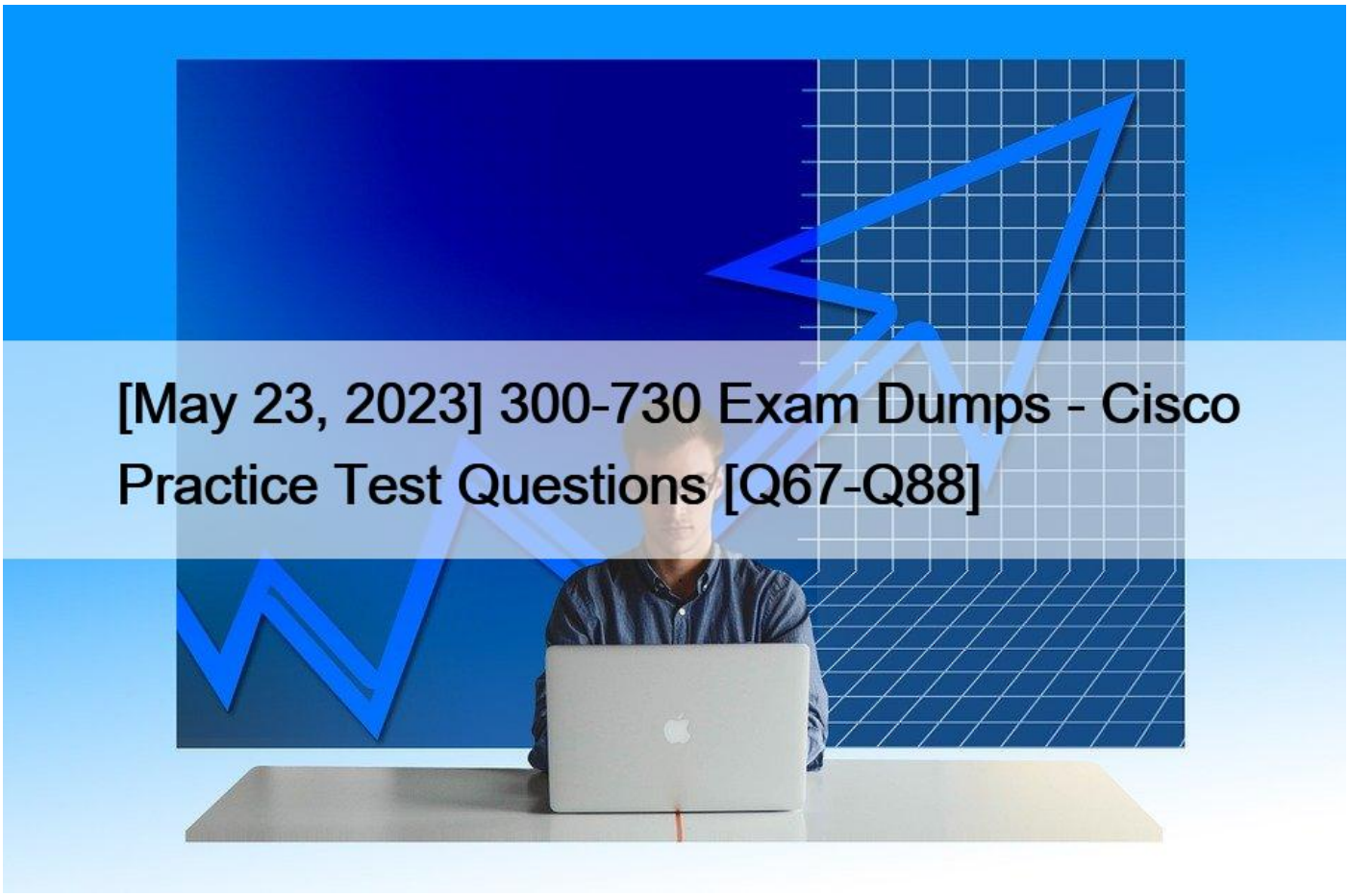
[May 23, 2023 300-730 Exam Dumps - Cisco Practice Test Questions [Q67-Q88



