- **Vendor:** Cisco
- **Exam Code:** 300-730
- **Exam Name:** Implementing Secure Solutions with Virtual Private Networks (SVPN)
- **New Updated Questions from Braindump2go (Updated in June/2021)**

QUESTION 76
An engineer is configuring clientless SSL VPN. The finance department has a database server that only they should access, but the sales department can currently access it. The finance and the sales departments are configured as separate group-policies. What must be added to the configuration to make sure the users in the sales department cannot access the finance department server?

A. tunnel group lock
B. smart tunnel
C. port forwarding
D. webtype ACL

Answer: A

QUESTION 77
An engineer has integrated a new DMVPN to link remote offices across the internet using Cisco IOS routers. When connecting to remote sites, pings and voice data appear to flow properly, and all tunnel stats show that they are up. However, when trying to connect to a remote server using RDP, the connection fails. Which action resolves this issue?

A. Adjust the MTU size within the routers.
B. Add RDP port to the extended ACL.
C. Replace certificate on the RDP server.
D. Change DMVPN timeout values.

Answer: A

QUESTION 78
Where must an engineer configure a preshared key for a site-to-site VPN tunnel configured on a Cisco ASA?

A. isakmp policy
B. group policy
C. crypto map
D. tunnel group

Answer: D

QUESTION 79
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

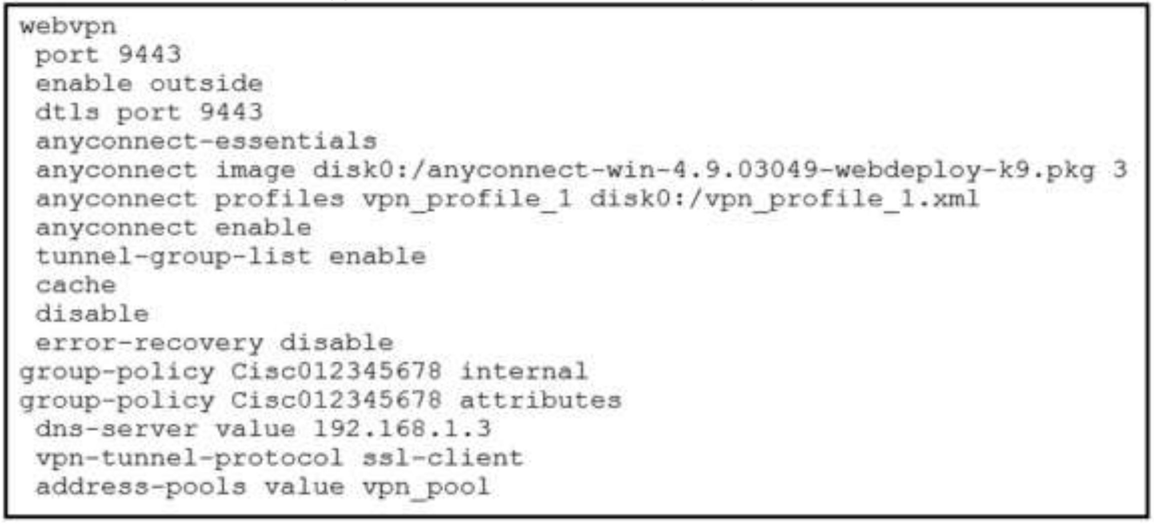
Answer: C

QUESTION 80
A network engineer must design a remote access solution to allow contractors to access internal servers. These contractors do not have permissions to install applications on their computers. Which VPN solution should be used in this design?

