Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

NEW 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.
Select and Place:

Answer Area

```
Router A
interface Tunnel1
   ip address 10.0.0.1 255.255.255.0
   ip nhrp mp multicast dynamic
   ip nhrp network-id 1
   ip nhrp [          ]
   no ip split-horizon eigrp 10
   tunnel source GigabitEthernet1
   tunnel mode gre multipoint

interface GigabitEthernet1
   ip address 1.1.1.1 255.255.255.0

router eigrp 10
   network 10.0.0.0 0.0.0.255


Router B
interface Tunnel1
   ip address 10.0.0.2 255.255.255.0
   ip nhrp nhs [        ] nbma [          ] multicast
   ip nhrp network-id 1
   ip nhrp [        ]
   tunnel source GigabitEthernet1
   tunnel mode gre multipoint

interface GigabitEthernet1
   ip address 2.2.2.2 255.255.255.0

router eigrp 10
   network 10.0.0.0 0.0.0.255
```

| 1.1.1.1 |

| 10.0.0.1 |

| redirect |

| shortcut |

| server-only |

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 2
On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

A. interface virtual-access
B. ip nhrp redirect
C. interface tunnel
D. interface virtual-template

Answer: D

NEW QUESTION 3
Which 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: BD

NEW QUESTION 4
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:
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

NEW QUESTION 5
Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?

A. svc import profile SSL_profile flash:simos-profile.xml
B. anyconnect profile SSL_profile flash:simos-profile.xml
C. crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
D. webvpn import profile SSL_profile flash:simos-profile.xml

Answer: C

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

NEW QUESTION 6
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

NEW QUESTION 7
Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

A. tunnel-group (general-attributes)
B. tunnel-group (webvpn-attributes)
C. webvpn (group-policy)
D. webvpn (global configuration)

Answer: D

NEW QUESTION 8
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: C

NEW QUESTION 9
Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the client uses the local DNS to perform FQDN resolution.
B. The rewriter enable command under the global webvpn configuration enables the rewriter functionality because that feature is disabled by default.
C. A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.
D. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution.
E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

Answer: CD

NEW QUESTION 10
Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

A. single sign-on
B. Smart Tunnel
C. WebType ACL
D. plug-ins

Answer: B

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

NEW QUESTION 10
Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?

A. auto-upgrade
B. auto-connect
C. auto-start
D. auto-run

Answer: C

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

NEW QUESTION 12
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: B

NEW QUESTION 13
Refer to the exhibit.

```
Spoke1#
      local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
      remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
      #pkts encaps: 200, #pkts encrypt: 200
      #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
      inbound esp sas:
      spi: 034B32CA36 (1261619766)
      outbound esp sas:
      spi:0xD601918E (1760427022)

Spoke2#
      local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
      remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
      #pkts encaps: 210, #pkts encrypt: 210,
      #pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
      inbound esp sas:
      spi: 03D601918E (1760427022)
      outbound esp sas:
      spi: 034BS2CA36 (1261619766)
```

An engineer is troubleshooting a new GRE over IPsec tunnel. The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2. Which type of traffic is being blocked?

A. ESP packets from spoke2 to spoke1
B. ISAKMP packets from spoke2 to spoke1
C. ESP packets from spoke1 to spoke2
D. ISAKMP packets from spoke1 to spoke2

Answer: A

NEW QUESTION 15
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: B

NEW QUESTION 20
Refer to the exhibit.

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):      encryption AES-CBC
ISAKMP: (0):      keylength of 256
ISAKMP: (0):      hash SHA256
ISAKMP: (0):      default group 14
ISAKMP: (0):      auth pre-share
ISAKMP: (0):      life type in seconds
ISAKMP: (0):      life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

A. An authentication failure occurs on the remote peer.
B. A certificate fragmentation issue occurs between both sides.
C. UDP 4500 traffic from the peer does not reach the router.
D. An authentication failure occurs on the router.

Answer: C

NEW QUESTION 23
Refer to the exhibit.

```
*Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D5684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
*Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
 VID Next payload: IDr, reserved: 0x0, length: 20
 IDr Next payload: AUTH, reserved: 0x0, length: 12
  Id type: IPv4 address, Reserved: 0x0 0x0
 AUTH Next payload: SA, reserved: 0x0, length: 28
  Auth method PSK, reserved: 0x0, reserved: 0x0
 SA Next payload: TSi, reserved: 0x0, length: 40
  last proposal: 0x0, reserved: 0x0, length: 35
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
   type: 1, reserved: 0x0, id: 3DES
   last transform: 0x3, reserved: 0x0: length: 8
   type: 3, reserved: 0x0, id: SHA96
   last transform: 0x0, reserved: 0x0: length: 8
   type: 5, reserved: 0x0, id: Don't use ESN
 TSi Next payload: TSr, reserved: 0x0, length: 24
  Num of TSs: 1, reserved 0x0, reserved 0x0
  TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
  start port: 0, end port: 65535
  start addr: 30.30.30.0, end addr: 30.30.30.255
 TSr Next payload: NOTIFY, reserved: 0x0, length: 24
  Num of TSs: 1, reserved 0x0, reserved 0x0
  TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
  start port: 0, end port: 65535
  start addr: 20.20.20.0, end addr: 20.20.20.255
 NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
  Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
 NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
  Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
 NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
  Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
```

The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch is the problem?

A. preshared key
B. peer identity
C. transform set
D. ikev2 proposal

Answer: B

NEW QUESTION 26
Refer to the exhibit.

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
    500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
    failed its sanity check or is malformed
```

Which type of mismatch is causing the problem with the IPsec VPN tunnel?

A. crypto access list
B. Phase 1 policy
C. transform set
D. preshared key

Answer: D

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

NEW QUESTION 31
Refer to the exhibit.

```
HUB configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 1 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 2 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local pre-shared-key flexvpn
 authentication remote rsa-sig
 pki trustpoint CA
aaa authorization group cert list default default
virtual-template 1
```

What is a result of this configuration?

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

Answer: A

NEW QUESTION 34
Which technology works with IPsec stateful failover?

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

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp1122512

NEW QUESTION 36
What are two functions of ECDH and ECDSA? (Choose two.)

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

Answer: CD

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

NEW QUESTION 41
What uses an Elliptic Curve key exchange algorithm?

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

Answer: B

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

NEW QUESTION 45
Which two remote access VPN solutions support SSL? (Choose two.)

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

Answer: BE

NEW QUESTION 47
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

NEW QUESTION 51
Which VPN does VPN load balancing on the ASA support?

A. VTI
B. IPsec site-to-site tunnels
C. L2TP over IPsec
D. Cisco AnyConnect

Answer: D

NEW QUESTION 53
Which parameter must match on all routers in a DMVPN Phase 3 cloud?

A. GRE tunnel key
B. NHRP network ID
C. tunnel VRF
D. EIGRP split-horizon setting

Answer: A

NEW QUESTION 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

NEW QUESTION 56
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

NEW QUESTION 57
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-730 Practice Exam Features:

* 300-730 Questions and Answers Updated Frequently

* 300-730 Practice Questions Verified by Expert Senior Certified Staff

* 300-730 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-730 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 300-730 Practice Test Here