FreeCram

# FreeCram


Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

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

We're not the only ones **happy** about FreeCram Practice Material ...

**12514+** customers in 100+ countries use FreeCram Test Engine. Meet our customers.

https://www.freecram.com

Free Exam/Cram Practice Materials.

**Exam** : **300-730J**

**Title** : Implementing Secure Solutions with Virtual Private Networks (300-730日本語版)

**Vendor** : Cisco

**Version** : DEMO

**QUESTION NO: 1**
ハブは、別のスポークの背後に存在するネットワークの NHRP
解決要求をスポークから受信した場合、どのようなアクションを実行しますか?
**A.** ハブは要求元のスポークに解決応答を返します。
**B.** ハブは独自の NHRP マッピングを更新します。
**C.** ハブは要求を宛先スポークに転送します。
**D.** ハブは、両方のスポークに応答できるように、2
番目のスポークが要求を送信するのを待機します。
***Answer:*** C

**QUESTION NO: 2**
ネットワーク管理者は、WebVPN か AnyConnect
のどちらかを選択するようユーザに要求することなく、Cisco ASA が Cisco AnyConnect
クライアントのダウンロードを自動的に開始することを望んでいます。このタスクを実行するコマンドはどれですか?
**A.** anyconnect ssl df-bit-ignore 有効化
**B.** anyconnect 質問なし デフォルトの anyconnect
**C.** anyconnect はデフォルトの anyconnect を有効にするよう要求します
**D.** anyconnect モジュール値のデフォルト
***Answer:*** B

**QUESTION NO: 3**
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:*** C
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533- AnyConnect-Configure-Basic-SSLVPN-for-I.html

**QUESTION NO: 4**
展示を参照してください。スポークと 2 つの DMVPN ハブ間の VPN
トンネルが起動しません。ネットワーク管理者は、フェーズ 1 とフェーズ 2
の暗号化、ハッシュ、および DH
グループの提案が両端で一致していることを確認しました。この問題の解決策は何ですか。

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
Dst             src             state          conn-id        slot     status
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0      ACTIVE
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0      ACTIVE (deleted)
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0      ACTIVE
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0      ACTIVE (deleted)


Router#debug crypto isakmp

01:12:45.250: ISAKMP:(0):Old State = IKE_READY
                      New State = IKE_I_MM1
01:12:45.250: ISAKMP:(0): beginning Main Mode exchange
01:12:45.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:45.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:12:55.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
01:12:55.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:55.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

**A.** 双方向 UDP 500/4500 トラフィックを確保します。
**B.** isakmp フェーズ 1 の有効期間を延長します。
**C.** VPN トラフィックの NAT ステートメントを追加します。
**D.** 共有トンネル保護を有効にします。
***Answer:*** A

