Cisco.300-730.v2022-03-04.q62

試験コード：	300-730
試験名称：	Implementing Secure Solutions with Virtual Private Networks
認証ベンダー：	Cisco
無料問題の数：	62
バージョン：	v2022-03-04
ページの閲覧量：	615
問題集の閲覧量：	7788

https://www.jpnshiken.com/shiken/Cisco.300-730.v2022-03-04.q62.html

質問: **1**
キーサーバーのグループからプライマリキーサーバーを選択するために最初に使用されるパラメーターはどれですか？
A. 最も優先度の高い値
B. 最小のIPアドレス
C. 最高のIPアドレス
D. コードバージョン
正解: **(**正解を表示します**)**

質問: **2**

```
HUB configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 1 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 2 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local pre-shared-key flexvpn
 authentication remote rsa-sig
 pki trustpoint CA
aaa authorization group cert list default default
virtual-template 1
```

展示を参照してください。この構成の結果は何ですか？

A. 認証方法が正しくないため、スポーク1は認証に失敗します。

B. スポーク2は認証をハブに渡し、フェーズ2に正常に進みます。

C. リモート認証方法が正しくないため、スポーク2は認証に失敗します。

D. スポーク1は認証をハブに渡し、フェーズ2に正常に進みます。

正解: **(**正解を表示します**)**

セクション :ASDMとCLIを使用したトラブルシューティング

質問: **3**

展示を参照してください。

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
    500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
    failed its sanity check or is malformed
```

どのタイプの不一致がIPsecVPNトンネルで問題を引き起こしていますか？

A. 暗号アクセスリスト

B. フェーズ1ポリシー

C. 変換セット

D. 事前共有キー

正解: **D (**コメントを発表する**)**

リファレンス：

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike

質問: **4**

FlexVPNサーバに接続するCiscoAnyConnectセキュアモビリティクライアントにローカル認証を使用するには、どの要件が必要ですか。

A. EAPクエリID

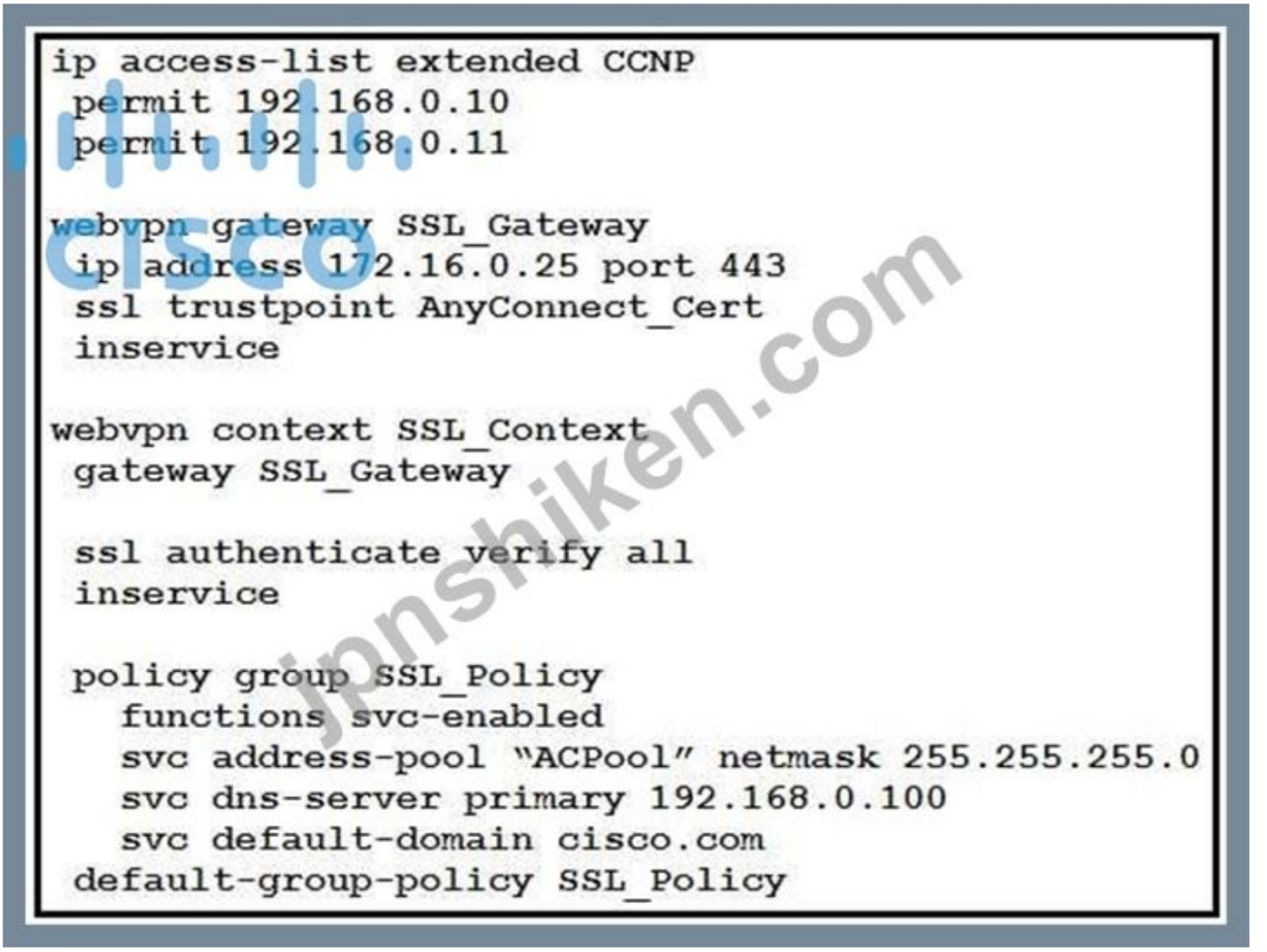
B. ユーザー名とパスワードの代わりに証明書を使用する

C. AnyConnectプロファイル

D. EAP-AnyConnect

正解: **(**正解を表示します**)**

質問: **5**



展示を参照してください。ユーザーが内部サーバにアクセスできるようにするには、CiscoAnyConnectをルータに設定する必要があります。192.168.0.10および192.168.0.11。他のすべてのトラフィックは、クライアントのローカルNICから送信される必要があります。この構成を実行するコマンドはどれですか？

A. svc split include 192.168.0.0 255.255.255.0

B. svc split include 192.168.0.0 255.255.255.0

C. svc split include acl CCNP

D. svcsplitはaclCCNPを除外します

正解: **(**正解を表示します**)**

セクション：安全な通信アーキテクチャ

説明/参照：

質問: **6**

CiscoASAクライアントレスSSLVPNソリューションに関する2つの説明のうち正しいものはどれですか。（2つ選択してください。）

A. クライアントがCisco ASA WebVPNポータルに接続し、URLバーを介してHTTPリソースにアクセスしようとすると、クライアントはローカルDNSを使用してFQDN解決を実行します。

B. グローバルwebvpn設定でのrewriter enableコマンドは、リライタ機能がデフォルトで無効になっているため、リライタ機能を有効にします。
C. Cisco ASAは、クライアントレスSSLVPNセッションとAnyConnectクライアントセッションを同時に許可できます。
D. クライアントがCisco ASA WebVPNポータルに接続し、URLバーを介してHTTPリソースにアクセスしようとすると、ASAは設定されたDNSサーバを使用してFQDN解決を実行します。
E. クライアントレスSSLVPNは、セキュリティで保護されたネットワークへのレイヤー3接続を提供します。
正解: **C,D** (コメントを発表する)
セクション :リモートアクセスVPN

質問: **7**
どのテクノロジーがIPsecステートフルフェールオーバーで機能しますか？
A. GLBR
B. HSRP
C. GRE
D. VRRP
正解: **B** (コメントを発表する)
セクション：安全な通信アーキテクチャ
説明/リファレンス：
https ://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ ft_vpnha.html#wp1122512

質問: **8**
企業の遠隔地は、MPLSを介してデータセンターに接続します。新しいリクエストでは、リモートロケーションに存在するユニキャストおよびマルチキャストトラフィックを暗号化する必要があります。この要件を満たすには、どの非トンネリングテクノロジーを使用する必要がありますか？
A. FlexVPN
B. GETVPN
C. DMVPN
D. SSL
正解: (正解を表示します)

質問: **9**
夜から正しいコマンドを左側のコード内の空白にドラッグアンドドロップして、動的なスポークツースポーク通信を可能にする設計を実装します。すべてのコメントが使用されるわけではありません。

Answer Area

Router A

