

300-730 Dumps

Implementing Secure Solutions with Virtual Private Networks (SVPN)

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



NEW QUESTION 1

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: B

NEW QUESTION 2

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 3

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 4

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:

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

NEW QUESTION 5

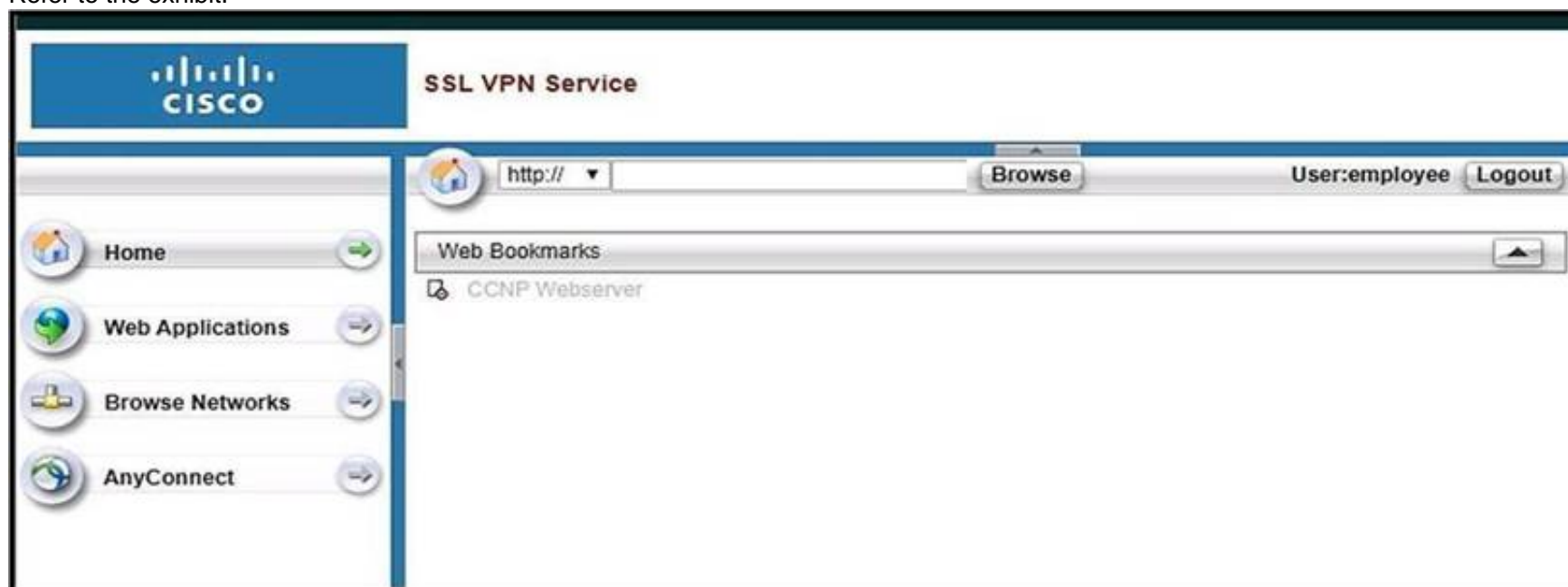
Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

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

Answer: D

NEW QUESTION 6

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 7

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 8

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 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 9

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

NEW QUESTION 10

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 10

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 13

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 15

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 20

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 23

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 28

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 31

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 34

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 36

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

NEW QUESTION 40

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 vpn-session-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 41

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 42

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 43

.....

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>