A. IKEv2 AnyConnect
B. Clientless
C. Port forwarding
D. SSL AnyConnect

Answer: B

QUESTION 81
Refer to the exhibit. Which type of Cisco VPN is shown for group Cisc012345678?



```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy Cisc012345678 internal
group-policy Cisc012345678 attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

A. Cisco AnyConnect Client VPN
B. DMVPN
C. Clientless SSLVPN
D. GETVPN

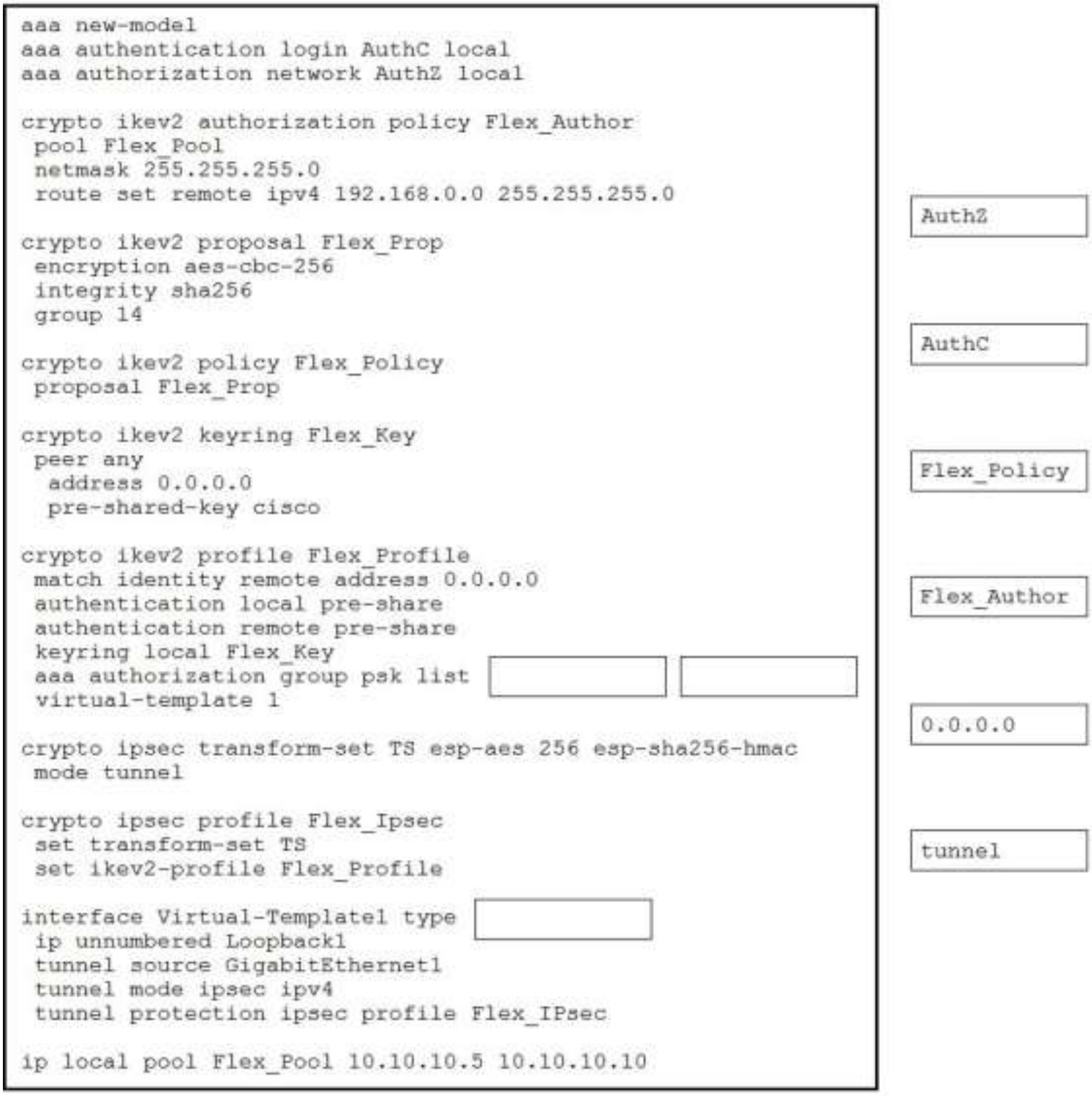
Answer: A

QUESTION 82
Which command shows the smart default configuration for an IPsec profile?

A. show run all crypto ipsec profile
B. ipsec profile does not have any smart default configuration
C. show smart-defaults ipsec profile
D. show crypto ipsec profile default

Answer: D

QUESTION 83
Drag and Drop Question
Drag and drop the code snippets from the right onto the blanks in the configuration to implement FlexVPN. Not all snippets are used.



```
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

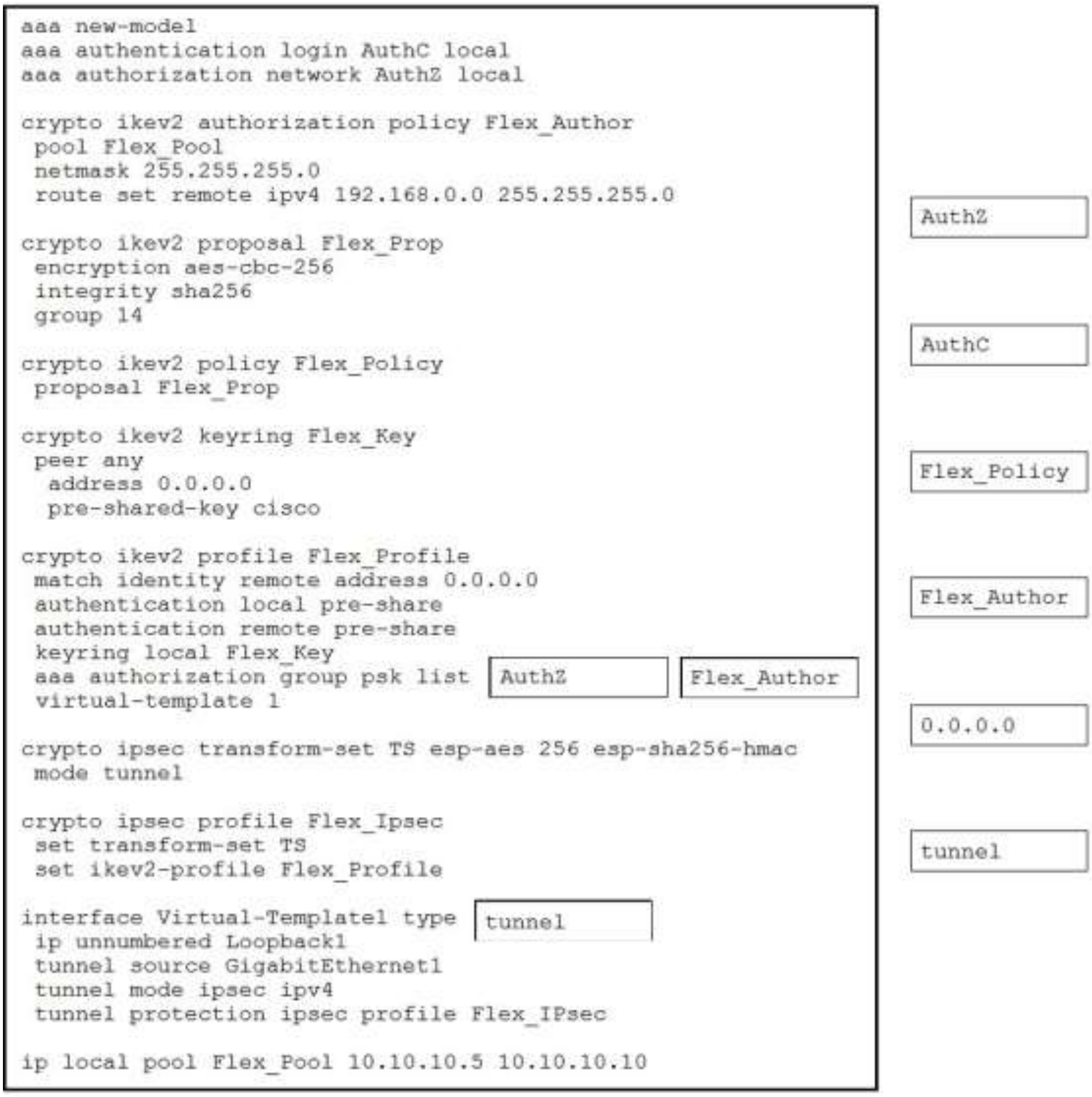
Flex_Policy

Flex_Author

0.0.0.0

tunnel

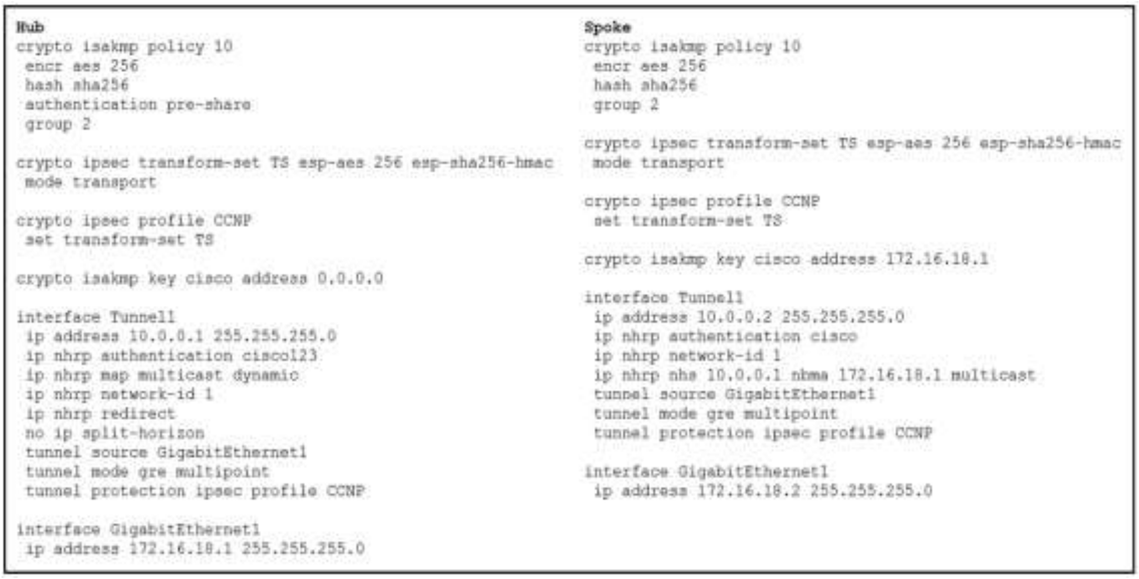
Answer:



```
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 84

Refer to the exhibit. The DMVPN spoke is not establishing a session with the hub. Which two actions resolve this issue? (Choose two.)



```
Hub
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 2

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

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 0.0.0.0

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 no ip split-horizon
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.1 255.255.255.0
```

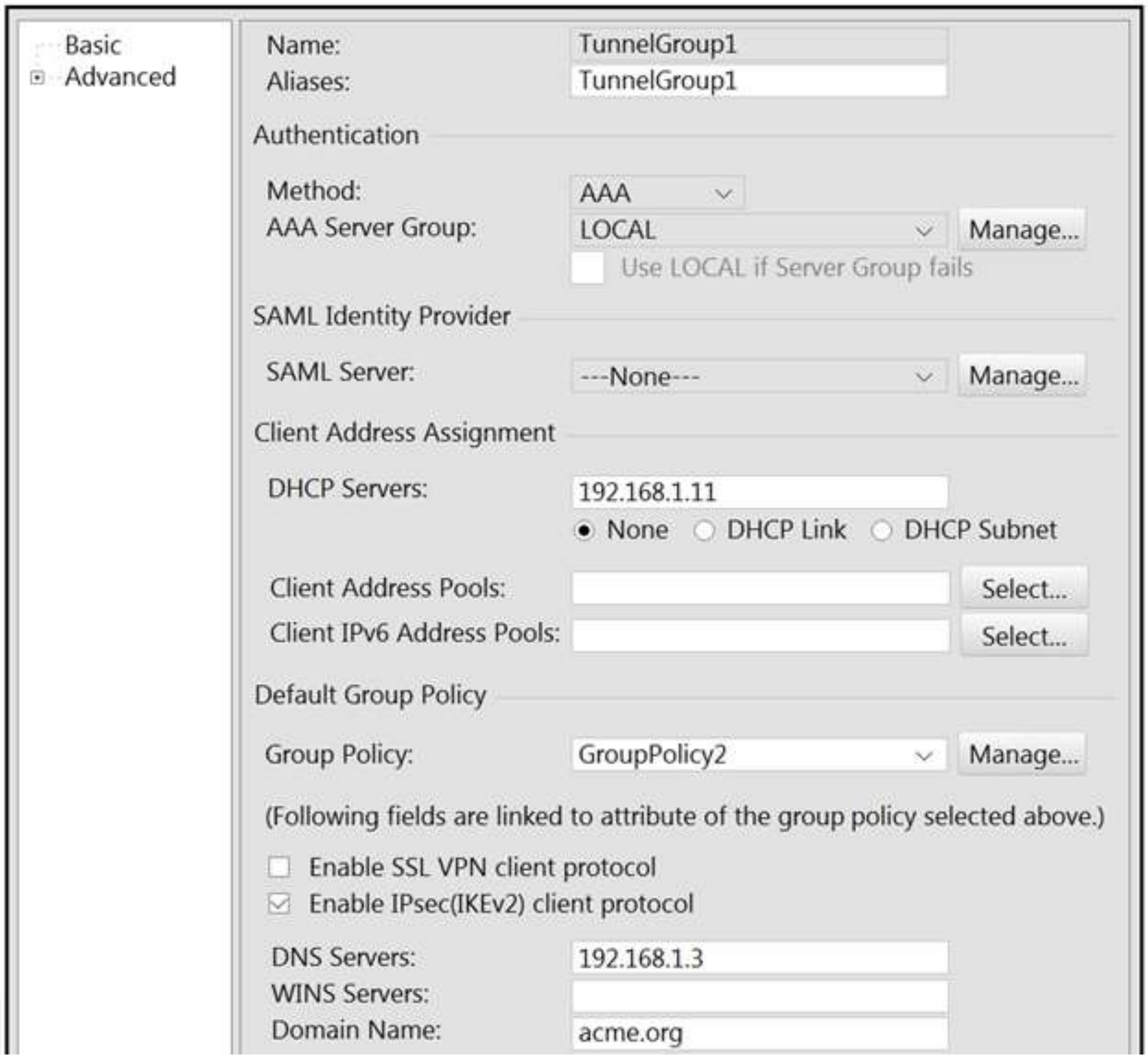
```
Spoke
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 2

