Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

NEW QUESTION 1
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 2
Refer to the exhibit.

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list
author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
```

What is configured as a result of this command set?

A. FlexVPN client profile for IPv6
B. FlexVPN server to authorize groups by using an IPv6 external AAA
C. FlexVPN server for an IPv6 dVTI session
D. FlexVPN server to authenticate IPv6 peers by using EAP

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-clnt.html

NEW QUESTION 3
Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

A. HTTP
B. ICA (Citrix)
C. VNC
D. RDP
E. CIFS

Answer: DE

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

NEW QUESTION 4
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 5
Refer to the exhibit.

XML profile

```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

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 Context1
  svc platform win seq 1
  policy group PolicyGroup1
   functions svc-enabled
```

B.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

D.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc module RDP
```

Answer: C

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

NEW QUESTION 6
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 7
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 8
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

NEW QUESTION 9
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 10
Refer to the exhibit.

```
IKEv2:(SESSION ID = 17,SA ID = 1):Processing IKE_AUTH message
IKEv2:IPSec policy validate request sent for profile CloudOne with psh index 1.

IKEv2:(SESSION ID = 17,SA ID = 1):
IKEv2:(SA ID = 1):[IPsec -> IKEv2] Callback received for the validate proposal - FAILED.

IKEv2-ERROR:(SESSION ID = 17,SA ID = 1):: There was no IPSEC policy found for received TS
IKEv2:(SESSION ID = 17,SA ID = 1):Sending TS unacceptable notify
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Get peer's preshared key for 68.72.250.251
IKEv2:(SESSION ID = 17,SA ID = 1):Generate my authentication data
IKEv2:(SESSION ID = 17,SA ID = 1):Use preshared key for id 68.72.250.250, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Generating IKE_AUTH message
IKEv2:(SESSION ID = 17,SA ID = 1):Constructing IDr payload: '68.72.250.250' of type 'IPv4 address'
IKEv2:(SESSION ID = 17,SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDr AUTH NOTIFY(TS_UNACCEPTABLE)

IKEv2:(SESSION ID = 17,SA ID = 1):Sending Packet [To 68.72.250.251:500/From 68.72.250.250:500/VRF i0:f0]
Initiator SPI : 3D527B1D50DBEEF4 - Responder SPI : 8C693F77F2656636 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 ENCR
```

Based on the debug output, which type of mismatch is preventing the VPN from coming up?

A. interesting traffic
B. lifetime
C. preshared key
D. PFS

Answer: B

Explanation:
If the responder's policy does not allow it to accept any part of the proposed Traffic Selectors, it responds with a TS_UNACCEPTABLE Notify message.

NEW QUESTION 10
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 15
Refer to the exhibit.

```
crypto isakmp 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 Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source GigabitEthernet1
 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:
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

NEW QUESTION 17
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

NEW QUESTION 19
.....

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