[May 23, 2023] 300-730 Exam Dumps - Cisco Practice Test Questions
New Real 300-730 Exam Dumps Questions

To pass the Cisco 300-730 certification exam, candidates must have a deep understanding of VPN technologies, including IPsec, SSL, and AnyConnect. They must also be familiar with VPN configuration and management tools such as Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD), and Cisco AnyConnect Secure Mobility Client. The exam also covers best practices for VPN deployment, including VPN tunneling, VPN authentication, and VPN troubleshooting.

The exam is designed for experienced network security professionals who have a minimum of three to five years of experience working with VPN technologies. Candidates should have a solid understanding of networking concepts, including TCP/IP, routing, switching, and firewall technologies. They should also be familiar with security concepts, such as authentication, authorization, and encryption.

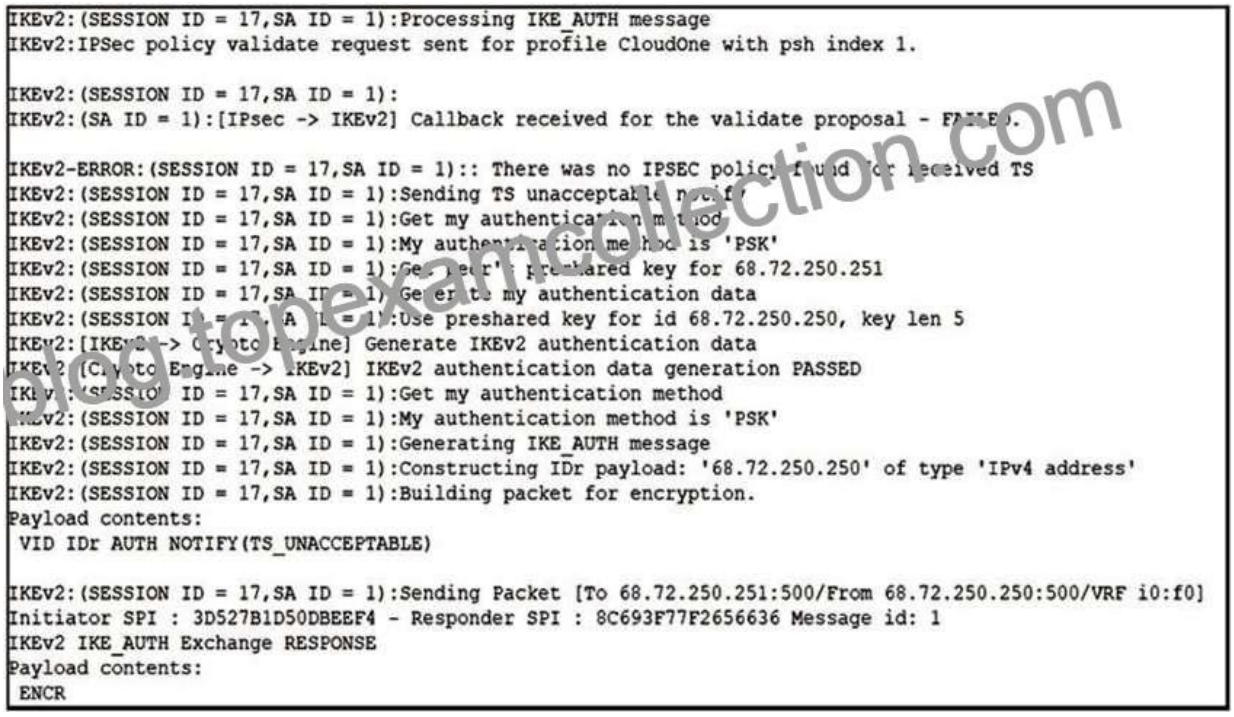
Q67. Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?
* tunnel-group (general-attributes)

* tunnel-group (webvpn-attributes)
* webvpn (group-policy)
* webvpn (global configuration)

Section: Remote access VPNs

Explanation/Reference:

Q68.



