

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.pass2lead.com/300-730.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?

- A. DMVPN with ISAKMP
- B. GETVPN with ISAKMP
- C. DMVPN with NHRP
- D. GETVPN with NHRP

Correct Answer: C

QUESTION 2

An administrator is setting up Cisco AnyConnect on a Cisco ASA with the requirement that AnyConnect automatically establishes a VPN when a company-owned laptop is connected to the internet outside of the corporate network. Which configuration meets these requirements?

- A. SBL with user certificate authentication
- B. TND with machine certificate authentication
- C. SBL with machine certificate authentication
- D. TND with user certificate authentication

Correct Answer: D

QUESTION 3

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.

Correct Answer: C

QUESTION 4

Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

- A. sequence numbers that enable scalable replay checking
- B. enabled use of ESP or AH
- C. design for use over public or private WAN
- D. no requirement for an overlay routing protocol

Correct Answer: D

QUESTION 5

Refer to the exhibit.

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page. ⓘ
 Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

➕ Add ✎ Edit 🗑 Delete Find: 🔍 ☺ ☹ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
Clientless	<input type="checkbox"/>	<input type="checkbox"/>	Clientless	AAA(LOCAL)	Clientless
AnyConnect	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AnyConnect	AAA(LOCAL)	GroupPolicy_AnyConnect

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Based on this ASDM output, which remote access technologies are allowed on the ASA?

- A. SSLAnyConnect VPN
- B. IKEv2 and SSL AnyConnect VPN
- C. SSL clientless VPN
- D. IKEv2 AnyConnect VPN

Correct Answer: B

[Latest 300-730 Dumps](#)

[300-730 VCE Dumps](#)

[300-730 Practice Test](#)