Free Questions for 300-730 by ebraindumps

Shared by Macias on 29-01-2024

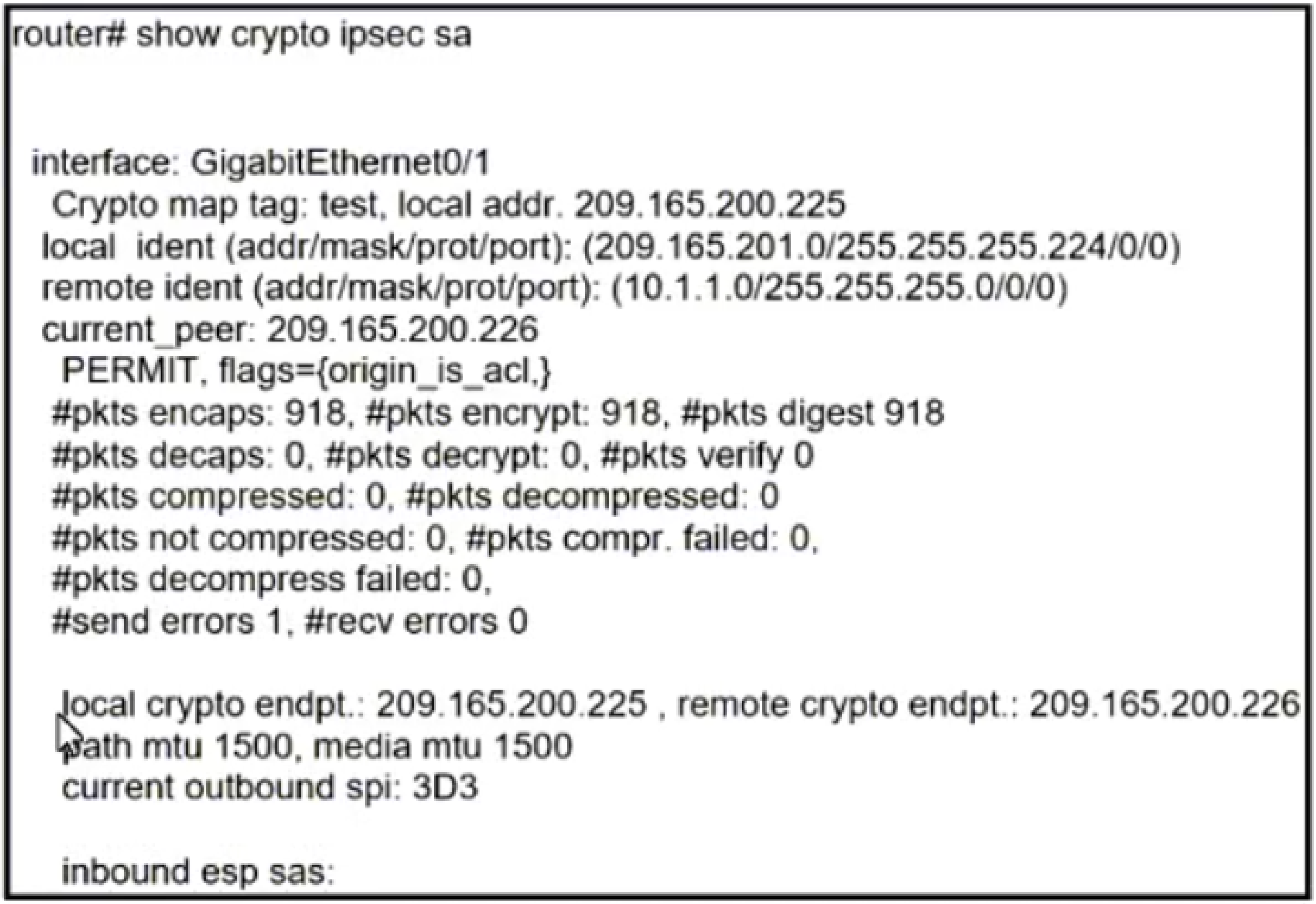
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A TCP based application that should be accessible over the VPN tunnel is not working. Pings to the appropriate IP address are failing.



```
router# show crypto ipsec sa


 interface: GigabitEthernet0/1
   Crypto map tag: test, local addr. 209.165.200.225
  local  ident (addr/mask/prot/port): (209.165.201.0/255.255.255.224/0/0)
  remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 209.165.200.226
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 918, #pkts encrypt: 918, #pkts digest 918
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0,
   #pkts decompress failed: 0,
   #send errors 1, #recv errors 0

    local crypto endpt.: 209.165.200.225 , remote crypto endpt.: 209.165.200.226
    path mtu 1500, media mtu 1500
    current outbound spi: 3D3

    inbound esp sas:
```