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

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 172.16.18.1

interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1 nbma 172.16.18.1 multicast
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.2 255.255.255.0
```

A. Change the spoke nhs to 172.16.18.1 and the nbma to 10.0.0.1.
B. Change the transform set to mode tunnel.
C. Change the ISAKMP policy authentication on the spoke to pre-shared.
D. Change the ISAKMP key address on the spoke to 0.0.0.0.
E. Change the nhrp authentication key on the spoke to cisco123.

Answer: DE

QUESTION 85

Refer to the exhibit. A network engineer is configuring a remote access SSLVPN and is unable to complete the connection using local credentials. What must be done to remediate this problem?



Name: TunnelGroup1

Aliases: TunnelGroup1

Authentication

Method: AAA

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server: ---None---

Client Address Assignment

DHCP Servers: 192.168.1.11

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: GroupPolicy2

(Following fields are linked to attribute of the group policy selected above.)

□ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

DNS Servers: 192.168.1.3

WINS Servers:

Domain Name: acme.org

A. Enable the client protocol in the Cisco AnyConnect profile.
B. Configure a AAA server group to authenticate the client.
C. Change the authentication method to local.
D. Configure the group policy to force local authentication.

Answer: A

QUESTION 86
Which two NHRP functions are specific to DMVPN Phase 3 implementation? (Choose two.)

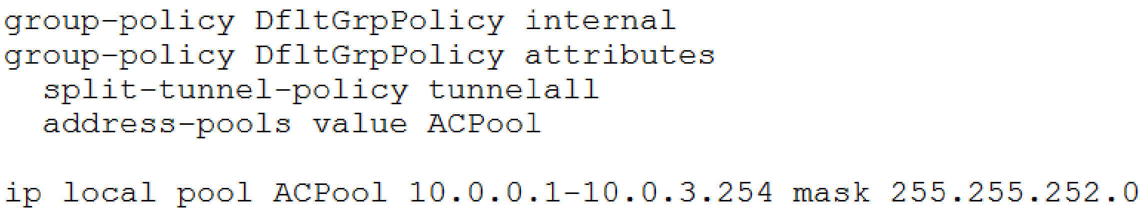
A. registration reply
B. redirect
C. resolution reply
D. registration request
E. resolution request

Answer: BC

QUESTION 87
A network engineer must implement an SSLVPN Cisco AnyConnect solution that supports 500 concurrent users, ensures all traffic from the client passes through the ASA, and allows users to access all devices on the inside interface

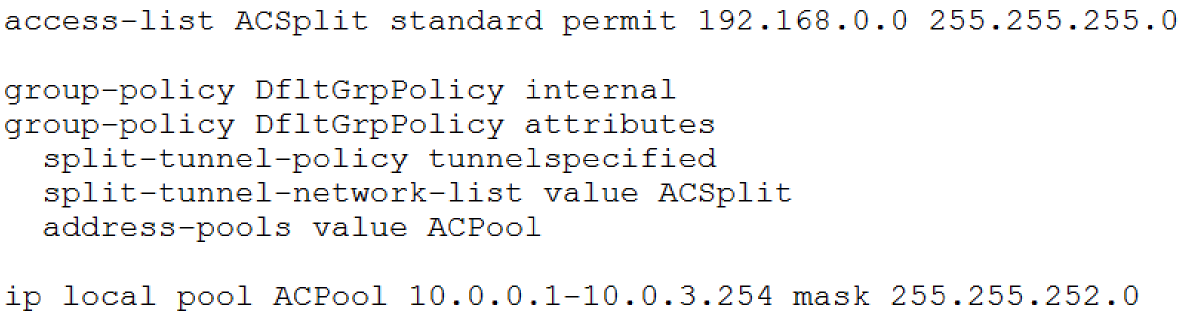
subnet (192.168.0.0/24). Assuming all other configuration is set up appropriately, which configuration implements this solution?

A.



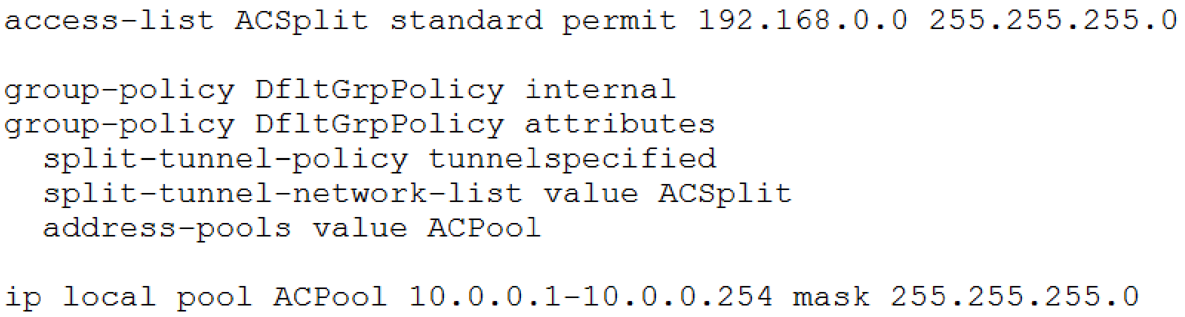
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

B.



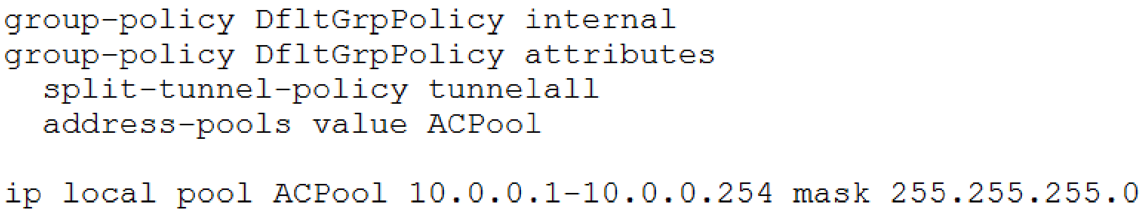
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

C.