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

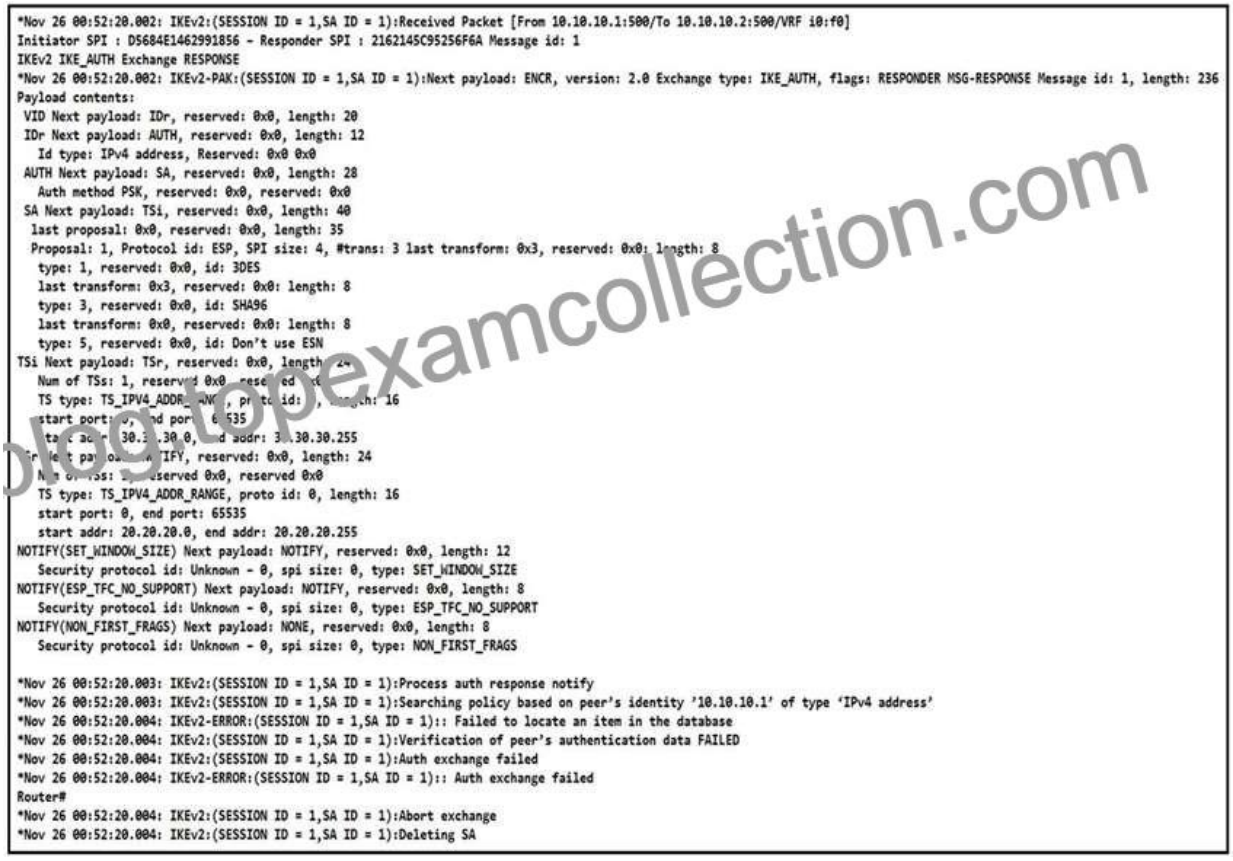
* interesting traffic
* lifetime
* preshared key
* PFS

Section: Troubleshooting using ASDM and CLI

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.