**QUESTION NO: 5**
図を参照してください。DMVPN フェーズ 2 構成からどのような 2 つの結論を導き出すべきでしょうか? (2 つ選択してください。)

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
ip mtu 1440
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 150
no ip split-horizon eigrp 100
no ip next-hop-self eigrp 100
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
```

**A.** Next-hop-self は必須です。
**B.** EIGRP ネイバー隣接関係は失敗します。
**C.** 動的ルーティング プロトコルとして EIGRP が使用されます。
**D.** EIGRP ルートの再配布は許可されません。
**E.** スポークツースポーク通信が許可されます。
***Answer:*** CE

**QUESTION NO: 6**
クライアントレスSSLVPNユーザーが利用できるようにするには、どのセクションでCisco ASAにブックマークまたはURLリストを設定する必要がありますか？
**A.** tunnel-group (general-attributes)
**B.** tunnel-group (webvpn-attributes)
**C.** webvpn (group-policy)
**D.** webvpn (global configuration)
***Answer:*** C
Explanation:
The bookmark is applied under the web vpn subconfiguration mode of the group policy.

**QUESTION NO: 7**
ユーザがブックマーク リストを使用して接続プロファイルを設定し、クライアントレス SSLVPN
接続をテストすると、すべてのブックマークがグレー表示されます。この動作を修正するには何をしなければなりませんか?
**A.** ブックマークを正しいグループ ポリシーに適用します。

**B.** ブックマークの下にある Web サーバーの正しいポートを指定します。
**C.** Cisco ASA で DNS サーバーを構成し、Web
サーバーのレコードがあることを確認します。
**D.** Cisco ASA と Web サーバー間の HTTP/HTTPS 接続を確認します。
***Answer:*** C

**QUESTION NO: 8**
ネットワーク エンジニアは、2 つの Cisco IOS ルータ間に FlexVPN
トンネルを実装しています。FlexVPN トンネルは、1500 の IP MTU
で構成されたインターフェイス上の暗号化されたトラフィックで終了します。会社には、ネットワークに出入りするフラグメント化されたトラフィックをドロップするセキュリティポリシーがあります。トンネルは、ユーザーと内部サーバーの間で TFTP
データを転送するために使用されます。TFTP トラフィックが VPN
を通過していない場合、最大 IP パケット サイズは 1500
になる可能性があります。暗号化されたペイロードが 90
バイトを追加すると仮定すると、TFTP トラフィックがドロップされることなく FlexVPN
トンネルを通過できるのはどの設定ですか?
**A.** トンネル IP MTU を 1500 に設定します。
**B.** トンネル tcp adjust-mss を 1460 に設定します。
**C.** トンネル IP MTU を 1400 に設定します。
**D.** トンネル tcp adjust-mss を 1360 に設定します。
***Answer:*** C
Explanation:
tcp adjust-mss is for tcp traffic only. TFTP is UDP.

**QUESTION NO: 9**
展示を参照してください。エンジニアは、ブランチ
サイトのルーターに新しいアドレスが割り当てられた後に発生した問題を診断しています。デバッグに基づいて、この問題を解決するには何をする必要がありますか?

```
IKEv2:(SESSION ID = 16,SA ID = 2):Received Packet [From 192.168.20.25:500/To 192.168.20.26:500/VRF i0:f0]
Initiator SPI : 334586B9AF754E5D - Responder SPI : AC90AD1EE140D901 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr AUTH SA TSi TSr NOTIFY(USE_TRANSPORT_MODE) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

 IKEv2:(SESSION ID = 16,SA ID = 2):Process auth response notify
 IKEv2:(SESSION ID = 16,SA ID = 2):Searching policy based on peer's identity '192.168.20.25' of type 'IPv4 address'
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Failed to locate an item in the database
 IKEv2:(SESSION ID = 16,SA ID = 2):Verification of peer's authentication data FAILED
 IKEv2:(SESSION ID = 16,SA ID = 2):Auth exchange failed
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Auth exchange failed
 IKEv2:(SESSION ID = 16,SA ID = 2):Abort exchange
IKEv2:(SESSION ID = 16,SA ID = 2):Deleting SA
IKEv2:(SESSION ID = 10,SA ID = 1):Retransmitting packet
```

**A.** リモート ピアの IP アドレスをサーバーの IKEv2 キーリングに追加します。
**B.** 両側で正しい事前共有キーが設定されていることを確認します。
**C.** デバイス間の UDP 500 パケットがドロップされないようにします。
**D.** リモート ピアの ID をサーバーの IKEv2 プロファイルに追加します。
***Answer:*** D

**QUESTION NO: 10**
VPN ヘッドエンドが異なるサイトにあるリモート ルーターの NAT 後の IP
アドレスを動的に学習できるのは、どのテクノロジーと VPN コンポーネントですか?
**A.** ISAKMP を使用した DMVPN
**B.** ISAKMP を使用した GETVPN
**C.** NHRP を使用した DMVPN
**D.** NHRP を使用した GETVPN
***Answer:*** C

**QUESTION NO: 11**
展示を参照してください。構成ではどのタイプの VPN が使用されていますか?

