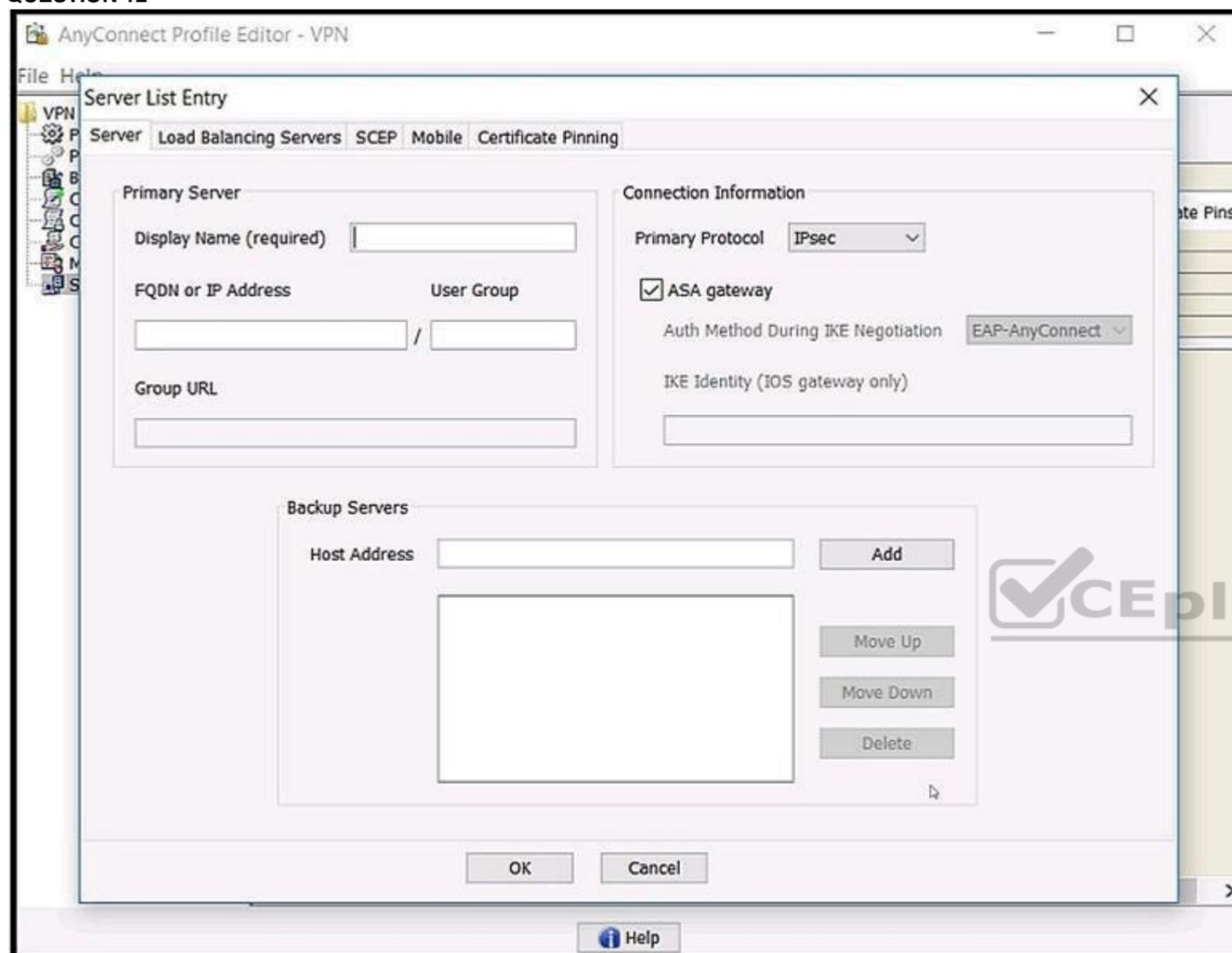
Correct Answer: C

Section: Remote access VPNs Explanation

Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html>

QUESTION 12



Refer to the exhibit. Which value must be configured in the User Group field when the Cisco AnyConnect Profile is created to connect to an ASA headend with IPsec as the primary protocol?

