



Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW 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 commands 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
```

1.1.1.1

10.0.0.1

redirect

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
```

shortcut

server-only

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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-summaps.html

NEW 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

Answer: B

NEW QUESTION 3

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 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

Answer: D

NEW 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.

Answer: A

NEW QUESTION 6

Refer to the exhibit.

```
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
```

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 7

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

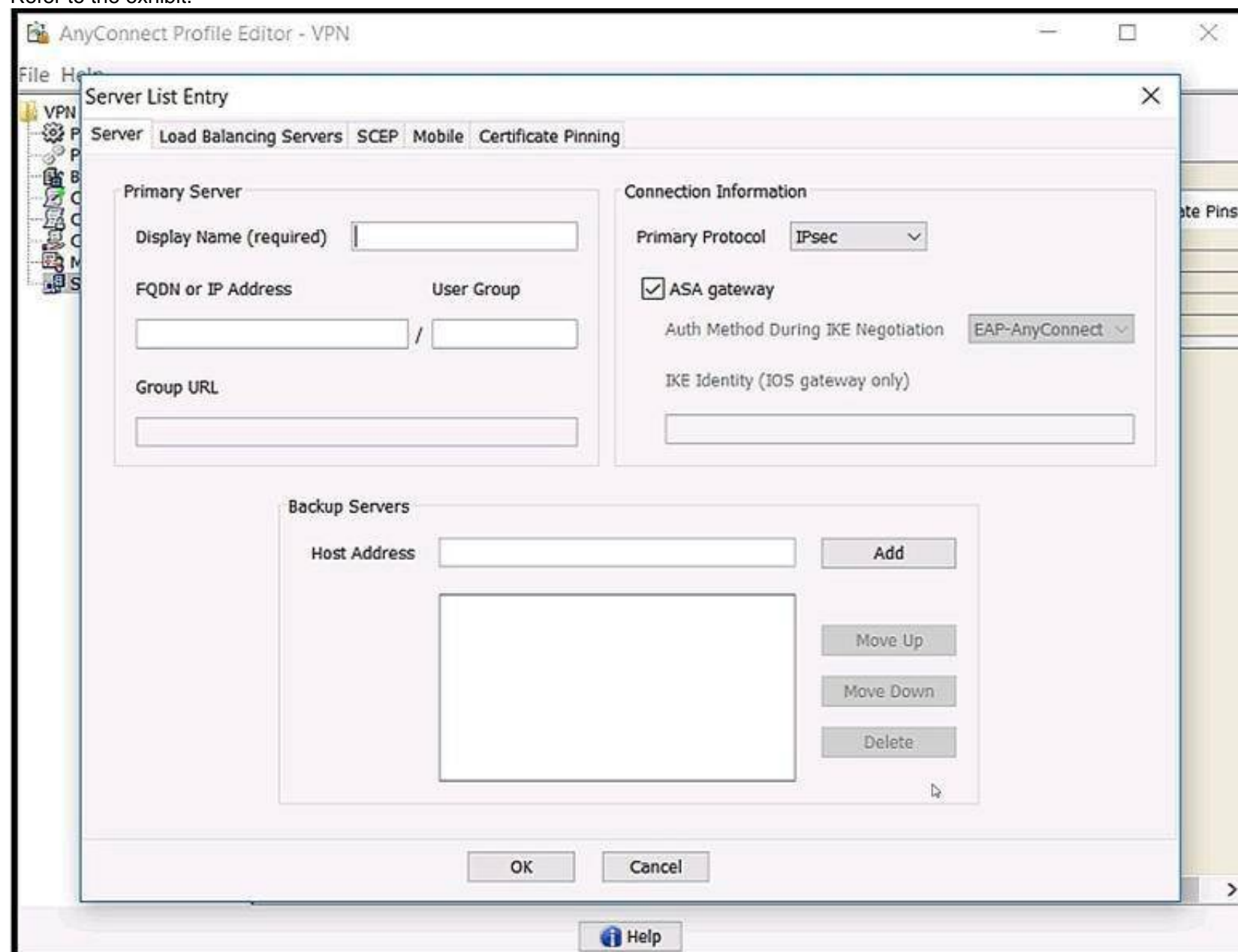
Answer: C

Explanation:

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

NEW QUESTION 8

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

Answer: D

Explanation:

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

NEW QUESTION 9

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/xr-3s/sec-flex-vpn-xr-3s-book/sec-cfg-flex-clnt.html

NEW QUESTION 10

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 10

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)

Answer: D

NEW QUESTION 14

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.

Answer: CD

NEW QUESTION 18

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

Answer: C

Explanation:

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

NEW QUESTION 19

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

Answer: D

Explanation:

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

NEW QUESTION 24

Refer to the exhibit.

```
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)
```


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

Answer: A

NEW QUESTION 25

Refer to the exhibit.

```
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
```

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.

Answer: C

NEW QUESTION 30

Refer to the exhibit.

```
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
```

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

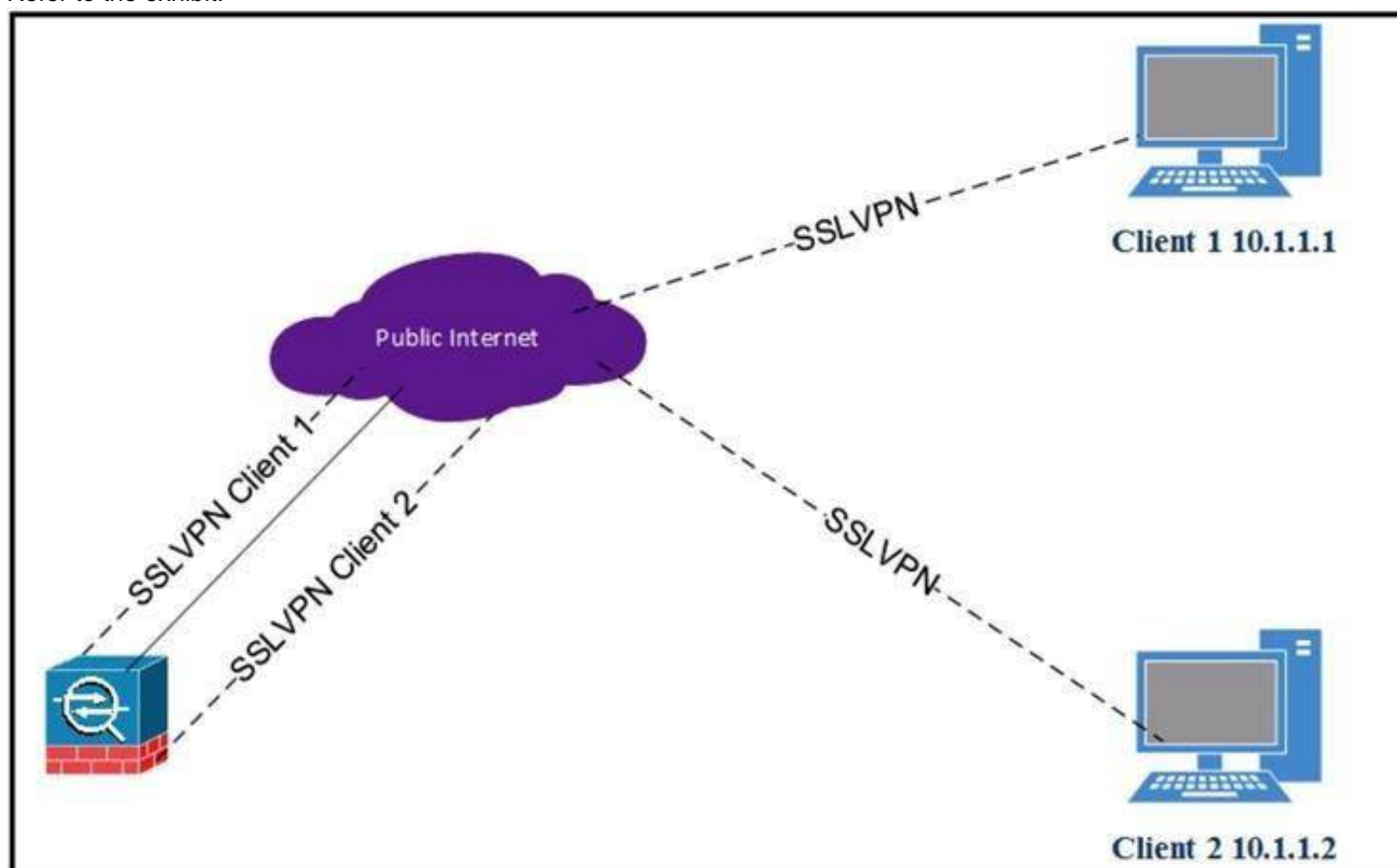
Answer: B

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.

