300-730$^{\text{Q\&As}}$

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

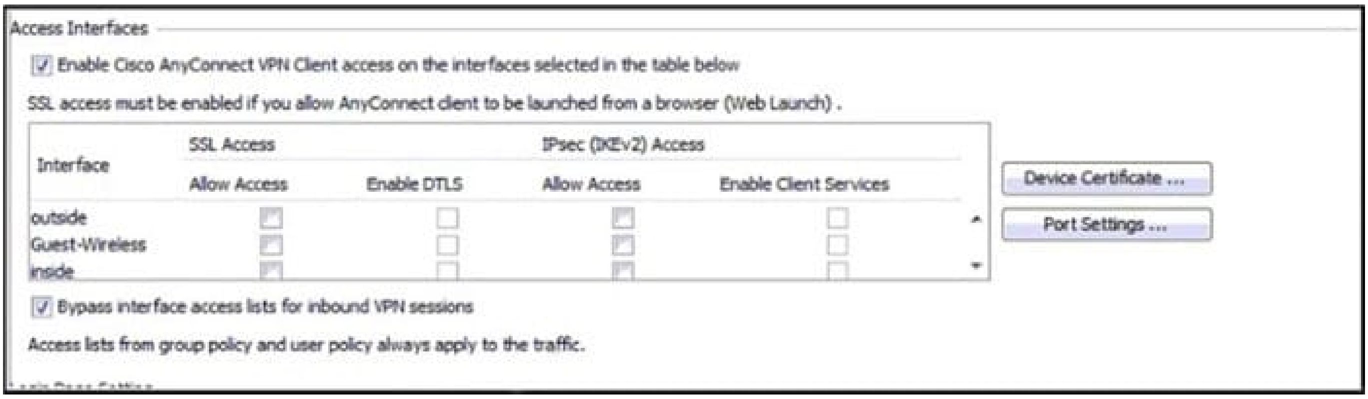
https://www.passapply.com/300-730.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.



Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	□	□	□	□
Guest-Wireless	□	□	□	□
inside	□	□	□	□

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

An engineer must allow Cisco AnyConnect users to access the outside interface using protocol UDP 500/4500. In addition, these clients must be able to establish an SSL connection to update Cisco AnyConnect software over the same connection. Which two actions must be taken to achieve this goal? (Choose two.)

A. IPsec (IKEv2) Allow Access must be checked on the outside interface.

B. SSL Enable DTLS must be checked on the outside interface.

C. Bypass interface access lists for inbound VPN sessions must be unchecked.

D. IPsec (IKEv2) Enable Client Services must be checked on the outside interface.

E. SSL Allow Access must be checked on the outside interface.

Correct Answer: AD

QUESTION 2

A network engineer has been tasked with configuring SSL VPN to provide remote users with access to the corporate network. Traffic destined to the enterprise IP range should go through the tunnel, and all other traffic should go directly to the Internet. Which feature should be configured to achieve this?

A. U-turning

B. hairpinning

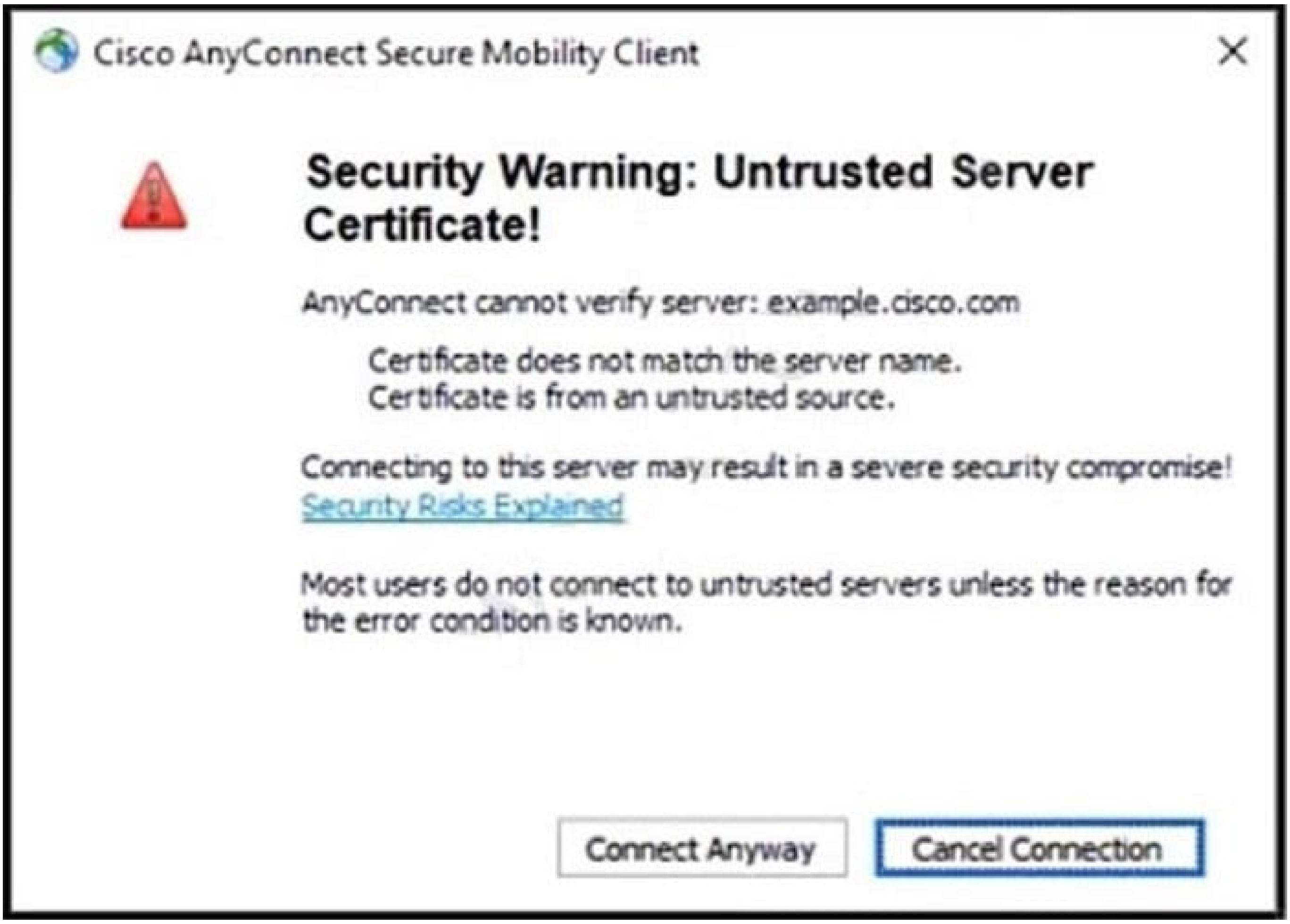
C. split-tunnel

D. dual-homing

Correct Answer: C

QUESTION 3

Refer to the exhibit.



Cisco AnyConnect Secure Mobility Client

Security Warning: Untrusted Server Certificate!

AnyConnect cannot verify server: example.cisco.com

Certificate does not match the server name.
Certificate is from an untrusted source.

Connecting to this server may result in a severe security compromise!
Security Risks Explained

Most users do not connect to untrusted servers unless the reason for the error condition is known.

A network administrator is setting up Cisco AnyConnect on an ASA headend. When users attempt to connect to the VPN, they are presented with this message. The administrator has replaced the ASA\\'s self-signed certificate with a certificate enrolled with the internal CA and has confirmed that the certificate is not revoked. Which two tasks will the administrator need to do to prevent users from seeing this message? (Choose two.)

A. Trust the issuing CA for the ASA identity certificate on the user\\'s PC.

B. Enroll and import an SSL certificate with the CN value example.cisco.com on the ASA.

C. Add the CN example.cisco.com to the AnyConnect XML certificate matching section.

D. Enable certificate authentication under the connection profile.

E. Add example.cisco.com to the server name list within the AnyConnect Local Policy.

Correct Answer: AB

QUESTION 4

After a user configures a connection profile with a bookmark list and tests the clientless SSLVPN connection, all of the bookmarks are grayed out. What must be done to correct this behavior?

A. Apply the bookmark to the correct group policy.

B. Specify the correct port for the web server under the bookmark.

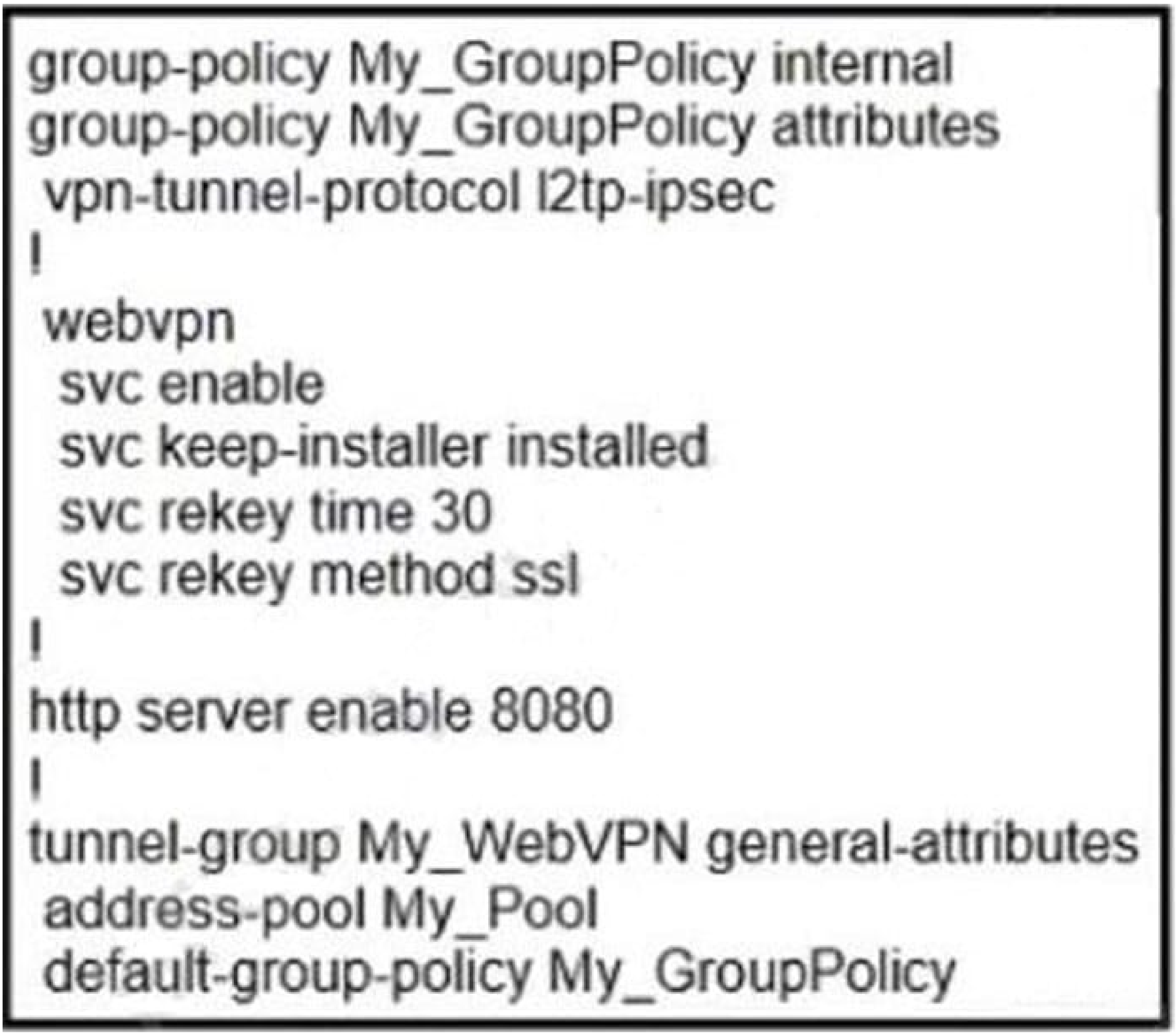
C. Configure a DNS server on the Cisco ASA and verify it has a record for the web server.