Q69.



```
*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
```


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

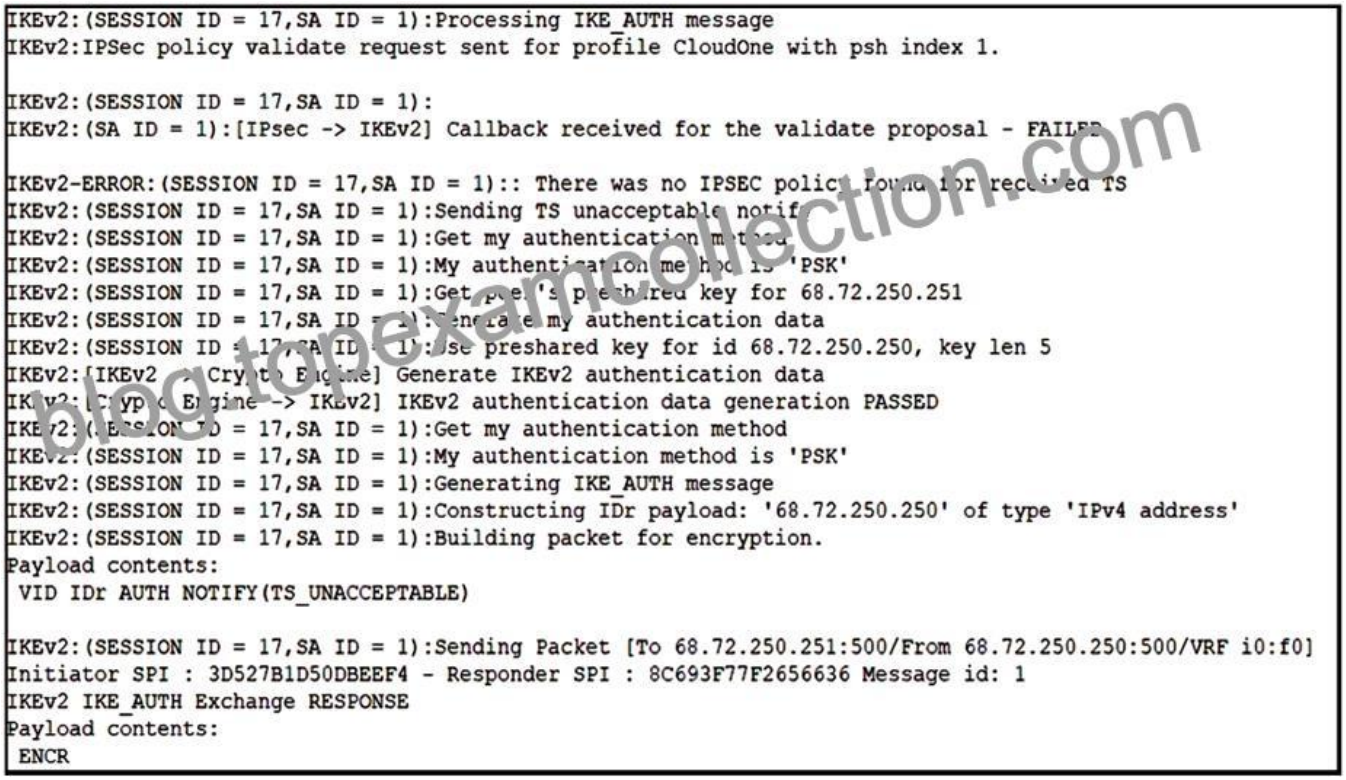
* preshared key
* peer identity
* transform set
* ikev2 proposal

Section: Troubleshooting using ASDM and CLI

Q70. An administrator must guarantee that remote access users are able to reach printers on their local LAN after a VPN session is established to the headquarters. All other traffic should be sent over the tunnel. Which split-tunnel policy reduces the configuration on the ASA headend?