```
!
interface Tunnel0
 vrf forwarding GREEN
 no ip address
 no ip redirects
 ipv6 address FE80::2001 link-local
 ipv6 address 2001:DB8:1:1::1/64
 ipv6 nhrp authentication cisco123
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 100
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf RED
!
```

**A.** GETVPN
**B.** FlexVPN
**C.** DMVPN
**D.** IPSec
***Answer:*** C

**QUESTION NO: 12**
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

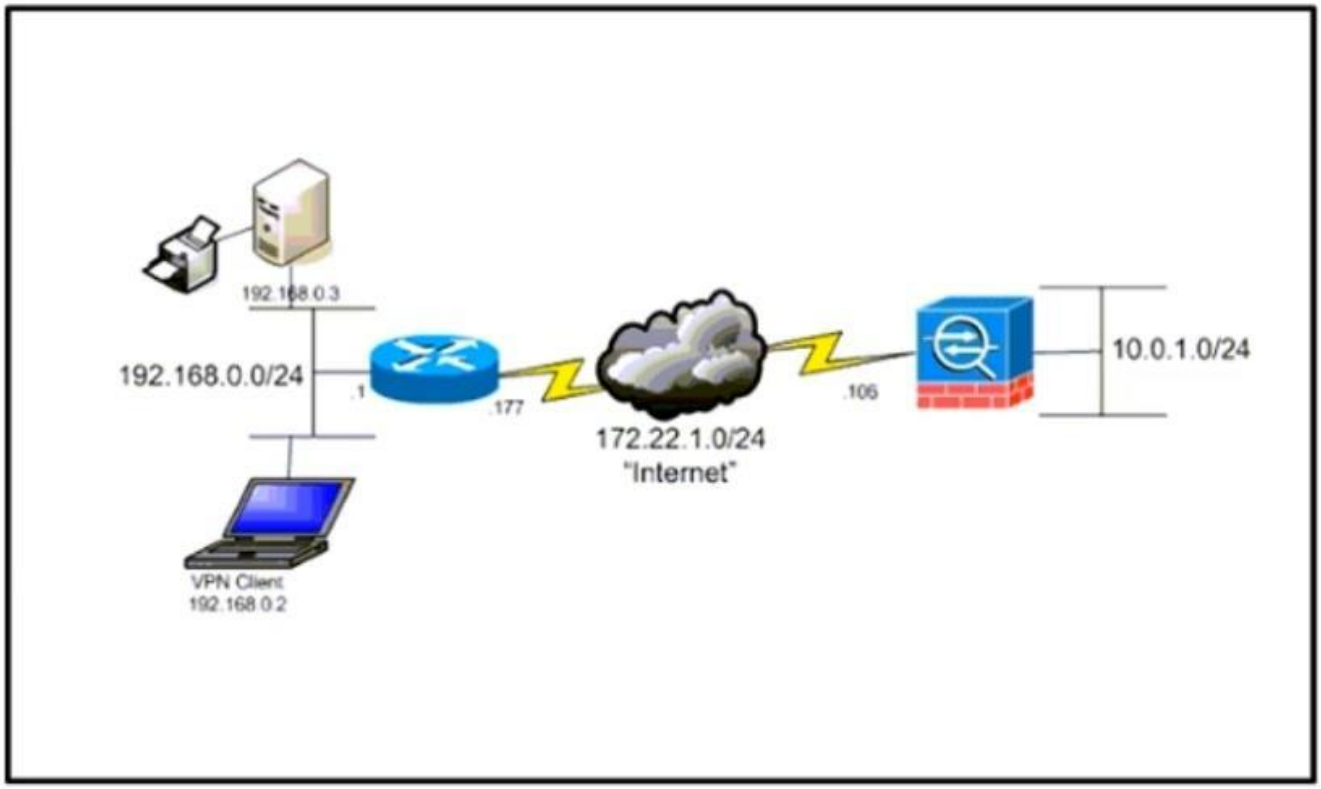
***Answer:*** C

Explanation:

https://integratingit.wordpress.com/2020/03/14/asa-vpn-load-balancing/

**QUESTION NO: 13**

展示を参照してください。ネットワーク管理者は、Cisco AnyConnect Secure Mobility Client が IKEv2
経由で企業リソースに安全にアクセスし、ローカルで印刷できるようにする必要があります。インターネット宛てのトラフィックは、引き続き Cisco ASA
にトンネリングする必要があります。この目的を達成するために、管理者はどの設定を使用しますか。




**A.** 192.168.0.3/32 に対する拒否を含む除外ポリシーを分割します。

**B.** 0.0.0.0/32 の許可を使用して除外ポリシーを分割します。

**C.** すべてのポリシーをトンネルします。

**D.** 192.168.0.0/24 の許可を含むポリシーを分割します。

***Answer:*** B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html

**QUESTION NO: 14**

展示を参照してください。IPsec Cisco AnyConnect クライアントは接続に失敗し、IOS ヘッドエンドへの接続が試行されるたびにこれらのデバッグが生成されます。どのアクションでこの問題を解決できますか?