- A. address-pool
- B. group-alias
- C. group-policy
- D. tunnel-group

Correct Answer: D

Section: Remote access VPNs Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-vpn.html

QUESTION 13

```
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: A

Section: Remote access VPNs Explanation

Explanation/Reference:

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

QUESTION 14

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

Correct Answer: DE

Section: Remote access VPNs Explanation

Explanation/Reference:

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>

QUESTION 15 Which configuration construct must be used in a FlexVPN tunnel?

- A. EAP configuration
- B. multipoint GRE tunnel interface
- C. IKEv1 policy
- D. IKEv2 profile



Correct Answer: D

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 16

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

Correct Answer: D

Section: Remote access VPNs

Explanation

Explanation/Reference:

QUESTION 17 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

Correct Answer: CD

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 18

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.

Correct Answer: C

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 19

Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

- A. tunnel-group (general-attributes)
- B. tunnel-group (webvpn-attributes)
- C. webvpn (group-policy)
- D. webvpn (global configuration)

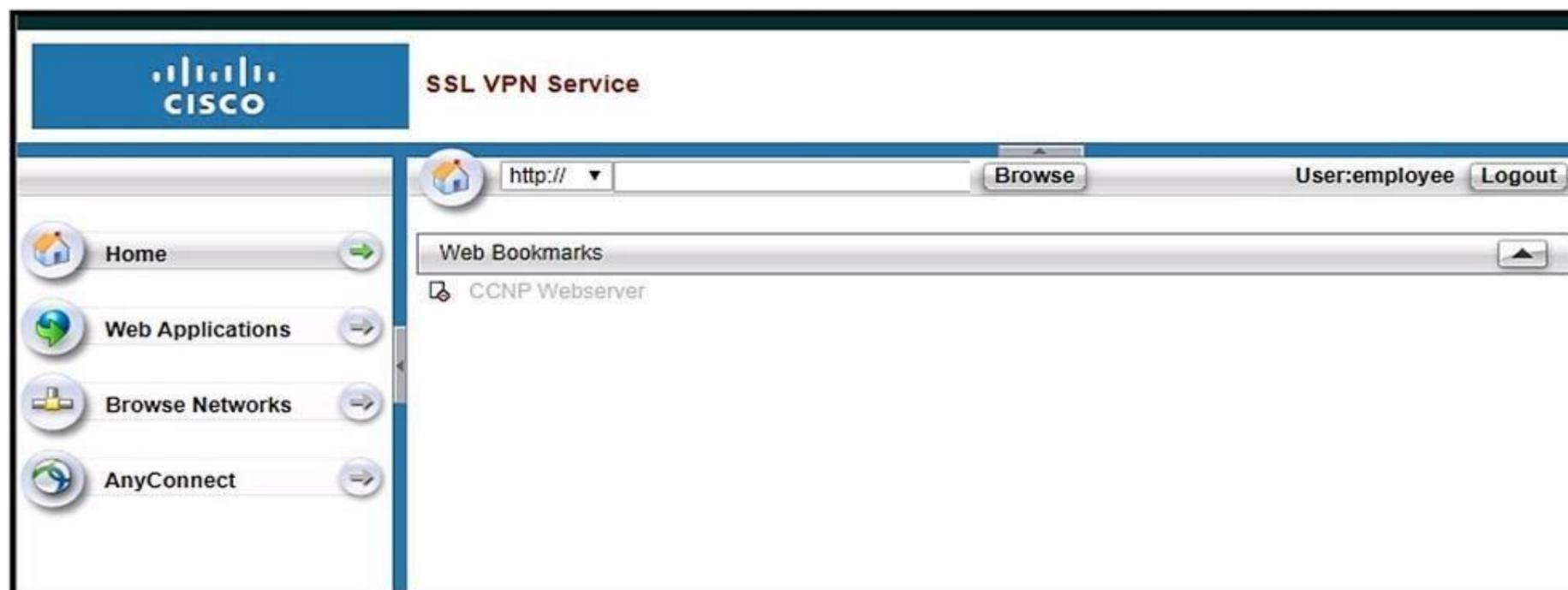


Correct Answer: D

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 20



Refer to the exhibit. Based on the exhibit, why are users unable to access CCNP Webservers bookmark?

- A. The URL is being blocked by a WebACL.
- B. The ASA cannot resolve the URL. The bookmark has been disabled.
- C. The user cannot access the URL.

Correct Answer: C

Section: Remote access VPNs Explanation

Explanation/Reference:



QUESTION 21 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.

Correct Answer: CD

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 22

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

Correct Answer: B
Section: Remote access VPNs Explanation

Explanation/Reference:
 Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_clientless_ssl.html#29951

QUESTION 23 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

Correct Answer: C
Section: Remote access VPNs Explanation

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

QUESTION 24

XML profile

```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

Refer to the exhibit. The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task? A.

