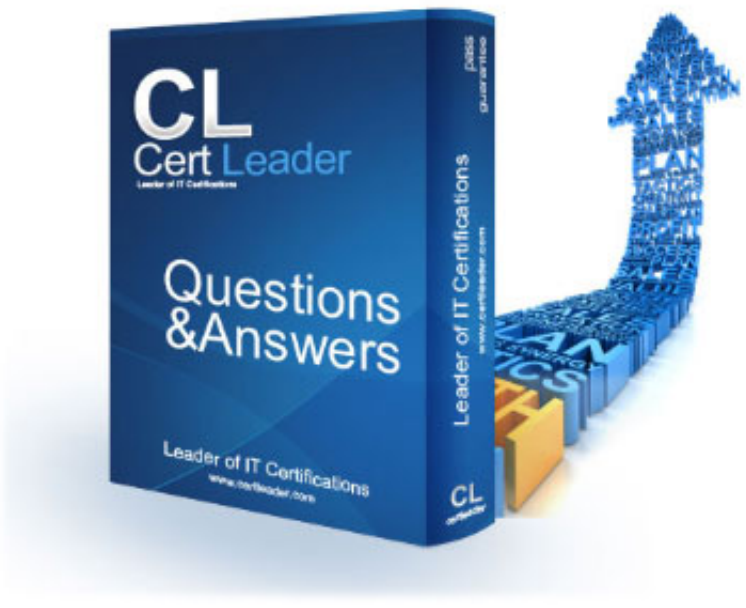
300-730 Dumps

Implementing Secure Solutions with Virtual Private Networks (SVPN)

https://www.certleader.com/300-730-dumps.html



NEW QUESTION 1
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 2
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 3
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 4
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.

Answer: CE

NEW QUESTION 5
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 6
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/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-clnt.html

NEW QUESTION 7
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

Answer: DE

Explanation:
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

NEW QUESTION 8
Which configuration construct must be used in a FlexVPN tunnel?

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

Answer: D

NEW QUESTION 9
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 10
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

Answer: B

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

NEW QUESTION 10
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 14
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. *$DfltIkeIdentityS*

Answer: B

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

NEW QUESTION 17
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.

Answer: B

Explanation:
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

NEW QUESTION 19
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 22
Refer to the exhibit.

```
*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
```

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

Answer: B

NEW QUESTION 26
Refer to the exhibit.

```
*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
```

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

Answer: D

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

NEW QUESTION 29
Refer to the exhibit.

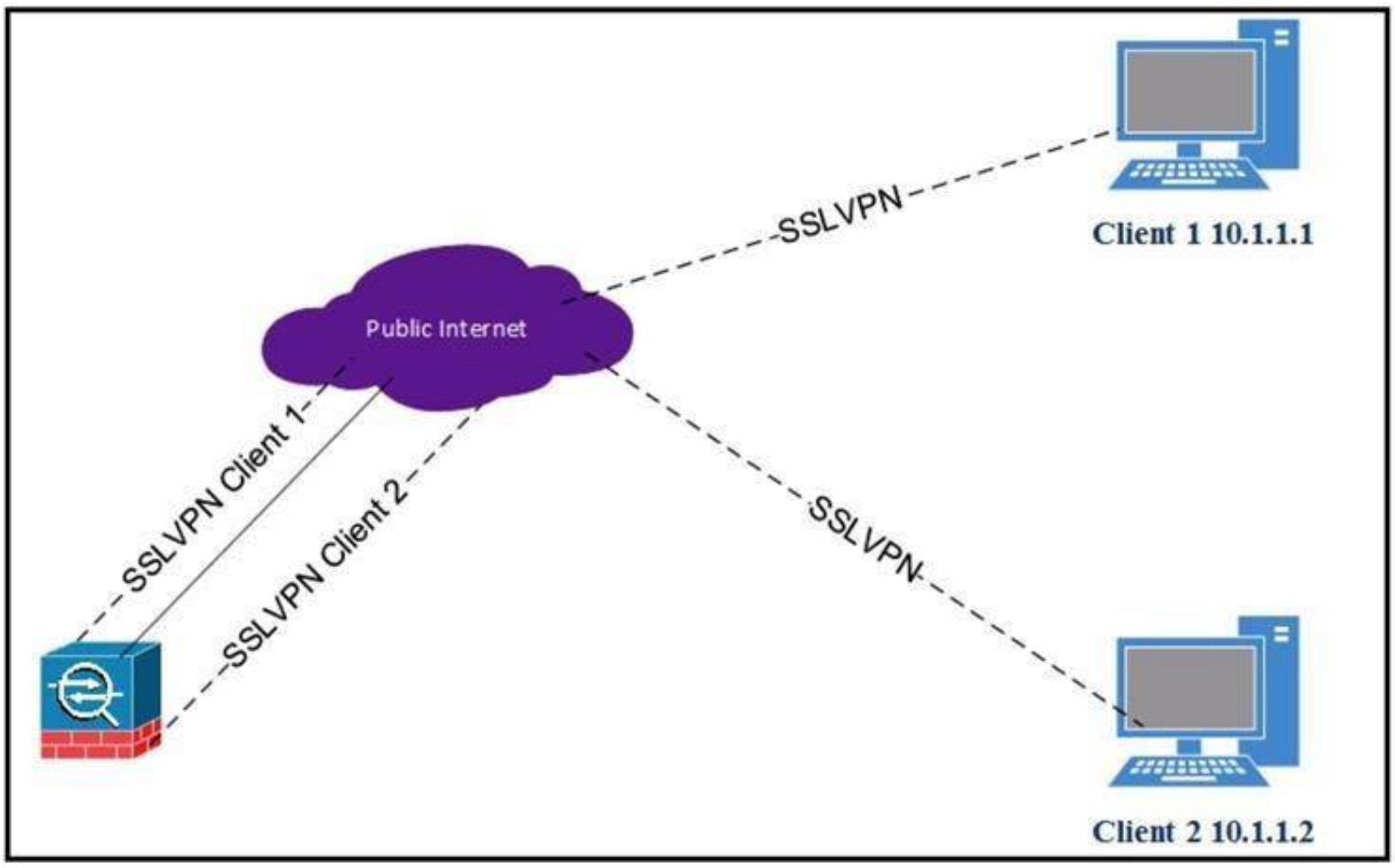
```
HUB configuration:

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
```