* include specified
* exclude specified
* tunnel specified
* dynamic exclude

Q71. Refer to the exhibit.



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

* interesting traffic
* lifetime
* preshared key
* PFS

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.

Q72. A network engineer must implement an SSLVPN Cisco AnyConnect solution that supports 500 concurrent users, ensures all traffic from the client passes through the ASA, and allows users to access all devices on the inside interface subnet (192.168.0.0/24). Assuming all other configuration is set up appropriately, which configuration implements this solution?

○ A.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

○ B.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

○ C.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

○ D.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```


* Option A
* Option B
* Option C
* Option D

Q73. 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?
* The XML profile is not configured correctly for the affected users.
* The new client image does not use the same major release as the current one.
* Client services are not enabled.
* Client software updates are not supported with IKEv2.

Q74. What are two advantages of using GETVPN to traverse over the network between corporate offices? (Choose two.)
* It has unique session keys for improved security.
* It supports multicast.
* It has QoS support.
* It is a highly scalable any to any mesh topology.
* It supports a hub-and-spoke topology.

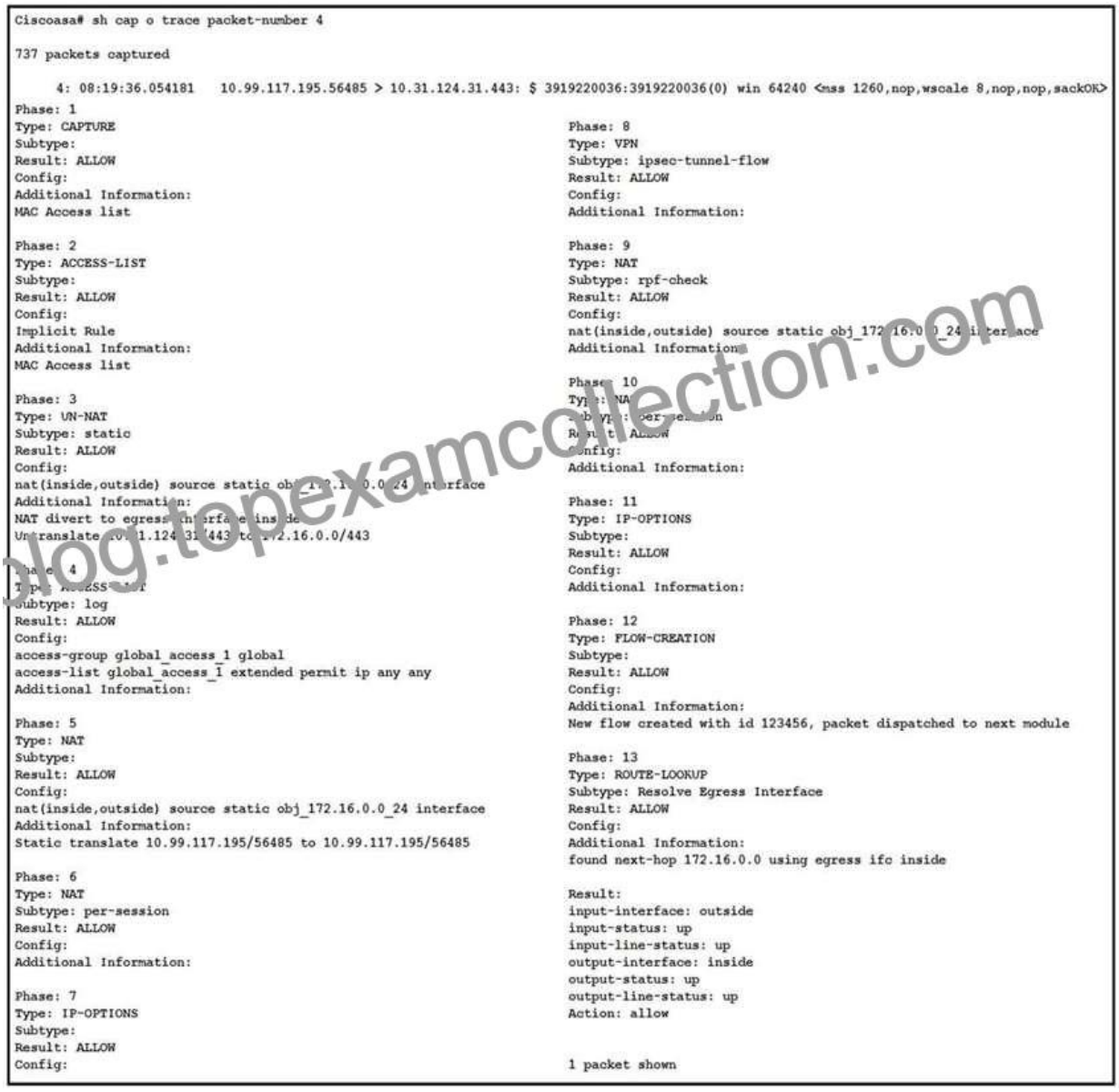
Q75. Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