NEW QUESTION 31

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

Answer: B

NEW QUESTION 34

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

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

Answer: C

Explanation:

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

NEW QUESTION 38

What uses an Elliptic Curve key exchange algorithm?

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

Answer: B

Explanation:

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

NEW QUESTION 40

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

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

Answer: BE

NEW QUESTION 41

Which VPN solution uses TBAR?

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

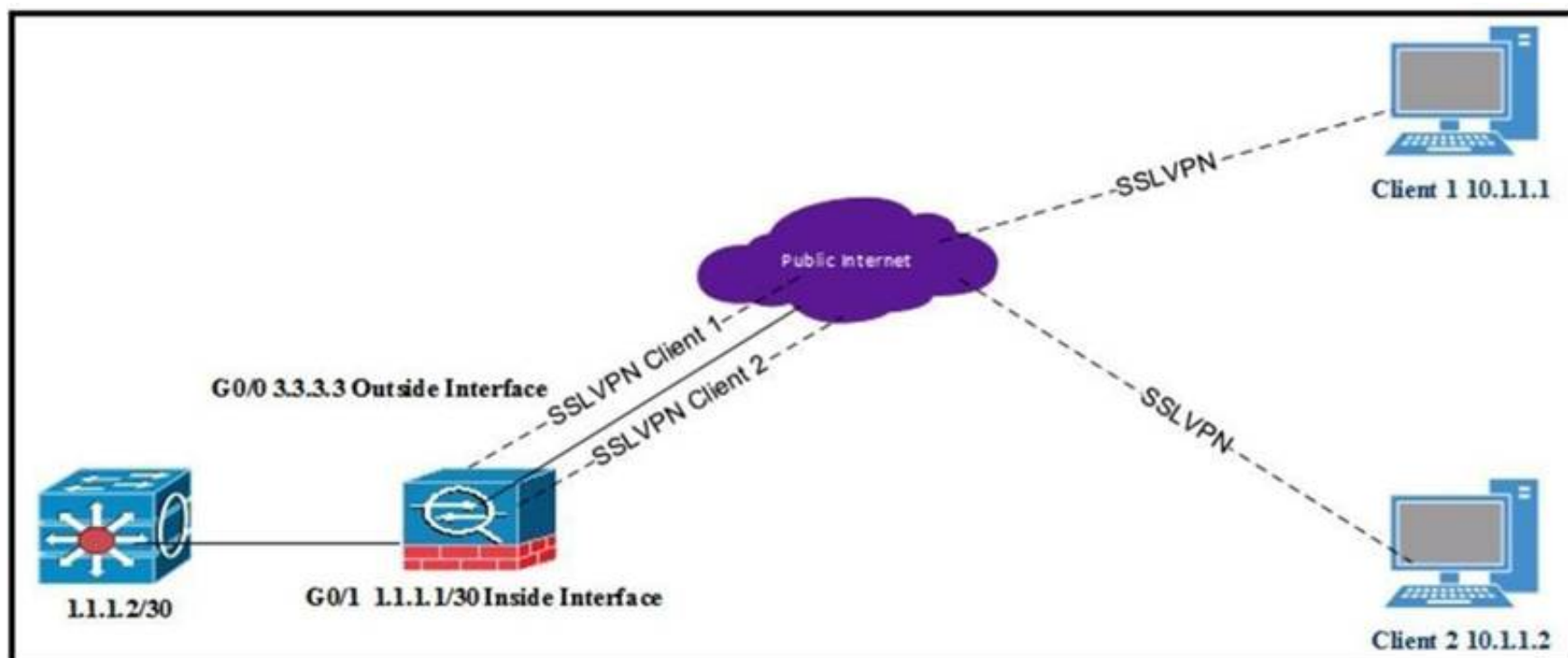
Answer: A

Explanation:

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

NEW QUESTION 42

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

Answer: D

NEW QUESTION 46

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

Answer: C

NEW 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

Answer: D

NEW QUESTION 53

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.

Answer: A

Explanation:

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

NEW QUESTION 56

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 57

Refer to the exhibit.

```
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
```

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

Answer: C

NEW QUESTION 58

.....

Relate Links

100% Pass Your 300-730 Exam with ExamBible Prep Materials

<https://www.exambible.com/300-730-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>