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.leads4pass.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

Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

A. show crypto ikev2 sa

B. show crypto isakmp sa

C. show crypto gkm

D. show crypto identity

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116413-configure-flexvpn-00.pdf

QUESTION 2

Refer to the exhibit.

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-clientless
 split-tunnel-policy tunnelall

tunnel-group Admins type remote-access
tunnel-group Admins general-attributes
 default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes
 group-alias Admins enable

tunnel-group Employee type remote-access
tunnel-group Employee webvpn-attributes
 group-alias Employee enable

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

Which VPN technology is allowed for users connecting to the Employee tunnel group?

A. SSL AnyConnect

B. IKEv2 AnyConnect

C. crypto map

D. clientless

Correct Answer: D

Since there is no vpn-tunnel-protocol defnied under the Employee tunnel-group this setting will be inherited from the DfltGrpPolicy And only ss-clientless is allowed in DfltGrpPolicy.

QUESTION 3

A network engineer is installing Cisco AnyConnect on company laptops so that users can access corporate resources remotely. The VPN concentrator is a Cisco router running IOS-XE 16.9.1 code and configured as a FlexVPN server that

uses local authentication and *$Cisc431089017$* as the key-id for the IKEv2 profile. Which two steps must be taken on the computer to allow a successful AnyConnect connection to the router? (Choose two.)

A. In the Cisco AnyConnect XML profile, set the IPsec Authentication method to EAP-AnyConnect.

B. In the Cisco AnyConnect XML profile, add the hostname and host address to the server list.

C. In the Cisco AnyConnect XML profile, set the user group field to DefaultAnyConnectClientGroup.

D. In the Cisco AnyConnect Local Policy, set the BypassDownloader option in the local to true.

E. In the Cisco AnyConnect Local Policy, add the router IP address to the Update Policy.

Correct Answer: AD

QUESTION 4

Which redundancy protocol must be implemented for IPsec stateless failover to work?

A. SSO

B. GLBP

C. HSRP

D. VRRP

Correct Answer: C

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

QUESTION 5

Refer to the exhibit.

```
Spoke1#
     local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     #pkts encaps: 200, #pkts encrypt: 200
     #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
     inbound esp sas:
     spi: 034B32CA36 (1261619766)
     outbound esp sas:
     spi:0xD601918E (1760427022)

Spoke2#
     local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     #pkts encaps: 210, #pkts encrypt: 210,
     #pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
     inbound esp sas:
     spi: 03D601918E (1760427022)
     outbound esp sas:
     spi: 034BS2CA36 (1261619766)
```

An engineer is troubleshooting a new GRE over IPsec tunnel. The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2. Which type of traffic is being blocked?

A. ESP packets from spoke2 to spoke1

B. ISAKMP packets from spoke2 to spoke1

C. ESP packets from spoke1 to spoke2

D. ISAKMP packets from spoke1 to spoke2

Correct Answer: A

QUESTION 6

A network engineer is configuring a server. The router will terminate encrypted VPN connections on g0/0, which is in the VRF "Internet". The clear-text traffic that must be encrypted before being sent out traverses g0/1, which is in the VRF "Internal". Which two VRF-specific configurations allow VPN traffic to traverse the VRF-aware interfaces? (Choose two.)

A. Under the IKEv2 profile, add the ivrf Internal command.

B. Under the virtual-template interface, add the ip vrf forwarding Internet command.

C. Under the IKEv2 profile, add the match fvrf Internal command.

D. Under the IKEv2 profile, add the match fvrf Internet command.

E. Under the virtual-template interface, add the tunnel vrf Internet command.

Correct Answer: DE

QUESTION 7

A user is experiencing delays on audio calls over a Cisco AnyConnect VPN. Which implementation step resolves this issue?

A. Change to 3DES Encryption.

B. Shorten the encryption key lifetime.

C. Install the Cisco AnyConnect 2.3 client for the user to download.

D. Enable DTLS.

Correct Answer: D

QUESTION 8

Which remote access VPN technology requires transform sets to be explicitly defined?