* Reduce the maximum SA limit on the local Cisco ASA.
* Increase the maximum in-negotiation SA limit on the local Cisco ASA.
* Remove the maximum SA limit on the remote Cisco ASA.
* Correct the crypto access list on both Cisco ASA devices.

Q76.



```
Ciscoasa# sh cap o trace packet-number 4

737 packets captured

     4: 08:19:36.054181   10.99.117.195.56485 > 10.31.124.31.443: $ 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow


1 packet shown
```


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?

* phase 9: rpf-check
* phase 5: NAT
* phase 4: ACCESS-LIST
* phase 3: UN-NAT

Section: Troubleshooting using ASDM and CLI

Q77. An engineer would like Cisco AnyConnect users to be able to reach servers within the 10.10.0.0/16 subnet while all other traffic is sent out to the Internet. Which IPsec configuration accomplishes this task?

A.
```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```

B.
```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

C.
```
crypto ikev1 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

D.
```
crypto ikev2 authorization policy Local_Authz_01
 route set remote ipv4 10.10.0.0 0.0.255.255
```

* Option A
* Option B
* Option C
* Option D

Q78. 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?

* crypto access list
* Phase 1 policy
* transform set
* preshared key

Reference:

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

Q79. Which redundancy protocol must be implemented for IPsec stateless failover to work?
* SSO
* GLBP
* HSRP
* VRRP

Reference:

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

Q80. Refer to the exhibit.

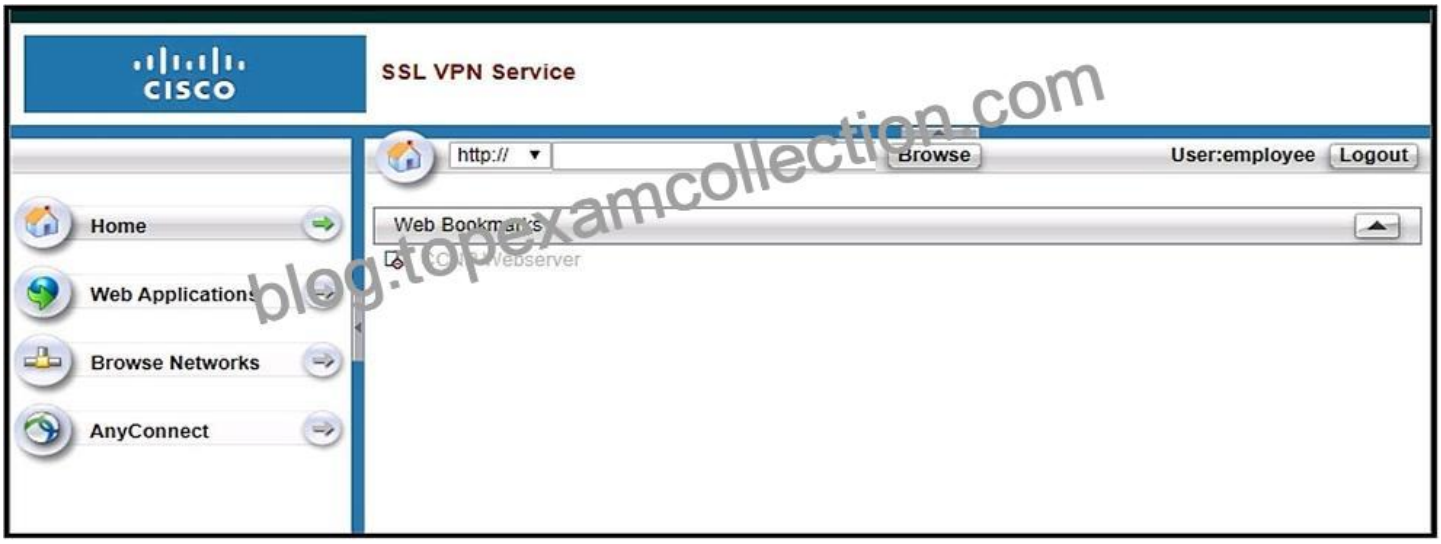
```
aaa authentication login default local
aaa authorization network Flex_AAA local