- 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
```

Correct Answer: C

Section: Remote access VPNs Explanation

Explanation/Reference:

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

QUESTION 25



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: BE

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 26

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

Correct Answer: D

Section: Remote access VPNs Explanation

Explanation/Reference:

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

QUESTION 27 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. *\$DfltIkeIdentity\$*

Correct Answer: B

Section: Remote access VPNs Explanation

Explanation/Reference:

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

QUESTION 28



```
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
```



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

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

Correct Answer: B

Section: Remote access VPNs Explanation

Explanation/Reference:

QUESTION 29

```

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: 034B32CA36 (1261619766)
  outbound esp sas:
  spi:0xD601918E (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: 034BS2CA36 (1261619766)

```

Refer 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?

- A. ESP packets from spoke2 to spoke1
- B. ISAKMP packets from spoke2 to spoke1
- C. ESP packets from spoke1 to spoke2
- D. ISAKMP packets from spoke1 to spoke2

Correct Answer: A

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

QUESTION 30 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**

Correct Answer: A

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

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

QUESTION 31

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.

Correct Answer: B

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

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

QUESTION 32 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.

Correct Answer: B

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

QUESTION 33

```
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>
```



Refer 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? A.

The HostName is incorrect.

- B. The IP address is incorrect.
- C. Primary protocol should be SSL.
- D. UserGroup must match connection profile.

Correct Answer: D

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

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

QUESTION 34

```
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

Section: Troubleshooting using ASDM and CLI

Explanation

Explanation/Reference:

QUESTION 35

```
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: B

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

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 36

```
*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
```



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?

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

Correct Answer: B

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

QUESTION 37

```
*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
```

Refer to the exhibit. 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



Correct Answer: D

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike>

QUESTION 38

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
```



Refer to the exhibit. 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.

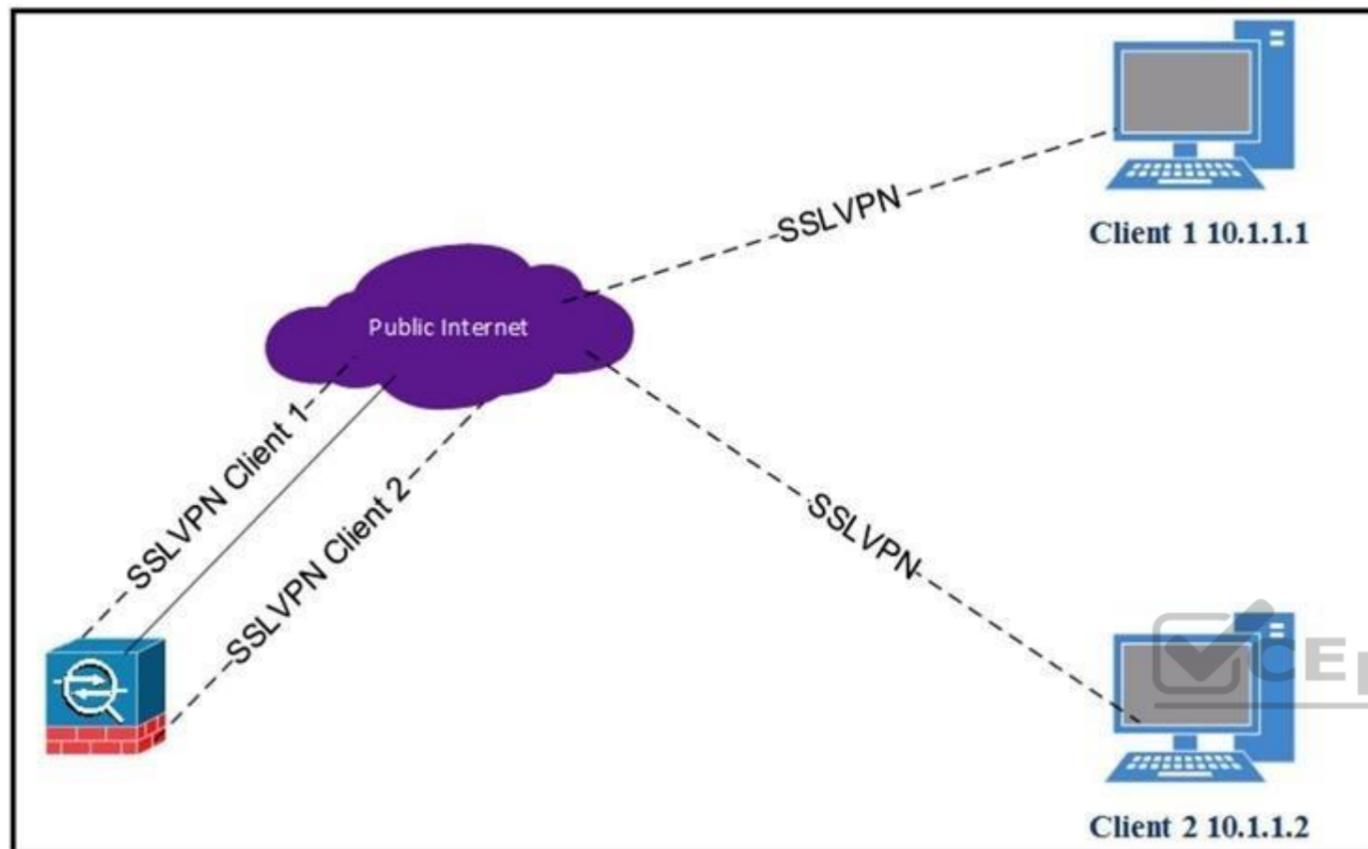
D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Correct Answer: A

