300-730Q&As

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which two features are valid backup options for an IOS FlexVPN client? (Choose two.)

A. HSRP stateless failover

B. DNS-based hub resolution

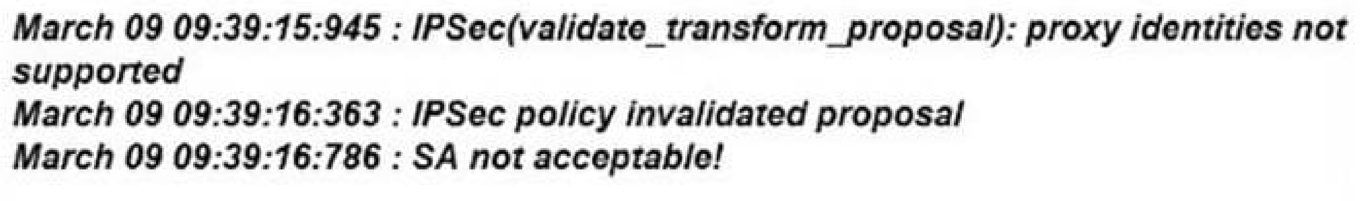
C. reactivate primary peer

D. tunnel pivot E. need distractor

Correct Answer: BC

QUESTION 2

Refer to the exhibit.



```
March 09 09:39:15:945 : IPSec(validate_transform_proposal): proxy identities not
supported
March 09 09:39:16:363 : IPSec policy invalidated proposal
March 09 09:39:16:786 : SA not acceptable!
```

Which action must be taken on the IPsec tunnel configuration to resolve the issue?

A. The access lists on each peer must mirror each other.

B. The transform set on each peer must match.

C. The access lists on each peer must be identical.

D. The transform set on each peer must be compatible.

Correct Answer: A

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

QUESTION 3

Which two types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose two.)

A. SAML

B. NTLM

C. Kerberos

D. OAuth 2.0

E. HTTP Basic

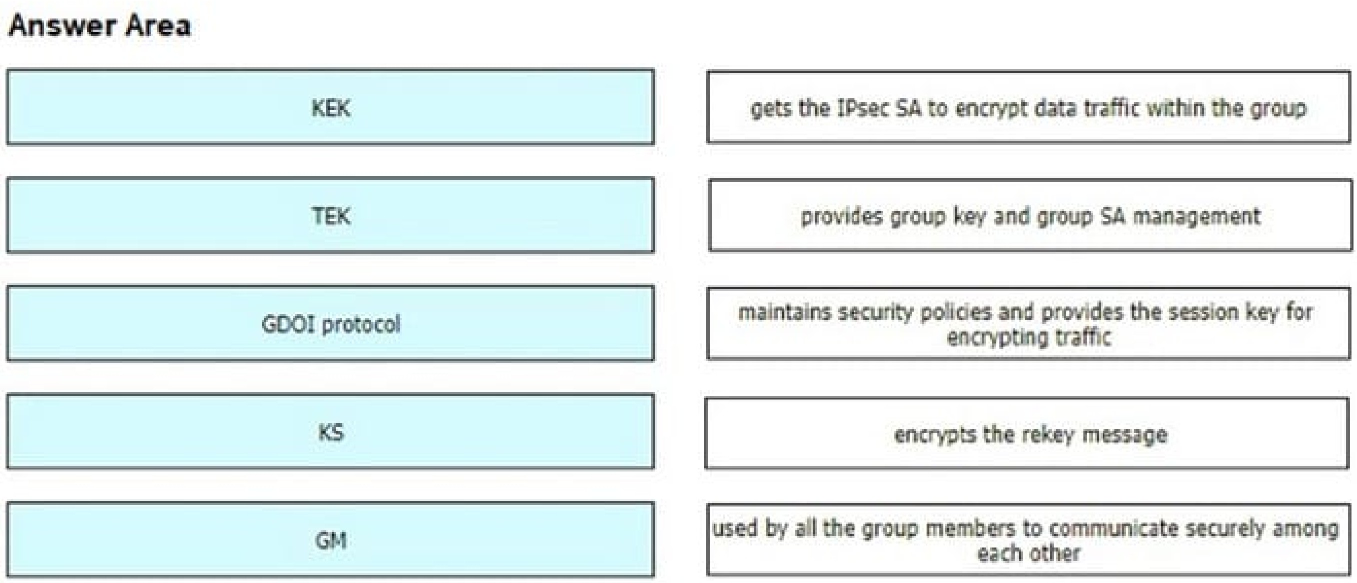
Correct Answer: BE

QUESTION 4

DRAG DROP

Drag and drop the GET VPN components from the left onto the correct descriptions on the right.

