

300-730 Dumps

Implementing Secure Solutions with Virtual Private Networks (SVPN)

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



NEW QUESTION 1

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 2

Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

- A. Add NHRP shortcuts on the hub.
- B. Add NHRP redirects on the spoke.
- C. Disable EIGRP next-hop-self on the hub.
- D. Enable EIGRP next-hop-self on the hub.
- E. Add NHRP redirects on the hub.

Answer: CE

NEW QUESTION 3

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 4

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

NEW QUESTION 5

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 6

Which configuration construct must be used in a FlexVPN tunnel?

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

Answer: D

NEW QUESTION 7

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

NEW QUESTION 8

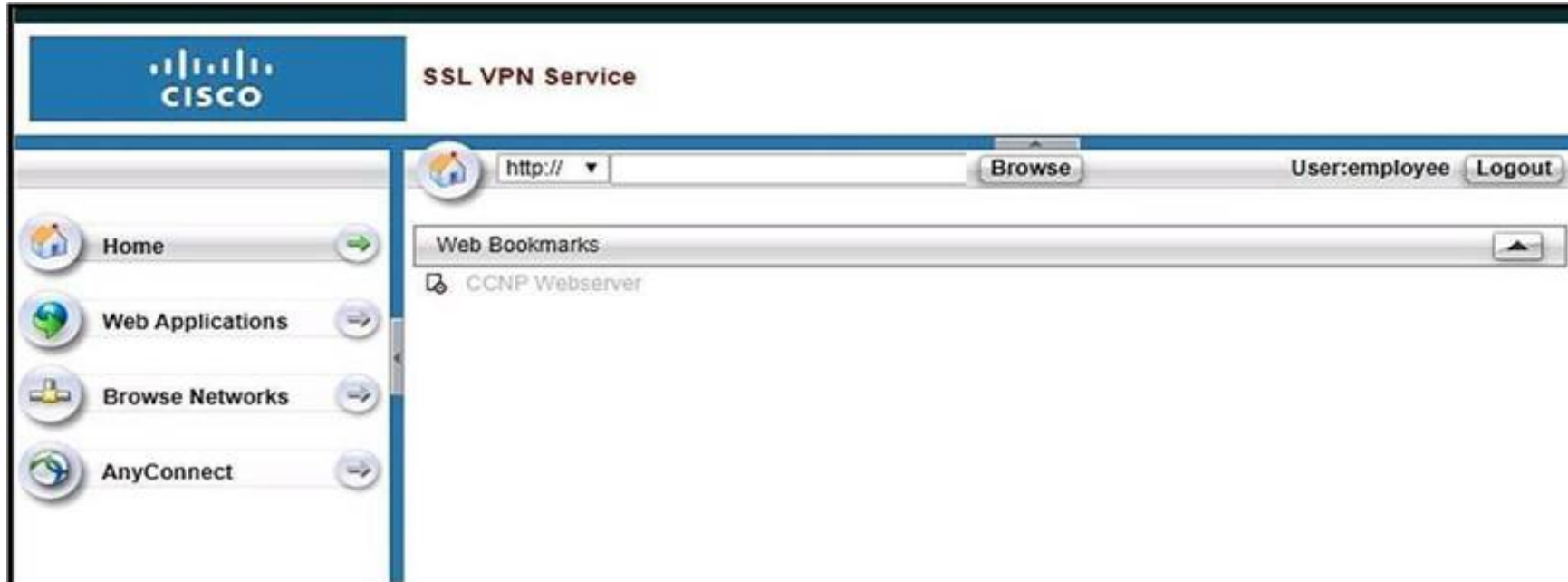
Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

- 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 9

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 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

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 15**

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 17

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 22

Refer to the exhibit.

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

NEW QUESTION 26

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

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

Answer: C

Explanation:

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

NEW QUESTION 27

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 30

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 35

Which VPN solution uses TBAR?

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

Answer: A

Explanation:

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

NEW QUESTION 37

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

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

Answer: AD

NEW QUESTION 41

Cisco AnyConnect clients need to transfer large files over the VPN sessions. Which protocol provides the best throughput?

- A. SSL/TLS
- B. L2TP
- C. DTLS
- D. IPsec IKEv1

Answer: C

NEW QUESTION 43

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 Tunnell
  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 45

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 47

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 51

Where is split tunneling defined for IKEv2 remote access clients on a Cisco router?

- A. IKEv2 authorization policy
- B. Group Policy
- C. virtual template
- D. webvpn context

Answer: B

NEW QUESTION 56

Which technology is used to send multicast traffic over a site-to-site VPN?

- A. GRE over IPsec on IOS router
- B. GRE over IPsec on FTD
- C. IPsec tunnel on FTD
- D. GRE tunnel on ASA

Answer: B

NEW QUESTION 60

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 61

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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