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

QUESTION 39



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`

Correct Answer: B

Section: Troubleshooting using ASDM and CLI Explanation

Explanation/Reference:

QUESTION 40

```

Ciscoasa# sh cap o trace packet-number 4

737 packets captured

      4: 08:19:36.054181  10.99.117.195.56485 > 10.31.124.31.443: $ 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up

```

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

Correct Answer: D

Section: Troubleshooting using ASDM and CLI

Explanation

Explanation/Reference:

QUESTION 41 Which redundancy protocol must be implemented for IPsec stateless failover to work?

- A. SSO
- B. GLBP
- C. HSRP
- D. VRRP

Correct Answer: C

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/17826-ipsec-feat.html>



QUESTION 42 Which technology works with IPsec stateful failover?

- A. GLBR
- B. HSRP
- C. GRE
- D. VRRP

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp1122512

QUESTION 43

What are two functions of ECDH and ECDSA? (Choose two.)

- A. nonrepudiation
- B. revocation
- C. digital signature
- D. key exchange
- E. encryption

Correct Answer: CD

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: https://tools.cisco.com/security/center/resources/next_generation_cryptography

QUESTION 44 What uses an Elliptic Curve key exchange algorithm?

- A. ECDSA
- B. ECDHE
- C. AES-GCM
- D. SHA

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: <https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>

QUESTION 45 Which two remote access VPN solutions support SSL? (Choose two.)

- A. FlexVPN
- B. clientless
- C. EZVPN
- D. L2TP
- E. Cisco AnyConnect

Correct Answer: BE

Section: Secure Communications Architectures

Explanation



Explanation/Reference:

QUESTION 46

Which VPN solution uses TBAR?