Select and Place:



Answer Area

KEK

TEK

GDOI protocol

KS

GM

gets the IPsec SA to encrypt data traffic within the group

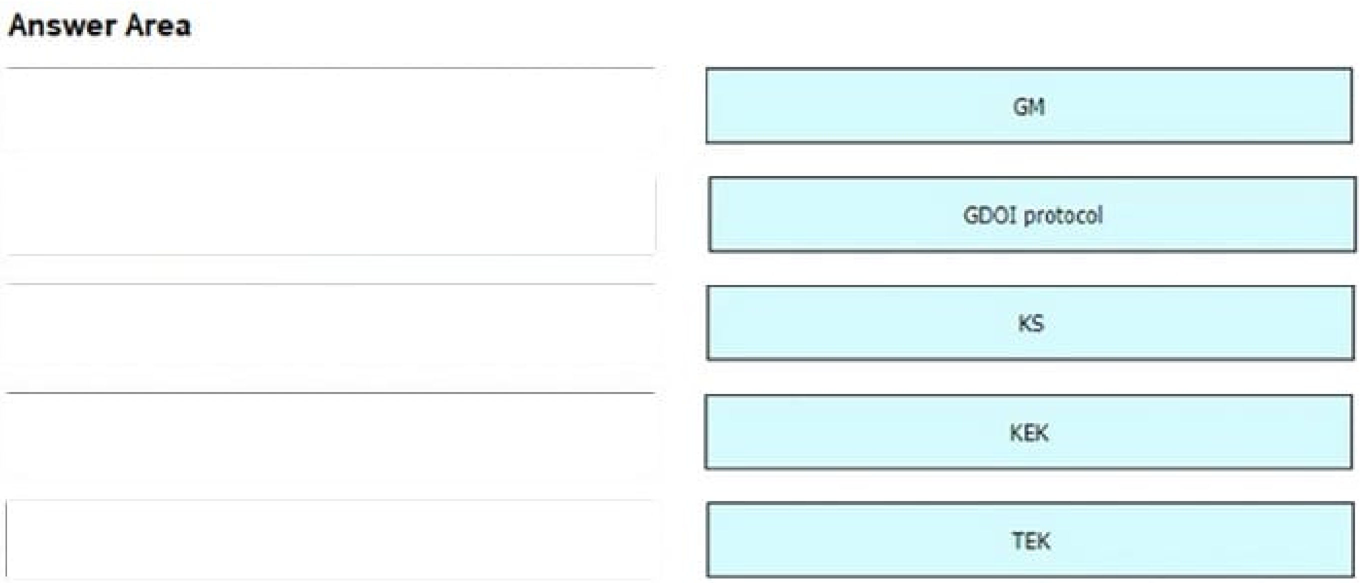
provides group key and group SA management

maintains security policies and provides the session key for encrypting traffic

encrypts the rekey message

used by all the group members to communicate securely among each other

Correct Answer:



Answer Area

GM

GDOI protocol

KS

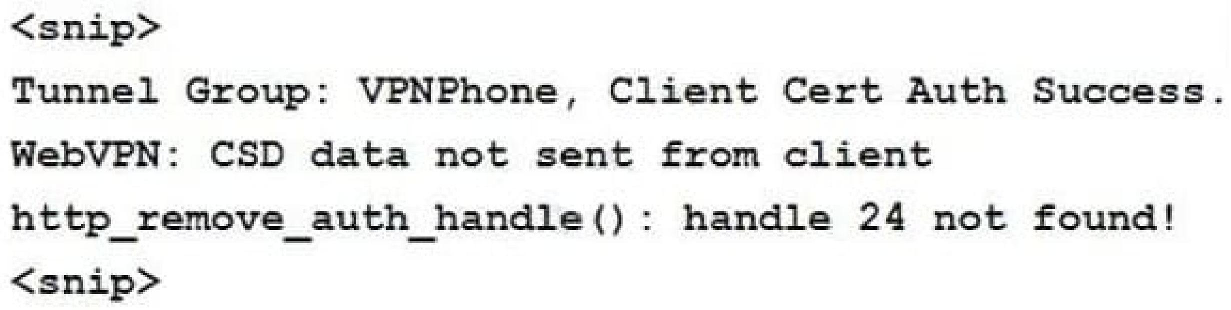
KEK

TEK

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

QUESTION 5

Refer to the exhibit.



```
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

A network administrator is setting up a phone VPN on a Cisco ASA. The phone cannot connect and the error is presented in a debug on the Cisco ASA. Which action fixes this issue?

A. Enable web-deploy of the posture module so that the module can be downloaded from the Cisco ASA to an IP phone.

B. Configure the Cisco ASA to present an RSA certificate to the phone for authentication.

C. Disable Cisco Secure Desktop under the connection profile VPNPhone.

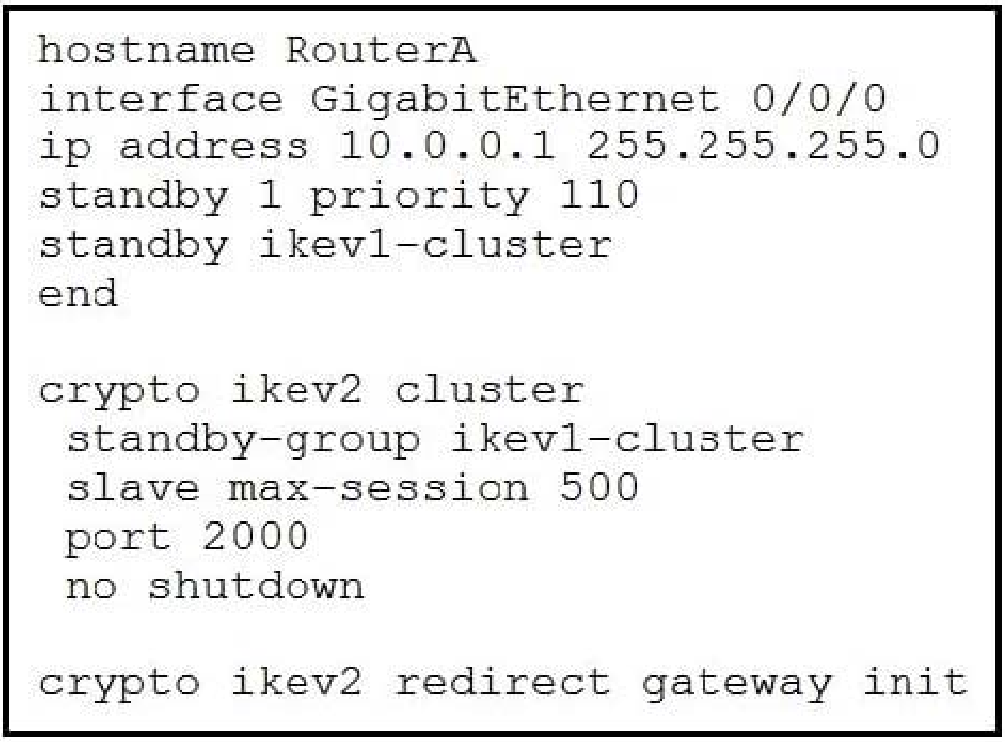
D. Install the posture module on the Cisco ASA.

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116162-trouble-anyconnect-vpn-phone-00.html

QUESTION 6

Refer to the exhibit.



```
hostname RouterA
interface GigabitEthernet 0/0/0
ip address 10.0.0.1 255.255.255.0
standby 1 priority 110
standby ikev1-cluster
end

crypto ikev2 cluster
 standby-group ikev1-cluster
 slave max-session 500
 port 2000
 no shutdown