D. Verify HTTP/HTTPS connectivity between the Cisco ASA and the web server.

Correct Answer: C

QUESTION 5

Refer to the exhibit.



```
group-policy My_GroupPolicy internal
group-policy My_GroupPolicy attributes
 vpn-tunnel-protocol l2tp-ipsec
!
 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
http server enable 8080
!
tunnel-group My_WebVPN general-attributes
 address-pool My_Pool
 default-group-policy My_GroupPolicy
```

Users cannot connect via AnyConnect SSLVPN. Which action resolves this issue?

A. Configure the ASA to act as a DHCP server.

B. Configure the HTTP server to listen on port 443.

C. Add an IPsec preshared key to the group policy.

D. Add ssl-client to the allowed list of VPN protocols.

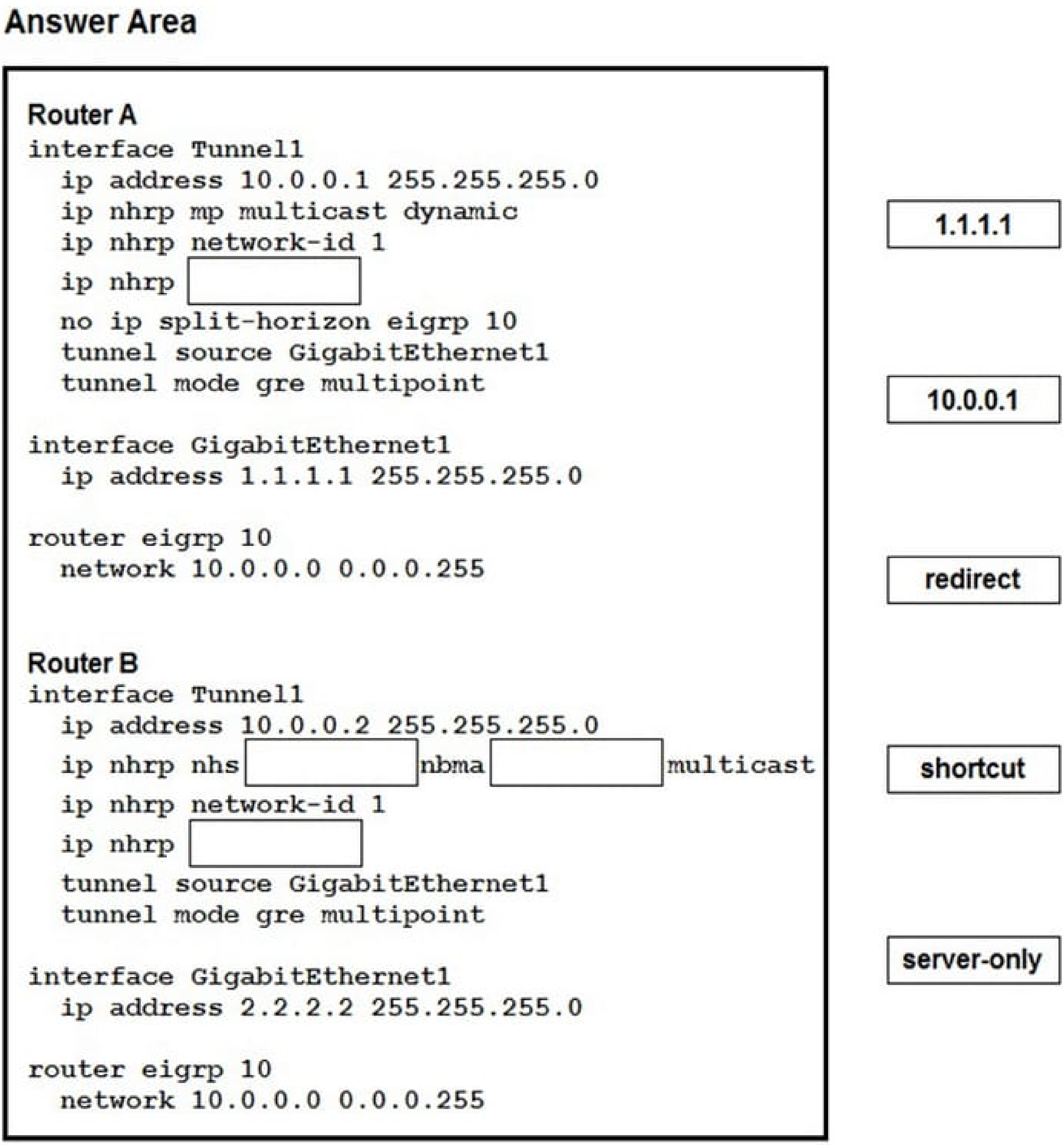
Correct Answer: D

QUESTION 6

DRAG DROP

Drag and drop the correct commands from the night 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 Tunnel1
  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 Tunnel1
  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

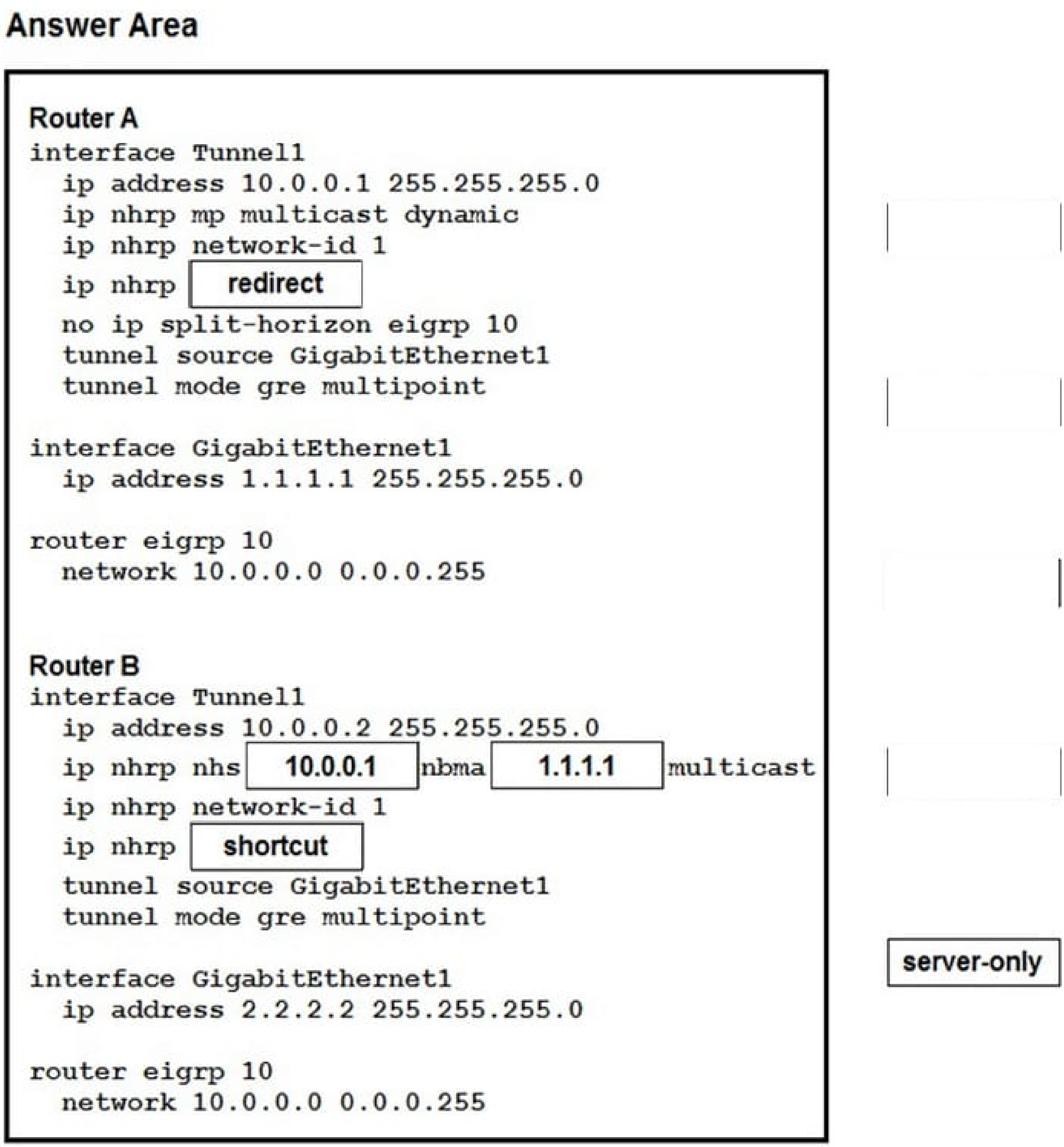
10.0.0.1

redirect

shortcut

server-only

Correct Answer:



Answer Area

Router A

```
interface Tunnel1
  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
```

Router B

```
interface Tunnel1
  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
```

server-only

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

QUESTION 7

In order to enable FlexVPN to use a AAA attribute list, which two tasks must be performed? (Choose two.)

A. Define the RADIUS server.

B. Verify that clients are using the correct authorization policy.

C. Define the AAA server.

D. Assign the list to an authorization policy.

E. Set the maximum segment size.

Correct Answer: BD

QUESTION 8

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

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

QUESTION 9

Which VPN does VPN load balancing on the ASA support?

A. VTI

B. IPsec site-to-site tunnels

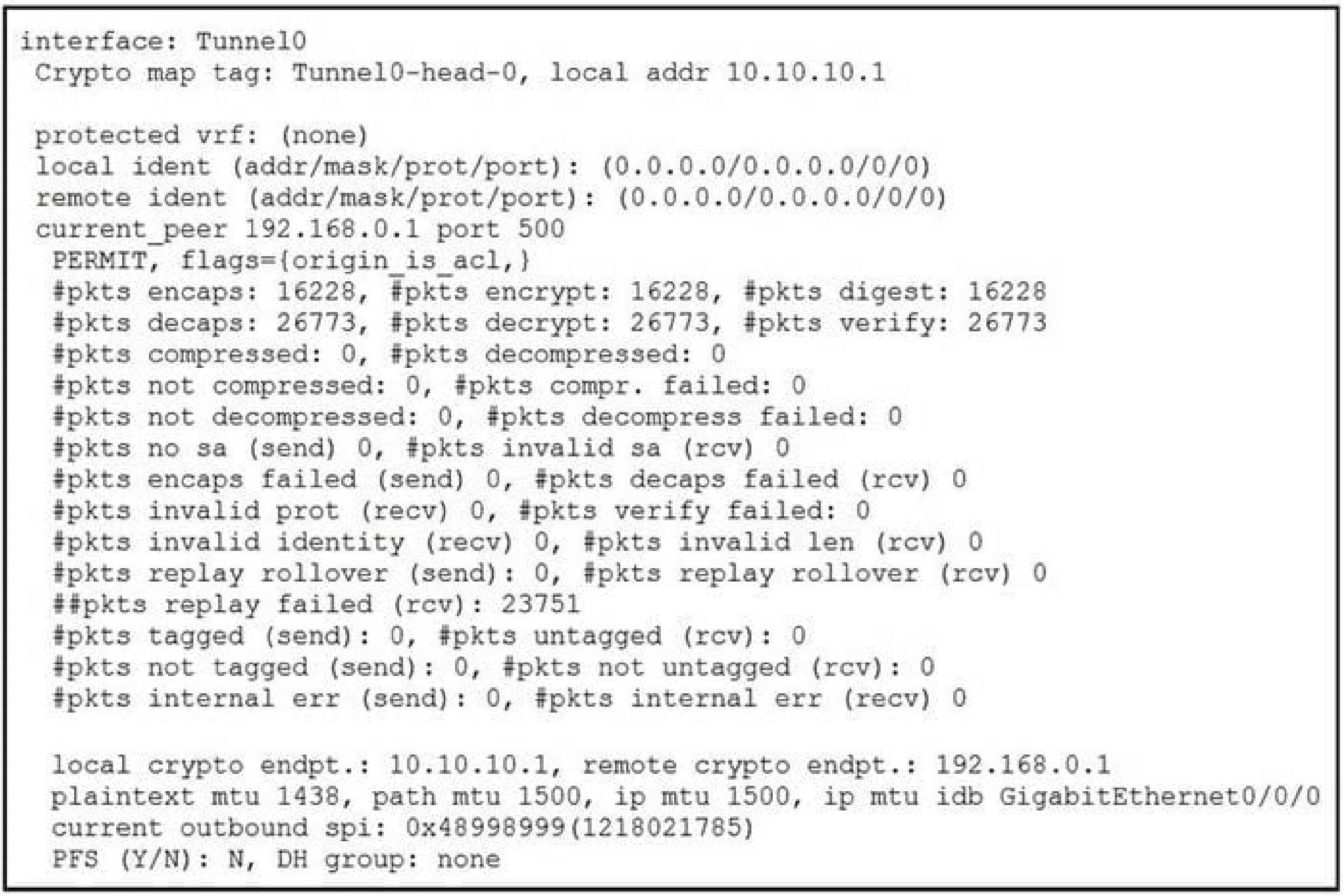
C. L2TP over IPsec

D. Cisco AnyConnect

Correct Answer: D

QUESTION 10

Refer to the exhibit.



```
interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

 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 192.168.0.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 16228, #pkts encrypt: 16228, #pkts digest: 16228
  #pkts decaps: 26773, #pkts decrypt: 26773, #pkts verify: 26773
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
  #pkts invalid prot (recv) 0, #pkts verify failed: 0
  #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
  ##pkts replay failed (rcv): 23751
  #pkts tagged (send): 0, #pkts untagged (rcv): 0
  #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (recv) 0

  local crypto endpt.: 10.10.10.1, remote crypto endpt.: 192.168.0.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
  current outbound spi: 0x48998999(1218021785)
  PFS (Y/N): N, DH group: none
```

Upon setting up a tunnel between two sites, users are complaining that connections to applications over the VPN are not working consistently. The output of show crypto ipsec sa was collected on one of the VPN devices. Based on this output, what should be done to fix this issue?

A. Lower the tunnel MTU.

B. Enable perfect forward secrecy.

C. Specify the application networks in the remote identity.

D. Make an adjustment to IPSec replay window.

Correct Answer: D

QUESTION 11

A network administrator wants the Cisco ASA to automatically start downloading the Cisco AnyConnect client without prompting the user to select between WebVPN or AnyConnect. Which command accomplishes this task?

A. anyconnect ssl df-bit-ignore enable

B. anyconnect ask none default anyconnect

C. anyconnect ask enable default anyconnect

D. anyconnect modules value default

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/vpn-anyconnect.html

QUESTION 12

An engineer is requesting an SSL certificate for a VPN load-balancing cluster in which two Cisco ASAs provide clientless SSLVPN access. The FQDN that users will enter to access the clientless VPN is asa.example.com, and users will be redirected to either asa1.example.com or asa2.example.com. The cluster FQDN and individual Cisco ASAs FQDNs resolve to IP addresses 192.168.0.1, 192.168.0.2, and 192.168.0.3 respectively. The issued certificate must be able to be used to validate the identity of either ASA in the cluster without returning any certificate validation errors. Which fields must be included in the certificate to meet these requirements?

A. CN=*.example.com, SAN=asa.example.com

B. CN=192.168.0.1, SAN=asa1.example.com, asa2.example.com

C. CN=asa.example.com, SAN=asa.example.com, asa1.example.com, asa2.example.com

D. CN=192.168.0.1, SAN=192.168.0.1, 192.168.0.2, 192.168.0.3

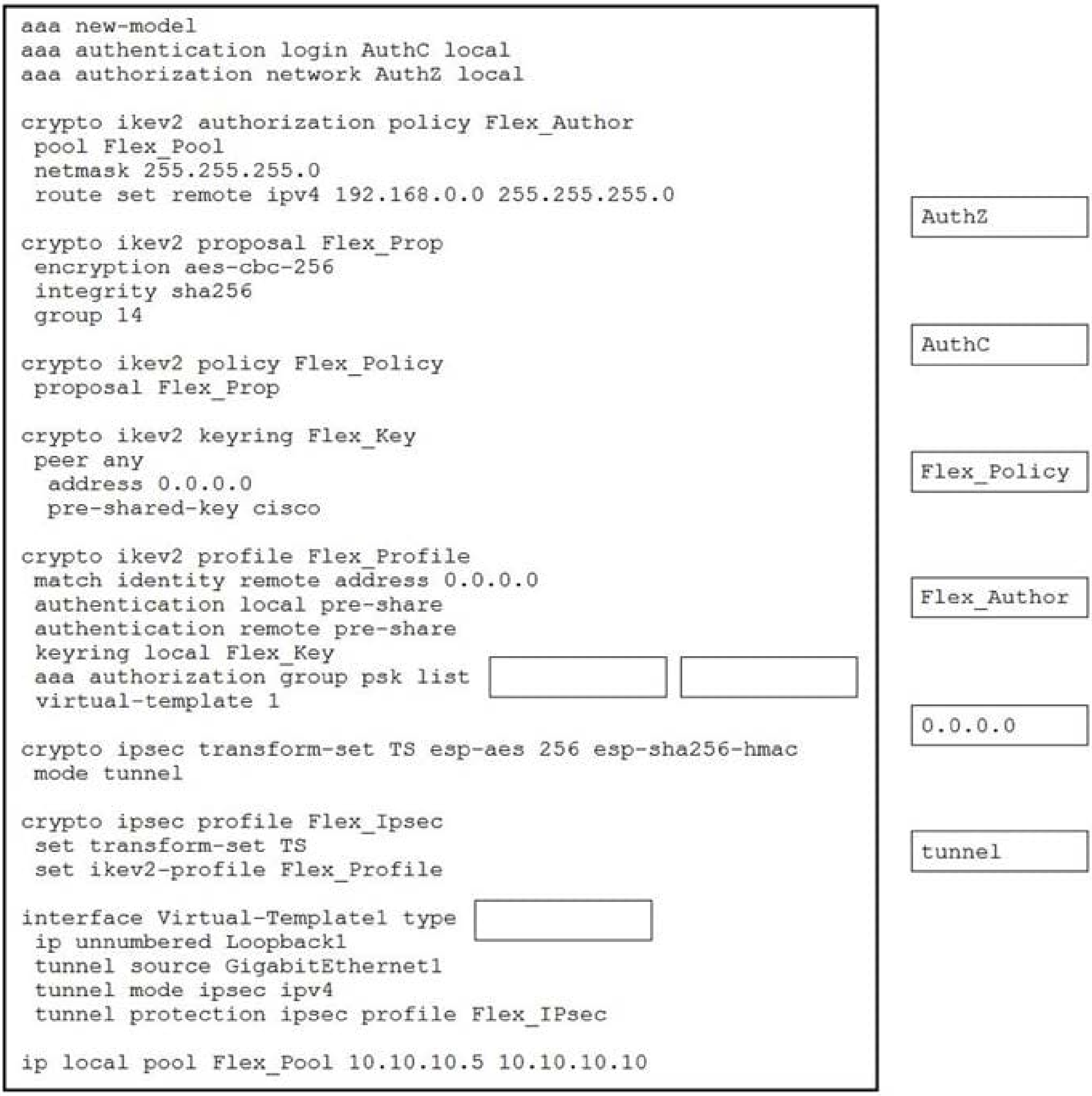
Correct Answer: C

QUESTION 13

DRAG DROP

Drag and drop the code snippets from the right onto the blanks in the configuration to implement FlexVPN. Not all snippets are used.

Select and Place:



```
aaa new-model
aaa authentication login AuthC local
aaa authorization network AuthZ local

crypto ikev2 authorization policy Flex_Author
 pool Flex_Pool
 netmask 255.255.255.0
 route set remote ipv4 192.168.0.0 255.255.255.0

crypto ikev2 proposal Flex_Prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Flex_Policy
 proposal Flex_Prop

crypto ikev2 keyring Flex_Key
 peer any
  address 0.0.0.0
  pre-shared-key cisco

crypto ikev2 profile Flex_Profile
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local Flex_Key
 aaa authorization group psk list
 virtual-template 1

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile Flex_Ipsec
 set transform-set TS
 set ikev2-profile Flex_Profile

interface Virtual-Template1 type
 ip unnumbered Loopback1
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flex_IPsec

ip local pool Flex_Pool 10.10.10.5 10.10.10.10
```

AuthZ

AuthC

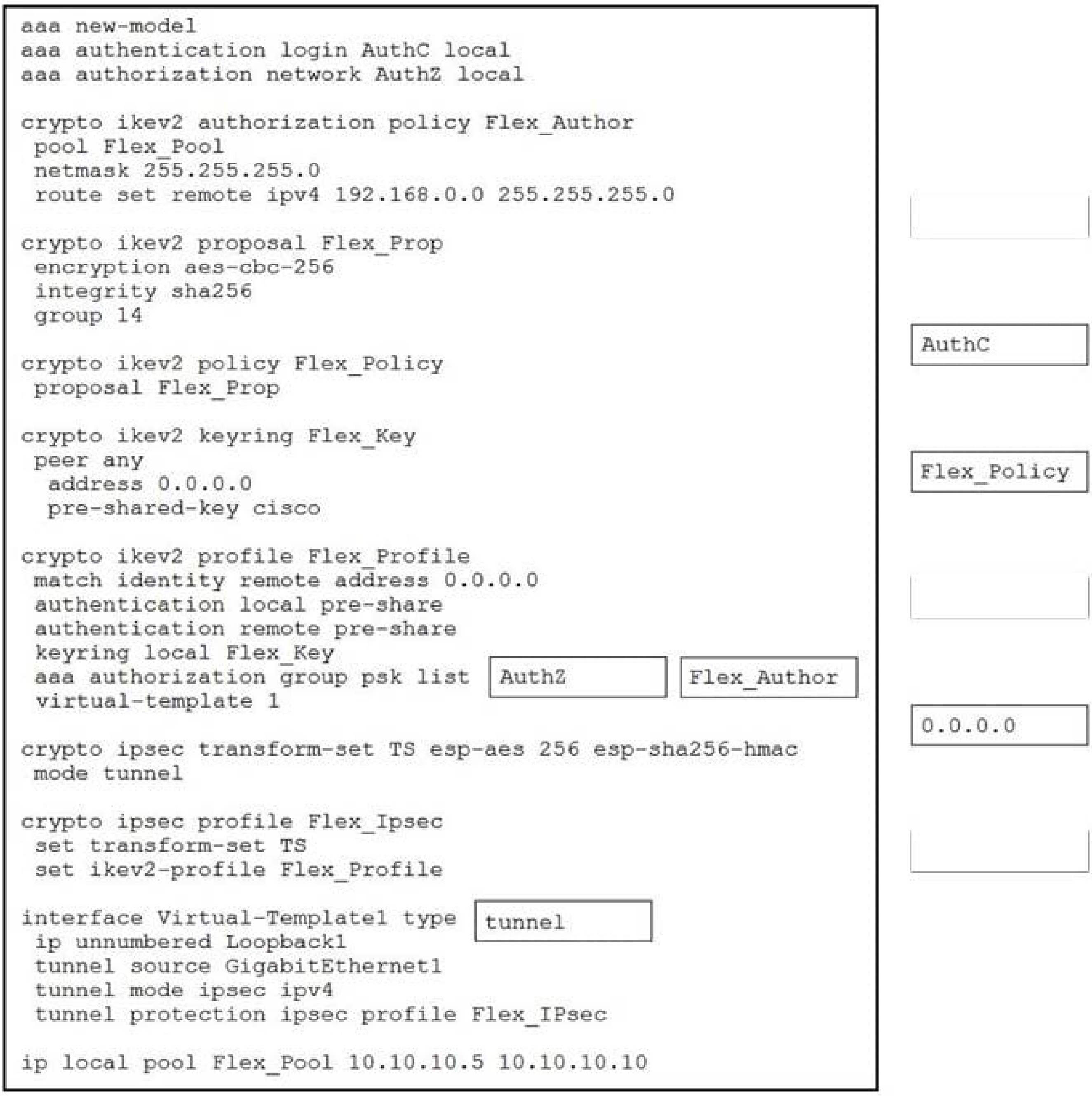
Flex_Policy

Flex_Author

0.0.0.0

tunnel

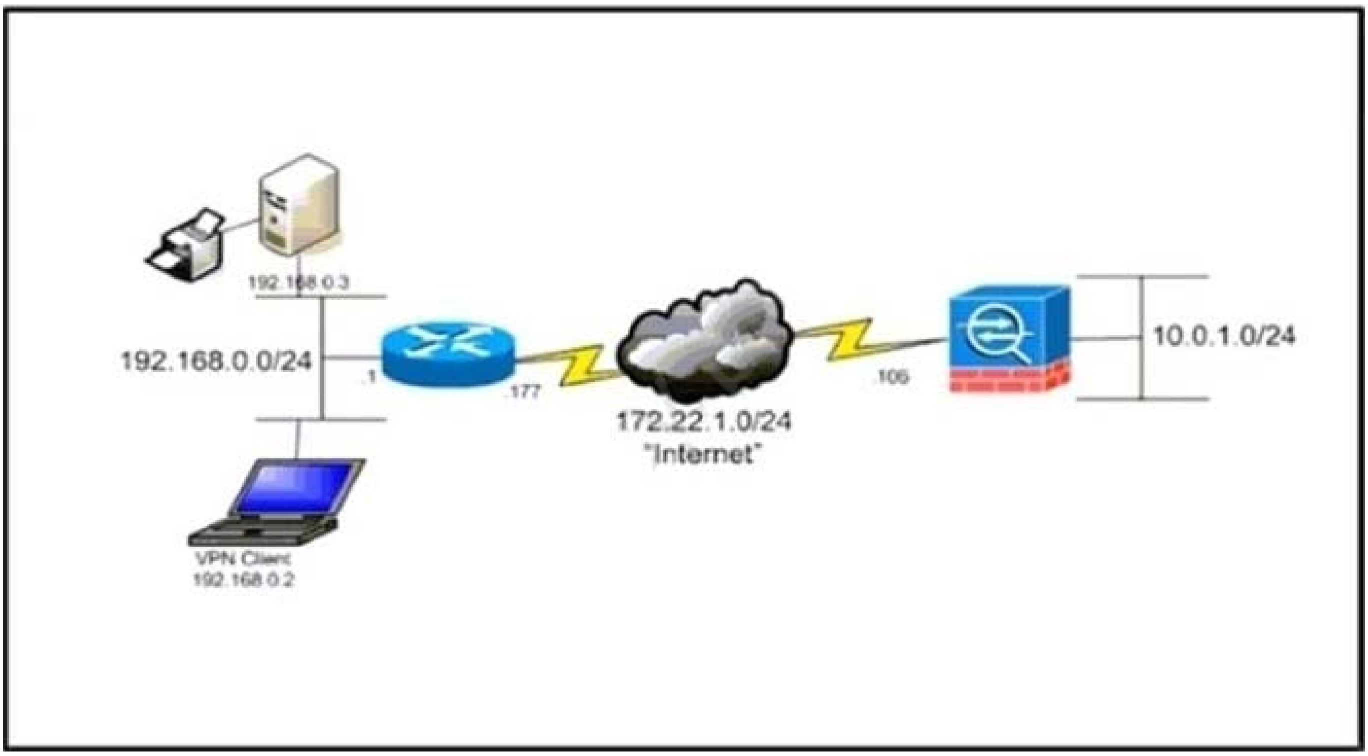
Correct Answer:



```
aaa new-model
aaa authentication login AuthC local
aaa authorization network AuthZ local

crypto ikev2 authorization policy Flex_Author
 pool Flex_Pool
 netmask 255.255.255.0
 route set remote ipv4 192.168.0.0 255.255.255.0

crypto ikev2 proposal Flex_Prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Flex_Policy
 proposal Flex_Prop

crypto ikev2 keyring Flex_Key
 peer any
  address 0.0.0.0
  pre-shared-key cisco

crypto ikev2 profile Flex_Profile
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local Flex_Key
 aaa authorization group psk list  AuthZ  Flex_Author
 virtual-template 1

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile Flex_Ipsec
 set transform-set TS
 set ikev2-profile Flex_Profile

interface Virtual-Template1 type  tunnel
 ip unnumbered Loopback1
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flex_IPsec

ip local pool Flex_Pool 10.10.10.5 10.10.10.10
```