- A. GETVPN
- B. VTI
- C. DMVPN
- D. Cisco AnyConnect

Correct Answer: A

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

QUESTION 47 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**

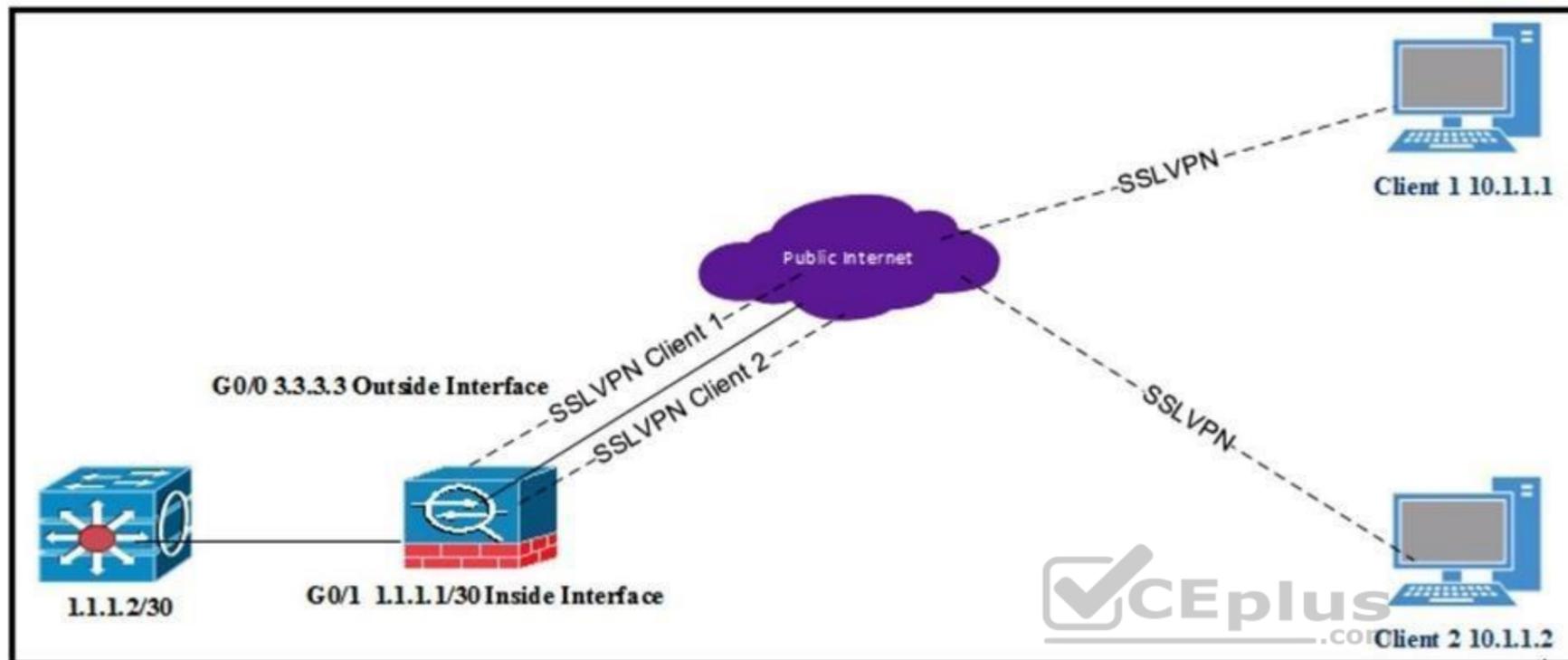
Correct Answer: AD

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 48



Refer to the exhibit. All internal clients behind the ASA are port address translated to the public outside interface that has an IP address of 3.3.3.3. Client 1 and client 2 have established successful SSL VPN connections to the ASA. What must be implemented so that "3.3.3.3" is returned from a browser search on the IP address?

- A. Same-security-traffic permit inter-interface under Group Policy
- B. Exclude Network List Below under Group Policy
- C. Tunnel All Networks under Group Policy
- D. Tunnel Network List Below under Group Policy

Correct Answer: D

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 49

Cisco AnyConnect clients need to transfer large files over the VPN sessions. Which protocol provides the best throughput?

- A. SSL/TLS
- B. L2TP
- C. DTLS
- D. IPsec IKEv1

Correct Answer: C

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 50

```
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
```



Refer to the exhibit. Which VPN technology is used in the exhibit?

- A. DVTI
- B. VTI
- C. DMVPN
- D. GRE

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpniips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

QUESTION 51

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

Correct Answer: D

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 52 Which parameter must match on all routers in a DMVPN Phase 3 cloud?

- A. GRE tunnel key
- B. NHRP network ID
- C. tunnel VRF
- D. EIGRP split-horizon setting

Correct Answer: A

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 53 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

Correct Answer: C

Section: Secure Communications Architectures

Explanation



Explanation/Reference:

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

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 vpn-session-db must be cleared manually.
- C. Configure a backup server in the XML profile.
- D. AnyConnect client must point to the standby IP address.

Correct Answer: A

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html

QUESTION 55 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.

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 56 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.

Correct Answer: A

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

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

QUESTION 57 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

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 58 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

Correct Answer: B

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 59 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



Correct Answer: D

Section: Secure Communications Architectures

Explanation

Explanation/Reference:

QUESTION 60

```
ip access-list extended CCNP
 permit 192.168.0.10
 permit 192.168.0.11

webvpn gateway SSL_Gateway
 ip address 172.16.0.25 port 443
 ssl trustpoint AnyConnect_Cert
 inservice

webvpn context SSL_Context
 gateway SSL_Gateway

ssl authenticate verify all
 inservice

policy group SSL_Policy
 functions svc-enabled
 svc address-pool "ACPool" netmask 255.255.255.0
 svc dns-server primary 192.168.0.100
 svc default-domain cisco.com
 default-group-policy SSL_Policy
```



Refer to the exhibit. Cisco AnyConnect must be set up on a router to allow users to access internal servers 192.168.0.10 and 192.168.0.11. All other traffic should go out of the client's local NIC. Which command accomplishes this configuration?

- A. **svc split include 192.168.0.0 255.255.255.0**
- B. **svc split exclude 192.168.0.0 255.255.255.0**
- C. **svc split include acl CCNP**
- D. **svc split exclude acl CCNP**

Correct Answer: C

Section: Secure Communications Architectures

Explanation

Explanation/Reference: