

Lead2Passed



Lead2Passed

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

Login / Register My Shopcart (1)

Input your exam code ...



Try before you buy

Download a free sample of any of our exam questions and answers

- ✓ Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
- ✓ PDF format: Easy to read and print learning materials, our products are available in PDF file format.
- ✓ Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

<http://www.lead2passed.com>

Valid Certification Exam Dumps Materials and Study Guide -
Lead2Passed

Exam : **300-209J**

Title : **Implementing Cisco Secure Mobility Solutions**

Vendor : **Cisco**

Version : **DEMO**

QUESTION NO: 1

展示を参照してください。

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                src                state                conn-id status
209.165.200.230   209.165.201.10   MM_KEY_EXCH         1005 ACTIVE
209.165.201.10   209.165.200.230   MM_KEY_EXCH         1004 ACTIVE
```

PSKを使用して、2つのインターネットルーター間にIKEv1 IPsecトンネルを実装しています。構成が完了すると、IPsec VPNトンネルはネゴシエートできません。問題を解決するには何を設定する必要がありますか？

- A.両方のルーターでISAKMPポリシーを一致させる
- B.両方のルーターで一致するPSK
- C.両方のルーターの正しいトンネル宛先
- D.両方のルーターのISAKMP ID

Answer: B

QUESTION NO: 2

エンジニアがリモートアクセス用にSSL

VPNを構成しています。パケット遅延の影響を受けやすいリアルタイムアプリケーションが使用されます。

SSL接続に関連する遅延と帯域幅の問題を回避するために、エンジニアはどの機能を有効にする必要がありますか？

- A.DPD
- B.IKEv2
- C.DTLS
- D.SVC

Answer: C

Explanation

Dead Peer Detection (DPD) ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed. To enable dead peer detection (DPD) and set the frequency with which either the AnyConnect client or the ASA gateway performs DPD

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpnanyconnect.html#id_33133

QUESTION NO: 3

どのコマンドがCisco適応型セキュリティアプライアンスからすべての暗号化設定をクリアしますか？

- A.暗号構成のクリア
- B.暗号化ipsecの構成をクリアします
- C.暗号マップをクリア
- D.暗号化ikev2 saをクリア

Answer: A

QUESTION NO: 4

ネットワークエンジニアがASAで設定されたVPNトンネルのトラブルシューティングを行っており、フェーズ1が完了していないことがわかりました。

IKEフェーズ1トンネルが正常にネゴシエートされるためには、どの構成パラメーターが一致する必要がありますか？

- A.SAライフタイム
- B.変換セット
- C.DHグループ
- D.アイドルタイムアウト

Answer: C

QUESTION NO: 5

ユーザーがクライアントレスSSL

VPNからアプリケーションを起動できるようにするには、どのテクノロジーをクライアントコンピューターにインストールする必要がありますか？

- A.Silverlight
- B.QuickTimeプラグイン
- C.フラッシュ
- D.Java

Answer: D

Explanation

Explantion/Refrence

Cisco redistributes the following open-source, Java-based components to be accessed as plug-ins for Web browsers in Clientless SSL VPN sessions.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/vpn/asdm-79-vpn-config/webvpnconfigure-gateway.pdf>

QUESTION NO: 6

Cisco IOS GETVPNのキーサーバの目的である2つのオプションはどれですか？

(2つ選択してください。)

- A.動的ルーティング情報を配布します
- B.グループメンバーを認証する
- C.通過データトラフィックを暗号化します
- D.静的ルーティング情報を配布します
- E.セキュリティポリシーを定義および配布します

Answer: B E

QUESTION NO: 7

SSL VPNの高可用性を提供できるテクノロジーはどれですか？

- A.アクティブ/パッシブフェールオーバー構成のCisco ASAペア
- B.トンネルグループマップへの証明書
- C.複数トンネル構成

D.DMVPN

Answer: A

QUESTION NO: 8

暗号化および整合性キーを安全に導出するために、ISAKMPはどのアルゴリズムを使用しますか？

A.ECDSA

B.Diffie- Hellman

C.AES

D.3DES

E.RSA

Answer: B

Explanation

A Diffie-Hellman group to determine the strength of the encryption-keydetermination algorithm.

The ASA uses this algorithm to derive the encryption and hash keys

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_configuration/vpn_ike.pdf

QUESTION NO: 9

PKIシステム内の信頼できるエンティティとは何ですか？

A.認証局

B.登録機関

C.ルート証明書

D.RSA認証サーバー

Answer: A

QUESTION NO: 10

どの暗号化アルゴリズムを避けることを推奨していますか？

A.HMAC-SHA1

B.AES-CBC

C.DES

D.HMAC-MD5

Answer: C

QUESTION NO: 11

ブランチ間で頻繁にVoIPコールを行うMPLSで接続されたブランチオフィスのコレクションに推奨されるVPNソリューションはどれですか？

A.DMVPN

B.サイト間

C.GETVPN

D.Cisco AnyConnect

Answer: C

QUESTION NO: 12

展示を参照してください。

```
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Received Packet [From
209.165.200.230:500/To 209.165.201.10:500/VRF i0:f0]
Initiator SPI : E96F3F6F56547EB0 - Responder SPI : 9AEF97215425DDA1
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
  NOTIFY (AUTHENTICATION_FAILED)

*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Process auth response notify
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Auth exchange failed
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Auth exchange failed

*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Auth exchange failed
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Abort exchange
R1#
*Nov 14 00:44:25.818: IKEv2: (SA ID = 1):Deleting SA
```

PSKを使用して、2つのインターネットルーター間にIKEv2 IPsecトンネルを実装しています。設定が完了すると、IPsec VPNトンネルはネゴシエートできません。問題をトラブルシューティングするには、デバッグを有効にします。問題を解決するためにどのアクションを実行しますか？

- A.両方のルーターでIKEv2キーリングアドレスとPSK設定を確認します
- B.IKEV2許可ポリシーを構成して、ピアルーターを許可します
- C.IKEv2ポリシーで使用されるDiffie-Hellmanキーを変更しますか？
- D.電子メールアドレスを使用して各ルーターのIKEv2 IDを構成します

Answer: A

QUESTION NO: 13

キーのインポートまたはエクスポート中にパスフレーズ保護を提供する暗号化方法はどれですか？

- A. RSA
- B. Blowfish
- C. Serpent
- D. AES

Answer: A

Explanation

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-dep

QUESTION NO: 14

展示を参照してください。

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=#
```

エンジニアがデバッグメッセージに遭遇します。どのアクションができる
エンジニアはこのエラーメッセージを排除するために取るのですか？

- A.VPNピアアドレスを修正します
- B.IPSec再生ウィンドウを調整します
- C.事前共有キーを変更して一致させます
- D.より強力な暗号化スイートを使用する

Answer: B

QUESTION NO: 15

エンジニアがIPsecサイト間トンネルのトラブルシューティングを行っており、トンネルの
状態がMM_WAIT_MSG6であることに気付きました。トンネルが確立されない原因として考
えられるものは何ですか？（2つ選択してください）

- A.暗号化ポリシーがルーターとリモートピア間で一致しません
- B.ルーターとリモートピアの事前共有キーが一致しません
- C.ルーターはIPv6を使用するメッセージを予期していますが、IPv4で受信しています
- D.ルーターはIKEv1を使用していますが、リモートピアはIKEv2を使用しています
- E.2つのルーター間のパスにNAT / PATがあり、UDP 4500がブロックされています

Answer: B E