```
interface Tunnel1
  ip address 10.0.0.1 255.255.255.0
  ip nhrp mp multicast dynamic
  ip nhrp network-id 1
  ip nhrp [          ]
  no ip split-horizon eigrp 10
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint

interface GigabitEthernet1
  ip address 1.1.1.1 255.255.255.0

router eigrp 10
  network 10.0.0.0 0.0.0.255
```

Router B

```
interface Tunnel1
  ip address 10.0.0.2 255.255.255.0
  ip nhrp nhs [          ] nbma [          ] multicast
  ip nhrp network-id 1
  ip nhrp [          ]
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint

interface GigabitEthernet1
  ip address 2.2.2.2 255.255.255.0

router eigrp 10
  network 10.0.0.0 0.0.0.255
```

1.1.1.1

10.0.0.1

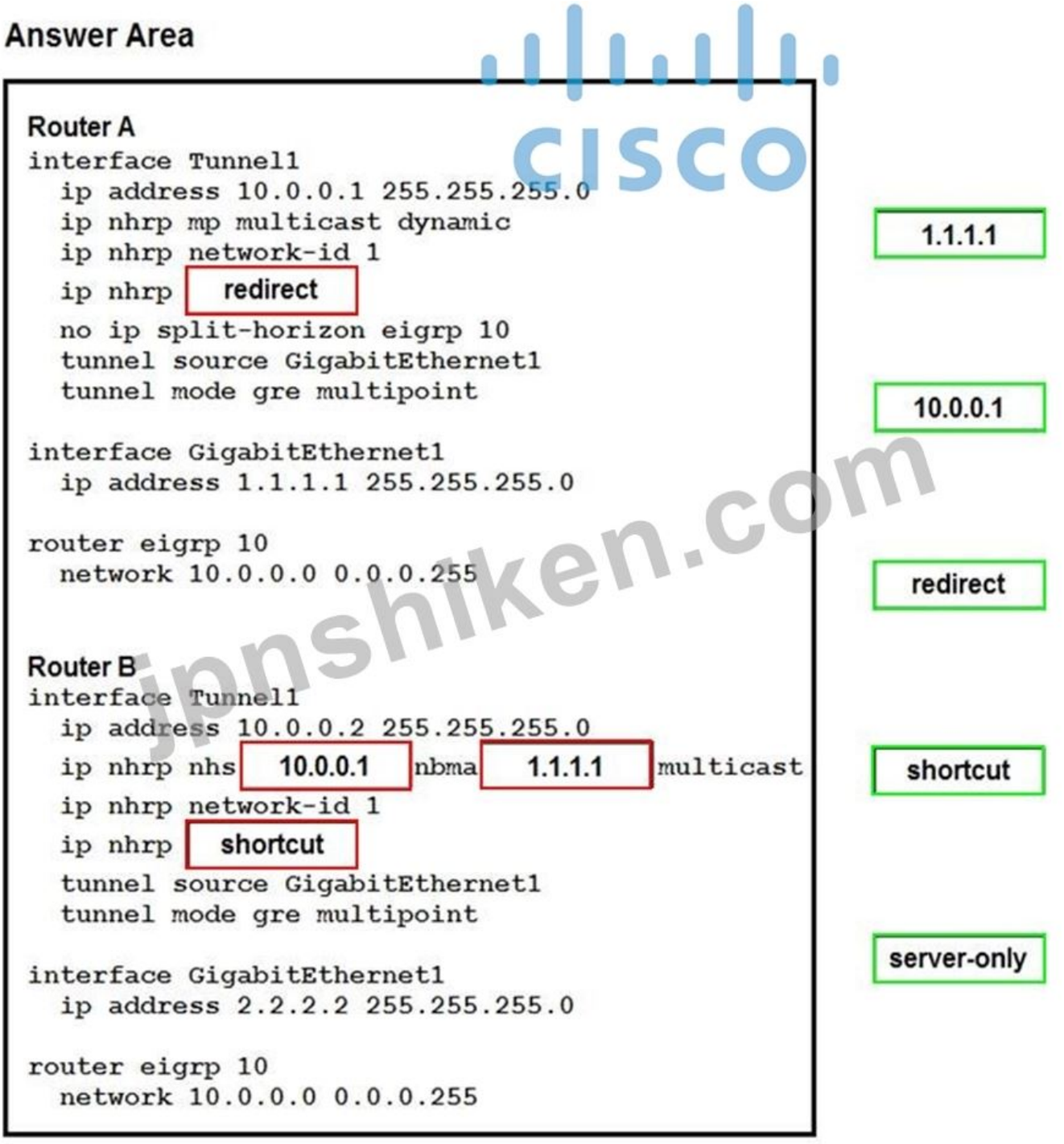
redirect

shortcut

server-only

正解:

Answer Area



1.1.1.1

10.0.0.1

redirect

shortcut

server-only

リファレンス：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn- dmvpn-summ-maps.html

質問: **10**
IPsec Cisco AnyConnectクライアントがデフォルト設定を使用している場合、IOS / IOS-XEヘッドエンドはどのIKEIDを受信することを期待していますか。
A. * $ RemoteAccessVpnClient $ *
B. * $ AnyConnectClient $ *
C. * $ SecureMobilityClient $ *

D. * $ DfltIkeIdentityS *
正解: **B** (コメントを発表する)

質問: **11**
CiscoルータのIKEv2リモートアクセスクライアントに対してスプリットトンネリングはどこで定義されていますか。
A. IKEv2認証ポリシー
B. グループポリシー
C. 仮想テンプレート
D. webvpnコンテキスト
正解: (正解を表示します)
セクション：安全な通信アーキテクチャ

質問: **12**

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
 address-pool split
 default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
 group-alias ikev2 enable
```

```
 -<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```


展示を参照してください。お客様は、XMLプロファイルを使用せずにCiscoAnyConnect接続を確立できます。AnyConnectドロップダウンでホスト「ikev2」が選択されている場合、接続は失敗します。この問題の原因は何ですか？
A. ホスト名が正しくありません。
B. IPアドレスが正しくありません。
C. プライマリプロトコルはSSLである必要があります。
D. UserGroupは接続プロファイルと一致する必要があります。

正解: (正解を表示します)
セクション :ASDMとCLIを使用したトラブルシューティング
説明/参照 :https ://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891

質問: **13**
CiscoAnyConnectクライアントにヘッドエンドの復元力を提供する2つの機能はどれですか。2つ選択してください。）
A. AnyConnect自動再接続
B. AnyConnectネットワークアクセスマネージャー
C. AnyConnectバックアップサーバー
D. ASAフェールオーバー
E. AnyConnectは常にオン
正解: (正解を表示します)
セクション :リモートアクセスVPN

質問: **14**
ルーターがハブを介してトラフィックを送信するのではなく、相互に動的に接続を形成し、動的ルーティングプロトコルを使用せずにルートをアドバタイズできるようにするには、どのVPNテクノロジーを使用する必要がありますか？
A. FlexVPN
B. GETVPN
C. DMVPNフェーズ2
D. DMVPNフェーズ3
正解: (正解を表示します)

質問: **15**

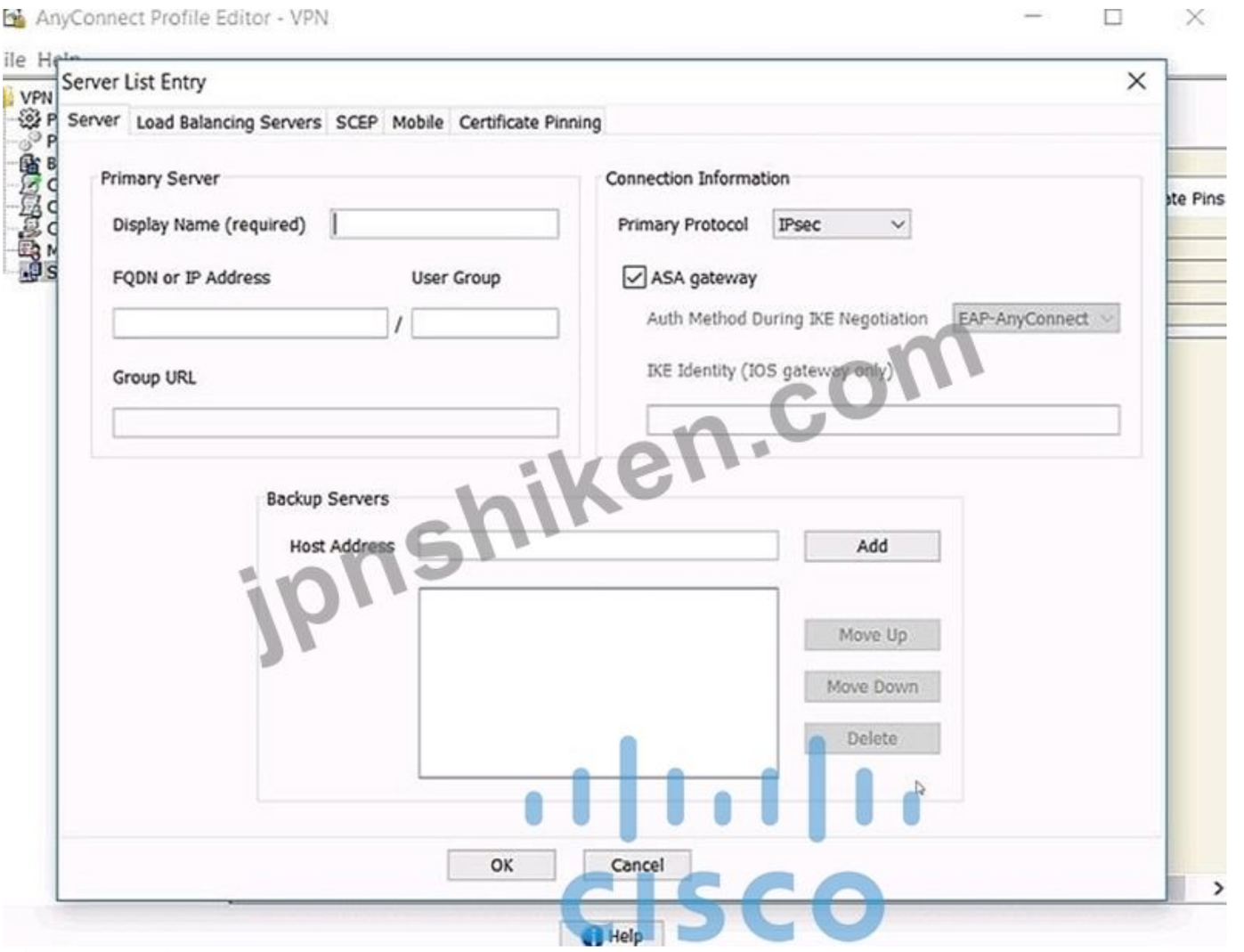
```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
    500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
    failed its sanity check or is malformed
```

展示を参照してください。どのタイプの不一致がIPsecVPNトンネルで問題を引き起こしていますか？
A. 暗号アクセスリスト
B. フェーズ1ポリシー
C. 変換セット
D. 事前共有キー
正解: **D** (コメントを発表する)
セクション :ASDMとCLIを使用したトラブルシューティング

説明/リファレンス :https ://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409- ipsec-debug-00.html＃ike

質問: **16**
Cisco AnyConnect Secure Mobility Clientは、あるグループのユーザにIKEv2を使用し、別のグループにSSLを使用するように設定されています。管理者がCiscoASAで新しいAnyConnectリリースを設定すると、IKEv2ユーザは接続時にそれを自動的にダウンロードできません。何が問題なのでしょう？
A. 影響を受けるユーザーに対してXMLプロファイルが正しく構成されていません。
B. 新しいクライアントイメージは、現在のイメージと同じメジャーリリースを使用していません。
C. クライアントサービスが有効になっていません。
D. クライアントソフトウェアの更新はIKEv2ではサポートされていません。
正解: **C** (コメントを発表する)
セクション :リモートアクセスVPN

質問: **17**
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CiscoAnyConnectプロファイルを作成する場合、[UserGroup]フィールドで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

正解: **(**正解を表示します**)**

リファレンス：

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

質問: **18**

展示を参照してください。

お客様は、RDPマシンでCiscoAnyConnectを起動する必要があります。どのIOS構成がこのタスクを実行しますか？

A.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
  svc platform win seq 1
  policy group PolicyGroup1
   functions svc-enabled
```

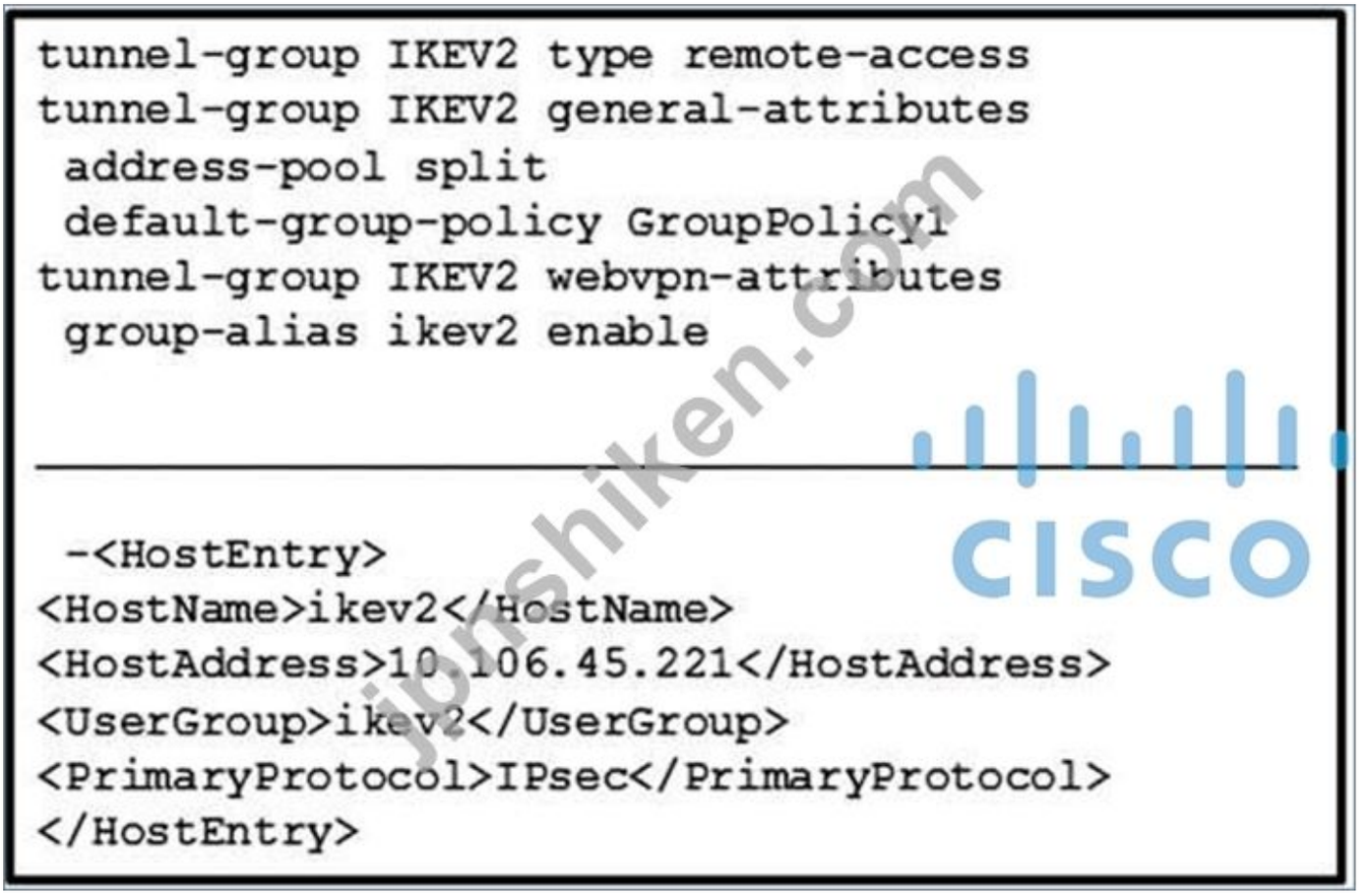
B.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

D.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc module RDP
```

A. オプションA
B. オプションC
C. オプションD
D. オプションB
正解: **(**正解を表示します**)**

質問: **19**



展示を参照してください。お客様は、XMLプロファイルを使用せずにCiscoAnyConnect接続を確立できます。

AnyConnectドロップダウンでホスト「ikev2」が選択されている場合、接続は失敗します。この問題の原因は何ですか？

A. ホスト名が正しくありません。

B. IPアドレスが正しくありません。

C. プライマリプロトコルはSSLである必要があります。

D. UserGroupは接続プロファイルと一致する必要があります。

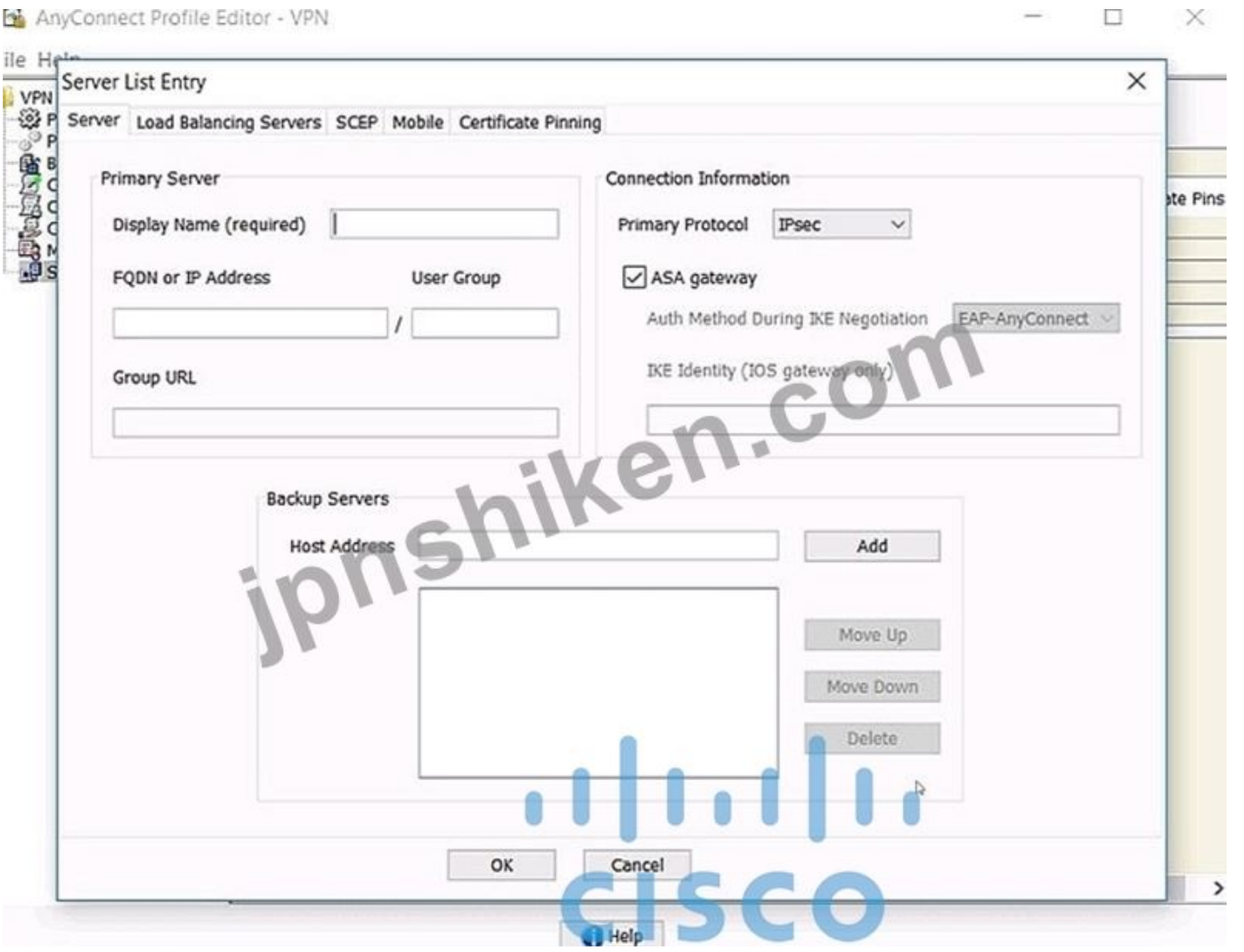
正解: **(**正解を表示します**)**

セクション :ASDMとCLIを使用したトラブルシューティング

説明/参照 :https ://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891

質問: **20**

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CiscoAnyConnectプロファイルを作成する場合、[UserGroup]フィールドでどの値を設定する必要がありますか。

A. グループポリシー
B. トンネルグループ
C. グループエイリアス
D. アドレスプール
正解: **(**正解を表示します**)**

質問: **21**
CiscoASAクライアントレスSSLVPNソリューションに関する2つの説明のうち正しいものはどれですか。2つ選択してください。)

A. クライアントがCisco ASA WebVPNポータルに接続し、URLバーを介してHTTPリソースにアクセスしようとすると、ASAは設定されたDNSサーバを使用してFQDN解決を実行します。
B. グローバルwebvpn設定でのrewriter enableコマンドは、リライタ機能がデフォルトで無効になっているため、リライタ機能を有効にします。
C. クライアントレスSSLVPNは、セキュリティで保護されたネットワークへのレイヤー3接続を提供します。

D. クライアントがCisco ASA WebVPNポータルに接続し、URLバーを介してHTTPリソースにアクセスしようとすると、クライアントはローカルDNSを使用してFQDN解決を実行します。
E. Cisco ASAは、クライアントレスSSLVPNセッションとAnyConnectクライアントセッションを同時に許可できます。
正解: (正解を表示します)

質問: **22**
展示を参照してください。

```
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed
policies
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy
found for received TS

*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001
CurState: R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```

ASAとリモートピア間のIKEv2サイト間トンネルが正常に構築されていません。デバッグ出力に基づいて問題を修正するものは何ですか？
A. 両方のVPNデバイスで暗号IPsecポリシーが一致していることを確認します。
B. ピアを検証するための正しい証明書をインストールします。
C. トンネルグループ名にピアIPアドレスを指定します。
D. 両方のVPNデバイスの暗号アクセスリストを修正します。
正解: (正解を表示します)

質問: **23**
FlexVPN展開では、スポークはハブに正常に接続されますが、スポークツースポークトンネルは形成されません。どのトラブルシューティング手順で問題が解決しますか？
A. スポークがリダイレクトメッセージを受信し、解決要求を送信することを確認します。
B. ハブ構成を確認して、NHRPショートカットが有効になっているかどうかを確認します。
C. スポーク構成を確認して、NHRPリダイレクトが有効になっているかどうかを確認します。
D. トンネルインターフェイスがVRF内に含まれていることを確認します。
正解: (正解を表示します)

質問: **24**
トラフィックセレクタの2番目のセットは、IKEv2を使用して2つのピア間でネゴシエートされます。どのIKEv2パケットに交換の詳細が含まれますか？
A. IKEv2情報
B. IKEv2 CREATE_CHILD_SA
C. IKEv2 IKE_SA_INIT

D. IKEv2 IKE_AUTH
正解: **A (**コメントを発表する**)**

質問: **25**
FlexVPNサーバに接続するCiscoAnyConnectセキュアモビリティクライアントにローカル認証を使用するには、どの要件が必要ですか。
A. ユーザー名とパスワードの代わりに証明書を使用する
B. EAP-AnyConnect
C. EAPクエリID
D. AnyConnectプロファイル
正解: **D (**コメントを発表する**)**
リファレンス：
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2- Remote-Access.html

質問: **26**
展示を参照してください。

```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:02:09, expire 00:00:01
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:13:25, 01:46:34
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 3.3.3.1
```

DMVPNトンネルはランダムにドロップしており、トンネル保護は設定されていません。どのスポーク構成がトンネルドロップを軽減しますか？

A.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

B.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

C.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 20
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```


D.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **(**正解を表示します**)**

質問: **27**
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、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。これらの請負業者には、コンピューターにアプリケーションをインストールする権限がありません。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. ポートフォワーディング
B. SSL AnyConnect
C. IKEv2 AnyConnect
D. クライアントレス
正解: **D (**コメントを発表する**)**

質問: **28**
どのテクノロジーがIPsecステートフルフェールオーバーで機能しますか？
A. VRRP
B. GRE
C. GLBR
D. HSRP
正解: **D (**コメントを発表する**)**

質問: **29**
IOSルータのフラッシュにアップロードされたCiscoAnyConnectプロファイルを識別するコマンドはどれですか。
A. svc import profile SSL_profile flash :simos-profile.xml
B. anyconnectプロファイルSSL_profile flash :simos-profile.xml
C. crypto vpn anyconnect profile 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
正解: **(**正解を表示します**)**
リファレンス：
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html

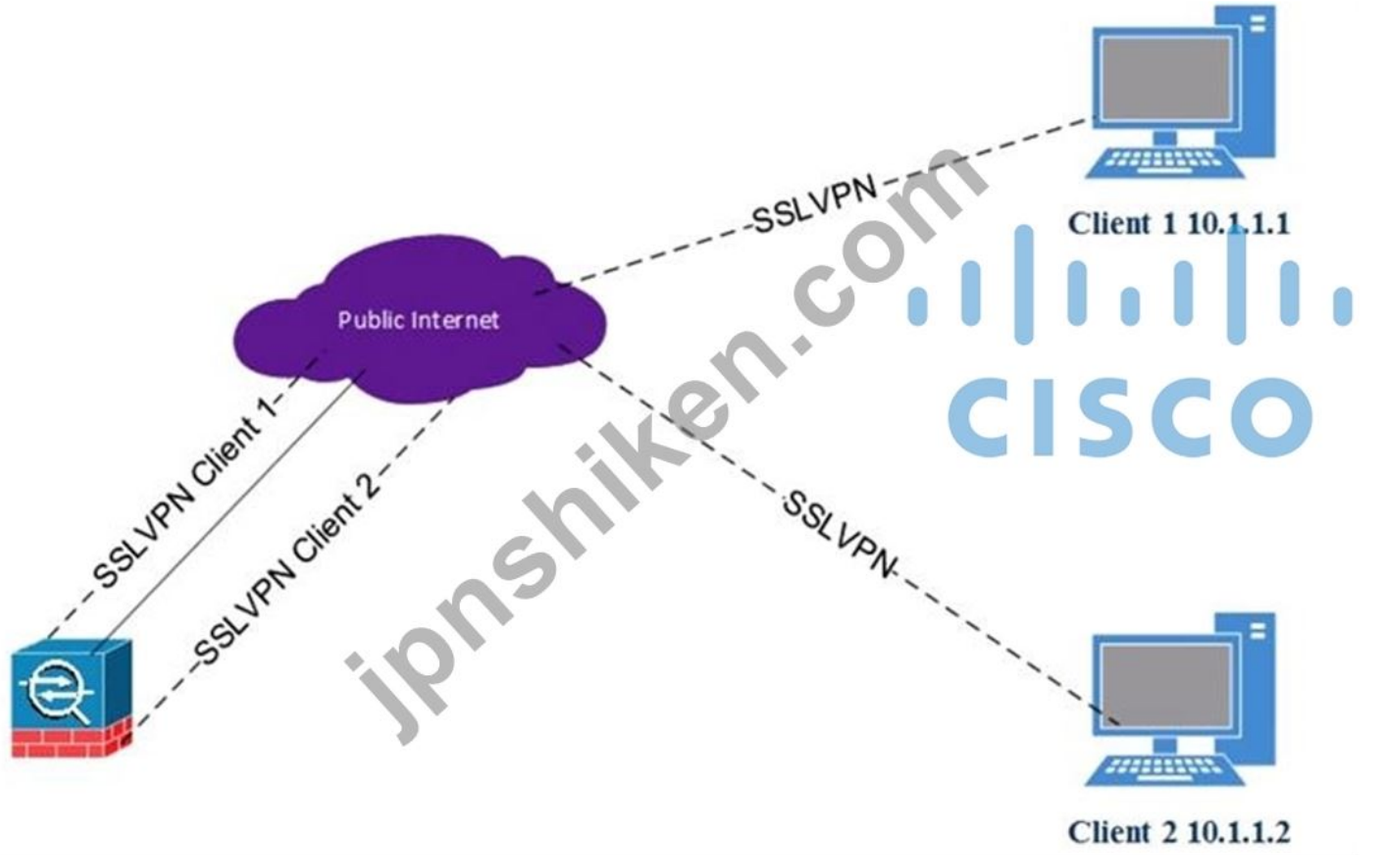
質問: **30**

展示を参照してください。お客様は、2つのCiscoASAデバイス間にIKEv2サイト間VPNトンネルを確立することはできません。syslogメッセージに基づいて、VPNトンネルを起動するアクションはどれですか。
A. ローカルCiscoASAの最大SA制限を減らします。
B. ローカルCiscoASAのネゴシエーション中の最大SA制限を増やします。
C. リモートCiscoASAの最大SA制限を削除します。
D. 両方のCiscoASAデバイスの暗号アクセスリストを修正します。
正解: **(**正解を表示します**)**
セクション :ルーターとファイアウォール上のサイト間仮想プライベートネットワーク

質問: **31**
GETVPNのどの機能がDMVPNとFlexVPNの制限ですか？
A. スケーラブルなリプレイチェックを可能にするシーケンス番号
B. ESPまたはAHの使用を有効にする

C. パブリックまたはプライベートWANで使用するための設計
D. オーバーレイルーティングプロトコルの要件はありません
正解: **D** (コメントを発表する)
セクション：安全な通信アーキテクチャ
説明/参照：

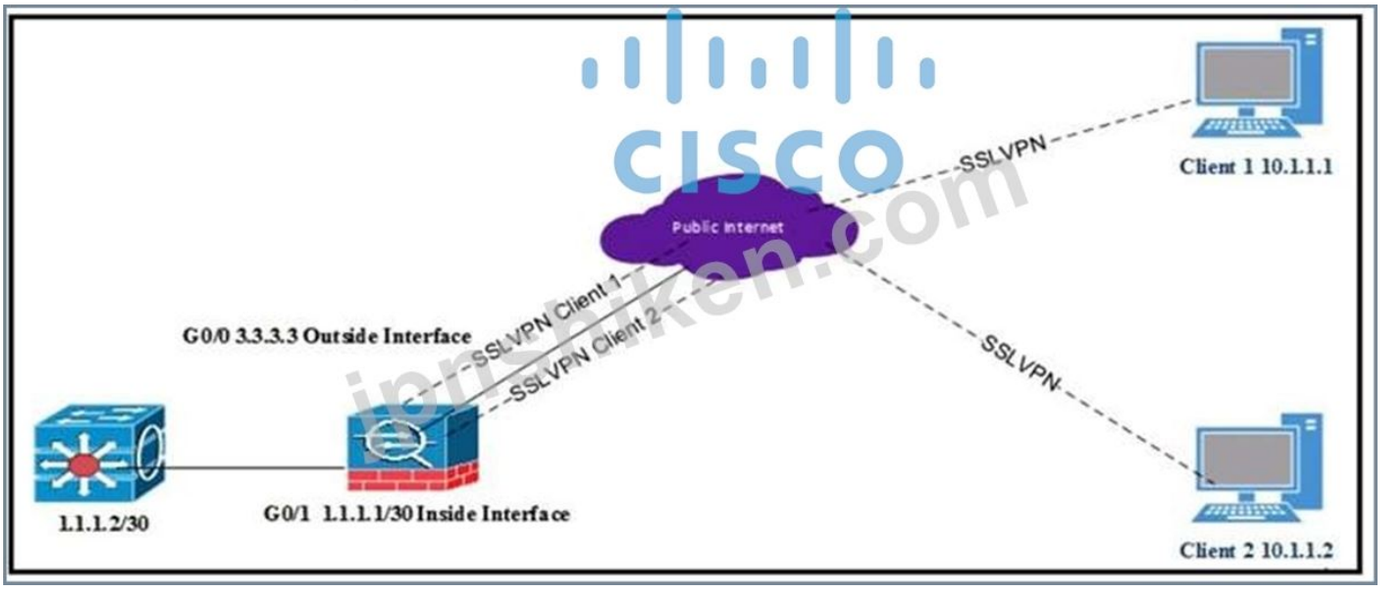
質問: **32**
展示を参照してください。



クライアント1はクライアント2と通信できません。両方のクライアントがCiscoAnyConnectを使用しており、ハブASAへのSSLVPN接続が正常に確立されています。
ASAのどのコマンドが欠落していますか？
A. dns-server value 10.1.1.3
B. same-security-traffic permit intra-interface
C. dns-server value 10.1.1.2

D. same-security-traffic permitinter-interface
正解: **B** (コメントを発表する)

質問: **33**
展示を参照してください。



ASAの背後にあるすべての内部クライアントは、3.3.3.3のIPアドレスを持つパブリック外部インターフェイスに変換されたポートアドレスです。クライアント1とクライアント2は、ASAへのSSLVPN接続を正常に確立しました。
IPアドレスのブラウザ検索から「3.3.3.3」が返されるようにするには、何を実装する必要がありますか？
A. グループポリシーの下ですべてのネットワークをトンネルする
B. グループポリシーの下の以下のトンネルネットワークリスト
C. グループポリシーで以下のネットワークリストを除外する
D. グループポリシーに基づくSame-security-traffic permitinter-interface
正解: (正解を表示します)

