ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

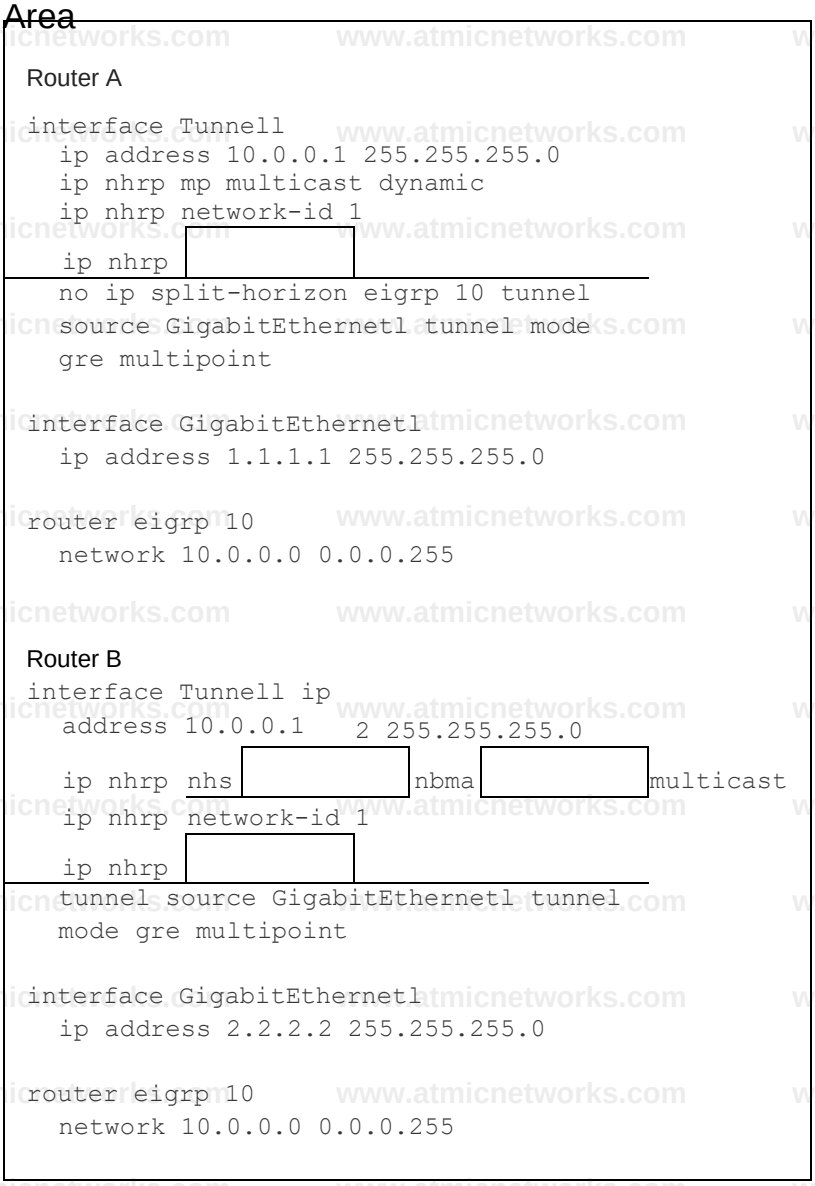
Warning: Keep connected with our support team for latest updates

Question: 1

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.

Answer Area



1.1.1.1

10.0.0.1

redirect

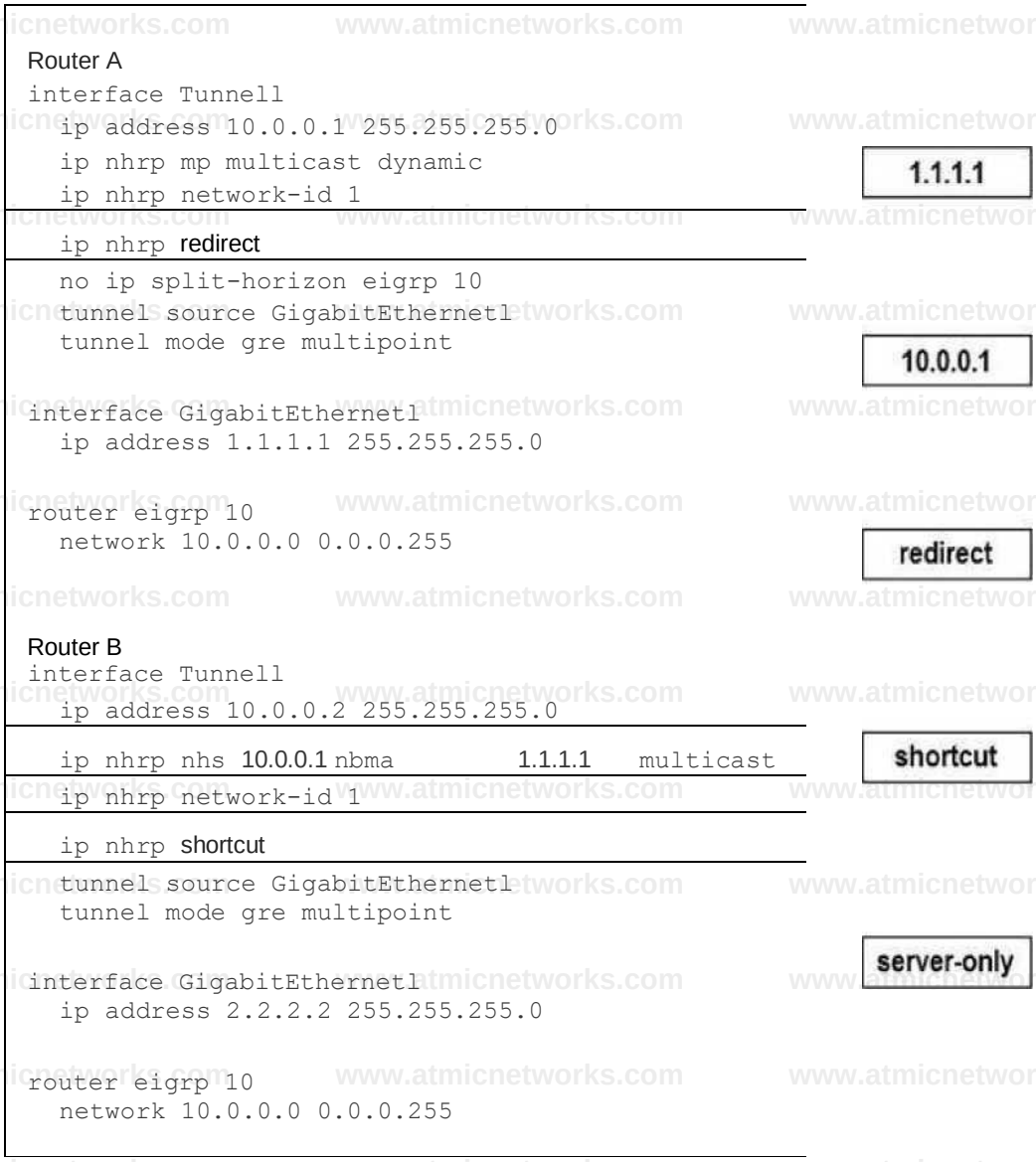
shortcut

server-only

Answer:

Explanation:

Answer Area



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: 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: C

Explanation:

The IKEv2 CREATE_CHILD_SA packet is used to establish a new security association (SA) between two peers. This packet contains the details of the exchange, including the traffic selectors, the cryptographic algorithms and keys to be used, and any other relevant information

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
11  .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
```

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 120 ip nhrp shortcut
 tunnel source GigabitEthernet0/1 tunnel mode gre
 multipoint
 end
```

C
```
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 GigabitEthernetO/1
tunnel mode gre multipoint end
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C Explanation:

https://www.globalknowledge.com/us-en/resources/resource-library/articles/understanding-next- hop-resolution-protocol-commands/

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

Explanation:

On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, the command that is needed for the hub to be able to terminate FlexVPN tunnels is interface virtual-template. The interface virtual-template command is used to configure a virtual template interface which provides a secure tunnel for FlexVPN connections. The other commands listed - interface virtual-access, ip nhrp redirect, and interface tunnel - are not related to FlexVPN and are not used to terminate FlexVPN tunnels.

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

Explanation:

KS (key server) is 'caretaker' of the GM group. Group registrations and authentication of GMs is taken care of by KS server. Any GM who wants to join the group is required to be successfully authenticated in the group and sends encryption keys and policy to be used within the group.

https://ipwithease.com/introduction-to-getvpn/

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 corapr. 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 GigabitEthernetl 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

Explanation:

Question: 7

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: DE

Explanation:
DMVPN disables the EIRGP next-hop-self with "no ip next-hop-self eigrp xxx" in DMVPN phase 2, and to go from Phase 2 to 3 you need use the NHRP protocol, and again enable EIRGP next-hop-self with "ip next-hop-self eigrp 134" under the tunnel interface 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-dmvpn.html#GUID-BF561439-BCC0-4AAF-80D9-1F7876CB7B81

Question: 8

Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

A. Reduce the maximum SA limit on the local Cisco ASA.
B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.
C. Remove the maximum SA limit on the remote Cisco ASA.
D. Correct the crypto access list on both Cisco ASA devices.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-3s/sec-ike-for-ipsec-vpns-xe-3s-book/sec-call-addmsn-ike.html

Question: 9

Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

A. group-alias
B. certificate map
C. optimal gateway selection
D. group-url
E. AnyConnect client version

Answer: AD

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

Question: 10

Which method dynamically installs the network routes for remote tunnel endpoints?

A. policy-based routing
B. CEF
C. reverse route injection
D. route filtering

Answer: C

Explanation:

Reverse route injection (RRI) is a method that dynamically installs the network routes for remote tunnel endpoints. The RRI feature allows the router to automatically learn the routes for the remote networks and automatically install these routes into the routing table. This eliminates the need for the administrator to manually configure and maintain the routes for the remote networks. This feature is commonly used in VPN environments, where the router at the VPN endpoint needs to learn the routes for the remote networks behind the other VPN endpoint. The other options such as policy-based routing, CEF, and route filtering are not used to dynamically install the network routes for remote tunnel endpoints

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn-availability-12-4t-book/sec-rev-rte-inject.html

Topic 2, Remote access VPNs

Question: 11

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

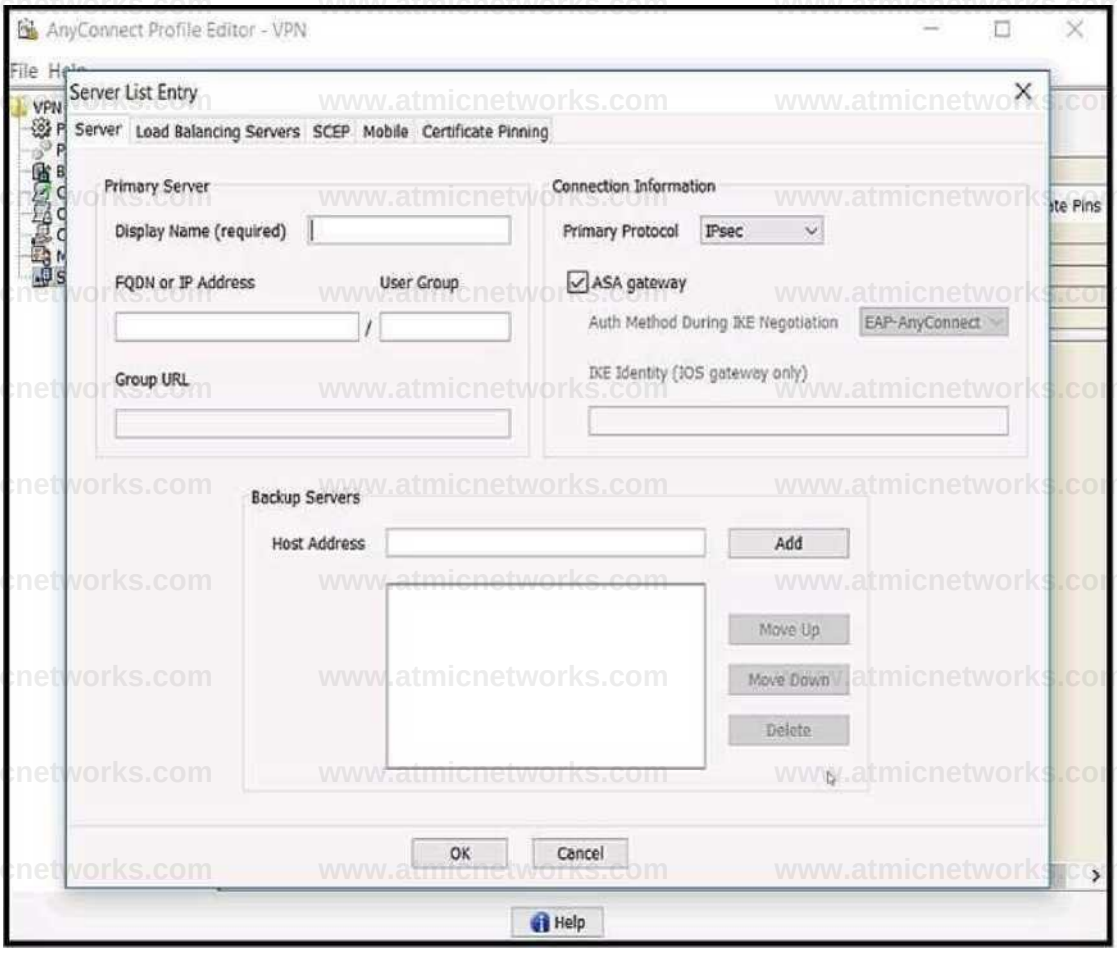
Answer: C

Explanation:

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

Question: 12

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:

The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-profile-editor.html#ID-1430-0000026c

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

Question: 13

Refer to the exhibit.

```
aaa new-model
```

```
aaa authorization network, local-group-author-list local I
crypto pki trustpoint trustpointl
 enrollment url http://192.168.3.1:80 revocation-check, crl
I
crypto pki certificate map certmapl 1 subject-name co cisco
I
crypto ikev2 authorization policy author-policyl
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl

crypto ikev2 profile ikev2-profilel match certificate certmapl
 authentication local rsa-sig authentication remote rsa-sig pki
 trustpoint trustpointl
 aaa authorization group cert list local-group-author-list author-
policyl
 virtual-template 1

crypto ipscc transform-set transferal esp-acs csp-sha-hmac

crypto ipsec profile ipsec-profilel set transform-set trans
transforml set ikev2-profile ikev2-profile1 i
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32 I
interface Virtual-Templatel type tunnel ipv6 unnumbered Ethemet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profilel i
ipv6 local pool v6-pool 2001:DB8:1::10/32 48 I
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: C

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116528-config-flexvpn-00.html

Question: 14

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: AE

Explanation:
HTTP (Hypertext Transfer Protocol) is used for transferring web resources, such as web pages and HTML documents, across the internet. CIFS (Common Internet File System) is used for sharing files and printers between computers on a network. ICA (Citrix), VNC (Virtual Network Computing), and RDP (Remote Desktop Protocol) are not enabled by default on the Cisco ASA Clientless SSL VPN portal.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn- config/webvpn-configure-gateway.html

Question: 15

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

Explanation:

The correct answer is D. IKEv2 profile. A FlexVPN tunnel requires an IKEv2 profile to define the parameters for the IKEv2 negotiation and the IPsec security association. The IKEv2 profile references the IKEv2 keyring, the authentication method, the identity of the peers, and other options. The IKEv2 profile is then applied to a virtual tunnel interface (VTI) or a dynamic virtual tunnel interface (DVTI) to protect the tunnel with IPsec12. An EAP configuration is used for authentication with Extensible Authentication Protocol (EAP), which is optional for FlexVPN3. A multipoint GRE tunnel interface is used for DMVPN, not FlexVPN. An IKEv1 policy is used for IKEv1, not IKEv2, which is the protocol for FlexVPN.

Question: 16

A Cisco AnyConnect client establishes a SSL VPN connection with an ASA at the corporate office. An engineer must ensure that the client computer meets the enterprise security policy. Which feature can update the client to meet an enterprise security policy?