Based on the output, what is a fix for this issue?

Options:

A- Add a route on the remote peer for 209.165.201.0/27.

B- Add a route on the local peer for 10.1.1.0/24.

C- Add a permit for TCP traffic going to 10.1.1.0/24.

D- Add a permit for TCP traffic going to 209.165.201.0/27.

Answer:

A

Question 2

Question Type: MultipleChoice

The corporate network security policy requires that all internet and network traffic must be tunneled to the corporate office. Remote workers have been provided with printers to use locally at home while they are remotely connected to the corporate network. Which two steps must be executed to allow printing to the local printers? (Choose two.)

Options:

A- Configure the split-tunnel-policy on the Cisco ASA to tunnelall.

B- Check the Allow Local LAN access checkbox in the Cisco AnyConnect client.

C- Add a persistent static route in the client OS for the local LAN network.

D- Configure the split-tunnel-policy on the Cisco ASA to excludespecified.

E- Configure the split-tunnel-policy on the Cisco ASA to tunnelspecified.

Answer:

B, D

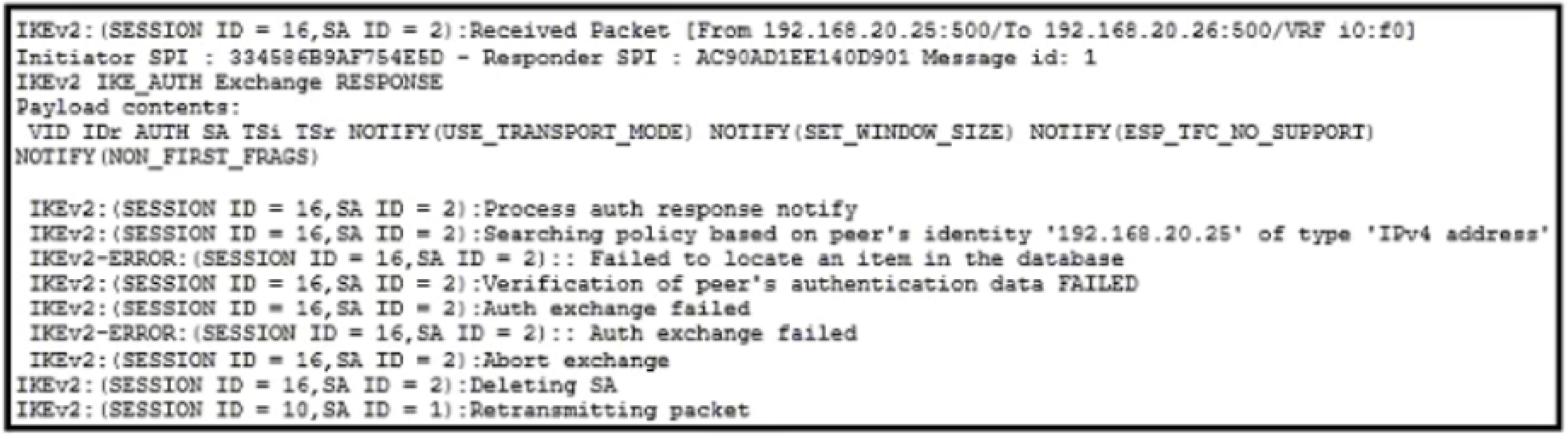
Explanation:

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



```
IKEv2:(SESSION ID = 16,SA ID = 2):Received Packet [From 192.168.20.25:500/To 192.168.20.26:500/VRF i0:f0]
Initiator SPI : 334586B9AF754E5D - Responder SPI : AC90AD1EE140D901 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr AUTH SA TSi TSr NOTIFY(USE_TRANSPORT_MODE) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

 IKEv2:(SESSION ID = 16,SA ID = 2):Process auth response notify
 IKEv2:(SESSION ID = 16,SA ID = 2):Searching policy based on peer's identity '192.168.20.25' of type 'IPv4 address'
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Failed to locate an item in the database
 IKEv2:(SESSION ID = 16,SA ID = 2):Verification of peer's authentication data FAILED
 IKEv2:(SESSION ID = 16,SA ID = 2):Auth exchange failed
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Auth exchange failed
 IKEv2:(SESSION ID = 16,SA ID = 2):Abort exchange
IKEv2:(SESSION ID = 16,SA ID = 2):Deleting SA
IKEv2:(SESSION ID = 10,SA ID = 1):Retransmitting packet
```

An engineer is diagnosing an issue that occurred after a router at a branch site was assigned a new address. Based on the debugs, what must be done to resolve this issue?

Options:

A- Add the remote peer's IP address to the server's IKEv2 keyring.

B- Ensure that the correct preshared keys are set on both sides.

C- Ensure that the UDP 500 packets between devices are not dropped.

D- Add the remote peer's identity to the server's IKEv2 profile.

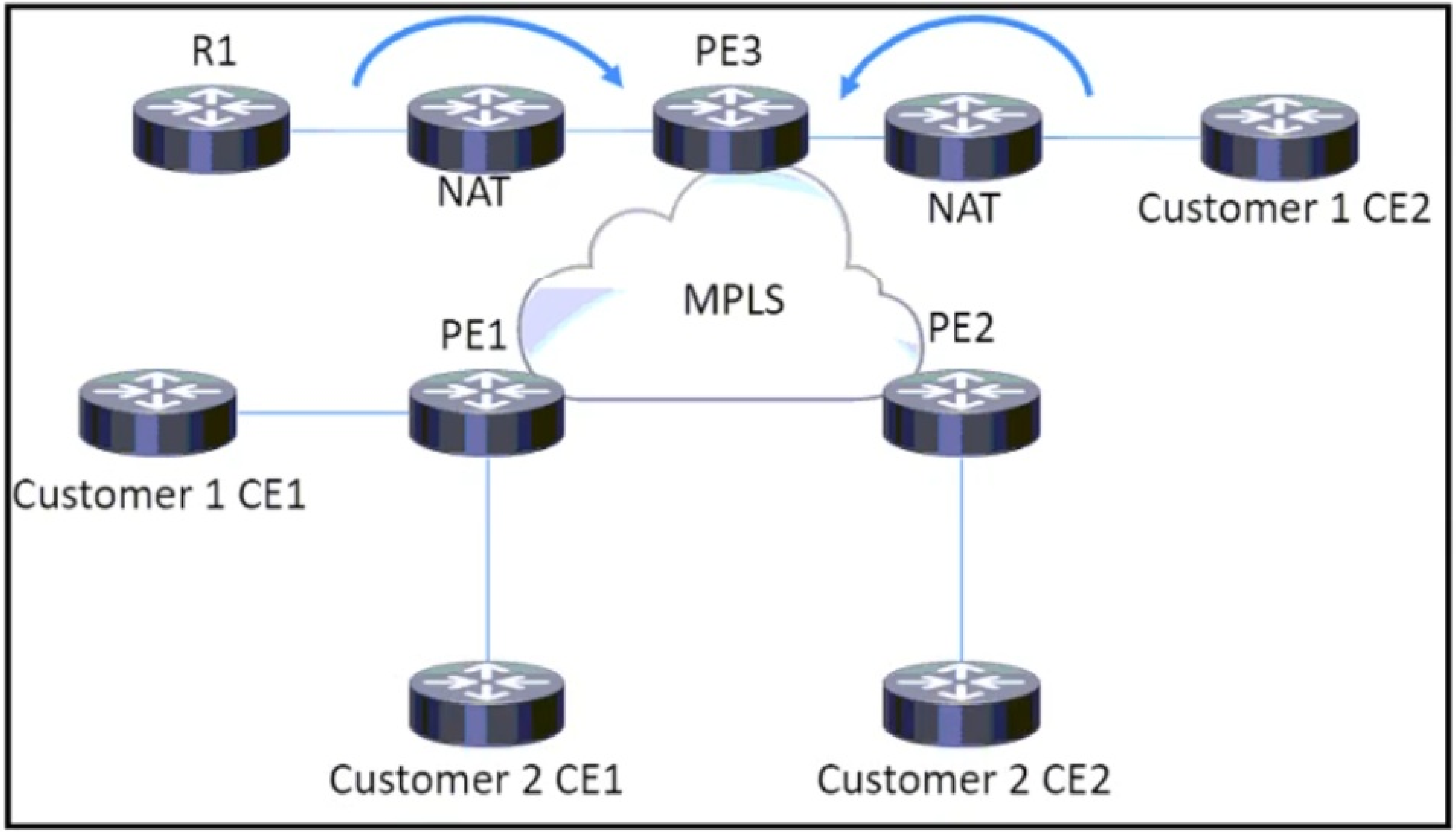
Answer:

D

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



Which component must be configured on routers for a GETVPN deployment work properly?

Options:

A- PE3: Key Server -- Customer 2 CEs: Group Members

B- Customer 1 CE1: Key Server -- R1 and Customer 1 CE2: Group Members

C- R1: Key Server -- Customer 1 CEs: Group Members

D- PE3: Key Server -- all CEs: Group Members

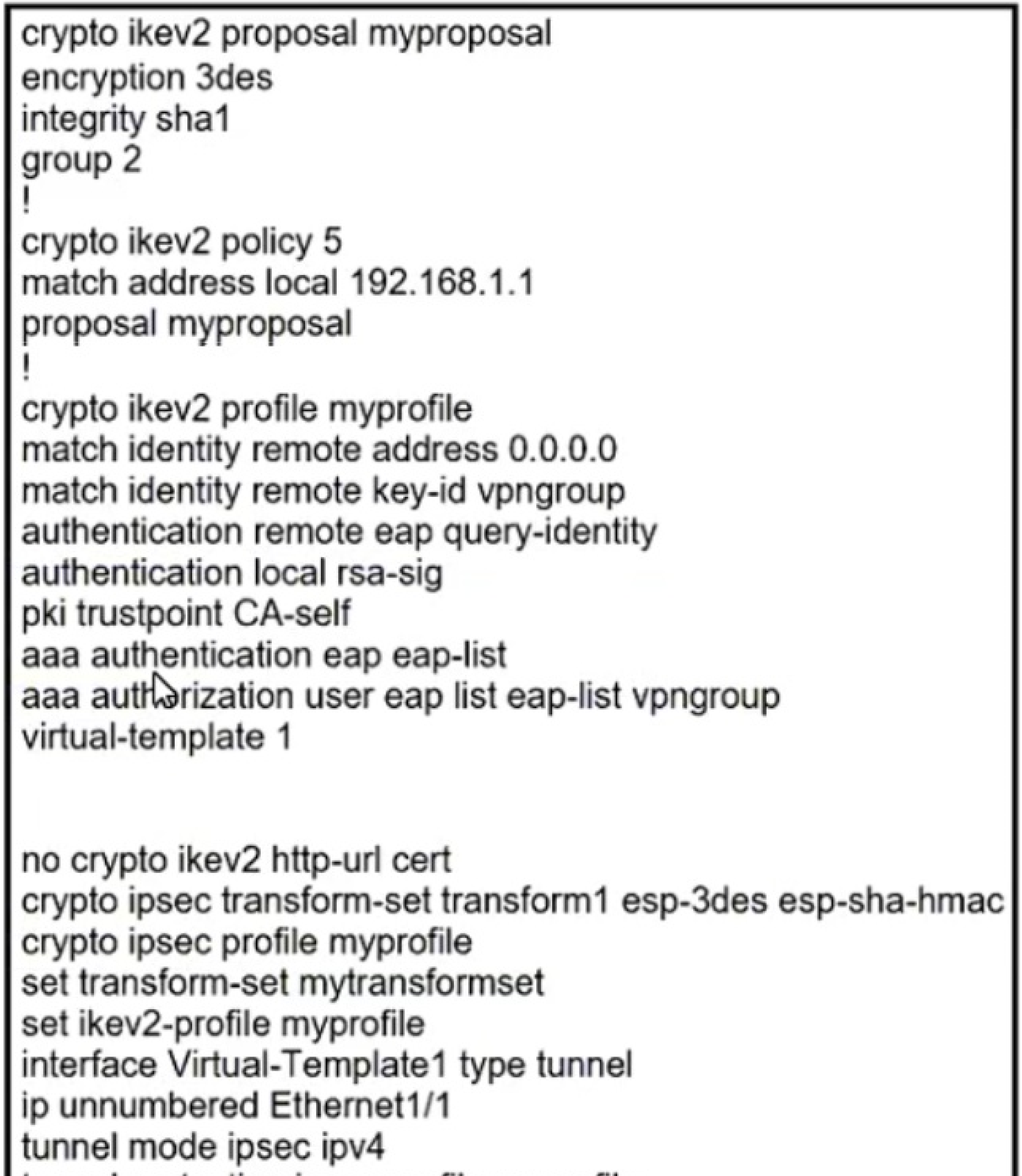
Answer:

A

Question 5

Question Type: **MultipleChoice**

Refer to the exhibit.



```
crypto ikev2 proposal myproposal
encryption 3des
integrity sha1
group 2
!
crypto ikev2 policy 5
match address local 192.168.1.1
proposal myproposal
!
crypto ikev2 profile myprofile
match identity remote address 0.0.0.0
match identity remote key-id vpngroup
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint CA-self
aaa authentication eap eap-list
aaa authorization user eap list eap-list vpngroup
virtual-template 1


no crypto ikev2 http-url cert
crypto ipsec transform-set transform1 esp-3des esp-sha-hmac
crypto ipsec profile myprofile
set transform-set mytransformset
set ikev2-profile myprofile
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet1/1
tunnel mode ipsec ipv4
```

Based on the output of the show run command, which remote access VPN technology is configured?

Options:

A- PPTP

B- SSLVPN Full Tunnel

C- FlexVPN

D- clientless SSLVPN

Answer:

C

Question 6

Question Type: **MultipleChoice**

What are two differences between ECC and RSA? (Choose two.)

Options:

A- Key generation in ECC is slower and more CPU intensive than RSA.

B- ECC can have the same security as RSA but with a shorter key size.

C- ECC cannot have the same security as RSA, even with an increased key size.

D- Key generation in ECC is faster and less CPU intensive than RSA.

E- ECC lags in performance when compared with RSA.

Answer:

B, D

Question 7

Question Type: MultipleChoice

Which VPN technology minimizes the impact on VPN performance when encrypting multicast traffic on a Private WAN?

Options:

A- DMVPN

B- IPsec VPN

C- FlexVPN

D- GETVPN

Answer:

D

Question 8

Question Type: **MultipleChoice**

A network engineer is implementing a FlexVPN tunnel between two Cisco IOS routers. The FlexVPN tunnels will terminate on encrypted traffic on an interface configured with an IP MTU of 1500, and the company has a security policy to drop fragmented traffic coming into or leaving the network. The tunnel will be used to transfer TFTP data between users and internal servers. When the TFTP traffic is not traversing a VPN, it can have a maximum IP packet size of 1500. Assuming the encrypted payload will add 90 bytes, which configuration allows TFTP traffic to traverse the FlexVPN tunnel without being dropped?

Options:

A- Set the tunnel IP MTU to 1500.

B- Set the tunnel tcp adjust-mss to 1460.

C- Set the tunnel IP MTU to 1400.

D- Set the tunnel tcp adjust-mss to 1360.

Answer:

C

Explanation:

https://www.networkworld.com/article/2224654/mtu-size-issues.html