crypto ikev2 authorization policy Flex_Auth
 route set remote ipv4 10.0.0.0 255.255.255.0

crypto ikev2 proposal Crypto_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Crypto_Policy
 proposal Crypto_Proposal

crypto ikev2 keyring FlexKey
 peer any
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !

crypto ikev2 profile IKEv2_Profile
 match identity remote address 192.168.0.12 255.255.255.255
 authentication local pre-share
 authentication remote pre-share
 keyring local FlexKey
 aaa authorization group cert list Flex_AAA Flex_Auth

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile FlexVPN_Ipsec
 set transform-set TS
 set ikev2-profile IKEv2_Profile

interface Tunnel1
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 192.168.0.12
 tunnel protection ipsec profile FlexVPN_Ipsec
```

The VPN tunnel between the FlexVPN spoke and FlexVPN hub 192.168.0.12 is failing. What should be done to correct this issue?
* Add the address 192.168.0.12 255.255.255.255 command to the keyring configuration.
* Add the match fvrf any command to the IKEv2 policy.
* Add the aaa authorization group psk list Flex_AAA Flex_Auth command to the IKEv2 profile configuration.
* Add the tunnel mode gre ip command to the tunnel configuration.

Q81. Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?
* DMVPN with ISAKMP
* GETVPN with ISAKMP
* DMVPN with NHRP
* GETVPN with NHRP

Q82. Which two components are required in a Cisco IOS GETVPN key server configuration? (Choose two.)
* RSA key
* IKE policy
* SSL cipher
* GRE tunnel
* L2TP protocol

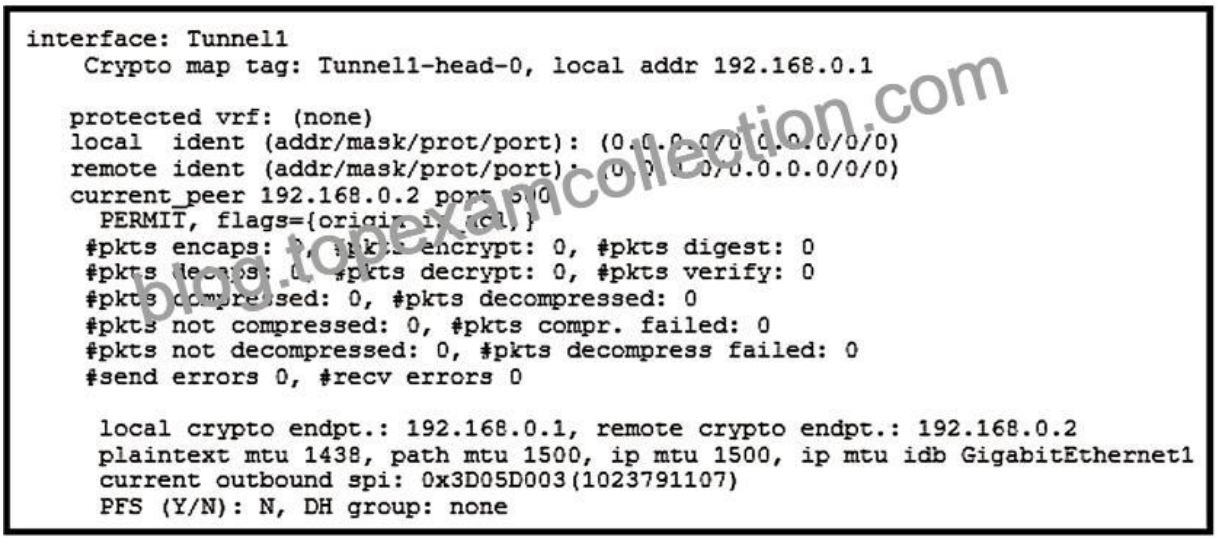
Q83. Refer to the exhibit.



Based on the exhibit, why are users unable to access CCNP Webserver bookmark?
* The URL is being blocked by a WebACL.
* The ASA cannot resolve the URL.
* The bookmark has been disabled.
* The user cannot access the URL.

https://community.cisco.com/t5/network-security/missing-ssl-vpn-bookmarks/td-p/1597023

Q84. Refer to the exhibit.



Which two tunnel types produce the show crypto ipsec sa output seen in the exhibit? (Choose two.)
* crypto map
* DMVPN
* GRE
* FlexVPN
* VTI

Q85. A network engineer must design a clientless VPN solution for a company. VPN users must be able to access several internal web servers. When reachability to those web servers was tested, it was found that one website is not being rewritten correctly by the ASA.