QUESTION 14

Refer to the exhibit.



The network administrator must allow the Cisco AnyConnect Secure Mobility Client to securely access the corporate resources via IKEv2 and print locally. Traffic that is destined for the Internet must still be tunneled to the Cisco ASA. Which configuration does the administrator use to accomplish this goal?

A. Split exclude policy with a deny for 192.168.0.3/32.

B. Split exclude policy with a permit for 0.0.0.0/32.

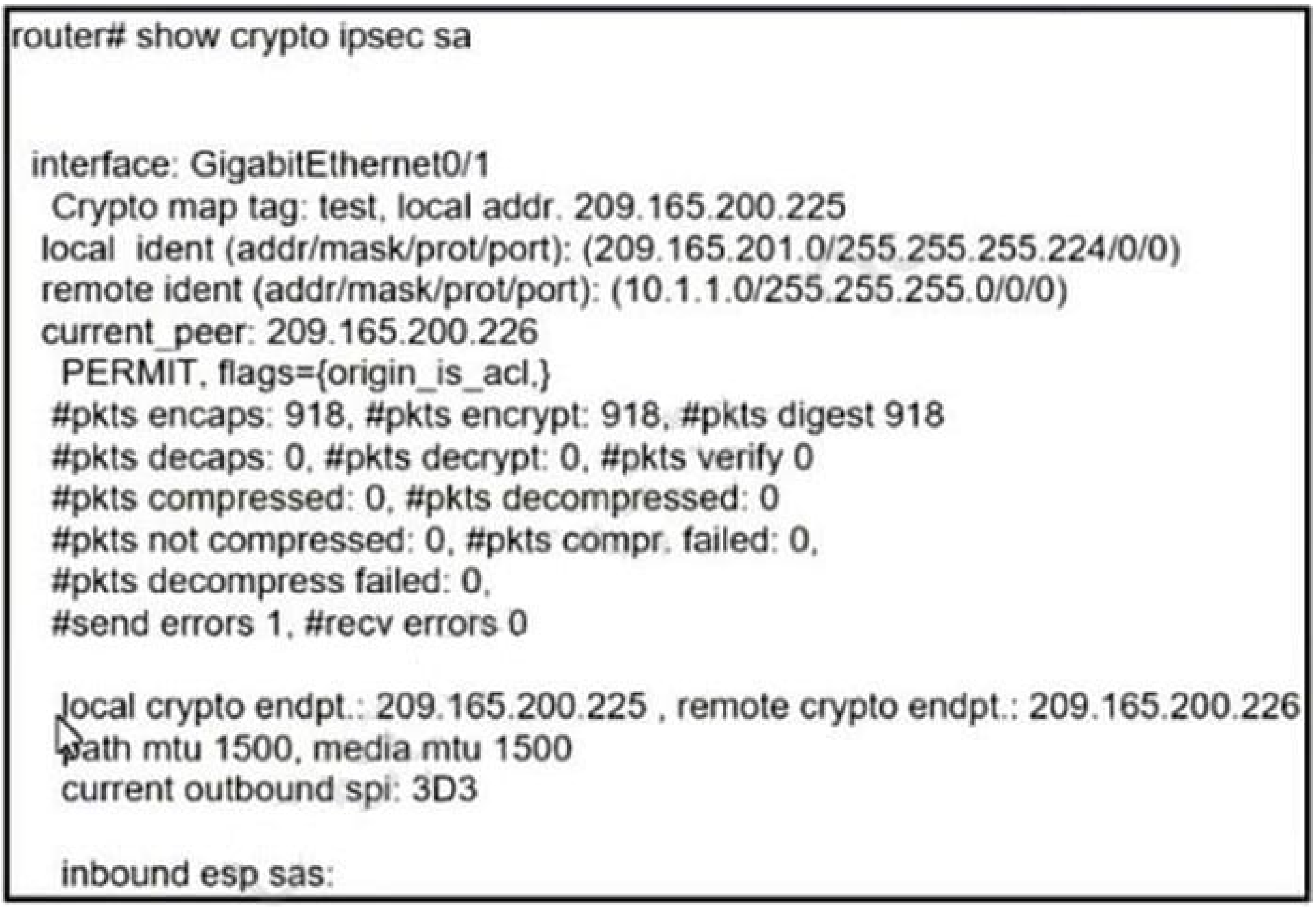
C. Tunnel all policy.

D. Split include policy with a permit for 192.168.0.0/24.

Correct Answer: B

QUESTION 15

Refer to the exhibit.



```
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:
```

A TCP based application that should be accessible over the VPN tunnel is not working. Pings to the appropriate IP address are failing. Based on the output, what is a fix for this issue?

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.

Correct Answer: A