

# Implementing Secure Solutions with Virtual Private Networks (300-730 Japanese Version)

1. ネットワーク エンジニアは、請負業者が内部サーバーにアクセスできるようにするリモートアクセス ソリューションを設計する必要があります。これらの請負業者は、コンピュータにアプリケーションをインストールする権限を持っていません。この設計ではどの VPN ソリューションを使用する必要がありますか？

A. SSL AnyConnect

B. Clientless

C. Port forwarding

D. IKEv2 AnyConnect

**Answer(s): B**

---

2. 展示を参照してください。構成出力に基づくと、VPN テクノロジーは何ですか？

A. L2VPN

B. DMVPN

C. site-to-site

D. multicast VPN

**Answer(s): A**

---

3. ネットワーク エンジニアは、会社のラップトップに Cisco AnyConnect をインストールして、ユーザーが会社のリソースにリモートでアクセスできるようにしています。VPN コンセントレ

ータは、IOS-XE 16.9.1 コードを実行し、ローカル認証と \*\$Cisc431089017\$\* を IKEv2 プロファイルのキー ID として使用する FlexVPN サーバーとして構成された Cisco ルーターです。ルーターへの AnyConnect 接続を成功させるために、コンピュータで実行する必要がある 2 つの手順はどれですか？（2つ選んでください。）

A. Cisco AnyConnect ローカル ポリシーで、ルーターの IP アドレスを更新ポリシーに追加します。

B. Cisco AnyConnect XML プロファイルで、ユーザー グループ フィールドを DefaultAnyConnectClientGroup に設定します。

C. Cisco AnyConnect XML プロファイルで、IPsec 認証方式を EAP-AnyConnect に設定します。

D. Cisco AnyConnect ローカル ポリシーで、ローカルの BypassDownloader オプションを true に設定します。

E. Cisco AnyConnect XML プロファイルで、ホスト名とホスト アドレスをサーバー リストに追加します。

**Answer(s): C,D**

---

4. ネットワーク管理者が Cisco ASA に IKEv2 Cisco AnyConnect を導入しました。現在の構成では、すべてのトラフィックが VPN を介してトンネリングされます。ユーザーからはクラウドベースのアプリケーションのパフォーマンスが低いという報告がありますが、オンプレミスサーバーへの接続に関する問題は報告されていません。Cisco Webex トラフィックのパケット分析では、重複 ACK がほとんどなく、RTT が高く、IP フラグメントがないことが示されています。

A. DTLS を使用するように Cisco AnyConnect を設定します。

B. Cisco AnyConnect トンネル MTU を減らします。

C. 動的スプリット トンネルの除外を設定します。

D. ASA の外部インターフェイスで QoS を設定します。

**Answer(s): C**

---

5. 展示を参照してください。ネットワーク管理者が Cisco ASA で電話 VPN を設定しています。電話が接続できず、Cisco ASA のデバッグにエラーが表示されます。どのアクションでこの問題を解決できますか？

A. ポスチャ モジュールの Web 展開を有効にして、モジュールを Cisco ASA から IP 電話にダウンロードできるようにします。

B. 認証のために電話機に RSA 証明書を提示するように Cisco ASA を設定します。

C. 接続プロファイル VPNPhone で Cisco Secure Desktop を無効にします。

D. Cisco ASA にポスチャ モジュールをインストールします。

**Answer(s): C**

---

6. 図を参照してください。DMVPN スポークはハブとのセッションを確立していません。この問題を解決するには、どの 2 つのアクションを実行すればよいですか? (2 つ選択してください)。

A. スポークの nhrp 認証キーを cisco123 に変更します。

B. スポーク上の ISAKMP キー アドレスを 0.0.0.0 に変更します。

C. スポーク上の ISAKMP ポリシー認証を事前共有に変更します。

D. スポーク NHS を 172.16.18.1 に、nbma を 10.0.0.1 に変更します。

E. 変換セットをトンネルモードに変更します。

**Answer(s): A,C**

---

7. 管理者は、今後の Cisco AnyConnect 展開にどの認証プロトコルを実装する必要があるかを決定しています。上層部からのセキュリティ要件のリストは、AnyConnect ユーザに C1\$c0451035084! などの複雑なパスワードの使用を強制する機能、パスワードの有効期限が切れる数日前にユーザに警告する機能、およびリモート アクセス セッション中にユーザがパスワードを変更できるようにする機能です。 。これらの要件を満たすにはどの認証プロトコルを使用する必要がありますか?

A. LDAPS

B. 半径

C. ケルベロス

D. TACACS+

**Answer(s): A**

---

8. GETVPNのどの機能がDMVPNおよびFlexVPNの制限ですか？

A. オーバーレイルーティングプロトコルは不要

B. ESPまたはAHの使用を有効化

C. スケーラブルな再生チェックを可能にするシーケンス番号

D. パブリックまたはプライベートWANを介して使用するための設計

**Answer(s): A**

---

9. DMVPN フェーズ 3 の実装に固有の 2 つの NHRP 機能はどれですか? (2つ選んでください。)

A. 登録応答

B. リダイレクト

C. 解決返信

D. 登録要求

E. 解決依頼

**Answer(s): C,E**

---

10. ネットワーク エンジニアがサーバーを構成しています。ルーターは、VRF「インターネット」にある g0/0 で暗号化された VPN 接続を終了します。送信前に暗号化する必要があるクリアテキストトラフィックは、VRF「内部」にある g0/1 を通過します。VPN トラフィックが VRF