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.

Answer: A

NEW QUESTION 33
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 35
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 are two functions of ECDH and ECDSA? (Choose two.)

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

Answer: CD

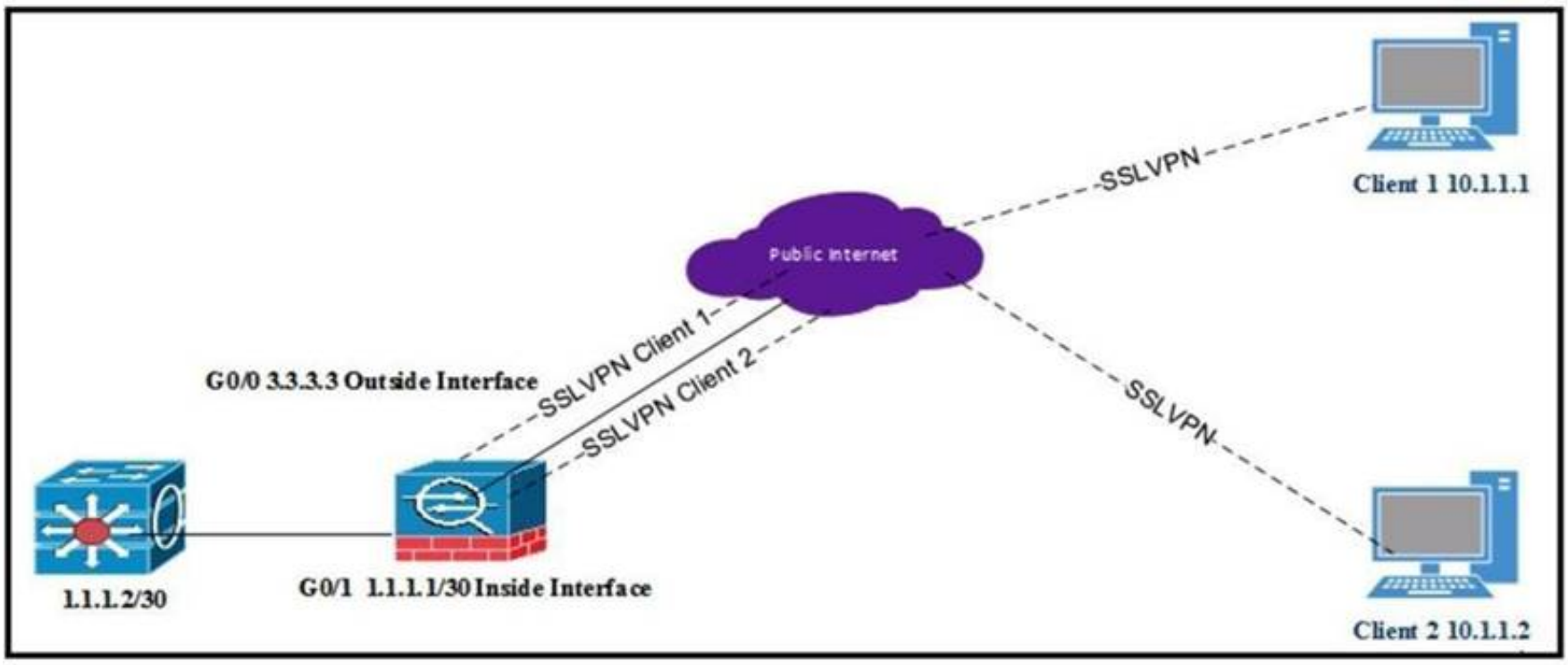
Explanation:
Reference: https://tools.cisco.com/security/center/resources/next_generation_cryptography

NEW QUESTION 41
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

Answer: AD

NEW QUESTION 44
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 45
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 48
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 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

Answer: A

NEW QUESTION 55
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 vpnsession-db must be cleared manually.
C. Configure a backup server in the XML profile.
D. AnyConnect client must point to the standby IP address.

Answer: A

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

NEW 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

Answer: B

NEW 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

Answer: B

NEW QUESTION 60
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 64
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-730 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-730-dumps.html