300-730 Q&As

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

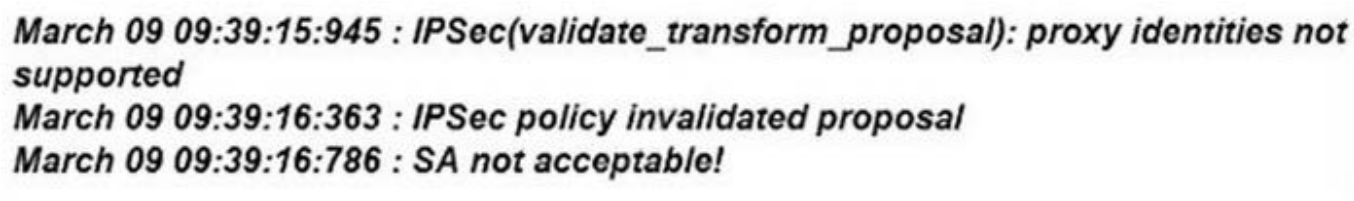
https://www.pass4itsure.com/300-730.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.



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 2

Which parameter in IPsec VPN tunnel configurations is optional?

A. hash

B. lifetime

C. encryption

D. Perfect Forward Secrecy

Correct Answer: D

QUESTION 3

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.

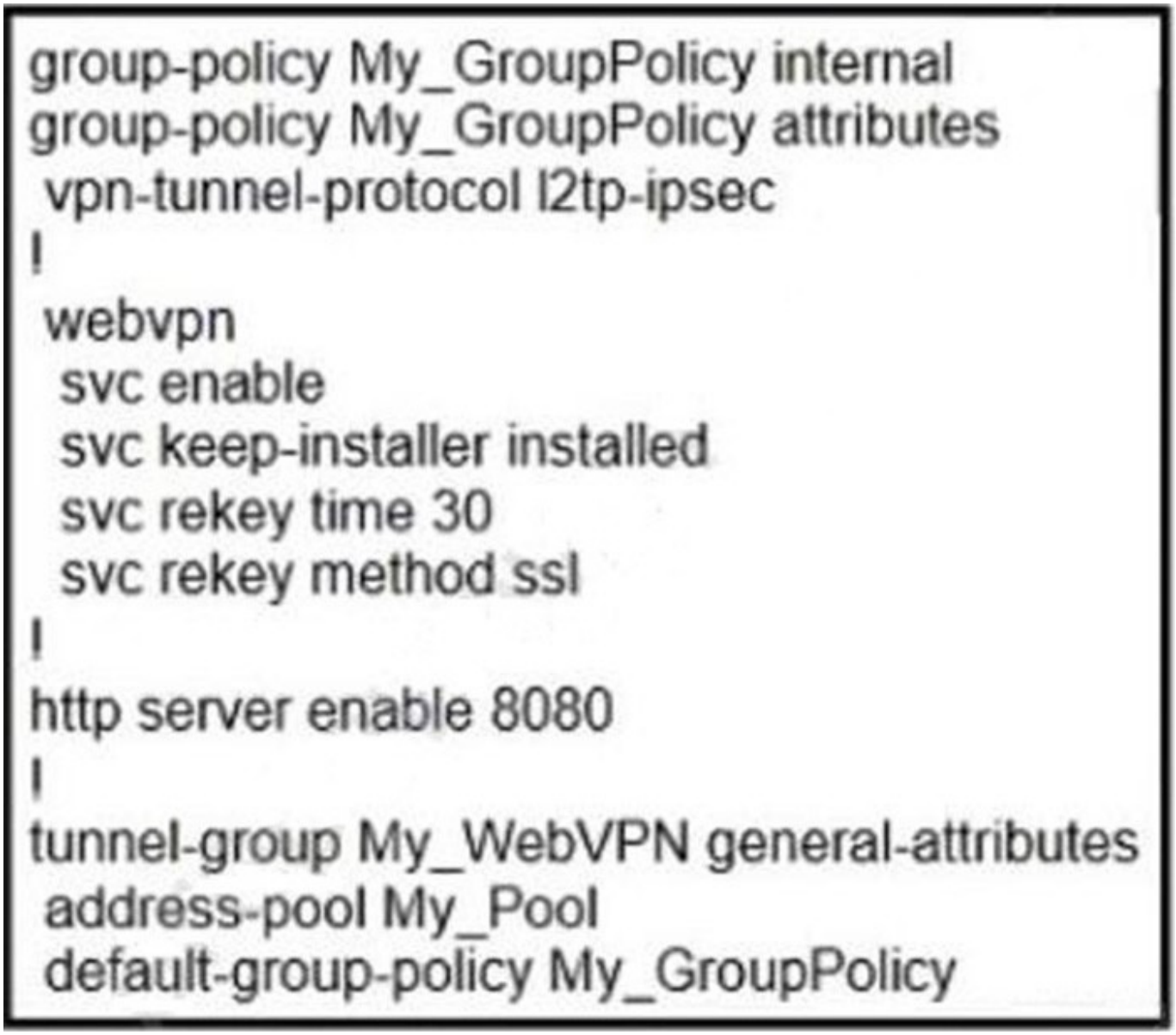
C. Spoke 2 fails the authentication because the remote authentication method is incorrect.

D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Correct Answer: A

QUESTION 4

Refer to the exhibit.



Users cannot connect via AnyConnect SSLVPN. Which action resolves this issue?

A. Configure the ASA to act as a DHCP server.

B. Configure the HTTP server to listen on port 443.

C. Add an IPsec preshared key to the group policy.

D. Add ssl-client to the allowed list of VPN protocols.

Correct Answer: D

QUESTION 5

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 6

Which Diffie Hellman group should be used when ECDH is required in a VPN configuration?

A. 24

B. 19

C. 16

D. 15

Correct Answer: B

QUESTION 7

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 8

Which technology works with IPsec stateful failover?

A. GLBR

B. HSRP

C. GRE

D. VRRP

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp1122512

QUESTION 9

When a FlexVPN is configured, which two components must be configured for IKEv2? (Choose two.)

A. method

B. profile

C. proposal

D. preference

E. persistence

Correct Answer: BC

QUESTION 10

Which two protocols does DMVPN leverage to build dynamic VPNs to multiple destinations? (Choose two.)

A. IKEv2

B. NHRP

C. mGRE

D. mBGP

E. GDOI

Correct Answer: BC

QUESTION 11

Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the client uses the local DNS to perform FQDN resolution.

B. The rewriter enable command under the global webvpn configuration enables the rewriter functionality because that feature is disabled by default.

C. A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.

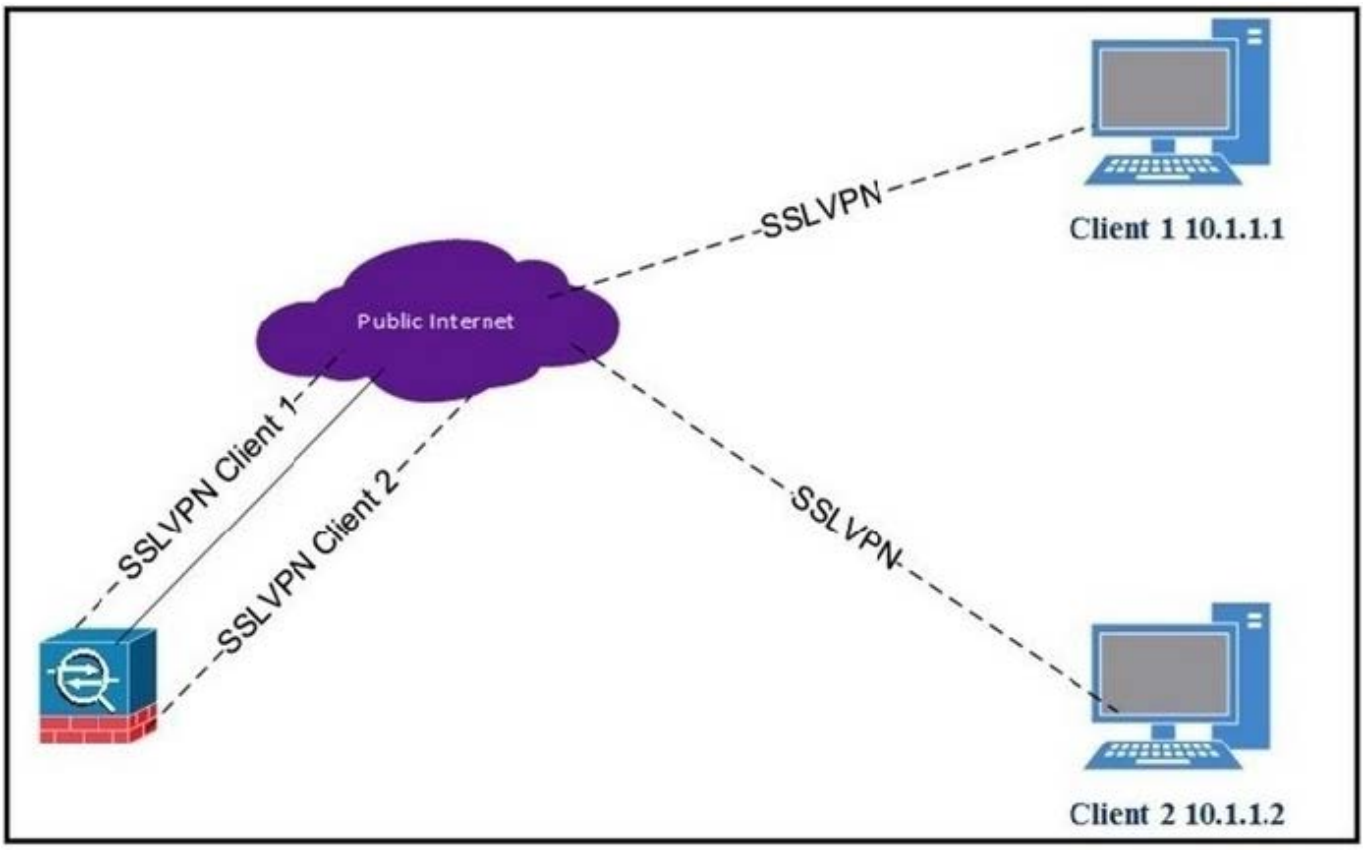
D. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution.

E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

Correct Answer: CD

QUESTION 12

Refer to the exhibit.



Client 1 cannot communicate with client 2. Both clients are using Cisco AnyConnect and have established a successful SSL VPN connection to the hub ASA. Which command on the ASA is missing?

A. dns-server value 10.1.1.2

B. same-security-traffic permit intra-interface

C. same-security-traffic permit inter-interface

D. dns-server value 10.1.1.3

Correct Answer: B

QUESTION 13

Refer to the exhibit.

An engineer must allow Cisco AnyConnect users to access the outside interface using protocol UDP 500/4500. In addition, these clients must be able to establish an SSL connection to update Cisco AnyConnect software over the same connection. Which two actions must be taken to achieve this goal? (Choose two.)

A. IPsec (IKEv2) Allow Access must be checked on the outside interface.

B. SSL Enable DTLS must be checked on the outside interface.

C. Bypass interface access lists for inbound VPN sessions must be unchecked.

D. IPsec (IKEv2) Enable Client Services must be checked on the outside interface.

E. SSL Allow Access must be checked on the outside interface.

Correct Answer: AD