```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

D.



```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

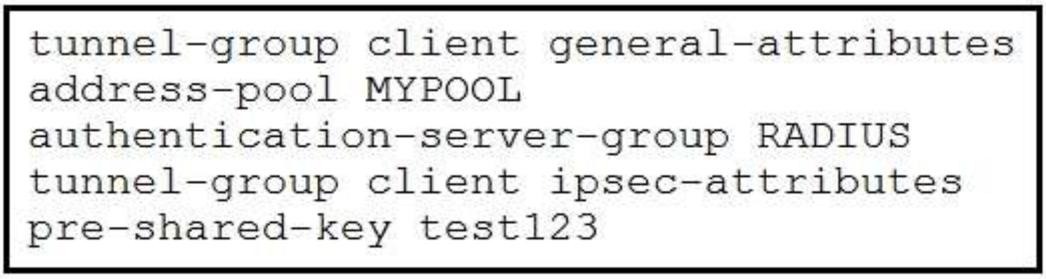
Answer: A

QUESTION 88
Which two features are valid backup options for an IOS FlexVPN client? (Choose two.)

A. HSRP stateless failover
B. DNS-based hub resolution
C. reactivate primary peer
D. tunnel pivot
E. need distractor

Answer: BC

QUESTION 89
Refer to the exhibit. Which type of VPN is used?



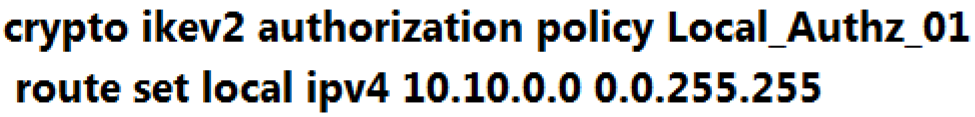
```
tunnel-group client general-attributes
address-pool MYPOOL
authentication-server-group RADIUS
tunnel-group client ipsec-attributes
pre-shared-key test123
```

A. GETVPN
B. clientless SSL VPN
C. Cisco Easy VPN
D. Cisco AnyConnect SSL VPN

Answer: C

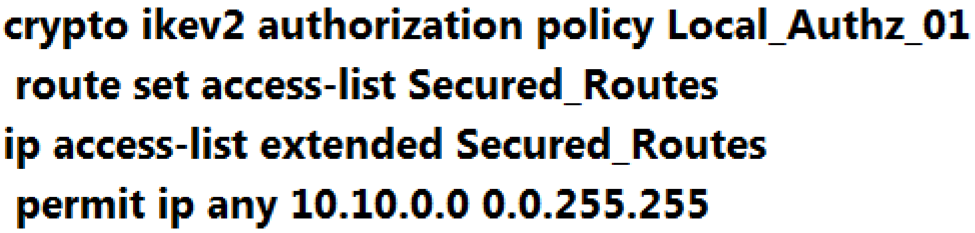
QUESTION 90
An engineer would like Cisco AnyConnect users to be able to reach servers within the 10.10.0.0/16 subnet while all other traffic is sent out to the Internet. Which IPsec configuration accomplishes this task?

A.



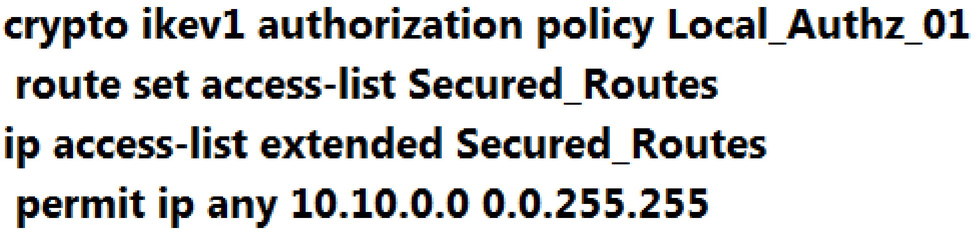
```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```

B.



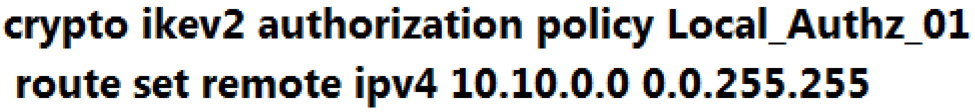
```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

C.