A. Clientless SSLVPN

B. IPSec

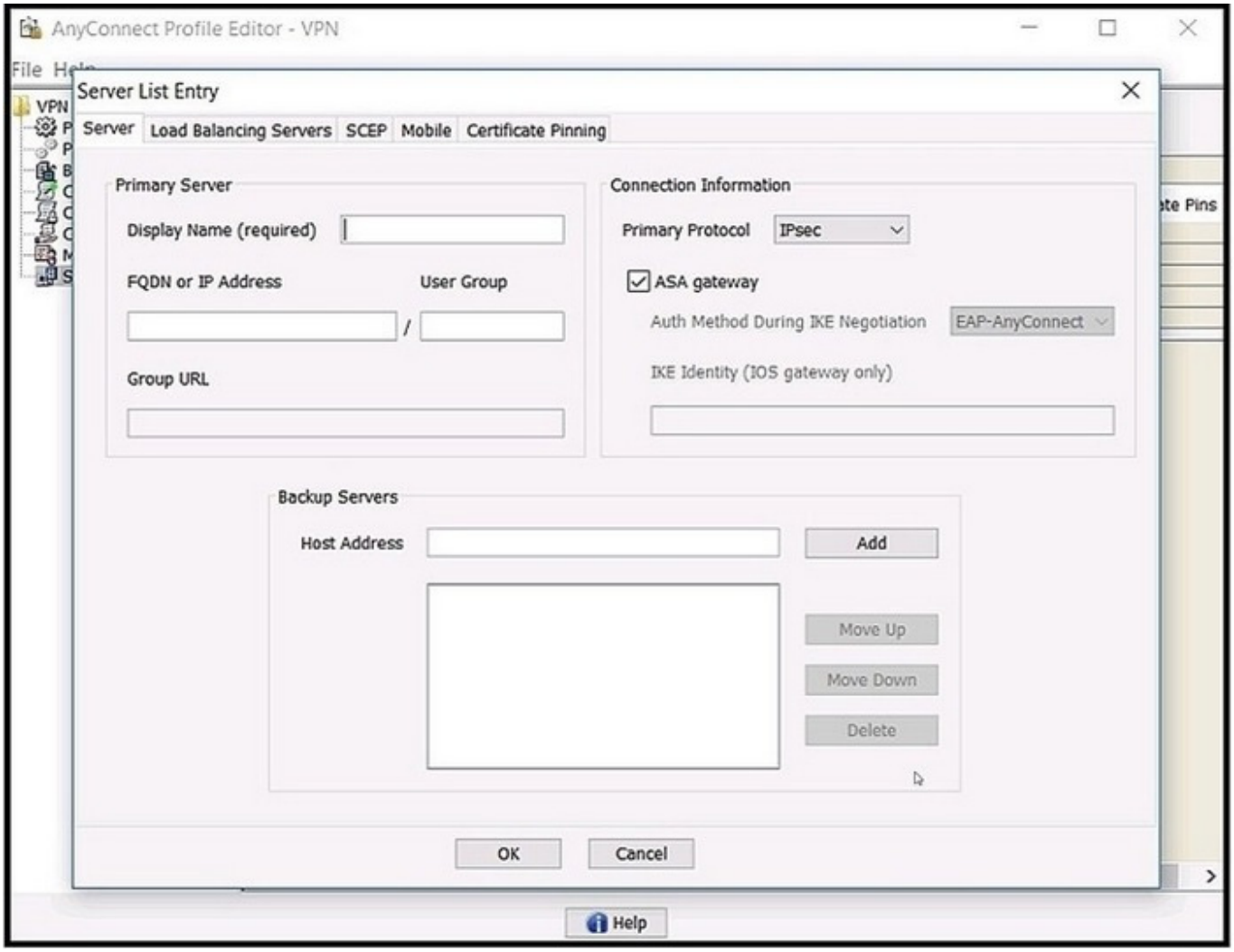
C. Cisco Anyconnect

D. FlexVPN

Correct Answer: B

QUESTION 9

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

Correct Answer: D

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

QUESTION 10

A network administrator wants to block traffic to a known malware site at https:/www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. Access Control policy with URL filtering

B. Prefilter policy

C. DNS policy

D. SSL policy

Correct Answer: A

The correct answer is A. Access Control policy with URL filtering. An Access Control policy is a type of policy that allows you to control how traffic is handled on your network based on various criteria, such as source and destination IP addresses, ports, protocols, applications, users, and URLs. URL filtering is a feature that enables you to block or allow traffic based on the URL category or reputation of the website. You can create custom URL objects to specify the exact URLs or domains that you want to block or allow. For example, you can create a URL object for https:/www.badsite.com and set it to block. This will prevent any traffic from reaching that site and any subdomains under it12.

B. Prefilter policy is a type of policy that allows you to perform fast actions on traffic before it reaches the Access Control policy. You can use prefilter rules to drop, fastpath, or trust traffic based on simple criteria, such as IP addresses or ports. However, prefilter rules do not support URL filtering, so you cannot use them to block traffic based on the website domain3.

C. DNS policy is a type of policy that allows you to inspect and modify DNS requests and responses on your network. You can use DNS rules to block, monitor, or sinkhole DNS

QUESTION 11

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?