```
IKEv2-ERROR:(SESSION ID = 20,SA ID = 1):: The peer's KE payload contained the wrong DH group
IKEv2-PAK:(SESSION ID = 20,SA ID = 1):Next payload: NOTIFY, version: 2.0 Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE Message id: 0, length: 38
Payload contents:
 NOTIFY(INVALID_KE_PAYLOAD)  Next payload: NONE, reserved: 0x0, length: 10
    Security protocol id: Unknown - 0, spi size: 0, type: INVALID_KE_PAYLOAD

IKEv2-ERROR:(SESSION ID = 20,SA ID = 1):Initial exchange failed: Initial exchange failed
```

**A.** DH グループの設定を修正します。
**B.** PFS設定を修正してください。
**C.** 整合性設定を修正します。
**D.** 暗号化設定を修正してください。
***Answer:*** A

**QUESTION NO: 15**
展示を参照してください。ネットワーク セキュリティ管理者は、2 つのサイト間でサイト間 IPsec VPN を構成した後、このエラー
メッセージを受け取ります。この問題の解決策は何ですか。

```
IPSEC(validate_proposal): invalid local address 192.168.10.1
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

**A.** トランスポート セットはサイト間で一致する必要があります。
**B.** IPsec ポリシーはサイト間で一致する必要があります。
**C.** ISAKMP ポリシーはサイト間で一致する必要があります。
**D.** 暗号マップを正しいインターフェースに適用する必要があります。
***Answer:*** D
Explanation:
The error message "IPSEC(validate_proposal): invalid local address 192.168.10.1" indicates that the IPsec tunnel cannot establish because the specified local address is incorrect or not reachable. One common cause of this issue is that the crypto map is not applied to the correct interface or is missing entirely.

**QUESTION NO: 16**
IPsecステートフルフェールオーバーで機能するテクノロジはどれですか。
**A.**GLBR
**B.**HSRP
**C.**GRE
**D.**VRRP
***Answer:*** B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp
1122512

**QUESTION NO: 17**
Cisco ASA でクライアントレス VPN を実装するには、どの 2
つのタスクを実行する必要がありますか? (2 つ選択してください。)

**A.** 接続プロファイルを構成する
**B.** AnyConnect パッケージをアップロードします。
**C.** 登録済みの X.509 証明書をインストールします。
**D.** 言語翻訳ファイルを設定します。
**E.** ポータルのカスタマイズを構成します。
***Answer:*** AC

**QUESTION NO: 18**
Cisco IOS GETVPN キー サーバ構成で必要な 2 つのコンポーネントはどれですか? （2つ選んでください。）
**A.** RSA キー
**B.** IKE ポリシー
**C.** SSL 暗号
**D.** GRE トンネル
**E.** L2TP プロトコル
***Answer:*** AB

**QUESTION NO: 19**
スポークツースポークトンネルが許可されていないFlexVPNハブアンドスポークトポロジで、ハブがFlexVPNトンネルを終端できるようにするには、どのコマンドが必要ですか？
**A.**インターフェース仮想アクセス
**B.**ip nhrpリダイレクト
**C.**インターフェーストンネル
**D.**インターフェース仮想テンプレート
***Answer:*** D
Explanation:
Spoke-to-Spoke traffic is not allowed and wanted, therefore redirect is not needed. But FlexVPN uses Virtual Templates to create Virtual Access interfaces for each connected Spoke.

**QUESTION NO: 20**
スマートトンネルが適切に機能するための要件は何ですか？
**A.**クライアントマシンでJavaまたはActiveXを有効にする必要があります。
**B.**アプリケーションはUDPである必要があります。
**C.**ステートフルフェイルオーバーを構成しないでください。
**D.**クライアントマシンのユーザーには、管理者アクセス権が必要です。
***Answer:*** A
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00.html

**QUESTION NO: 21**
企業本社のユーザーが、L2L IPsec VPN
に接続されている支社サイトのネットワーク共有にアクセスできません。トラブルシューテ

ィング中に、ネットワーク セキュリティ エンジニアは Cisco ASA でパケット
トレーサを実行してユーザ
トラフィックをシミュレートし、暗号化カウンタが増加しているのに復号化カウンタが増加していないことを発見しました。この問題を修正するには、何を構成する必要がありますか?

**A.** リモート ピア
デバイスのルーティングを調整して、トラフィックをトンネル経由で戻します。

**B.** リモート
ピアの事前共有キーを調整して、トラフィックがトンネルを通過できるようにします。

**C.** 双方向トラフィックを許可するようにトランスフォーム セットを調整します。

**D.** リモート ピアのピア IP アドレスを調整して、トラフィックを ASA に戻します。

***Answer:*** A

**QUESTION NO: 22**
展示を参照してください。ユーザーは AnyConnect SSLVPN
経由で接続できません。どのアクションでこの問題を解決できますか?

```
group-policy My_GroupPolicy internal
group-policy My_GroupPolicy attributes
 vpn-tunnel-protocol l2tp-ipsec
!
 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
http server enable 8080
!
tunnel-group My_WebVPN general-attributes
 address-pool My_Pool
 default-group-policy My_GroupPolicy
```

**A.** ASA を DHCP サーバとして動作するように設定します。

**B.** HTTP サーバーをポート 443 でリッスンするように構成します。

**C.** グループ ポリシーに IPsec 事前共有キーを追加します。

**D.** ssl-client を VPN プロトコルの許可リストに追加します。

***Answer:*** D

**QUESTION NO: 23**
FlexVPN で使用するのに推奨される暗号化技術はどれですか? (2 つ選択してください。)
**A.** SHA (HMAC variant)
**B.** Diffie-Hellman
**C.** DES
**D.** MD5 (HMAC variant)
***Answer:*** AB

**QUESTION NO: 24**
展示を参照してください。ネットワーク エンジニアが Cisco IOS ルータでリモート
アクセス VPN を設定していますが、Cisco Secure Client
クライアントからの接続を確立できません。どのアクションでこの問題を解決できますか。

```
aaa authentication login EAP_AUTHC local
aaa authorization exec default local
aaa authorization network EAP_AUTHZ local
!
!
crypto pki trustpoint TP_AnyConnect
enrollment selfsigned
usage ike
serial-number none
fqdn Router.com
ip-address none
subject-name cn=r01.companyx.com
subject-alt-name r01.companyx.com
revocation-check none
rsakeypair AnyConnect
!
!
crypto ikev2 profile AC_EAP
match identify remote key-id *$AnyConnectClient$*
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint TP-AnyConnect
aaa authentication anyconnect-eap EAP_AUTHC
aaa authorization group anyconnect-eap list EAP_AUTHZ ikev2-auth-policy
aaa authorization user anyconnect-eap cached
!
no crypto ikev2 http-url cert
!
```

**A.** ikev2 プロファイルで対称キーを使用します。
**B.** セキュア クライアント IKE ID を *$Default$* に変更します。
**C.** 暗号 ikev2 http-url 証明書を有効にします。
**D.** 自己署名証明書を有効な証明書に置き換えます。
***Answer:*** D
Explanation:
In the given configuration, the trustpoint TP_AnyConnect is using a self-signed certificate (enrollment selfsigned). When using Cisco Secure Client (formerly AnyConnect) with IKEv2,

the client expects a valid, trusted certificate issued by a Certificate Authority (CA).
Since self-signed certificates are not trusted by default, the client may reject the connection, causing the VPN tunnel to fail. To resolve this issue, the engineer should:
1. Obtain and install a trusted CA-signed certificate on the router.
2. Update the crypto pki trustpoint configuration to use the new certificate.
3. Ensure the certificate Common Name (CN) and Subject Alternative Name (SAN) match the VPN gateway's FQDN.