



Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which statement about GETVPN is true?

- A. The configuration that defines which traffic to encrypt originates from the key server.
- B. TEK rekeys can be load-balanced between two key servers operating in COOP.
- C. The pseudotime that is used for replay checking is synchronized via NTP.
- D. Group members must acknowledge all KEK and TEK rekeys, regardless of configuration.

Answer: A

NEW QUESTION 2

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 3

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

NEW QUESTION 4

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: BE

NEW QUESTION 5

Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

- A. *\$SecureMobilityClient\$*

- B. *\$AnyConnectClient\$*
- C. *\$RemoteAccessVpnClient\$*
- D. *\$DfltIkeIdentityS*

Answer: B

Explanation:

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

NEW QUESTION 6

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-summaps.pdf

NEW QUESTION 7

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 8

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 9

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 10

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

NEW QUESTION 10

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_vpniips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

NEW QUESTION 12

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>

NEW QUESTION 16

Refer to the exhibit.

```
ip access-list extended CCNP
 permit 192.168.0.10
 permit 192.168.0.11

webvpn gateway SSL_Gateway
 ip address 172.16.0.25 port 443
 ssl trustpoint AnyConnect_Cert
 inservice

webvpn context SSL_Context
 gateway SSL_Gateway

 ssl authenticate verify all
 inservice

policy group SSL_Policy
 functions svc-enabled
 svc address-pool "ACPool" netmask 255.255.255.0
 svc dns-server primary 192.168.0.100
 svc default-domain cisco.com
 default-group-policy SSL_Policy
```

Cisco AnyConnect must be set up on a router to allow users to access internal servers 192.168.0.10 and 192.168.0.11. All other traffic should go out of the client's local NIC. Which command accomplishes this configuration?

- A. svc split include 192.168.0.0 255.255.255.0
- B. svc split exclude 192.168.0.0 255.255.255.0
- C. svc split include acl CCNP
- D. svc split exclude acl CCNP

Answer: C

NEW QUESTION 18

.....

Relate Links

100% Pass Your 300-730 Exam with ExamBible Prep Materials

<https://www.exambible.com/300-730-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>