crypto ikev2 redirect gateway init
```

Which type of VPN implementation is displayed?

A. IKEv1 cluster

B. IKEv2 backup gateway

C. IKEv2 load balancer

D. IKEv2 reconnect

Correct Answer: C

QUESTION 7

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

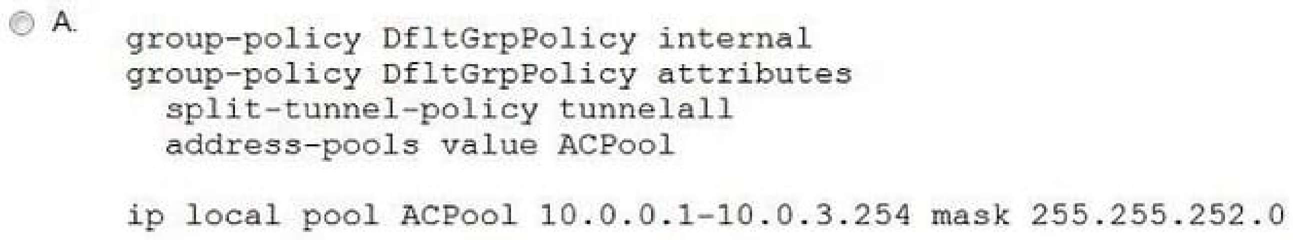
D. webvpn import profile SSL_profile flash:simos-profile.xml

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html

QUESTION 8

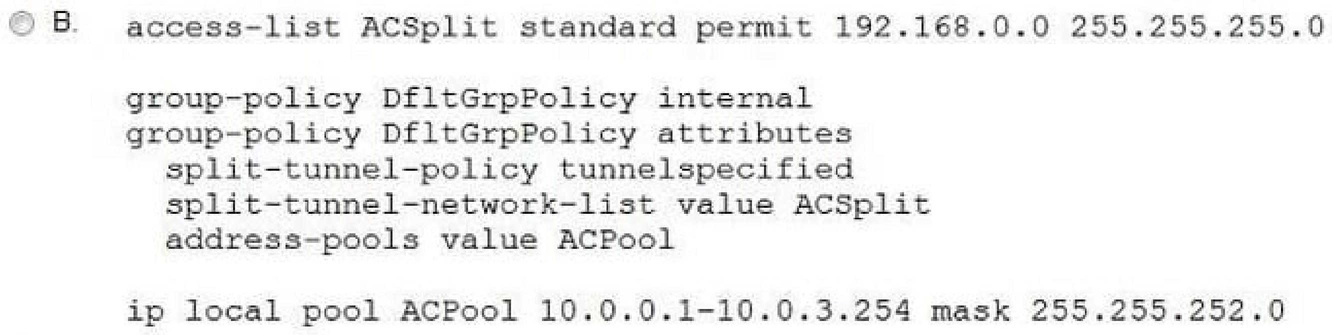
A network engineer must implement an SSLVPN Cisco AnyConnect solution that supports 500 concurrent users, ensures all traffic from the client passes through the ASA, and allows users to access all devices on the inside interface subnet (192.168.0.0/24). Assuming all other configuration is set up appropriately,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

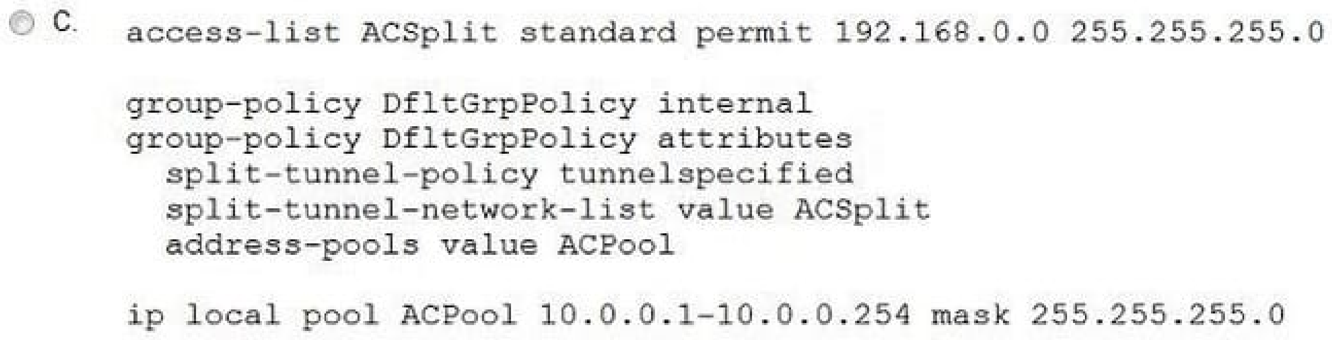


○ B.

```
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
```

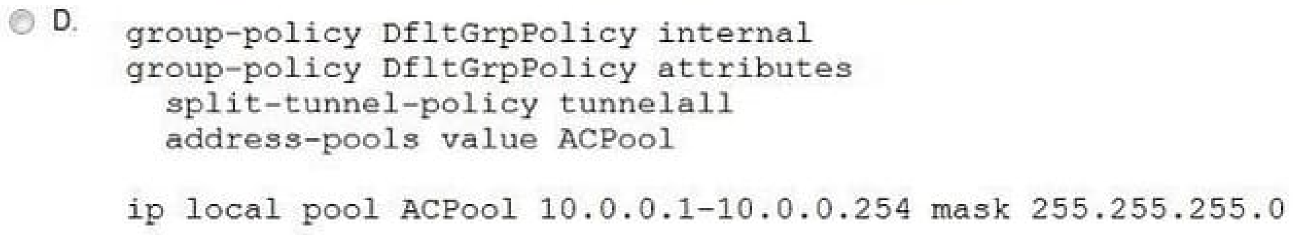


○ C.

```
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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

First, tunnelall to ensure all trafic is passing through ASA (so answer is A or D). second, we need 500 users so the Pool in D is not ensuring this requirement (only 254 ip) so Answer is A.

QUESTION 9

Users cannot log in to a Cisco ASA using clientless SSLVPN. Troubleshooting reveals the error message "WebVPN session terminated: Client type not supported". Which step does the administrator take to resolve this issue?

A. Enable the Cisco AnyConnect premium license on the Cisco ASA.

B. Have the user upgrade to a supported browser.

C. Increase the simultaneous logins on the group policy.

D. Enable the clientless VPN protocol on the group policy.

Correct Answer: D

QUESTION 10

In order to enable FlexVPN to use a AAA attribute list, which two tasks must be performed? (Choose two.)

A. Define the RADIUS server.

B. Verify that clients are using the correct authorization policy.

C. Define the AAA server.

D. Assign the list to an authorization policy.

E. Set the maximum segment size.

Correct Answer: BD

QUESTION 11

What are two differences between ECC and RSA? (Choose two.)

A. Key generation in ECC is slower and more CPU intensive than RSA.

B. ECC can have the same security as RSA but with a shorter key size.

C. ECC cannot have the same security as RSA, even with an increased key size.

D. Key generation in ECC is faster and less CPU intensive than RSA.

E. ECC lags in performance when compared with RSA.

Correct Answer: BD

QUESTION 12

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?

A. Set up a smart tunnel with the IP address of the web server.

B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.

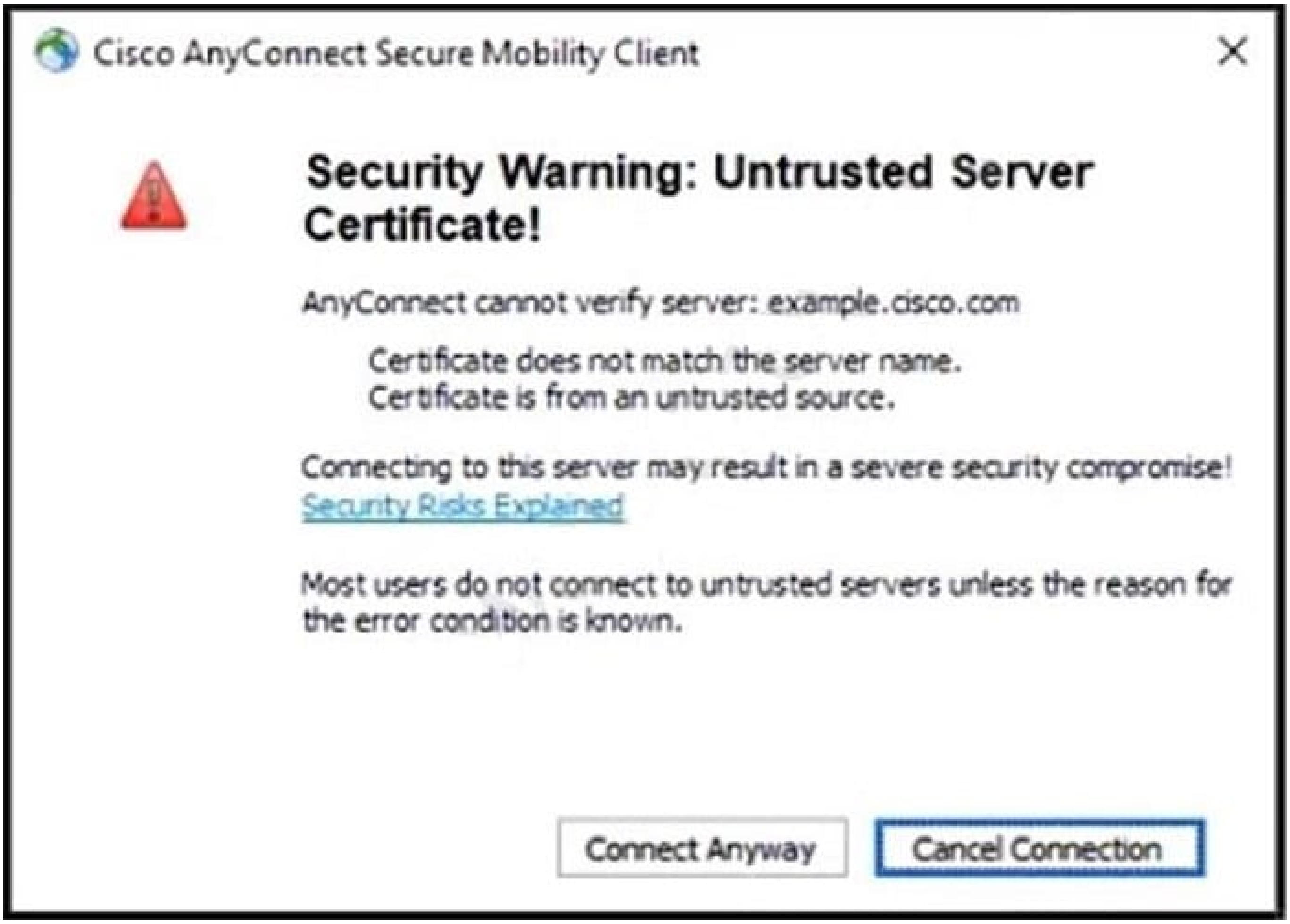
C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.

D. Set up a WebACL to permit the IP address of the web server.

Correct Answer: B

QUESTION 13

Refer to the exhibit.



Cisco AnyConnect Secure Mobility Client

Security Warning: Untrusted Server Certificate!

AnyConnect cannot verify server: example.cisco.com

Certificate does not match the server name.
Certificate is from an untrusted source.

Connecting to this server may result in a severe security compromise!
Security Risks Explained

Most users do not connect to untrusted servers unless the reason for the error condition is known.

A network administrator is setting up Cisco AnyConnect on an ASA headend. When users attempt to connect to the VPN, they are presented with this message. The administrator has replaced the ASA\\'s self-signed certificate with a certificate enrolled with the internal CA and has confirmed that the certificate is not revoked. Which two tasks will the administrator need to do to prevent users from seeing this message? (Choose two.)

A. Trust the issuing CA for the ASA identity certificate on the user\\'s PC.

B. Enroll and import an SSL certificate with the CN value example.cisco.com on the ASA.

C. Add the CN example.cisco.com to the AnyConnect XML certificate matching section.

D. Enable certificate authentication under the connection profile.

E. Add example.cisco.com to the server name list within the AnyConnect Local Policy.

Correct Answer: AB

QUESTION 14

What uses an Elliptic Curve key exchange algorithm?

A. ECDSA

B. ECDHE

C. AES-GCM

D. SHA

Correct Answer: B

Reference: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

QUESTION 15

A user at a company HQ is having trouble accessing a network share at a branch site that is connected with a L2L IPsec VPN. While troubleshooting, a network security engineer runs a packet tracer on the Cisco ASA to simulate the user

traffic and discovers that the encryption counter is increasing but the decryption counter is not. What must be configured to correct this issue?

A. Adjust the routing on the remote peer device to direct traffic back over the tunnel.

B. Adjust the preshared key on the remote peer to allow traffic to flow over the tunnel.

C. Adjust the transform set to allow bidirectional traffic.

D. Adjust the peer IP address on the remote peer to direct traffic back to the ASA.

Correct Answer: A