What is a potential solution for this issue while still allowing it to be a clientless VPN setup?
* Set up a smart tunnel with the IP address of the web server.
* Set up a NAT rule that translates the ASA public address to the web server private address on port 80.
* Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.
* Set up a WebACL to permit the IP address of the web server.

Q86. Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?
* svc import profile SSL_profile flash:simos-profile.xml
* anyconnect profile SSL_profile flash:simos-profile.xml
* crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
* webvpn import profile SSL_profile flash:simos-profile.xml

Q87. Refer to the exhibit.

```
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed
policies
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy
found for received TS

*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001
CurState: R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```


An IKEv2 site-to-site tunnel between an ASA and a remote peer is not building successfully. What will fix the problem based on the debug output?

* Ensure crypto IPsec policy matches on both VPN devices.
* Install the correct certificate to validate the peer.
* Correct crypto access list on both VPN devices.
* Specify the peer IP address in the tunnel group name.

To fix the problem with the IKEv2 site-to-site tunnel between an ASA and a remote peer based on the debug output, you should ensure that the crypto IPsec policy matches on both VPN devices. The debug output indicates that the crypto policies on the two VPN devices are mismatched, which is preventing the tunnel from building successfully. Installing the correct certificate to validate the peer, correcting the crypto access list on both VPN devices, and specifying the peer IP address in the tunnel group name will not fix the problem.

Q88. While troubleshooting, an engineer finds that the show crypto isakmp sa command indicates that the last state of the tunnel is MM_KEY_EXCH. What is the next step that should be taken to resolve this issue?

* Verify that the ISAKMP proposals match.
* Ensure that UDP 500 is not being blocked between the devices.
* Correct the peer’s IP address on the crypto map.
* Confirm that the pre-shared keys match on both devices.