A. The XML profile is not configured correctly for the affected users.

B. The new client image does not use the same major release as the current one.

C. Client services are not enabled.

D. Client software updates are not supported with IKEv2.

Correct Answer: C

On ASDM, under connection profile -> access interfaces -> IPSEC (IKEv2) Access : you can check or uncheck the boxes for "allow access" and "enable client access"

QUESTION 12

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

A. HSRP stateless failover

B. DNS-based hub resolution

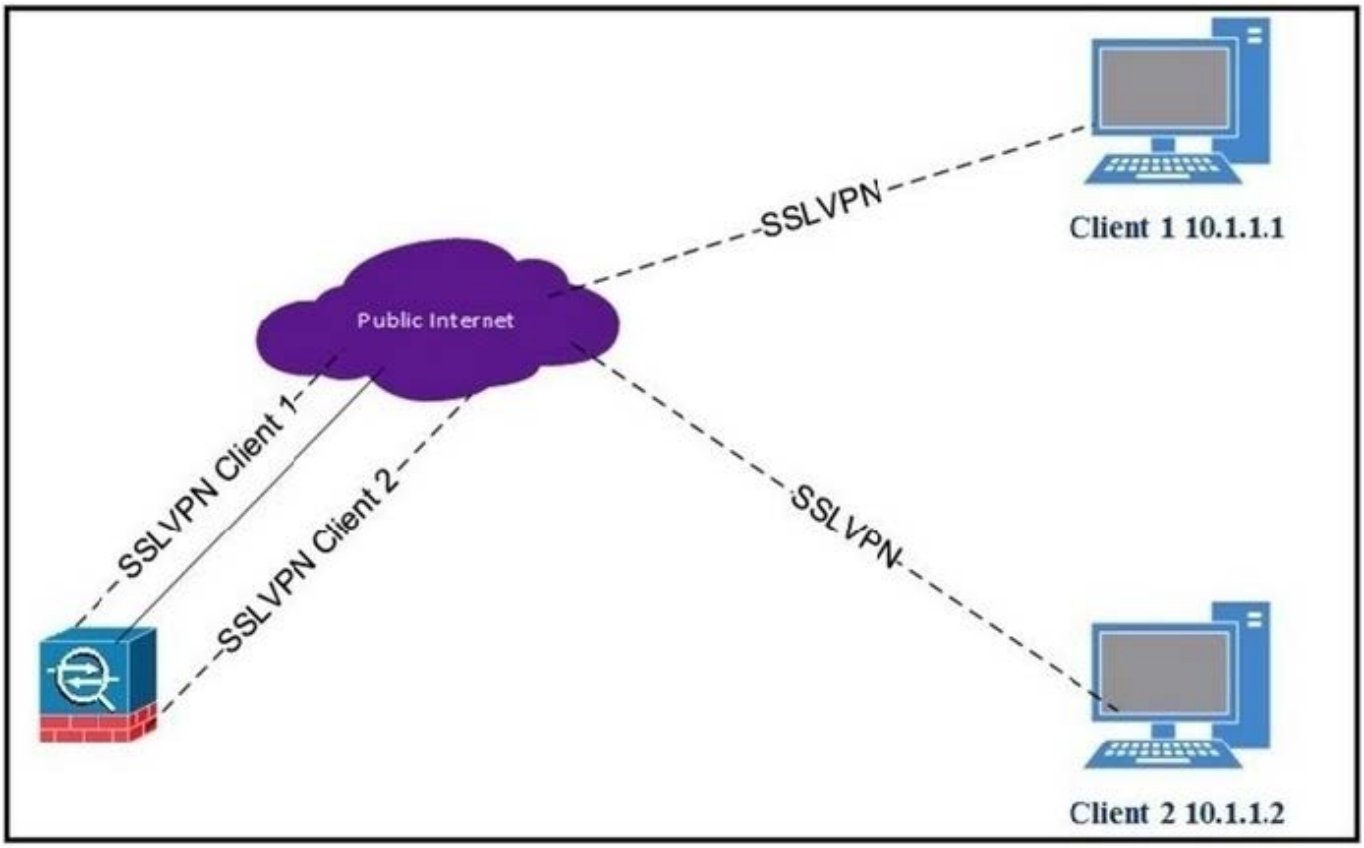
C. reactivate primary peer

D. tunnel pivot E. need distractor

Correct Answer: BC

QUESTION 13

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 14

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

Correct Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

QUESTION 15

An engineer notices that while an employee is connected remotely, all traffic is being routed to the corporate network. Which split-tunnel policy allows a remote client to use their local provider for Internet access when working from home?

A. tunnelall

B. excludeall

C. tunnelspecified

D. excludespecified

Correct Answer: C