認識インターフェイスを通過できるようにする VRF 固有の設定はどれですか？（2つ選んでください。）

A. IKEv2 プロファイルの下に、match fvrfl Internet コマンドを追加します。

B. virtual-template インターフェイスの下に、tunnel vrf Internet コマンドを追加します。

C. virtual-template インターフェイスの下に、ip vrf forwarding Internet コマンドを追加します。

D. IKEv2 プロファイルの下に、ivrf Internal コマンドを追加します。

E. IKEv2 プロファイルの下に、match fvrfl Internal コマンドを追加します。

**Answer(s):** A,B

---

11. 展示を参照してください。プライマリ プロトコルとして IPsec を使用して ASA ヘッドエンドに接続するために Cisco AnyConnect プロファイルを作成する場合、ユーザー グループ フィールドにどの値を設定する必要がありますか。

A. アドレスプール

B. グループエイリアス

C. グループポリシー

D. トンネルグループ

**Answer(s):** D

---

12. IOSルータのフラッシュにアップロードされたCisco AnyConnectプロファイルを識別するコマンドはどれですか。

A. svcインポートプロファイルSSL\_profile flash : simos-profile.xml

B. anyconnectプロファイルSSL\_profile flash : simos-profile.xml

C. 暗号vpn anyconnectプロファイルSSL\_profile flash : simos-profile.xml

D. webvpnインポートプロファイルSSL\_profile flash : simos-profile.xml

**Answer(s): C**

---

13. エンジニアは、新しい DMVPN を統合して、Cisco IOS ルータを使用してインターネット全体でリモート オフィスをリンクしました。リモート サイトに接続すると、ping と音声データが適切に流れているように見え、すべてのトンネル統計はそれらが稼働していることを示しています。ただし、RDP を使用してリモート サーバーに接続しようとする、接続に失敗します。この問題を解決するアクションはどれですか？

A. ルーター内の MTU サイズを調整します。

B. RDP サーバー上の証明書を置き換えます。

C. RDP ポートを拡張 ACL に追加します。

D. DMVPN タイムアウト値を変更します。

**Answer(s): A**

---

14. Cisco ASAはアクティブ/スタンバイモードで設定されています。Cisco AnyConnectユーザーがフェイルオーバーイベントの後に接続できるようにするために何が必要ですか？

A. AnyConnectイメージを両方のフェールオーバーASAデバイスにアップロードする必要があります。

B. vpnsession-dbは手動でクリアする必要があります。

C. XMLプロファイルでバックアップサーバーを構成します。

D. AnyConnectクライアントはスタンバイIPアドレスを指す必要があります。

**Answer(s): A**

---

15. エンジニアは、2つのCisco ASAがクライアントレスSSLVPNアクセスを提供するVPNロードバランシングクラスタのSSL証明書を要求しています。クライアントレスVPNにアクセスするためにユーザーが入力するFQDNはasa.example.comで、ユーザーはasa1.example.comまたはasa2.example.comにリダイレクトされます。クラスタFQDNと個々

の Cisco ASA FQDN は、それぞれ IP アドレス 192.168.0.1、192.168.0.2、および 192.168.0.3 に解決されます。発行された証明書は、証明書検証エラーを返さずにクラスタ内のいずれかの ASA の ID を検証するために使用できる必要があります。これらの要件を満たすには、どのフィールドを証明書に含める必要がありますか？

A. CN=\*.example.com、SAN=asa.example.com

B. CN=192.168.0.1、SAN=asa1.example.com、asa2.example.com

C. CN=asa.example.com、SAN=asa.example.com、asa1.example.com、asa2.example.com

D. CN=192.168.0.1、SAN=192.168.0.1、192.168.0.2、192.168.0.3

**Answer(s): C**

---

16. エンジニアは IPsec VPN を構成しており、信頼性が高く、ACK とシーケンスをサポートする認証プロトコルを選択したいと考えています。

A. ESP

B. AES-256

C. AES-192

D. IKEv1

**Answer(s): A**

---

17. 管理者は、内部 RDP サーバにアクセスする必要があるユーザのために ASA で VPN を設定しています。セキュリティ上の制限により、Microsoft RDP クライアントは、グループポリシーによってクライアントワークステーションでの実行がブロックされています。これらのユーザが RDP サーバにアクセスできるようにするために、管理者はどの VPN 機能を実装する必要がありますか？

A. クライアントレス プロキシ

B. クライアントレス リライター

C. クライアントレス プラグイン

D. スマート トンネリング

**Answer(s): C**

---

18. エンジニアは接続の問題を調査し、Cisco FTD でパケット キャプチャ機能を使用することを決定する必要があります。目標は、Cisco FTD デバイスを通過する実際のパケットを確認し、出力の一部として Snort 検出アクションを確認することです。Capture-traffic コマンドを発行すると、パケットのみが表示されます。この問題を解決するにはどのアクションを実行すればよいでしょうか？

A. Capture-traffic コマンドの後に -T オプションを使用してトレースを指定します

B. Cisco FMC CLI ではなく Cisco FMC GUI 内でトレースを実行します。

C. キャプチャトラフィックコマンドの一部として冗長オプションを使用します。

D. キャプチャコマンドを使用し、トレースオプションを指定して必要な情報を取得します。

**Answer(s): A**

---

19. IOS FlexVPN クライアントの有効なバックアップ オプションはどれですか? (2つ選んでください。)

A. HSRP ステートレス フェイルオーバー

B. DNS ベースのハブ解決

C. プライマリ ピアを再アクティブ化

D. トンネルピボット

E. ディストラクタが必要

**Answer(s): B,C**

---



20. 展示を参照してください。顧客は最初の試行でのみ AnyConnect 接続を確立できます。その後の試行は失敗します。何が問題なのでしょう？

A. プライマリ プロトコルは SSL である必要があります。

B. IKEv2 はパス上でブロックされています。

C. UserGroup は接続プロファイルの名前とは異なる必要があります。

D. UserGroup は接続プロファイルの名前と同じである必要があります。

**Answer(s): D**

---