A. Endpoint Assessment
B. Cisco Secure Desktop
C. Basic Host Scan
D. Advanced Endpoint Assessment

Answer: D

Explanation:

"If the end user disables antivirus or personal firewall after successfully establishing the VPN connection, our Advanced Endpoint Assessment feature attempts to re-enable that application within approximately 60 seconds."
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/configure-posture.html#ID-1407-00000047

Question: 17

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

Explanation:
According to the Implementing Secure Solutions with Virtual Private Networks (SVPN) documents and learning resources available at cisco.com, the two features that provide headend resiliency for Cisco AnyConnect clients are:
AnyConnect Backup Servers: This feature allows the AnyConnect client to automatically connect to a backup server in case the primary server is unreachable or fails. The backup server list is configured on the ASA or IOS headend and pushed to the client during the VPN connection establishment. The client can also manually select a backup server from the list if needed. This feature enhances the availability and reliability of the VPN service for the clients12.
ASA failover: This feature enables two identical ASAs to be paired together as an active/standby or active/active pair. The ASAs synchronize their configuration and state information and monitor each other's health. If the active ASA fails or becomes unreachable, the standby ASA takes over the traffic and VPN sessions without any disruption for the clients. This feature provides high availability and redundancy for the VPN headend34.
1: AnyConnect Backup Servers 2: Redundancy options for IOS Headend for AnyConnect Clients 3: ASA Failover 4: AnyConnect Implementation and Performance/Scaling Reference for COVID-19 Preparation

Question: 18

Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

A. The XML profile is not configured correctly for the affected users.
B. The new client image does not use the same major release as the current one.
C. Client services are not enabled.
D. Client software updates are not supported with IKEv2.

Answer: C

Explanation:
https://community.cisco.com/t5/vpn/anyconnect-service-port-not-enabled/td-p/2968124

Question: 19

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: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn- config/webvpn-configure-policy-groups.html says clearly: In group-policy webvpn configuration mode, you can specify (list of things, including url-list).

Question: 20

Refer to the exhibit.

Based on the exhibit, why are users unable to access CCNP Webserver bookmark?

A. The URL is being blocked by a WebACL.
B. The ASA cannot resolve the URL.
C. The bookmark has been disabled.
D. The user cannot access the URL.

Answer: B

Explanation:
https://community.cisco.com/t5/network-security/missing-ssl-vpn-bookmarks/td-p/1597023

Question: 21

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

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/webvpn.html

Question: 22

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: D

Explanation:

Plug-ins are extensions to the Clientless SSL VPN feature that enable the ASA to handle non-standard applications and Web resources so that they display correctly over a Clientless SSL VPN connection. Plug-ins are software components that the ASA downloads to the remote user's browser. The plugins provide support for applications and protocols that are not natively supported by Clientless SSL VPN, such as Java, ActiveX, SSH, Telnet, and RDP. Plug-ins can also provide enhanced functionality and security for Web applications, such as Outlook Web Access and Lotus iNotes.

You can read more about plug-ins and how to configure them in the document [ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.7] 1.

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

Question: 23

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

Question: 24

Refer to the exhibit.

The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?

A crypto vpn anyconnect profile Profile 1 flash:RDP.xml webvpn context Contextl svc platform win seq 1 policy group PolicyGroupI functions svc-enabled

B crypto vpn anyconnect profile Profile 1 flash:RDP.xml webvpn context Contextl browser-attribute import flash:RDP.xml

C crypto vpn anyconnect profile Profile 1 flash:RDP.xml webvpn context Contextl policy group PolicyGroupI
svc profile Profilel

E. crypto vpn anyconnect profile Profile 1 flash:RDP.xml webvpn context Contextl policy group PolicyGroupI
svc module RDP

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

Reference: https://community.cisco.com/t5/vpn/starting-anyconnect-vpn-through-rdp-session-on- cisco-891/td- p/2128284

Question: 25

Refer to the exhibit.

Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)

A. group-url https://172.16.31.10/General enable
B. group-policy General internal
C. authentication aaa
D. authentication certificate
E. group-alias General enable

Answer: CE

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

Question: 26

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: B

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

Remote-Access.pdf

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

Question: 27

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

Question: 28

Refer to the exhibit.

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes banner none dns-server value
 10.10.10.10 vpn-tunnel-protocol ssl-clientless default-domain value
 cisco.com address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes vpn-simultaneous-logins 10 vpn-tunnel-
 protocol ikev2 ssl-clientless split-tunnel-policy tunnelall

tunnel-group Admins type remote-access tunnel-group Admins general-
attributes default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes group-alias Admins enable

tunnel-group Employee type remote-access tunnel-group Employee webvpn-
attributes group-alias Employee enable

webvpn enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable tunnel-group-list enable
```

Which VPN technology is allowed for users connecting to the Employee tunnel group?

A. SSL AnyConnect
B. IKEv2 AnyConnect
C. crypto map
D. clientless

Answer: D

Explanation:

When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. To view the default group policy.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/vpngrp.ht ml

Topic 3, Troubleshooting using ASDM and CLI

Question: 29

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)
      flpkts encaps: 200, flpkts encrypt: 200
      Kpkts decaps: 0, flpkts 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)

Spoke2fl
      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)
      Upkts encaps: 210, flpkts encrypt: 210,
      flpkts decaps: 200, flpkts 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

Explanation:

Question: 30

Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

A. show crypto ikev2 sa
B. show crypto isakmp sa
C. show crypto gkm
D. show crypto identity

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116413-configure- flexvpn-00.pdf

Question: 31

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

On receiving the redirect, Spoke1 initiates a resolution request for Host2 over the point-to-point tunnel interface (the same interface over which it received the redirect). The resolution request traverses the routed path (Spoke1-hub-spoke2). On receiving the resolution request, Spoke2 determines that it is the exit point

and needs to respond to the resolution request.
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html

Question: 32

An engineer is troubleshooting a new DMVPN setup on a Cisco IOS router. After the show crypto isakmp sa command is issued, a response is returned of "MM_NO_STATE." Why does this failure occur?

A. The ISAKMP policy priority values are invalid.
B. ESP traffic is being dropped.
C. The Phase 1 policy does not match on both devices.
D. Tunnel protection is not applied to the DMVPN tunnel.

Answer: C

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976- dmvpn-troubleshoot-00.html
The MMNOSTATE failure occurs when the ISAKMP policy priority values are not configured correctly on both devices. The ISAKMP policy priority values are used to determine the order in which the ISAKMP policies are applied. If the priority values do not match between the two devices, the ISAKMP tunnel may not be established correctly, resulting in the MMNOSTATE failure. To resolve this issue, the engineer should ensure that the ISAKMP policy priority values are configured correctly on both the router and the peer.

Question: 33

Refer to the exhibit.

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
 address-pool split
 default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
 group-alias ikev2 enable

-----------------------------------------------------

 -<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

The customer can establish a Cisco AnyConnect connection without using an XML profile. When the host "ikev2" is selected in the AnyConnect drop down, the connection fails. What is the cause of this issue?

A. The HostName is incorrect.
B. The IP address is incorrect.
C. Primary protocol should be SSL.
D. UserGroup must match connection profile.

Answer: D

Explanation:

Reference: https://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta- p/3157891
User Group—Specify a user group. The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.

Question: 34

Refer to the exhibit.

```
ISAKMP: (0}beginning Main Mode exchange
ISAKMP-PAK: (0) sending packet to 192.163.0.8 cy_port 509 peer_port 500 (I) MM_NO_SIATE
ISAKMP-PAK: (0):received packet from 192.163.0.3 dport 500 sport 500 Global (I? MM_N0_57AIE
ISAKMP (0):01d State - IKE_I_MH1 New State - IKE_I_MM2
ISAKMP (0):found peer pre-shared key matching 192.163.0.3
: (0):local preshared key found
ISAKMP (0):Checking ISAKMP transform 1 against priority 10 policy
: (0): encryption AES-CBC
ISAKMP (0): keylength of 256
: (0): hash SHA2S6
ISAKMP (0): default group 14
: (0): auth pre-share
ISAKMP (0): life type in seconds
: (0); life duration (basic) of 1200
ISAKMP (0):atts are acceptable. Next payload is 0
```

```
ISAKMP-PAK: (0):sending packet to 192.163.0.3 myjport 500 peer_port 500 (1} MM_SA_5ETUP
ISAKMP: (O)sOld State - IKE_I_HM2 Hew State - IKE_I_MH3 '
ISAKMP-PAK: (0):received packet from 192.165.0.3 Sport 500 sport 500 Global (I) MM_SA_SEIUP
ISAKMP: (0)sold State = IKE_I_MH3 New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.165.0.5
ISAKMP: (1005):01d State - IKE_I_MM4 Mew State = IKE_I_MM4
ISAKMP: j1005):pre-shared key authentication using id type IE_IPV4_ADOK
ISAKMP-PAK: (IMS) s sending packet to 192.168.0.6 myjport 4500 neer_port 4500 (I) MM KE¥_EXCH ISAKMP: (1005):01d State =
IKE_I_MM4 New State - IKE_I_MM5 " "
I5AKMP-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 192.168.0.3 myjort 4500 peerjort 4500 (II MH_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global {I) MM_KE¥_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

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/113594-trouble-ios-ike-00.html#anc12

Question: 35

Refer to the exhibit.

```
IKEv2:(SESSION ID = II,SA ID = 1):Processing IKE_AUTH message
IKEvZ: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-SRR0R:(SESSION ID = 17,SA ID = 1):: There was no IPSEC policy found for received TS
IKEV2:(SESSION ID = 17,SA ID = J)(Sending TS unacceptable notify
IKEv2:(SESSION ID = 17,SA ID = 1)(Get my authentication method
!KEv2:(SESSION ID = 17,SA ID = I):Ny authentication method is 'PSK'
IKEv2:(SESSION ID ■ 17,SA ID * 1)(Get peer's preshared key for 63.72.250.251
IKEv2:(SESSION ID ■ 17,SA ID ■ 1)(Generate my authentication data
IKEV2;(SESSION ID = 17,SA ID = I)(Use preshared key for id 68.72.250,250, key len 5
IKEV2:[IKEVZ -> 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(TSJJHACCEPTAB1E)

IKEv2:(SESSION ID = 17,SA ID = 1)(Sending Packet (To 68.72.250.251:500/From 68.72.250.250:500/VRF iO:fO)
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: A

Explanation:

The first of the two TS payloads is known as TSi (Traffic Selector- initiator). The second is known as TSr (Traffic Selector-responder). TSi specifies the source address of traffic forwarded from (or the destination address of traffic forwarded to) the initiator of the Child SA pair. https://www.rfc- editor.org/rfc/rfc5996#page-40

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.

Question: 36

Refer to the exhibit.

```
•Nov 2G 00:52:20.602: IKEv2:(SESSION ID = 1,SA ID = l):Received Packet [From 10.10.10.1:500/To 10.16.10.2:500/VRF i0:fe]
Initiator SPI I D5684E1462991856 - Responder SPI : 216214SC95256F6A Message id: 1
IKEv2 IKE.AUTH Exchange RESPONSE
'Nov 26 00:52:20.002: IKEv2-PAK:(SESSION 10 = 1,SA ID = l):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
     lOr Next payload: AUTH, reserved: 0x0, length: 12
        Id type: IPv4 address, Reserved: 0x0 0x0
     AUTH Next payload: SA, reserved: 0x0, length: 28
        Auth rethod 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: 30.39.30.0, end addr: 39.30.39.255
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(SETWINDOW.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.SUPPQRT
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 »  l):Process auth response notify
•Nov 26       00:52:20.003:     IKEv2:(SESSION IDa1,SA     ID a  1):Searching policy based       on peer'sidentity '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       00:52:20.094:     IKEv2;(SESSION ID=1,SA     ID =  1):Verification of peer's       authenticationdata FAILED
•Nov 26       00:52:20.004;     IKEv2;(SESSION ID=1,SA     ID =  l);Auth exchange failed
•Nov 26 00:52:20.004: IKEv2-ERR0R:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
•Nov 26 09:52:20.004; IKEv2;(SESSION ID = 1,SA ID = 1):Abort exchange
•Nov 26 00:52:20.004; IKEv2;(SESSION ID = 1,SA ID ■ l);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

Explanation:

Question: 37

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:

IKE Message from X.X.X.X Failed its Sanity Check or is Malformed

This debug error appears if the pre-shared keys on the peers do not match. In order to fix this issue, check the pre-shared keys on both sides.

1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its sanity check or is malformed

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#anc17

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

Question: 38

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


SPORE 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


SPORE 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?

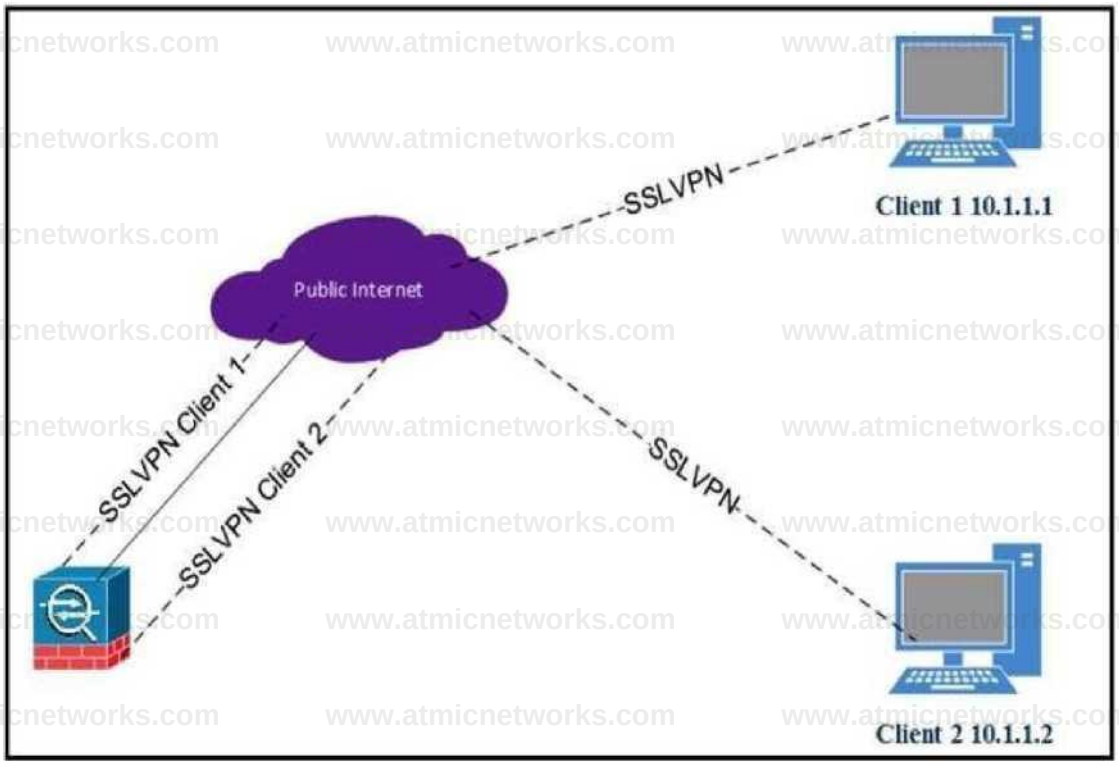
A. Spoke 1 fails the authentication because the authentication methods are incorrect.
B. Spoke 2 passes the authentication to the hub and successfully proceeds to phase 2.
C. Spoke 2 fails the authentication because the remote authentication method is incorrect.
D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Answer: A

Explanation:

Question: 39

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 AS

A. 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

Explanation:

The same-security-traffic intra-interface command lets traffic enter and exit the same interface, which is normally not allowed. This feature might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it

might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the security appliance is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the security appliance and then out again to the other spoke.

Question: 40

Refer to the exhibit.

```
Ciscoasa# sh cap o trace packet-number 4

737 packets captured

   4: 09:19:36.054131       10.99.117,195.56485 > 10.31.124.31.443:      $ 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscala 8,nop,nop,sackOK>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype;
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj 172.16.0.0 24 interface
Additional Information:
NAT divert to egress interface inside
Vntranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST Subtype: log
Result: ALLOW
Config:
access-group global access 1 global
access-list global access 1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj 172.16.0.0 24 interface
Additional Information:
Static translate 10.03.117.195/564S5 to 10.99.117.195/564S5

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj 172.16.0.0 24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside
Result:
input-interface; outside
input-status: up
input-line-status; up
output-interface: inside output-status: up

output-line-status: up
Action: allow

1 packet shown
```

An SSL client is connecting to an ASA headend. The session fails with the message “Connection attempt has timed out. Please verify Internet connectivity.” Based on how the packet is processed, which phase is causing the failure?

A. phase 9: rpf-check
B. phase 5: NAT

C. phase 4: ACCESS-LIST
D. phase 3: UN-NAT

Answer: D

Explanation:

Topic 4, Secure Communications Architectures

Question: 41

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

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

Answer: C

Explanation:

IPsec failover fallsinto two categories:statelessfailover and stateful failover.Statelessfailover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary-to-secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

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

Question: 42

Which technology works with IPsec stateful failover?

A. GLBR
B. HSRP
C. GRE
D. VRRP

Answer: B

Explanation:

HSRP (Hot Standby Router Protocol). HSRP is a Cisco proprietary protocol that provides stateful failover for IPsec virtual private networks (VPNs). It is used to create a virtual router in order to provide redundancy in the event of an IPsec VPN failure. HSRP works by assigning a single primary router to manage the connection and forwarding traffic to the secondary router if the primary router fails.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

Question: 43

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

Question: 44

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/

Question: 45

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

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

Answer: BE

Explanation:

Question: 46

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/xe-3s/sec-get- vpn-xe-3s-book/sec-get-vpn.html

Question: 47

Which two commands help determine why the NHRP registration process is not being completed even after the IPsec tunnel is up? (Choose two.)

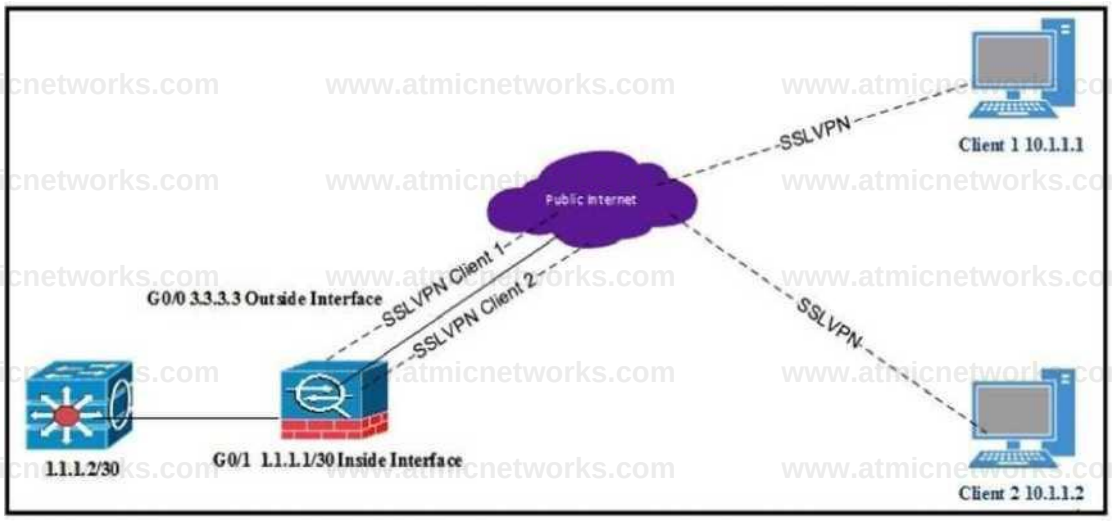
A. show crypto isakmp sa
B. show ip traffic
C. show crypto ipsec sa
D. show ip nhrp traffic
E. show dmvpn detail

Answer: AD

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

Question: 48

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 AS A. 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: C

Explanation:

The reason is that by default, the SSL VPN clients use split tunneling, which means they only send traffic destined for the corporate network through the VPN tunnel, and use their local gateway for other traffic, such as browsing the internet. This means that when they search for their IP address on a browser, they will see their local IP address, not the IP address of the ASA.

To change this behavior, you need to configure the Group Policy on the ASA to tunnel all networks, which means that all traffic from the SSL VPN clients will go through the VPN tunnel, regardless of the destination. This way, when they search for their IP address on a browser, they will see the IP address of the ASA, which is 3.3.3.3.

To configure tunnel all networks under Group Policy, you can use either ASDM or CLI. For example, using ASDM, you can follow these steps1:

Choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies.

Select the group policy that you want to modify and click Edit.

In the Edit Internal Group Policy window, choose Advanced > Split Tunneling.

In the Policy drop-down list, choose Tunnel All Networks.

Click OK and then Apply.

Using CLI, you can enter these commands:

ciscoasa(config)# group-policy <group_policy_name> attributes ciscoasa(config-group-policy)# split tunnel-policy tunnelall

Question: 49

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

Explanation:

Question: 50

Refer to the exhibit.

```
crypto isakrap policy 10 encr aes 256 hash sha256
 authentication pre-share group 14

crypto isakmp key cisco address 0.0.0.0

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

```
crypto ipsec profile CCNP set transform-set TS

interface Tunnell
 ip address 10.0.0.1 255.255.255.0
 tunnel source GigabitEthernetl
 tunnel mode ipsec ipv4
 tunnel destination 172.18.10.2
 tunnel protection ipsec profile CCNP
```

Which VPN technology is used in the exhibit?

A. DVTI
B. VTI
C. DMVPN
D. GRE

Answer: B

Explanation:
https://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd8029d629.html

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/zZ- Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

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

Explanation:

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

Explanation:

NHRP network IDs are locally significant and can be different. It makes sense from a deployment and maintenance perspective to use unique network ID numbers (using the ip nhrp network-id command) across all routers in a DMVPN network, but it is not necessary that they be the same.
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-dmvpn.html

Question: 53

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

Answer: C

Explanation:

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

Question: 54

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

Question: 55

Which benefit of FlexVPN is a limitation of DMVPN using IKEv1?

A. GRE encapsulation allows for forwarding of non-IP traffic.
B. IKE implementation can install routes in routing table.
C. NHRP authentication provides enhanced security.
D. Dynamic routing protocols can be configured.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec- flex-vpn-15-mt-book/sec-flex-spoke.html

Question: 56

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

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: A

Explanation:

https://www.cisco.com/c/en/us/support/docs/routers/3600-series-multiservice-platforms/91193- rtr-ipsec-internet-connect.html

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: A

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/216276-configure-route-based-site-to-site-vpn-t.html#anc6

Question: 59

Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

A. sequence numbers that enable scalable replay checking
B. enabled use of ESP or AH
C. design for use over public or private WAN
D. no requirement for an overlay routing protocol

Answer: D

Explanation:
one benefit of GET VPN is Simplified network design due to leveraging of native routing infrastructure (no overlay routing protocol needed) f mismatch is causing the problem with the IPsec VPN

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

Explanation:

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

Topic 5, Mixed Questions

Question: 61

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: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general- cli/acl-webtype.pdf

Question: 62

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

Explanation:

Question: 63

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

Explanation:

Question: 64

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

Explanation:

Question: 65

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

Explanation:

Question: 66

Refer to the exhibit.

```
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 l.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
```

Which type of Cisco VPN is shown for group Cisc012345678?

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

Answer: A

Explanation:
https://learningnetwork.cisco.com/s/question/0D53i00000Q4COCCA3/anyconnect-ssl-vpn

Question: 67

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

Explanation:

The following table lists the commands that are enabled with the IKEv2 Smart Defaults feature, along with the default values.

Device# show crypto ipsec profile default

IPSEC profile default
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N): N
PFS (Y/N): N
Transform sets={
default: { esp-aes esp-sha-hmac },
}

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-ikev2-flex.html

Question: 68

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.

```
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

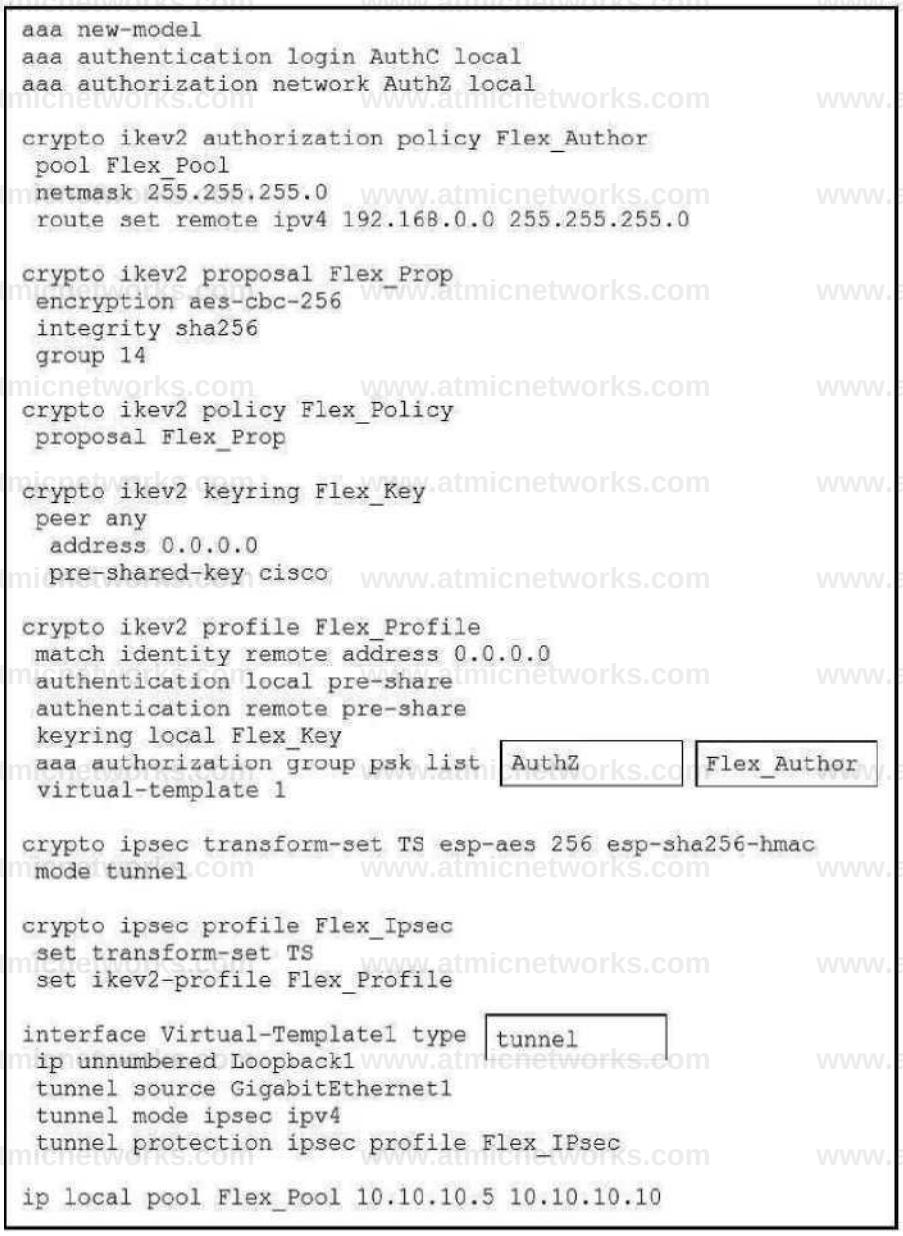
Flex_Author

0.0.0.0

tunnel

Answer:

Explanation:



Question: 69

Refer to the exhibit.

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 Tunnell
  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 GigabitEthernetl
  tunnel mode gre multipoint
  tunnel protection ipsec profile CCNP


interface GigabitEthernetl
  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 172.16.16.1

interface Tunnell
   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 GigabitEthernetl
   tunnel mode gre multipoint
   tunnel protection ipsec profile CCNP

interface GigabitEthernetl
   ip address 172.16.18.2 255.255.255.0
```

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

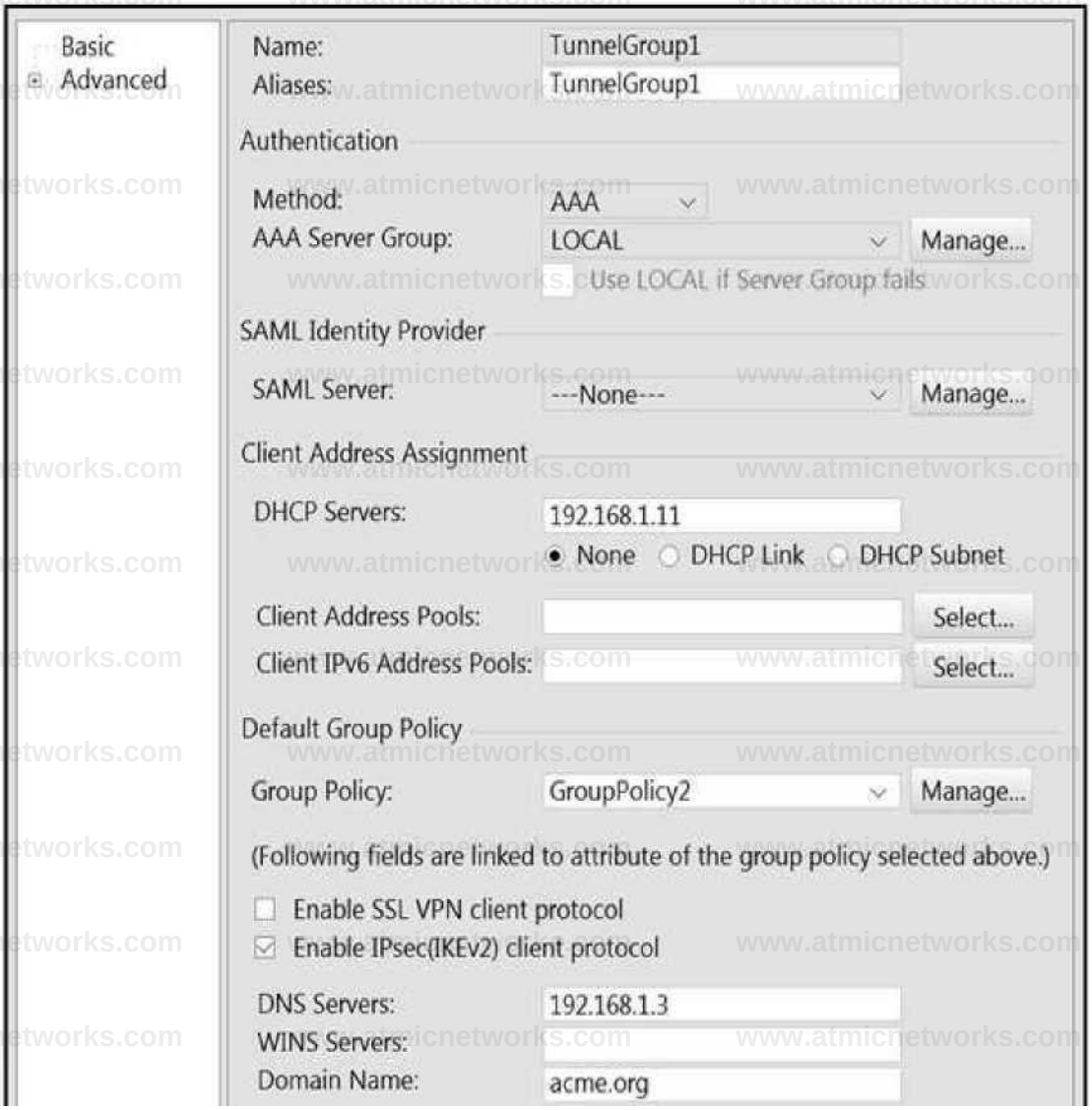
A. Change the spoke nhs to 172.16.18.1 and the nbma to 10.0.0.1.
B. Change the transform set to mode tunnel.
C. Change the ISAKMP policy authentication on the spoke to pre-shared.
D. Change the ISAKMP key address on the spoke to 0.0.0.0.
E. Change the nhrp authentication key on the spoke to cisco123.

Answer: CE

Explanation:

Question: 70

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?

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

Explanation:

Question: 71

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

Explanation:

NHRP redirect is a function that allows the hub to inform the source spoke of a better path to reach the destination spoke, by sending an NHRP redirect message containing the IP address of the destination spoke. This triggers the source spoke to send an NHRP resolution request to the destination spoke, in order to establish a direct spoke-to-spoke tunnel1.

NHRP resolution reply is a function that allows the destination spoke to respond to the NHRP resolution request from the source spoke, by sending an NHRP resolution reply containing its own IP address and the IP address of the source spoke. This confirms the establishment of the direct spoke- to-spoke tunnel, and also allows the destination spoke to create a reciprocal tunnel to the source spoke2.

These two functions are specific to DMVPN Phase 3, because they enable spoke-to-spoke communication without requiring a dynamic routing protocol or going through the hub. In DMVPN Phase 1 and Phase 2, NHRP registration request, registration reply, and resolution request are also used, but they have different purposes and effects3.

Question: 72

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?

O 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

OB 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

'-' $ 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

A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

"ensures all traffic from the client passes through the ASA" that is one of the requirements. Meaning all traffic should

pass through the tunnel, I know they mention 192.168.0.0 network but that is just to confuse.

Question: 73

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

Explanation:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg- flex-clnt.html#GUID-CA7D6429-5F13-4CB9-BE2E-EDFCFB3792B3

Question: 74

Refer to the exhibit.

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

Which type of VPN is used?

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

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn- config/vpn-easyvpn.html

Question: 75

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 LocalAuthzOl

route set local ipv4 10.10.0.0 0.0.255.255

B

crypto ikev2 authorization policy Local Authz Ol

route set access-list Secured_Routes

ip access-list extended SecuredRoutes

permit ip any 10.10.0.0 0.0.255.255

crypto ikevl authorization policy Local Authz Ol

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

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:

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-serv.html

Question: 76

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

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/pix-500-series-security-appliances/99103- pix-asa-vpn-filter.html#anc6

Question: 77

Refer to the exhibit.

```
interface: TunnelO
  Crypto map tag: TunnelO—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,)
    Ipkts encaps: 16228, #pkts encrypt: 16228, Ipkts digest: 16228
    Ipkts decaps: 26773, Ipkts decrypt: 26773, #pkts verify: 26773
    #pkts compressed: 0, #pkts decompressed: 0
    Ipkts not compressed: 0, Ipkts compr. failed: 0
    Ipkts not decompressed: 0, Ipkts decompress failed: 0
    Ipkts no sa (send) 0, Ipkts invalid sa (rev) 0
    Ipkts encaps failed (send) 0, Ipkts decaps failed (rev) 0
    ♦pkts invalid prot (reev) 0, #pkts verify failed: 0
    Ipkts invalid identity (reev) 0, Ipkts invalid len (rev) 0
    Ipkts replay rollover (send): 0, Ipkts replay rollover (rev) 0
    llpkts replay failed (rev): 23751
    ♦pkts tagged (send): 0, Ipkts untagged (rev): 0
    Ipkts not tagged (send): 0, Ipkts not untagged (rev): 0
    Ipkts internal err (send): 0, Ipkts internal err (reev) 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.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xe-16-8/sec- ipsec-data-plane-xe-16-8-book/sec-ipsec-antireplay.html#GUID-1FF00FBB-0746-48B2-A02A- 2BB066BEDEF8

Question: 78

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

Explanation:
https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc15:~:text=simultaneous%2Dlogins%2020-,WebVPN%20Clients%20Cannot%20Hit%20Bookmarks%20and%20is%20Grayed%20Out,-Problem

Question: 79

Refer to the exhibit.

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

Which type of VPN is being configured, based on the partial configuration snippet?

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

Answer: A

Explanation:

Question: 80

An administrator is designing a VPN with a partner's non-Cisco VPN solution. The partner's VPN device will negotiate an IKEv2 tunnel that will only encrypt subnets 192.168.0.0/24 going to 10.0.0.0/24. Which technology must be used to meet these requirements?

A. VTI
B. crypto map
C. GETVPN
D. DMVPN

Answer: B

Explanation:

Question: 81

A company's remote locations connect to the data centers via MPLS. A new request requires that unicast and multicast traffic that exits in the remote locations be encrypted. Which non-tunneled technology should be used

to satisfy this requirement?

A. SSL
B. FlexVPN
C. DMVPN
D. GETVPN

Answer: D

Explanation:

Question: 82

While troubleshooting, an engineer finds that the show crypto isakmp sa command indicates that the last state of the tunnel is MM_KEY_EXCH. What is the next step that should be taken to resolve this issue?

A. Verify that the ISAKMP proposals match.
B. Ensure that UDP 500 is not being blocked between the devices.
C. Correct the peer's IP address on the crypto map.
D. Confirm that the pre-shared keys match on both devices.

Answer: D

Explanation:
https://www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.html

Question: 83

Which VPN technology must be used to ensure that routers are able to dynamically form connections with each other rather than sending traffic through a hub and be able to advertise routes without the use of a dynamic routing protocol?

A. FlexVPN
B. DMVPN Phase 3
C. DMVPN Phase 2
D. GETVPN

Answer: B

Explanation:
DMVPN stands for Dynamic Multipoint VPN, which is a technology that allows routers to dynamically form VPN tunnels with each other without requiring a pre-configured static crypto map. DMVPN uses Multipoint GRE (mGRE) interfaces and Next Hop Resolution Protocol (NHRP) to establish direct connections between routers. DMVPN has three phases of operation, each with different features and benefits.
DMVPN Phase 1 is the basic configuration, where all spokes are configured with a single mGRE interface that points to the hub as the NHRP server. The spokes can only communicate with the hub, not with each other. All traffic must go through the hub, which creates a bottleneck and increases latency.
DMVPN Phase 2 improves on Phase 1 by allowing spoke-to-spoke communication without going through the hub. This is achieved by using NHRP to dynamically resolve the IP address of the destination spoke and create a direct GRE tunnel between the spokes. However, this still requires the use of a dynamic routing protocol to advertise routes between the spokes, which adds overhead and complexity.

DMVPN Phase 3 further enhances Phase 2 by enabling spoke-to-spoke communication without requiring a dynamic routing protocol. This is done by using NHRP shortcut switching and NHRP redirect messages. When a spoke wants to send traffic to another spoke, it sends an NHRP resolution request to the hub, which responds with an NHRP redirect message containing the IP address of the destination spoke. The source spoke then creates a direct GRE tunnel with the destination spoke and switches the traffic to the new tunnel. The hub also sends an NHRP resolution reply to the destination spoke, informing it of the source spoke's IP address. The destination spoke then creates a direct GRE tunnel with the source spoke and switches the traffic to the new tunnel. This way, the spokes can communicate directly without using a dynamic routing protocol or going through the hub.

Question: 84

An administrator is setting up AnyConnect for the first time for a few users. Currently, the router does not have access to a RADIUS server. Which AnyConnect protocol must be used to allow users to authenticate?

A. EAP-GTC
B. EAP-MSCHAPv2
C. EAP-MD5
D. EAP-AnyConnect

Answer: D

Explanation:

Question: 85

Refer to the exhibit.

```
interface Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp map multicast dynamic
ip nhrp network-id 1
no ip split-horizon eigrp 90
ip next-hop-self eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
```

DMVPN spoke-to-spoke traffic works, but it passes through the hub, and never sends direct spoke-to- spoke traffic. Based on the tunnel interface configuration shown, what must be configured on the hub to solve the issue?

A. Enable NHRP redirect.
B. Enable split horizon.
C. Enable IP redirects.

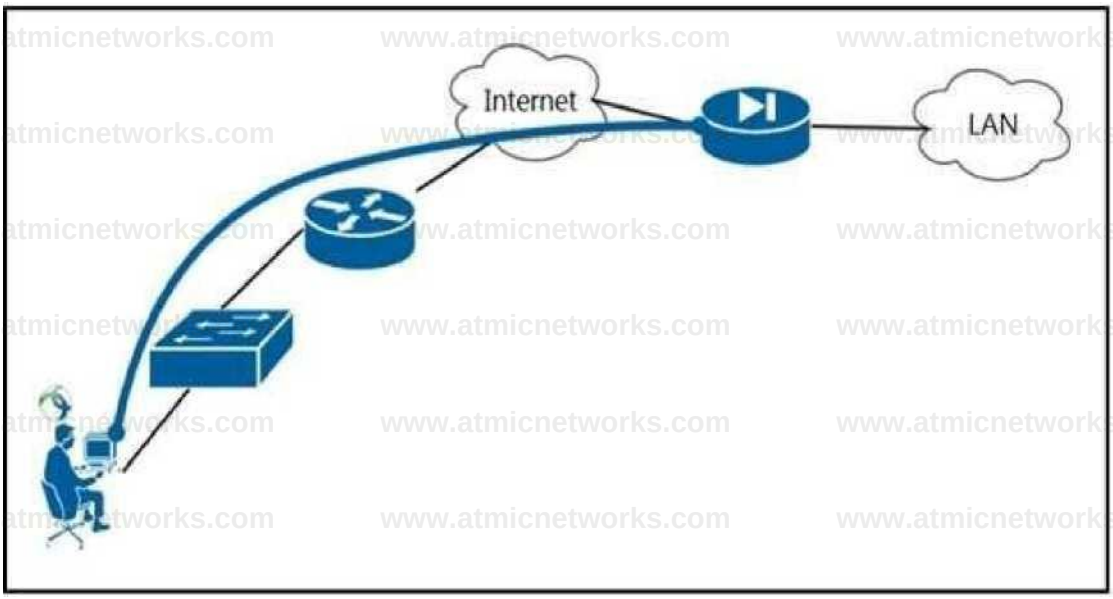
D. Enable NHRP shortcut.

Answer: A

Explanation:

Question: 86

Refer to the exhibit.



A user is connecting from behind a PC with a private IP Address. Their ISP provider is blocking TCP port 443. Which AnyConnect XML configuration will allow the user to establish a connection with the ASA?

```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.202.129</HostAddress>
  < PrimaryProtocol >IPsec
    <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
  </PrimaryProtocol>
</HostEntry>
```

B
```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.200.225</HostAddress>
  <PrimaryProtocol>IPsec
    <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
  </PrimaryProtocol>
</HostEntry>
```

L <HostEntry>
<HostName>RAVPN</HostName>
< HostAddress >209.165.202.129 </HostAddress>
</HostEntry>

D <HostEntry>
<HostName>RAVPN</HostName>
< HostAddress >209.165.200.225 </HostAddress>
</HostEntry>

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Explanation:

Question: 87

Refer to the exhibit.

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
ip mtu 1440
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 150
no ip split-horizon eigrp 100
no ip next-hop-self eigrp 100
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
```

Which two conclusions should be drawn from the DMVPN phase 2 configuration? (Choose two.)

A. Next-hop-self is required.
B. EIGRP neighbor adjacency will fail.
C. EIGRP is used as the dynamic routing protocol.

D. EIGRP route redistribution is not allowed.

E. Spoke-to-spoke communication is allowed.

Answer: CE

Explanation:

The premise is that we are looking at a DMVPN phase 2 configuration. That means that spoke-to- spoke traffic should be allowed. Remember that phase 2 requires the "no ip next-hop-self" command with EIGRP

Question: 88

Refer to the exhibit.

```
aaa authentication login default local
aaa authorization network Flex AAA local

crypto ikev2 authorization policy Flex_Auth
 route set remote ipv4 10.0.0.0 255.255.255.0

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

crypto ikev2 policy Crypto_Policy
 proposal Crypto_Proposal

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

crypto ikev2 profile IKEv2 Profile
 match identity remote address 192.168.0.12 255.255.255.255 authentication local pre-share
 authentication remote pre-share
 keyring local FlexKey
 aaa authorization group cert list Flex AAA Flex Auth
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac mode tunnel

crypto ipsec profile FlexVPN_Ipsec
 set transform-set TS
 set ikev2-profile IKEv2_Profile

interface Tunnell
 ip address negotiated
 tunnel source GigabitEthernetl
 tunnel mode ipsec ipv4
 tunnel destination 192.168.0.12
 tunnel protection ipsec profile FlexVPN Ipsec
```

The VPN tunnel between the FlexVPN spoke and FlexVPN hub 192.168.0.12 is failing. What should be done to correct this issue?

A. Add the address 192.168.0.12 255.255.255.255 command to the keyring configuration.
B. Add the match fvrf any command to the IKEv2 policy.
C. Add the aaa authorization group psk list Flex_AAA Flex_Auth command to the IKEv2 profile configuration.
D. Add the tunnel mode gre ip command to the tunnel configuration.

Answer: C

Explanation:

Question: 89

Refer to the exhibit.

```
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed policies
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy found for received TS

*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001
CurState: R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```

An IKEv2 site-to-site tunnel between an ASA and a remote peer is not building successfully. What will fix the problem based on the debug output?

A. Ensure crypto IPsec policy matches on both VPN devices.
B. Install the correct certificate to validate the peer.
C. Correct crypto access list on both VPN devices.
D. Specify the peer IP address in the tunnel group name.

Answer: C

Explanation:

To fix the problem with the IKEv2 site-to-site tunnel between an ASA and a remote peer based on the debug output, you should ensure that the crypto IPsec policy matches on both VPN devices. The debug output indicates that the crypto policies on the two VPN devices are mismatched, which is preventing the tunnel from building successfully. Installing the correct certificate to validate the peer, correcting the crypto access list on both VPN devices, and specifying the peer IP address in the tunnel group name will not fix the problem.

Question: 90

Refer to the exhibit.

```
webvpn
  port 9443
  enable outside
  dtls port 9443
  anyconnect-essentials
  anyconnect image diskO:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
  anyconnect profiles vpn profile 1 diskO:/vpn profile l.xml
  anyconnect enable
  tunnel-group-list enable
  cache
  disable
  error-recovery disable
group-policy vpn_policy internal
group-policy vpn_policy attributes
```

```
dns-server value 192.168.1.3
vpn-tunnel-protocol ssl-client
address-pools value vpn_pool
```

A network engineer is reconfiguring clientless SSLVPN during a maintenance window, and after testing the new configuration, is unable to establish the connection. What must be done to remediate this problem?

A. Enable client services on the outside interface.
B. Enable clientless protocol under the group policy.
C. Enable DTLS under the group policy.
D. Enable auto sign-on for the user's IP address.

Answer: B

Explanation:
https://networksec-solutions.com/cisco-asa-ssl-clientless-vpn/

Question: 91

What are two purposes of the key server in Cisco IOS GETVPN? (Choose two.)

A. to download encryption keys
B. to maintain encryption policies
C. to distribute routing information
D. to encrypt data traffic
E. to authenticate group members

Answer: BE

Explanation:
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-GETVPNDesignGuide-AUG14.pdf

Question: 92

An engineer notices that while an employee is connected remotely, all traffic is being routed to the corporate network. Which split-tunnel policy allows a remote client to use their local provider for Internet access when working from home?

A. tunnelall
B. excludeall
C. tunnelspecified
D. excludespecified

Answer: C

Explanation:

Question: 93

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.

Answer: BD

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116032-flexvpn-aaa-config-example-00.html

Question: 94

Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?

A. DMVPN with ISAKMP
B. GETVPN with ISAKMP
C. DMVPN with NHRP
D. GETVPN with NHRP

Answer: C

Explanation:

Question: 95

An engineer must configure remote desktop connectivity for offsite admins via clientless SSL VPN, configured on a Cisco ASA to Windows Vista workstations. Which two configurations provide the requested access? (Choose two.)

A. Telnet bookmark via the Telnet plugin
B. RDP2 bookmark via the RDP2 plugin
C. VNC bookmark via the VNC plugin
D. Citrix bookmark via the ICA plugin
E. SSH bookmark via the SSH plugin

Answer: BC

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/webvpn-configure-gateway.html

Question: 96

A network engineer must design a clientless VPN solution for a company. VPN users must be able to access several internal web servers. When reachability to those web servers was tested, it was found that one website is not being rewritten correctly by the AS

A. What is a potential solution for this issue while still allowing it to be a clientless VPN setup?

A. Set up a smart tunnel with the IP address of the web server.
B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.

C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.
D. Set up a WebACL to permit the IP address of the web server.

Answer: B

Explanation:

Question: 97

Which two types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose two.)

A. SAML
B. NTLM
C. Kerberos
D. OAuth 2.0
E. HTTP Basic

Answer: BE

Explanation:
The auto-signon command is a single sign-on method for users of clientless SSL VPN sessions. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).
https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/vpn/asa-916-vpn- config/webvpn-configure-policy-groups.html#ID-2439-00001438

Question: 98

Refer to the exhibit.

```
hostname RouterA
interface GigabitEthernet 0/0/0
ip address 10.0.0.1 255.255.255.0
standby 1 priority 110
standby ikev1-cluster
end

crypto ikev2 cluster
 standby-group ikev1-cluster
 slave max-session 500
 port 2000
 no shutdown

crypto ikev2 redirect gateway init
```

Which type of VPN implementation is displayed?

A. IKEv1 cluster
B. IKEv2 backup gateway
C. IKEv2 load balancer
D. IKEv2 reconnect

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-10/sec- flex-vpn-xe-16-10-book/sec-cfg-clb-supp.html

Question: 99

A network engineer is setting up a clientless SSLVPN on a Cisco AS

A. Remote users must be able to access an internal webserver via the URL example.com. Which two steps accomplish this task? (Choose two.)

A. Configure a bookmark for the webserver.
B. Configure routing so that the user's computer can reach the webserver.
C. Configure a DNS server that can resolve the webserver URL.
D. Configure a browser plugin on the Cisco ASA.
E. Configure routing so that the Cisco ASA can reach the webserver.

Answer: A, C

Explanation:

Question: 100

A network engineer has set up a FlexVPN server to terminate multiple FlexVPN clients. The VPN tunnels are established without issue. However, when a Change of Authorization is issued by the RADIUS server, the FlexVPN server does not update the authorization of connected FlexVPN clients. Which action resolves this issue?

A. Add the aaa server radius dynamic-author command on the FlexVPN clients.
B. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN server.
C. Add the aaa server radius dynamic-author command on the FlexVPN server.
D. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN clients.

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-10/sec- flex-vpn-xe-16-10-book/sec-ikev2-flex-coa.html

Question: 101

A company needs to ensure only corporate issued laptops and devices are allowed to connect with the Cisco AnyConnect client. The solution should be applicable to multiple operating systems, including Windows, MacOS, and Linux, and should allow for remote remediation if a corporate issued device is stolen. Which solution should be used to accomplish these goals?

A. Use a DAP registry check on the system to determine the relationship with the corporate domain.
B. Use a DAP file check on the system to determine the relationship with the corporate domain.
C. Install and authenticate user certificates on the corporate devices.
D. Install and authenticate machine certificates on the corporate devices

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/vpn/asdm-78-vpn-config/vpn- asdm-dap.html#ID-2184-00000017

Question: 102

When a FlexVPN is configured, which two components must be configured for IKEv2? (Choose two.)

A. method
B. profile
C. proposal
D. preference
E. persistence

Answer: B, C

Explanation:

https://www.cisco.com/c/en/us/support/security/flexvpn/products-configuration-examples-list.html

Question: 103

A DMVPN spoke router tunnel is up and passing traffic, but it cannot establish an EIGRP neighbor relationship with the hub router. Which solution resolves this issue?

A. Enable EIGRP Split Horizon on the hub tunnel interface.
B. Remove the EIGRP stub configuration on the spoke tunnel interface.
C. Enable the EIGRP next hop self feature on the hub tunnel interface.
D. Configure the dynamic NHRP multicast map on the hub tunnel interface.

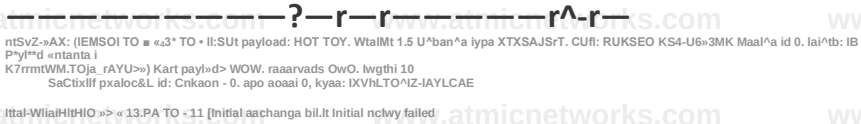
Answer: D

Explanation:

DMVPN is an NBMA network, which doesn't support multicast at all. The only reason we can get it working to the hub is because of the nhrp multicast command we add to the tunnel interface.

Question: 104

Refer to the exhibit.



An IPsec Cisco AnyConnect client is failing to connect and generates these debugs every time a connection to an IOS headend is attempted. Which action resolves this issue?

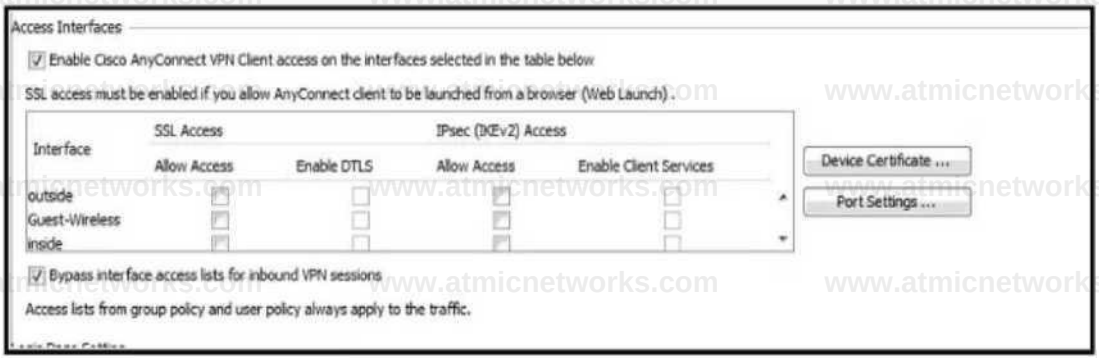
A. Correct the DH group setting.
B. Correct the PFS setting.
C. Correct the integrity setting.
D. Correct the encryption setting.

Answer: A

Explanation:

Question: 105

Refer to the exhibit.



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.

Answer: A, D

Explanation:

Question: 106

Refer to the exhibit.

```
vrr dct>nibc^v5li>»
    rd 1:1
    route-target import 1:1
    route-target Import 1 1 route-target
    Import 10 10

interlace TunnelO vrt forwarding Yeeow
    Ip address 10 0 0 1 256.255.256.0
    Ip nhrp network-Id too
     Ip nhrp authentication Vallow no ip
    Iplil-horiton eigrp 1 tunnel key ICO

interface EtbcmetO.O vrt forwarding
    Yudow
    Ip address 192 1W0 1 255 266 256 0

router eigrp 1

    address-family Ipv4 vrt Yedow
       NdKNriMt boo t
       network 110.0.0 0 0 0.255
       network 192 1M0 0 exit-add toss-
    family
!
routar ogp 1

    address-family ipv4 vrt Yoflow
       redistribute connected redisirteute
       eigrp t
    exit-address-family
```

```
vrt dcriniuonTted^ rd 2 J
    route-target export 2.2
    route-target Import 2 2
    route-target Import 1# 10

interlace Tunnd2 vrt forwarding Red
    ipaddress 10 0 2 1 255 255 255 0 ip
    rthrp network-rd 102 ip nhrp
    authentication Red no ip spiit homon
    eigrp 1 tunnel key 102

interlace Ethernet1/0 vrt forwarding Red
    ip address 192 160 2 1 266 256 255 0
!
router eigrp 1

    address-family Ipv4 vrt Red
       redteinbvte bop 1 network 100.2 0
       00.0 255 network 192 1 60 2 0
    exit-addross-famdy

route! bgp 1

    address-family ipv4 vrt Rad
       redistribute connected redistribute
       eigrp 1
    exit-address-family
```

```
vrt dtfirutionuroJn^
    rd 3 3
    route-target Import 3.3
    route-target Import j 3
    route-target Import 1010

Interface Tunncl4
    vrt forwarding Croon
    ipaddress 10 0 4'255 255 255 0
    ip nhrp network-Id 104
     ip nhrp authentication Omen no ip
    spllt-boriton eigrp 1 tunnel key 104

interface Ethernci2O
    vrt forwarding Green
    ■paddross 192 119 4 1 265 255 256 0

router eigrp 1

    address-family Ipv4 vrt Orenn
       redistribute bgp 1 network 10 0 4 0 0
       0.0.255 network 192.1M A0
    exit -address -fa mily

router Opp 1

    address-family Ipv4 vrt Groon
       redistribute connected redistribute
       eigrp 1
    exit-address-family
```

Based on the configuration output, what is the VPN technology?

A. site-to-site
B. DMVPN

C. L2VPN
D. multicast VPN

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14122-24.html#configs

Question: 107

A user at a company HQ is having trouble accessing a network share at a branch site that is connected with a L2L IPsec VPN. While troubleshooting, a network security engineer runs a packet tracer on the Cisco ASA to simulate the user traffic and discovers that the encryption counter is increasing but the decryption counter is not. What must be configured to correct this issue?

A. Adjust the routing on the remote peer device to direct traffic back over the tunnel.
B. Adjust the preshared key on the remote peer to allow traffic to flow over the tunnel.
C. Adjust the transform set to allow bidirectional traffic.
D. Adjust the peer IP address on the remote peer to direct traffic back to the ASA.

Answer: A

Explanation:

Question: 108

A user is experiencing delays on audio calls over a Cisco AnyConnect VPN. Which implementation step resolves this issue?

A. Change to 3DES Encryption.
B. Shorten the encryption key lifetime.
C. Install the Cisco AnyConnect 2.3 client for the user to download.
D. Enable DTLS.

Answer: D

Explanation:

Question: 109

Users cannot log in to a Cisco ASA using clientless SSLVPN. Troubleshooting reveals the error message "WebVPN session terminated: Client type not supported". Which step does the administrator take to resolve this issue?

A. Enable the Cisco AnyConnect premium license on the Cisco ASA.
B. Have the user upgrade to a supported browser.
C. Increase the simultaneous logins on the group policy.

D. Enable the clientless VPN protocol on the group policy.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa- 00.html#anc15

Question: 110

An administrator is setting up a VPN on an ASA for users who need to access an internal RDP server. Due to security restrictions, the Microsoft RDP client is blocked from running on client workstations via Group Policy. Which VPN feature should be implemented by the administrator to allow these users to have access to the RDP server?

A. clientless proxy
B. smart tunneling
C. clientless plug-in
D. clientless rewriter

Answer: C

Explanation:

Question: 111

An administrator is planning a VPN configuration that will encrypt traffic between multiple servers that will be passing unicast and multicast traffic. This configuration must be able to be implemented without the need to modify routing within the network. Which VPN technology must be used for this task?

A. FlexVPN
B. VTI
C. GETVPN
D. DMVPN

Answer: C

Explanation:

The VPN technology that must be used for this task is GETVPN (Group Encrypted Transport VPN). GETVPN is designed to encrypt both unicast and multicast traffic while preserving the original source and destination IP addresses, and it does not require any changes to the existing routing infrastructure. Additionally, GETVPN provides a scalable and efficient solution for encrypting traffic within a network, making it a good choice for this scenario.

Question: 112

Refer to the exhibit.

```
Router#show crypto isakmp sa

IPv4 Crypto ISARMP SA
Dst             src             state          conn-id    slot      status
10.10.10.1      172.IC.1.1      *<_NO_STATE    0          0         ACTIVE
10.10.10.1      172.16.1.1      WLNOSTATE      0          0         ACTIVE (deleted)
172.IT.0.5      172.16.1.1      MH NO STATE    0          0         ACTIVE
172.17.0.5      172.16.1.1      M< HO STATE    0          0         ACTIVE (deleted)

  01:12:45.250: ISAKMP:(0):01d State = IKE_READY New State - IRE_I_MM1
  01:12:45.250: ISAKMP:(0): beginning Hain Mode exchange 01:12:45.250: ISAKHP:(0): sending packet to 10.10.10.1
          ayport 500 peerport 500 (I) MM_NO_STATE 01:12:45.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:12:55.250: ISARMP:(0): retransaitting phase 1 MH_NO_STATE. 01:12:55.250: ISAKMP (0:0): increaenting error counter on
sa, attempt 1 of 5: retransmit phase 1 01:12:55.250: ISAKMP:(0): retransmitting phase 1 HH_NO_STATE 01:12:55.250:
ISARMP:(0): sending packet to 10.10.10.1
          my port 500 peer port 500 (I) MMNOSTATE 01:12:55.250: ISAKMP:(0):Sending an IRE IPv4 Packet.
01:13:04.250: ISARMP:(0): retransmitting phase 1 MMNOSTATE. 01:13:04.250: ISAKMP:(0): retransmitting phase 1
MM_NO_STATE. 01:13:04.250: ISAKMP (0:0): incrementing error counter on sa, attempt 2 of 5: retransmit phase 1 01:13:04.250:
ISAKMP:(0): retransmitting phase 1 MMNOSTATE
```

VPN tunnels between a spoke and two DMVPN hubs are not coming up. The network administrator has verified that the encryption, hashing, and DH group proposals for Phase 1 and Phase 2 match on both ends. What is the solution to this issue?

A. Ensure bidirectional UDP 500/4500 traffic.
B. Increase the isakmp phase 1 lifetime.
C. Add NAT statements for VPN traffic.
D. Enable shared tunnel protection.

Answer: A

Explanation:

Question: 113

A network engineer is configuring a server. The router will terminate encrypted VPN connections on g0/0, which is in the VRF "Internet". The clear-text traffic that must be encrypted before being sent out traverses g0/1, which is in the VRF "Internal". Which two VRF-specific configurations allow VPN traffic to traverse the VRF-aware interfaces? (Choose two.)

A. Under the IKEv2 profile, add the ivrf Internal command.
B. Under the virtual-template interface, add the ip vrf forwarding Internet command.
C. Under the IKEv2 profile, add the match fvrf Internal command.
D. Under the IKEv2 profile, add the match fvrf Internet command.
E. Under the virtual-template interface, add the tunnel vrf Internet command.

Answer: DE

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116000-flexvpn-config-00.html crypto ikev2 profile CProfile
match fvrf internet // ("out vrf")
...

virtual-template 1

...

interface virtual-template 1 type tunnel

vrf forwarding internal // (internal vrf)

...

tunnel vrf internet // (out vrf)

Question: 114

What is a characteristic of GETVPN?

A. An ACL that defines interesting traffic must be configured and applied to the crypto map.
B. Quick mode is used to create an IPsec SA.
C. The remote peer for the IPsec session is configured as part of the crypto map.
D. All peers have one IPsec SPI for inbound and outbound communication.

Answer: D

Explanation:

In GETVPN, all group members share a common security association (SA) database and the same keys for encryption and decryption. This approach avoids the need for per-peer IPsec SAs and simplifies the configuration and management of the VPN. Instead of using multiple SAs, GETVPN uses a single SA with a unique Group Domain of Interpretation (GDOI) group key that is distributed to all group members.

Question: 115

Refer to the exhibit.

```
group-pohcy My_GroupPolicy internal
group-pohcy My_GroupPohcy attributes
 vpn-tunnel-protocol I2tp ipsec

[redacted]
webvpn
    svc enable
    svc keep-installer installed
    svc rekey lime 30
    svc rekey method ssl

 http server enable 8080
 i
tunnel-group My_WebVPN general-attributes
 addresspool MyPool
```

default-group-pohcy 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.

Answer: D

Explanation:

Question: 116

An administrator must guarantee that remote access users are able to reach printers on their local LAN after a VPN session is established to the headquarters. All other traffic should be sent over the tunnel. Which split-tunnel policy reduces the configuration on the ASA headend?

A. include specified B. exclude specified C. tunnel specified D. dynamic exclude

Answer: B

Explanation:

You could in theory "tunnel specified" and list every subnet aside from the local one in the split tunnel list, but that is cumbersome and clearly not the best answer from the "reduce the configuration" requirement. Exclude only the local subnet and continue with your day.

Question: 117

Refer to the exhibit.

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, s|u - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * • candidate default. U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP a - application route + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

172.16. 0.0/16 is variably subnetted. 8 subnets, 2 masks
B 172.16.0.0/16 [200/0] via 172.16.1.1, 00:06:27
H 172.16.0.1/32 is directly connected, 00:06:38, Tunnel2
S % 172.16.1.1/32 is directly connected, Tunnel7
C 172.16.1.3/32 is directlyconnected, Tunnel7
H 172.16.1.4/32 is directlyconnected, 00:01:30, Virtual-Access 10
S 172.16.2.1/32 is directlyconnected, Tunnel2
C 172.16.2.3/32 is directlyconnected, Tunnel2
H 172.16.2.4/32 [250/1] via 172.16 2.3,00:01:30, Virtual-AccesslO
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, EthernetO/1
L 192.168.1.3/32 is directly connected, EthernetO/1
172.17. .4.0/32 is subnetted, 1 subnets
H 192.168.4.4 [250/1] via 172.16.1.3, 00:01:30, Virtual-AccesslO

Given the output of the show ip route command, which remote access VPN technology is in use?

A. Reverse Route Injection
B. FlexVPN
C. Dynamic Crypto Map
D. DMVPN

Answer: B

Explanation:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex- spoke.html

Question: 118

A network engineer is installing Cisco AnyConnect on company laptops so that users can access corporate resources remotely. The VPN concentrator is a Cisco router running IOS-XE 16.9.1 code and configured as a FlexVPN server that uses local authentication and *$Cisc431089017$* as the key-id for the IKEv2 profile. Which two steps must be taken on the computer to allow a successful AnyConnect connection to the router? (Choose two.)

A. In the Cisco AnyConnect XML profile, set the IPsec Authentication method to EAP-AnyConnect.
B. In the Cisco AnyConnect XML profile, add the hostname and host address to the server list.

C. In the Cisco AnyConnect XML profile, set the user group field to DefaultAnyConnectClientGroup.
D. In the Cisco AnyConnect Local Policy, set the BypassDownloader option in the local to true.
E. In the Cisco AnyConnect Local Policy, add the router IP address to the Update Policy.

Answer: BE

Explanation:

B. In the Cisco AnyConnect XML profile, adding the hostname and host address to the server list ensures that the AnyConnect client knows the address of the VPN concentrator (router) to connect to. E. In the Cisco AnyConnect Local Policy, adding the router IP address to the Update Policy allows the client to connect to the router for updates and configuration.

Question: 119

A network engineer is setting up Cisco AnyConnect 4.9 on a Cisco ASA running ASA software 9.1. Cisco AnyConnect must connect to the Cisco ASA before the user logs on so that login scripts can work successfully. In addition, the VPN must connect without user intervention. Which two key steps accomplish this task? (Choose two.)

A. Create a Network Access Manager profile with a client policy set to connect before user logon.
B. Create a Cisco AnyConnect VPN profile with Start Before Logon set to true.
C. Issue an identity certificate to the trusted root CA folder in the machine store.
D. Create a Cisco AnyConnect VPN profile with Always On set to true.
E. Create a Cisco Anyconnect VPN Management Tunnel profile.

Answer: B, C

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa- software/215442-configure-anyconnect-management-vpn-tunn.html

Question: 120

A network engineer has almost finished setting up a clientless VPN that allows remote users to access internal HTTP servers. Users must enter their username and password twice: once on the clientless VPN web portal and again to log in to internal HTTP servers. The Cisco ASA and the HTTP servers use the same Active Directory server to authenticate users. Which next step must be taken to

allow users to enter their password only once?

A. Use LDAPS and add password management to the clientless tunnel group.
B. Configure auto-sign-on using NTLM authentication.
C. Set up the Cisco ASA to authenticate users via a SAML 2.0 IDP.
D. Create smart tunnels for the HTTP servers.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa- 00.html#anc17

Question: 121

What must be configured in a FlexVPN deployment to allow for direct communication between spokes connected to different hubs?

A. EIGRP must be used as routing protocol.
B. Hub routers must be on same Layer 2 network.
C. Load balancing must be disabled.
D. A GRE tunnel must exist between hub routers.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/118888-configure-flexvpn-00.html

Question: 122

Refer to the exhibit.

```
Flex-spoke#crypto ikev2 authorization policy default
 route set interface
 route set remote ipv4 192.168.200.0 255.255.255.0

Flex-spoke#crypto ikev2 profile default
 aaa authorization group psk list default default
!--- Output is truncated ---!

Flex-spoke#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local            Remote           fvrf/ivrf        Status
1      10.0.20.41/500      172.18.3.143/500     none/none        READY
    Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: RSA
    Life/Active Time: 86400/6845 sec
    CE id: 1043, Session-id: 22
    Status Description: Negotiation done
    Local spi: 3413E984EC151E8D      Remote spi: 92479BD873F59132
    Local id: 10.0.20.41
    Remote id: hostname=flex-hub.cisco.com,cn=flex-hub.cisco.com
    Local req msg id:  0          Remote req msg id:  4
    Local next msg id: 0          Remote next msg id: 4
    Local req queued:  0          Remote req queued:  4
    Local window:      5          Remote window:      5
    DPD configured for 60 seconds, retry 2
    NAT-T is not detected
    Cisco Trust Security SGT is disabled      Initiator of SA : No

    Remote subnets:
    10.0.0.1 255.255.255.255
    192.168.100.0 255.255.255.0

 IPv6 Crypto IKEv2  SA
```

An engineer has configured a spoke to connect to a FlexVPN hub. The tunnel is up, but pings fail when the engineer attempts to reach host 192.168.200.10 behind the spoke, and traffic is sourced from host 192.168.100.3, which is behind the FlexVPN server. Based on packet captures, the engineer discovers that host 192.168.200.10 receives the icmp echo and sends an icmp reply that makes it to the inside interface of the spoke. Based on the output in the exhibit captured on the spoke by the engineer, which action resolves this issue?

A. Add the aaa authorization group cert list default default command to the spoke ikev2 profile. B. Add the route set remote ipv4 192.168.200.0 255.255.255.0 command to the hub authorization policy.

C. Add the aaa authorization group cert list default default command to the hub ikev2 profile.

D. Add the route set remote ipv4 192.168.100.0 255.255.255.0 command to the spoke authorization policy.

Answer: D

Explanation:

The problem is that the spoke does not have a route to the host 192.168.100.3, which is behind the FlexVPN server. The spoke only has a default route to the tunnel interface, which points to the FlexVPN hub. Therefore, when the spoke receives the icmp reply from host 192.168.200.10, it does not know how to forward it to host 192.168.100.3.

One way to solve this problem is to add a route to the host 192.168.100.3 on the spoke using the route set remote ipv4 command in the authorization policy on the spoke. This command allows the FlexVPN server to push a route to the FlexVPN client during IKEv2 authorization. For example: crypto ikev2 authorization policy default route set remote ipv4 192.168.100.0 255.255.255.0 This way, the spoke will have a more specific route to host 192.168.100.3 via the tunnel interface, and will be able to forward the icmp reply correctly.

Question: 123

Which DMVPN feature allows spokes to be deployed with dynamically assigned public IP addresses?

A. 2547oDMVPN
B. NHRP
C. OSPF
D. NAT Traversal

Answer: B

Explanation:

Question: 124

Refer to the exhibit.

```
interface Ethernet0
 nameif outside
 security-level0
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.0.1 255.255.255.0
!
object network InsideNet
subnet 10.7.7.0 255.255.255.0
!
object network RemoteNet
subnet 10.8.8.0 255.255.255.0
!
nat (inside,outside) source static InsideNet InsideNet destination static RemoteNet RemoteNet
!
access-list cmap10 extended permit ip object InsideNet object RemoteNet
!
route outside 0.0.0.0 0.0.0.0 172.16.1.1
!
crypto ipsec ikev1 transform-set AES256 esp-aes-256 esp-sha-hmac
!
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
!
crypto map cmap 10 match address cmap10
crypto map cmap 10 set peer 172.17.1.1
crypto map cmap 10 set ikev1 transform-set AES256
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key Cisco123
```

An engineer is building an IKEv1 tunnel to a peer Cisco ASA, but the tunnel is failing. Based on the configuration in the exhibit, which action must be taken to allow the VPN tunnel to come up?

A. Add a route for the 10.7.7.0/24 network to egress the outside interface.
B. Enable IKEv1 on the outside interface.
C. Change the IKEv1 policy number to be at least 256.
D. Change the transform set mode to transport.

Answer: B

Explanation:

Question: 125

An engineer has successfully established a Phase 1 and Phase 2 tunnel between two sites. Site A has internal subnet 192.168.0.0/24 and Site B has internal subnet 10.0.0.0/24. The engineer notices that no packets are decrypted at Site B. Pings to 192.168.0.1 from internal Site B devices make it to the

Site B router, and the Site A router has incrementing encrypt and decrypt counters. What must be done to ensure bidirectional communication between both sites?

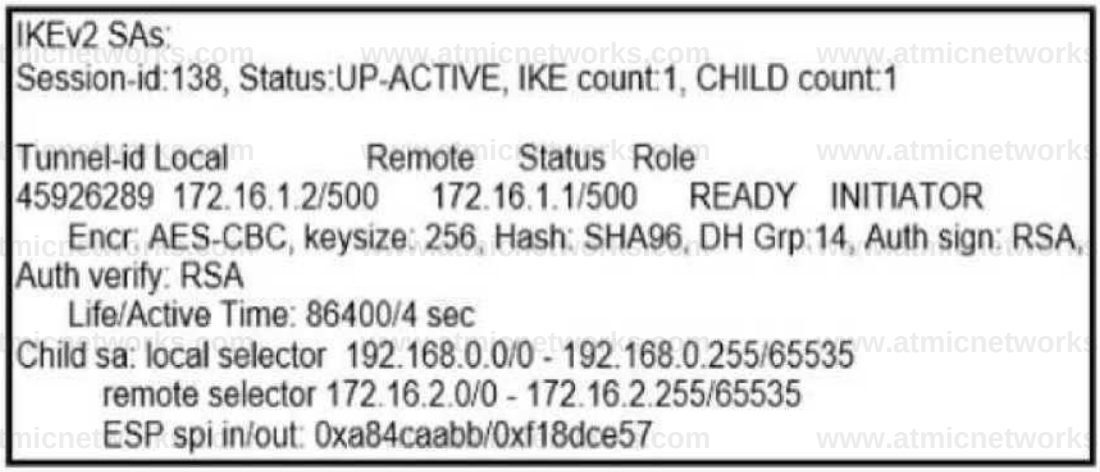
A. Modify the routing at Site B so that traffic is sent to Site A.
B. Configure the correct DH group on both devices.
C. Allow protocol ESP or AH on the firewall in front of the Site B router.
D. Enable PFS on the headend device.

Answer: C

Explanation:

Question: 126

Refer to the exhibit.



A Cisco ASA is configured as a client to a router running as a FlexVPN server. The router is configured with a virtual template to terminate FlexVPN clients. Traffic between networks 192.168.0.0/24 and 172.16.20.0/24 does not work as expected. Based on the show crypto ikev2 sa output collected from the Cisco ASA in the exhibit, what is the solution to this issue?

A. Modify the crypto ACL on the router to permit network 192.168.0.0/24 to network 172.16.20.0/24.
B. Modify the crypto ACL on the ASA to permit network 192.168.0.0/24 to network 172.16.20.0/24. C. Modify the crypto ACL on the ASA to permit network 172.16.20.0/24 to network 192.168.0.0/24. D. Modify the crypto ACL on the router to permit network 172.16.20.0/24 to network 192.168.0.0/24.

Answer: B

Explanation:

the show crypto ukev2 sa output from the ASA, the local selector is 192.168.0.0/24 the remote selector is 172.16.2.0/24 (which is wrong , should be .20.0/24) . so , the ACL in the ASA should be to

permit 192.168.0.0/24 to 172.16.20.0/24

Question: 127

A user is trying to log in to a Cisco ASA using the clientless SSLVPN feature and receives the error message "clientless (browser) SSLVPN access is not allowed". Which step should the Cisco ASA administrator take to resolve this issue?

A. Enable the clientless VPN protocol on the group policy.
B. Validate that the correct license is in use on the ASA for WebVPN.
C. Increase the number of simultaneous logins allowed on the group policy.
D. Verify that a user account exists in the local AAA database for the user.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc12

https://community.cisco.com/t5/vpn/clientless-vpn-clientless-browser-ssl-vpn-access-is-not- allowed/td-p/1569690

Question: 128

Which feature allows a DMVPN Phase 3 spoke to switch to an alternate hub when the primary hub is unreachable?

A. multicast PIM
B. backup NHS
C. per-tunnel jitter probes
D. NHRP shortcut

Answer: B

Explanation:

The DMVPN-Tunnel Health Monitoring and Recovery (Backup NHS) feature allows you to control the number of connections to the Dynamic Multipoint Virtual Private Network (DMVPN) hub and allows you to switch to alternate hubs in case of a connection failure to the primary hubs.

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn- dmvpn-backup-nhs.html#:~:text=The%20DMVPN%2DTunnel%20Health%20Monitoring%20and%20Recovery%20(Backup%20NHS),failure%20to%20the%20primary%20hubs.

Backup NHS, or Next Hop Server, is a feature of DMVPN Phase 3 that allows a spoke router to switch to an alternate hub when the primary hub is unreachable. This is accomplished by using a secondary IP address for the hub router, which is used as the next hop for any traffic sent by the spoke router to the hub.

Question: 129

An engineer is using DMVPN to provide secure connectivity between a data center and remote sites. Which two routing protocols should be used between the routers? (Choose two.)

A. IS-IS
B. BGP
C. RIPv2
D. OSPF
E. EIGRP

Answer: B, E

Explanation:

Question: 130

Which remote access VPN technology requires the use of the IPsec-proposal configuration option?

A. clientless SSLVPN
B. SSLVPN Full Tunnel
C. IKEv2-based VPN
D. IKEv1-based VPN

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn- config/vpn-remote-access.html

The IPsec-proposal configuration option is used to specify the encryption, integrity, and authentication algorithms that will be used in the IPsec protocol. In the case of IKEv2-based VPN, this option is used to configure the IPsec security associations (SA) that will be established between the VPN client and the VPN gateway during IKEv2 negotiation. IKEv2 uses IPsec as its underlying encryption and authentication protocol, so the IPsec-proposal configuration is essential to establishing a secure VPN tunnel using IKEv2

Question: 131

Over the weekend, an administrator upgraded the Cisco ASA image on the firewalls and noticed that users cannot connect to the headquarters site using Cisco AnyConnect. What is the solution for this issue?

A. Upgrade the Cisco AnyConnect client version to be compatible with the Cisco ASA software image. B. Upgrade the Cisco AnyConnect Network Access module to be compatible with the Cisco ASA software image.
C. Upgrade the Cisco AnyConnect client driver to be compatible with the Cisco ASA software image. D. Upgrade the

Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asa-vpn-compatibility.html#Cisco_Reference.dita_60cec583-01b8-4cb2-a6e3-2fe87a6b0f82

Question: 132

Which two components are required in a Cisco IOS GETVPN key server configuration? (Choose two.)

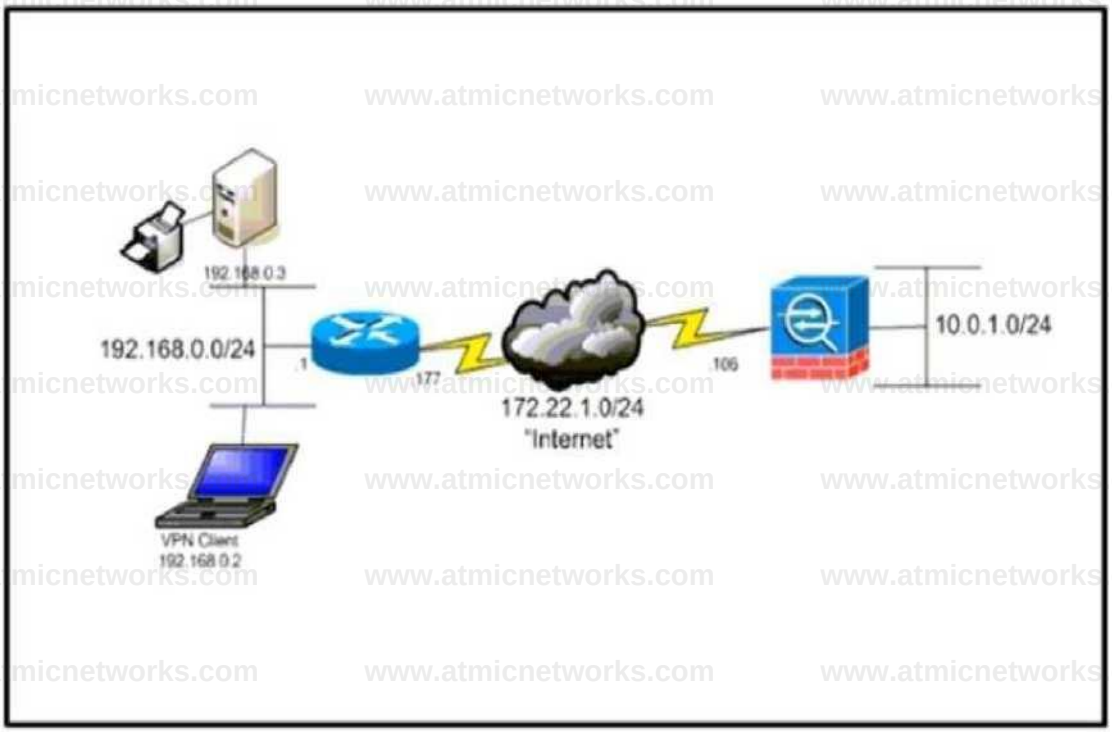
A. RSA key
B. IKE policy
C. SSL cipher
D. GRE tunnel
E. L2TP protocol

Answer: A, B

Explanation:

Question: 133

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 AS

A. 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.

Answer: B

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: 134

An organization wants to distribute remote access VPN load across 12 VPN headend locations supporting 25,000 simultaneous users. Which load balancing method meets this requirement?

A. one VPN profile per site
B. DNS-based load balancing
C. AnyConnect native load balancing
D. equal cost, multipath load balancing

Answer: B

Explanation:

Question: 135

What are two advantages of using GETVPN to traverse over the network between corporate offices? (Choose two.)

A. It has unique session keys for improved security.
B. It supports multicast.
C. It has QoS support.
D. It is a highly scalable any to any mesh topology.
E. It supports a hub-and-spoke topology.

Answer: B, D

Explanation:

Question: 136

Why must a network engineer avoid usage of the default X.509 certificate when implementing clientless SSLVPN on an ASA?

A. The certificate must be managed by the local CA.
B. The certificate is regenerated at each reboot.
C. The default X.509 certificate is not supported for SSLVPN.
D. The certificate is too weak to provide adequate security.

Answer: B

Explanation:

By default, the ASA generates a self-signed X.509 certificate upon startup. This certificate is used in order to serve client connections by default. It is not recommended to use this certificate because its authenticity cannot be verified by the browser. Furthermore, this certificate is regenerated upon each reboot so it changes after each reboot.
https://www.cisco.com/c/en/us/support/docs/security- vpn/webvpn-ssl-vpn/119417-config-asa-00.html

Question: 137

An engineer has configured Cisco AnyConnect VPN using IKEv2 on a Cisco IOS router. The user cannot connect in the

Cisco AnyConnect client, but receives an alert message "Use a browser to gain access." Which action does the engineer take to resolve this issue?

A. Reset user login credentials.
B. Correct the URL address.
C. Connect using HTTPS.
D. Disable the HTTP server.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115755-flexvpn-ike-eap-00.html

Question: 138

A router is being configured for IKEv2 AnyConnect using AnyConnect-EAP. How would the administrator separate profiles for administrators and employees so that authorization differs when they connect?

A. Define group aliases on the headend and have the user pick the appropriate alias when they connect
B. Define group-urls on the headend and create two XML profiles to match the administrator and user group urls
C. Create a certificate map and match on the appropriate certificate fields
D. Define key-ids on the headend and create two XML profiles to match the administrator and user key-ids.

Answer: B

Explanation:

According to the document Configure FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database, one way to separate profiles for administrators and employees is to use group-urls on the headend and create two XML profiles to match the administrator and user group urls. This allows the headend to assign different group-policies and tunnel-groups based on the group-url that the user connects to. For example:

webvpn enable outside anyconnect image disk0:/anyconnect-win-4.6.03049-webdeploy-k9.pkg 1 anyconnect enable tunnel-group-list enable group-policy Admin internal group-policy Admin attributes vpn-tunnel-protocol ikev2 ssl-client address-pools value AdminPool group-policy User internal group-policy User attributes vpn-tunnel-protocol ikev2 ssl-client address-pools value UserPool tunnel-group Admin type remote-access tunnel-group Admin general-attributes default-

group-policy Admin tunnel-group Admin webvpn-attributes group-url https://10.0.0.1/Admin enable tunnel-group User type remote-access tunnel-group User general-attributes default-group-policy User tunnel-group User webvpn-attributes group-url https://10.0.0.1/User enable

The XML profiles can be created with the AnyConnect Profile Editor and uploaded to the headend.

The profile for administrators should have the server list entry as:

<ServerList> <HostEntry> <HostName>Admin</HostName> <HostAddress>10.0.0.1</HostAddress> <PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>Admin</UserGroup> </HostEntry> </ServerList>

The profile for users should have the server list entry as:

<ServerList> <HostEntry> <HostName>User</HostName> <HostAddress>10.0.0.1</HostAddress>
<PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>User</UserGroup> </HostEntry>
</ServerList>
This way, when the user connects to the headend, they can choose either Admin or User from the drop-down list and get the appropriate authorization based on their group-url.

Question: 139

Which parameter in IPsec VPN tunnel configurations is optional?

A. hash
B. lifetime
C. encryption
D. Perfect Forward Secrecy

Answer: D

Explanation:

Question: 140

A company is setting up a dynamic crypto map on the Cisco ASA at the headquarters to accept connections from the branch offices. There will be no IP subnet overlap between the branch offices, but the engineer does not know which encryption domains will be requested by the branch offices. Additionally, the company security policy states that routing protocol traffic should not leave the HQ network. Which solution should be used to route traffic back to the branches from the Cisco ASA with minimal administrative effort?

A. Configure Reverse Route Injection on the dynamic crypto map.
B. Configure a default route with the tunneled keyword on all branch routers.
C. Configure static routes for remote subnets.
D. Configure snapshot routing with EIGRP to send out of band routing updates.

Answer: A

Explanation:

Question: 141

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?

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

Question: 142

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

A. DMVPN
B. IPsec VPN
C. FlexVPN
D. GETVPN

Answer: D

Explanation:

Question: 143

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

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

Explanation:

Question: 144

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 transform 1 esp-3des esp-
                sha-hmac
crypto ipsec profile myprofile
set transform-set mytransformset
set ikev2-profile myprofile
interface Virtual-Templatel type tunnel
ip unnumbered Ethernet1/1
tunnel mode ipsec ipv4
tunnel protection ipsec profile myprofile
```

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

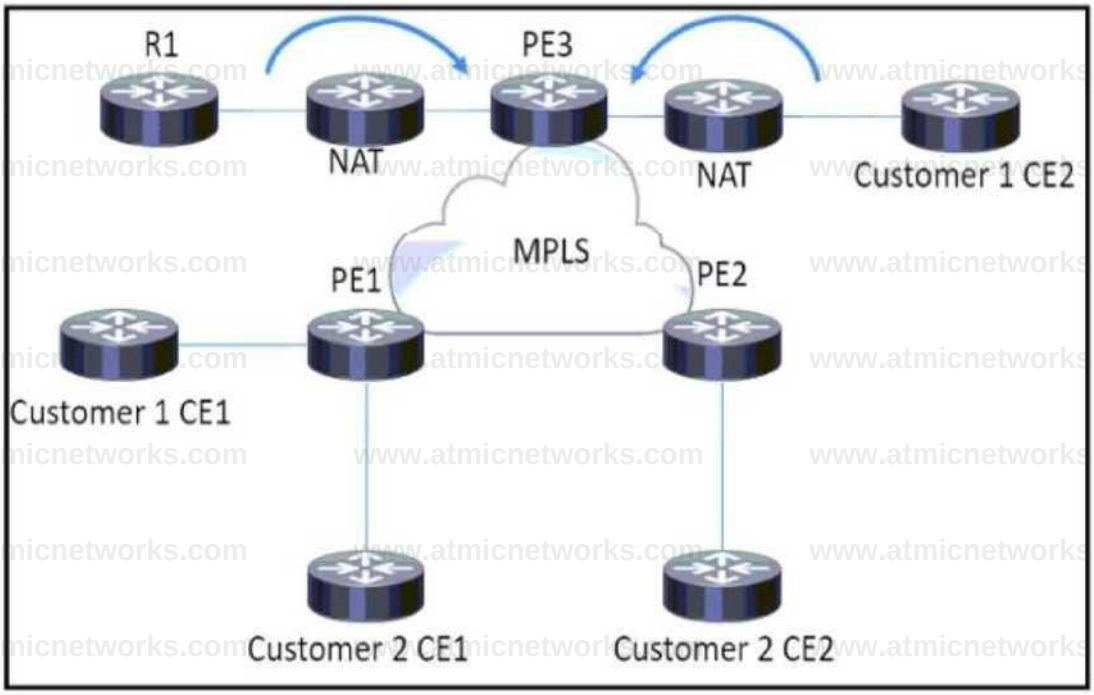
A. PPTP
B. SSLVPN Full Tunnel
C. FlexVPN
D. clientless SSLVPN

Answer: C

Explanation:

Question: 145

Refer to the exhibit.



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

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

Explanation:

Question: 146

Refer to the exhibit.

```
llXva: ISISS1W IE - lf,SA ID = 2i :ae='ived Packet 1F«n Ul.l«!.M.25:S00/To m.U3.21>.2«:«)0mr 10:f0]
Initiatoi SPI : 334M«B9K7MIED - Raapondax SPI kCMUnttltOWOl Maaaaoa id: 1
IKEW »_AUIB Exchange RESPONSE
Payload content*:
    VID IDs AuTB SA TSI ISr NOTIFY OSE TRANSPORT MODE) NOTIFY!SSI WINDOW SIZE MOTIFS ESP TFC MO SUPPORT!
NOTIFY lNW_FIR5T_mO51

    nxv2: (SESSION ID = 16,SA ID = 2 : Process each response notify
    mv3: (SESSION ID * 16,SA ID » 2: Searching policy bated on peer'* identity *192.166.20.21* of type 'IPv4 address
    IKE72-£A5.CR. SESSION ID • 16,SI ID - 2) : ; Filled to locate an men in the database
    XKBvS:•SESSION ID = 16,SA 0 = 2) Verification of peer's authentication data FAILED
    IKEv2:(SESSION ID - 1€,SA ID - 21 Auth exchange failed
    IKEvi-EARCR: SESSION ID ® 16.SA ID ■ 2):: Auth exchange failed
    ■REv2: (SESSION ID * 16, SA ID * 2! :Abort exchange
XREv2: (SESSION ID = 16,SA ID - 2) :EeUtinq SA
IKEvJ:(SESSION ID * 10,SA ID ■ 11:Retranemitting 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?

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

Explanation:

Question: 147

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.)

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: BD

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: 148

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 GigabitEthernetO/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={ongin_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
```

Jocal crypto endpt. 209 165 200 225 . remote crypto endpt.: 209 165 200.226
^ath mtu 1500. media mtu 1500
current outbound spi: 3D3

inbound esp sas

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.

Answer: A

Explanation:

Question: 149

When troubleshooting FlexVPN spoke-to-spoke tunnels, what should be verified first?

A. NHRP redirect is enabled on the hub.
B. The spokes have sent a resolution request.
C. NHRP cache entries exist on the spoke.
D. NHO routes exist on the spokes.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec- flex-vpn-15-mt-book/sec-flex-spoke.html

Question: 150

An engineer is building an IKEv1 tunnel to a peer Cisco ASA, but the tunnel is failing. Based on the configuration in the exhibit, which action must be taken to allow the VPN tunnel to come up?

```
interface EthernotO named outside
security-tevelo ip address 172.16 1.2 255.255 255.0

interface Ethernet! nameif inside
security level IOC
ipaddress 10.1.0.1 255.255.255 0 l
object network In jideNet subnet 10.7.7.0 255.255.255.0 i
object network RemoteNet Subnet 10 8 8 0 255 255 255.0
l
nat (mside.outsce) soixce static InsideNet Inside-Net destination static RemoteNet Remot eNet l
access list cmaplO extended permit ip object inside Net object RemoteNet

route outside 0.0.0.00.0.0.0172.16.1.1 l
crypto ipsec ikevl transform-set AES256 esp-aes- 256 esp-sba-hmac
crypto ikevl policy 10
authentication pre share
encryption ides hash sha
```

```
group 2 lifetime 86400

crypto map cmap 10 match addresscmaplO
crypto map cmap 10 set peer 172.17.1.1
crypto map cmap 10 set ikevl transform set AES256 I
tunnel-group 172.17.1.1 typeipsec-121
tunnel-gro JO 172.17.1.1 ipsec-attributes
 ikevl pre-shared-key Ciscol 23
```

A. Add a route for the 10.7.7.0/24 network to egress the outside interface.
B. Enable IKEv1 on the outside interface.
C. Change the IKEv1 policy number to be at least 256.
D. Change the transform set mode to transport.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425- configure-ipsec-00.html

Question: 151

An organization wants to implement a site-to-site VPN solution that must be able to support 350 sites with direct communications between all sites, fully encrypt the packet header and payload, and support propagation of routing information over IPsec. Which solution meets these requirements?

A. IPsec full mesh
B. DMVPN
C. GETVPN
D. FlexVPN

Answer: D

Explanation:

https://networklessons.com/cisco/ccie-enterprise-infrastructure/flexvpn-ikev2-routing

Question: 152

Refer to the exhibit.

```
interface Tunnel119
 ip address 172.20.58.7 255.255.0.0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel destination 128.17.64.8
 tunnel protection ipsec profile DMVPN_profile
end
```

Which type of VPN tunnel is configured?

A. Multipoint GRE
B. DMVPN
C. FlexVPN
D. GRE over IPsec

Answer: D

Explanation:

Question: 153

Refer to the exhibit.

```
interface EthernetO
 nameifoutside
 security-level 0
 ip address 172.16.1.2 255.255.255.0

interface Ethernet!
 nameifinside
 security-level 100
 ipaddress 10.1.0.1 255.255.255.0

object network InsideNet
subnet 10.1.7.0 255.255.255.0

object network RemoteNet
subnet 10.1.9.0 255.255.255.0

object network RemoteNet2
subnet 10.1.10.0 255.255.254.0

object network RemoteNet3
subject 10.1.11.0 255.255.255.0

route outside 0.0.0.0 0.0.0.0 172.16.1.1
route outside 10.1.11.0 255.255.255.0 172.16.1.1
```

```
access-list cmap10 extended permit ip object InsideNet object RemoteNet access-list
cmap20 extended permit ip object InsideNet object RemoteNet2 access-list cmap30
extended permit ip object InsideNet object RemoteNet3 I
crypto ipsec ikevl transform-set AES256 esp-aes-256 esp-sha-hmac I
crypto ikevl policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
no crypto isakmp nat-traversal

crypto map cmap 10 match address crnapIO
crypto map cmap 10 set peer 172.17.1.1
crypto map cmap 20 set ikevl transform-set AES256
crypto map cmap 20 match address cmap20
crypto map cmap 20 set peer 172.18.1.1
crypto map cmap 20 set ikevl transform-set AES256
crypto map cmap 30 match address cmap30
crypto map cmap 30 set peer 172.19.1.1
crypto map cmap 30 set ikevl transform-set AES256
crypto map cmap interface outside
```

An engineer has configured two new VPN tunnels to 172.18.1.1 and 172.19.1.1. However, communication between 10.1.0.10 and 10.1.11.10 does not function. Which action should be taken to resolve this issue?

A. Remove and reapply the crypto map to the interface.
B. Insert routes for the 10.1.9.0/24 and 10.1.10.0/24 subnets.
C. Modify the transform set to use transport mode.
D. Adjust the network objects to match the appropriate subnets.

Answer: D

Explanation:

Question: 154

Refer to the exhibit.

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.

Answer: AB

Explanation:

Question: 155

A DMVPN spoke is configured with IKEv1 to secure the tunnel. Despite having a configuration similar to other working spokes, the tunnel is not coming up. Packet captures on the spoke show packets leaving the spoke router, but not making it to the hub router. Which solution resolves this issue?

A. Configure the spoke and hub to use the same IKE version.
B. Ensure that devices between the hub and spoke are not blocking ESP traffic.
C. Ensure that devices between the hub and spoke are not blocking GRE traffic.
D. Enable the tunnel interface with the no shutdown command.

Answer: B

Explanation:

Question: 156

Users are getting untrusted server warnings when they connect to the URL https://asa.lab from their browsers. This URL resolves to 192.168.10.10, which is the IP address for a Cisco ASA configured for a clientless VPN. The VPN was recently set up and issued a certificate from an internal CA server. Users can connect to the VPN by ignoring the message, however, when users access other webservers that use certificates issued by the same internal CA server, they do not experience this issue. Which action resolves this issue?

A. Import the CA that signed the certificate into the machine trusted root CA store.
B. Reissue the certificate with asa.lab in the subject alternative name field.
C. Import the CA that signed the certificate into the user trusted root CA store.
D. Reissue the certificate with 192.168.10.10 in the subject common name field.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html

Question: 157

Over which two transport mediums is FlexVPN deployed? (Choose two.)

A. 5G
B. VPLS
C. internet
D. MPLS
E. DWDM

Answer: CD

Explanation:

Transport network: FlexVPN can be deployed either over a public internet or a private Multiprotocol Label Switching (MPLS) VPN network.
https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

Question: 158

A network administrator is troubleshooting a FlexVPN tunnel. The hub router is unable to ping the spoke router's tunnel interface IP address of 192.168.1.2, even though the tunnel is showing up. The output of the debug ip packet CLI command on the hub router shows the following entry.

IP: tableid=0123456789 s=192.168.1.1 (local), d=192.168.1.2 (loopback2), routed via FIB.

What must be configured to fix this issue?

A. A matching IKEv2 pre-shared key on the hub and spoke routers in the crypto keyring configuration. B. An outbound ACL on the dynamic VTI of the hub router that allows ICMP traffic to 192.168.1.2.
C. An IKEv2 authorization policy must be configured on the spoke router to advertise the interface route.
D. A route map must be configured on hub router to set the next hop for 192.168.1.2 to the dynamic VTI.

Answer: C

Explanation:

Question: 159

A network engineer must configure the Cisco ASA so that Cisco AnyConnect clients establishing an SSL VPN connection create an additional tunnel for real-time traffic that is sensitive to packet delays. If this additional tunnel experiences any issues, it must fall back to a TLS connection. Which two Cisco AnyConnect features must be configured to accomplish this task? (Choose two.)

A. DTLS
B. DSCP Preservation
C. DPD
D. SSL Rekey
E. OMTU

Answer: AC

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn- config/vpn-anyconnect.html

Configure Dead Peer Detection Dead Peer Detection (DPD) ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed. To enable dead peer detection (DPD) and set the frequency with which either the AnyConnect client or the ASA gateway performs DPD, do the following: Before you begin This feature applies to connectivity between the ASA gateway and the AnyConnect SSL VPN Client only. It does not work with IPsec since DPD is based on the standards implementation that does not allow padding, and CLientless SSL VPN is not supported. If you enable DTLS, enable Dead Peer Detection (DPD) also. DPD enables a failed DTLS connection to fallback to TLS. Otherwise, the connection terminates.

Question: 160

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

Answer: C

Explanation:

https://integratingit.wordpress.com/2020/03/14/asa-vpn-load-balancing/

Question: 161

An administrator is setting up Cisco AnyConnect on a Cisco ASA with the requirement that AnyConnect automatically establishes a VPN when a company-owned laptop is connected to the

internet outside of the corporate network. Which configuration meets these requirements?

A. SBL with user certificate authentication
B. TND with machine certificate authentication
C. SBL with machine certificate authentication
D. TND with user certificate authentication

Answer: B

Explanation:

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).
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#id_100236

Question: 162

Which command must be configured on the tunnel interface of a FlexVPN spoke to receive a dynamic IP address from the hub?

A. ip address negotiated
B. ip unnumbered
C. ip address dhcp
D. ip address pool

Answer: A

Explanation:

https://integratingit.wordpress.com/2018/03/31/configuring-flexvpn-external-aaa-with-radius/ interface Tunnel0
ip address negotiated
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 1.1.1.5
tunnel protection ipsec profile IPSEC_PROFILE

Question: 163

An engineer is implementing the FlexVPN solution on a Cisco IOS router. The router must only terminate VPN requests and must not initiate them. Additionally, the interface must support VPNs from other routers and Cisco AnyConnect connections. Which interface type must be configured to meet these requirements?

A. point-to-point GRE tunnel interface
B. multipoint GRE tunnel interface
C. static virtual tunnel interface
D. virtual template interface

Answer: D

Explanation:

The correct interface type to meet these requirements is the virtual template interface. This interface allows for the creation of multiple virtual access interfaces, which can be used for various types of remote access VPN connections, including site-to-site and AnyConnect VPNs. The virtual template interface can be configured to terminate VPN requests from other routers and allow for dynamic creation of VPN sessions, while also supporting AnyConnect VPN connections.

Question: 164

DRAG DROP

Drag and drop the GETVPN components from the left onto the descriptions on the right.

Answer Area

IPsec	resolves the remote overlay address and dynamically discovers the transport endpoint needed to establish a secure tunnel
IKEv2	distributes overlay labels for the network on different VRFs
NHRP	secures the data traffic between the spoke and the hub after the remote spoke is discovered dynamically
MPLS	adds static routes to the tunnel overlay address of a peer as a directly connected route
MBGP	enables tag switching for data packets

Answer:

Explanation:

IPSec: Secures the data traffic,..
IKEv2: Adds statics routes,..
NHRP: Resolves the remote,..
MPLS: Enables tag switching for data,..
MPBGP: Distributes overlay,..

Question: 165

Refer to the exhibit.

```
<snip>
  Tunnel Group: VPNPhone, Client Cert Auth Success. WebVPN:
CSD data not sent from client http_remove_auth_handle () :

handle 24 not found?

<snip>
```

A network administrator is setting up a phone VPN on a Cisco AS

A. The phone cannot connect and the error is presented in a debug on the Cisco ASA. Which action fixes this issue?

A. Enable web-deploy of the posture module so that the module can be downloaded from the Cisco ASA to an IP phone.
B. Configure the Cisco ASA to present an RSA certificate to the phone for authentication.
C. Disable Cisco Secure Desktop under the connection profile VPNPhone.
D. Install the posture module on the Cisco ASA.

Answer: C

Explanation:

CSD and IP phones: Currently, IP phones do not support Cisco Secure Desktop (CSD) and do not connect when CSD is enabled for the tunnel group or globally in the ASA.

Question: 166

Which two protocols does DMVPN leverage to build dynamic VPNs to multiple destinations? (Choose two.)

A. IKEv2 B. NHRP C. mGRE D. mBGP E. GDOI

Answer: BC

Explanation:

Question: 167

DRAG DROP

Drag and drop the GET VPN components from the left onto the correct descriptions on the right.

Answer Area

Answer:

Explanation:

KEK - Encrypts the rekey message

TEK - Used by all the group members to communicate securely among each other

"The TEK becomes the IPsec SA with which the group members within the same group communicate. The KEK encrypts the rekey message."

GDOI protocol - Provides group key and group AS management

"DGOI is defined as the Internet Security Association Key Management Protocol (ISAKMP) Domain of Interpretation (DOI) for group key management."

KS - Maintains security policies and provides the session key for encrypting traffic

"The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. When a group member registers, the key server downloads this policy and the keys to the group member. The key server also rekeys the group before existing keys expire."

GM - Gets the IPSec SA to encrypto data traffic within the group

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html#GUID-C8F2200D-C50E-408B-966F-249EC70AADD0

Question: 168

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

Answer: B

Explanation:

https://networklessons.com/cisco/asa-firewall/cisco-asa-anyconnect-remote-access-vpn#:~:text=The%20anyconnect%20ask%20command%20specifies,of%20the%20anyconnect%20client%20automatically.

Question: 169

An administrator is deciding which authentication protocol should be implemented for their upcoming Cisco AnyConnect deployment. A list of the security requirements from upper management are: the ability to force AnyConnect users to use complex passwords such as C1$c0451035084!, warn users a few days before their password expires, and allow users to change their password during a remote access session. Which authentication protocol must be used to meet these requirements?

A. LDAPS
B. RADIUS
C. Kerberos
D. TACACS+

Answer: A

Explanation:

To enforce complex passwords—for example, to require that a password contain upper- and lowercase letters, numbers, and special characters—enter the password-management command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn- config/vpn-groups.html

Question: 170

Which clientless SSLVPN supported feature works when the http-only-cookie command is enabled?

A. Citrix load balancer
B. port reflector
C. Java rewriter -
D. Java plug-ins
E. script browser

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/asdm74/vpn/asdm-74-vpn-config/webvpn-troubleshooting.html

The following Clientless SSL VPN features will not work when the http-only-cookie command is enabled:

- Java plug-ins
- Java rewriter
- Port forwarding
- File browser
- Sharepoint features that require desktop applications (for example, MS Office applications)
- AnyConnect Web launch
- Citrix Receiver, XenDesktop, and Xenon
- Other non-browser-based and browser plugin-based applications

Question: 171

A network engineer must expand a company's Cisco AnyConnect solution. Currently, a Cisco ASA is set up in North America and another will be installed in Europe with a different IP address. Users should connect to the ASA that has the lowest Round Trip Time from their network location as measured by the AnyConnect client. Which solution must be implemented to meet this requirement?

A. VPN Load Balancing
B. IP SLA
C. DNS Load Balancing
D. Optimal Gateway Selection

Answer: D

Explanation:

Optimal Gateway Selection (OGS). OGS is a feature that can be used in order to determine which gateway has the lowest Round Trip Time (RTT) and connect to that gateway. One can use the OGS feature in order to minimize latency for Internet traffic without user intervention. With OGS, Cisco AnyConnect Secure Mobility Client (AnyConnect) identifies and selects which secure gateway is best for connection or reconnection. OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection.

Question: 172

An engineer is creating an URL object on Cisco FMC. How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website.
C. Use the subject common name from the website certificate.
D. Define the path to the individual webpage that uses HTTPS.

Answer: B

Explanation:

Use the FQDN including the subdomain for the website. According to the Firepower Management Center Configuration Guide, Version 6.61, when you create a URL object, you must use the fully qualified domain name (FQDN) of the website, including any subdomains, and omit the protocol prefix (HTTP or HTTPS). For example, to match www.example.com, you must enter www.example.com as the URL object value, not http://www.example.com or https://www.example.com. The system automatically matches both HTTP and HTTPS traffic for the same FQDN. Specifying the protocol to match (HTTP or HTTPS) is not required and will result in an invalid URL object. Using the subject common name from the website certificate or defining the path to the individual webpage that uses HTTPS are not supported options for URL objects.

Question: 173

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe
B. inline tap
C. promiscuous
D. bypass

Answer: C

Explanation:

The correct answer is C. promiscuous mode. In promiscuous mode, the Cisco IPS appliance operates as a passive device that monitors a copy of the network traffic and analyzes it for malicious activity. The appliance does not affect the traffic flow, but it can generate alerts, logs, and reports based on the configured security policy. Promiscuous mode is useful for initial deployment and baseline analysis, as well as for monitoring low-risk segments of the network12.

A. failsafe mode is a feature that determines how the appliance behaves when a hardware or software failure occurs. It does not affect the normal traffic flow or analysis3. B. inline tap mode is a variation of inline mode that allows the appliance to pass traffic without inspection in case of a power failure or a software crash. It does not allow the appliance to collect data without affecting traffic4. D. bypass mode is a feature that enables the appliance to bypass traffic without inspection when it is overloaded or under maintenance. It does not allow the appliance to analyze traffic and generate alerts.

1: How the Sensor Functions 2: Cisco ASA IPS Module Quick Start Guide 3: Failsafe Mode 4: Inline Tap Mode : Bypass Mode

Question: 174

A network administrator wants to block traffic to a known malware site at https:/www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which

type of policy must the network administrator use to accomplish this goal?

A. Access Control policy with URL filtering
B. Prefilter policy
C. DNS policy
D. SSL policy

Answer: A

Explanation:

The correct answer is A. Access Control policy with URL filtering. An Access Control policy is a type of policy that allows you to control how traffic is handled on your network based on various criteria, such as source and destination IP addresses, ports, protocols, applications, users, and URLs. URL filtering is a feature that enables you to block or allow traffic based on the URL category or reputation of the website. You can create custom URL objects to specify the exact URLs or domains that you want to block or allow. For example, you can create a URL object for https:/www.badsite.com and set it to block. This will prevent any traffic from reaching that site and any subdomains under it12.

B. Prefilter policy is a type of policy that allows you to perform fast actions on traffic before it reaches the Access Control policy. You can use prefilter rules to drop, fastpath, or trust traffic based on simple criteria, such as IP addresses or ports. However, prefilter rules do not support URL filtering, so you cannot use them to block traffic based on the website domain3.

C. DNS policy is a type of policy that allows you to inspect and modify DNS requests and responses on your network. You can use DNS rules to block, monitor, or sinkhole DNS queries based on the requested domain name or the response IP address. However, DNS policy does not prevent packets from being sent to the malicious site; it only prevents the DNS resolution of the domain name. A client could still access the site if they know the IP address or use an alternative DNS server.

D. SSL policy is a type of policy that allows you to decrypt and inspect encrypted traffic on your network. You can use SSL rules to determine which traffic to decrypt based on various criteria, such as certificate attributes, cipher suites, or URL categories. However, SSL policy does not block traffic; it only decrypts it for further inspection by other policies.

Question: 175

An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Specify the trace using the -T option after the capture-traffic command
B. Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI
C. Use the verbose option as a part of the capture-traffic command
D. Use the capture command and specify the trace option to get the required information

Answer: A

Explanation:

The correct answer is A. Specify the trace using the -T option after the capture-traffic command. According to the document Use Firepower Threat Defense Captures and Packet Tracer, the capturetraffic command allows you to capture packets on the Snort engine domain of the FTD device. However, by default, it only shows the packet headers and does not include the Snort detection actions. To see the Snort detection actions, you need to use the -T

option, which enables tracing. For example: capture-traffic -T

This will show the packet headers along with the Snort verdicts, such as allow, block, or replace. You can also use other options to filter or save the capture output1.

B. Performing the trace within the Cisco FMC GUI instead of the Cisco FMC CLI is not a valid option, because the FMC GUI does not support packet capture or tracing on the FTD device. You can only use the FMC GUI to view and export captures that are taken on the FTD CLI1.

C. Using the verbose option as a part of the capture-traffic command is not a valid option, because there is no verbose option for this command. The verbose option is only available for the capture command, which is used to capture packets on the LINA engine domain of the FTD device1.

D. Using the capture command and specifying the trace option to get the required information is not a valid option, because the capture command does not have a trace option. The capture command allows you to capture packets on the LINA engine domain of the FTD device, but it does not show the Snort detection actions. The trace option is only available for the packet-tracer command, which is used to simulate a packet going through the FTD device and show its processing steps1.