```
crypto ikev1 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

D.



```
crypto ikev2 authorization policy Local_Authz_01
 route set remote ipv4 10.10.0.0 0.0.255.255
```

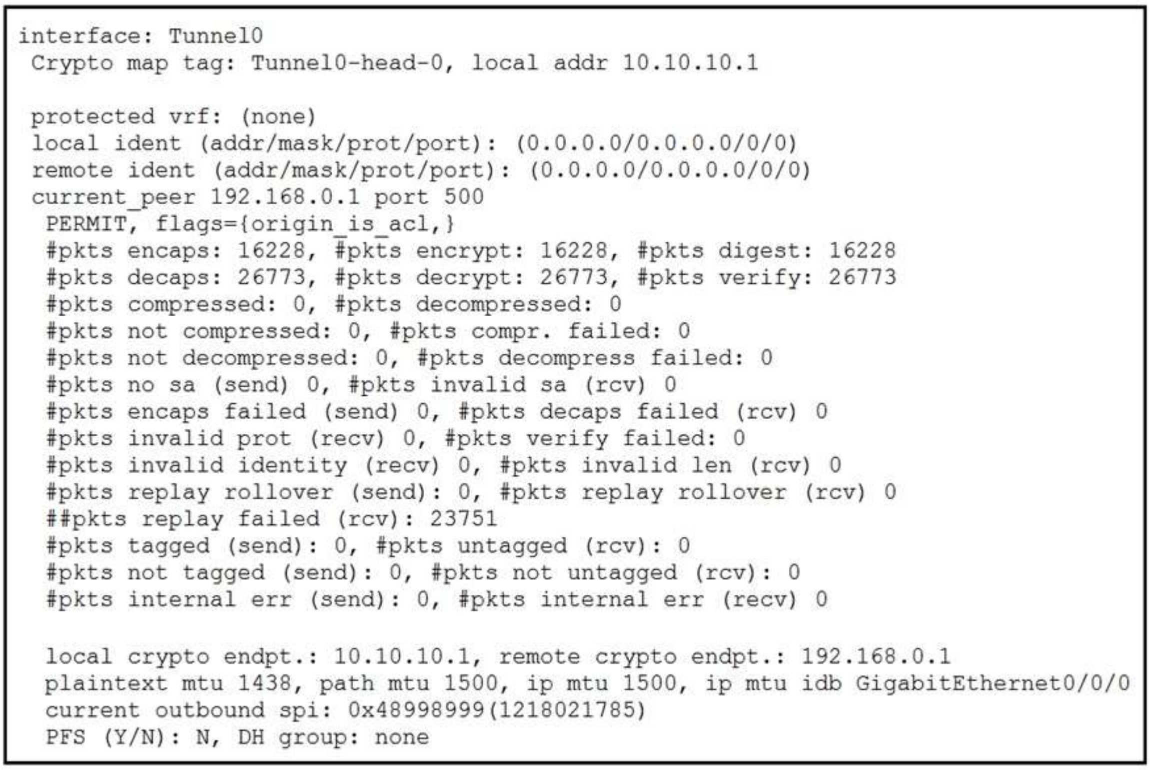
Answer: B

QUESTION 91
Which Cisco AnyConnect component ensures that devices in a specific internal subnet are only accessible using port 443?

A. routing
B. WebACL
C. split tunnel
D. VPN filter

Answer: D

QUESTION 92
Refer to the exhibit. 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?



```
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
```

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.

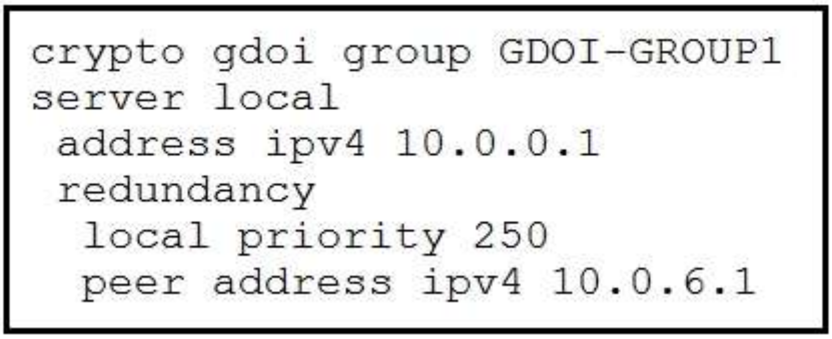
Answer: A

QUESTION 93
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.

Answer: C

QUESTION 94
Refer to the exhibit. Which type of VPN is being configured, based on the partial configuration snippet?



```
crypto gdoi group GDOI-GROUP1
server local
 address ipv4 10.0.0.1
 redundancy
  local priority 250
  peer address ipv4 10.0.6.1
```

A. GET VPN with COOP key server
B. GET VPN with dual group member
C. FlexVPN load balancer
D. FlexVPN backup gateway

Answer: A