質問: **34**
CiscoASAクライアントレスSSLVPNポータルでデフォルトで有効になっている2種類のWebリソースまたはプロトコルはどれですか。（2つ選択してください。）
A. HTTP
B. ICA（Citrix）
C. CIFS
D. VNC
E. RDP
正解: **C,E** (コメントを発表する)

質問: **35**

IPsec Cisco AnyConnectクライアントがデフォルト設定を使用している場合、IOS / IOS-XEヘッドエンドはどのIKEIDを受信することを期待していますか。
A. * $ SecureMobilityClient $ *
B. * $ AnyConnectClient $ *
C. * $ RemoteAccessVpnClient $ *
D. * $ DfltIkeIdentityS *
正解**: (**正解を表示します**)**
セクション :リモートアクセスVPN
説明/リファレンス :https ://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect- IKEv2-Remote-Access.html

質問**: 36**
展示を参照してください。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list
author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
```


このコマンドセットの結果として何が構成されますか？

A. IPv6のFlexVPNクライアントプロファイル

B. IPv6dVTIセッション用のFlexVPNサーバー

C. EAPを使用してIPv6ピアを認証するFlexVPNサーバー
D. IPv6外部AAAを使用してグループを許可するFlexVPNサーバー
正解: **(**正解を表示します**)**

質問: **37**
展示を参照してください。

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
 address-pool split
 default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
 group-alias ikev2 enable
```

```
 -<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

お客様は、XMLプロファイルを使用せずにCiscoAnyConnect接続を確立できます。AnyConnectドロップダウンでホスト「kev2」が選択されている場合、接続は失敗します。この問題の原因は何ですか？
A. ホスト名が正しくありません。
B. IPアドレスが正しくありません。
C. プライマリプロトコルはSSLである必要があります。
D. UserGroupは接続プロファイルと一致する必要があります。
正解: **(**正解を表示します**)**

質問: **38**
展示を参照してください。

どのタイプのVPNが使用されていますか？

A. クライアントレスSSL VPN

B. Cisco Easy VPN

C. GETVPN

D. Cisco AnyConnect SSL VPN

正解: **B (**コメントを発表する**)**

質問: **39**

SSLをサポートする2つのリモートアクセスVPNソリューションはどれですか？ 2つ選択してください。）

A. L2TP

B. EZVPN

C. Cisco AnyConnect

D. FlexVPN

E. クライアントレス

正解: **(**正解を表示します**)**

質問: **40**

ユーザーがWebVPNポータルページにログインしたときに、スマートトンネルを自動的に開始するコマンドはどれですか。

A. 自動接続

B. 自動実行

C. 自動アップグレード

D. 自動起動

正解: **(**正解を表示します**)**

質問: **41**

管理者は、数人のユーザーのために初めてAnyConnectをセットアップしています。現在、ルーターはRADIUSサーバーにアクセスできません。ユーザーが認証できるようにするには、どのAnyConnectプロトコルを使用する必要がありますか？

A. EAP-MSCHAPv2

B. EAP-MD5

C. EAP-AnyConnect

D. EAP-GTC

正解: **(**正解を表示します**)**

質問: **42**
展示を参照してください。

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
 address-pool split
 default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
 group-alias ikev2 enable
```

```
 -<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

お客様は、XMLプロファイルを使用せずにCiscoAnyConnect接続を確立できます。AnyConnectドロップダウンでホスト 「ikev2」が選択されている場合、接続は失敗します。この問題の原因は何ですか？

A. ホスト名が正しくありません。
B. IPアドレスが正しくありません。
C. プライマリプロトコルはSSLである必要があります。
D. UserGroupは接続プロファイルと一致する必要があります。
正解: **(**正解を表示します**)**
リファレンス：
https://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891

質問: **43**
展示を参照してください。

```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy vpn_policy internal
group-policy vpn_policy attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

ネットワークエンジニアがメンテナンスウィンドウ中にクライアントレスSSLVPNを再構成しており、新しい構成をテストした後、接続を確立できません。この問題を修正するには何をする必要がありますか？

A. ユーザーのIPアドレスの自動サインオンを有効にします。

B. グループポリシーでDTLSを有効にします。

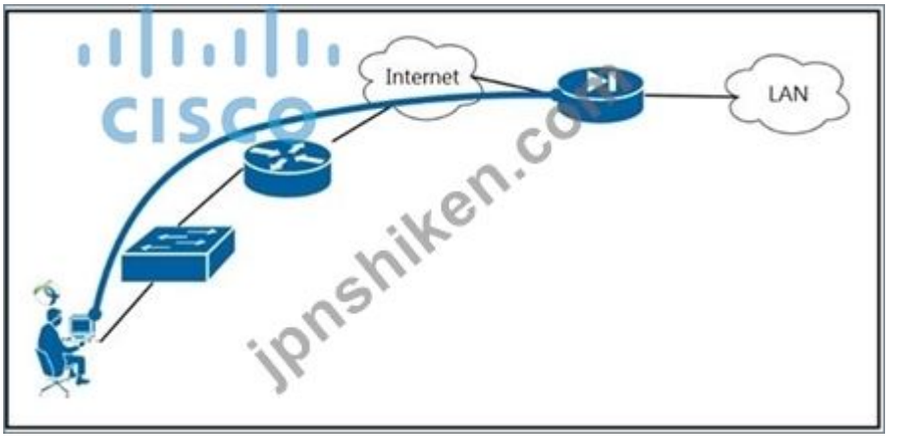
C. 外部インターフェースでクライアントサービスを有効にします。

D. グループポリシーでクライアントレスプロトコルを有効にします。

正解: **(**正解を表示します**)**

質問: **44**

展示を参照してください。



ユーザーがプライベートIPアドレスを使用してPCの背後から接続しています。彼らのISPプロバイダーはTCPポート443をブロックしています。ユーザーがASAとの接続を確立できるようにするAnyConnectXML構成はどれですか。

A.

```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.202.129</HostAddress>
  <PrimaryProtocol>IPsec
    <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
  </PrimaryProtocol>
</HostEntry>
```

B.

```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.200.225</HostAddress>
  <PrimaryProtocol>IPsec
    <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
  </PrimaryProtocol>
</HostEntry>
```

C.

```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.202.129</HostAddress>
</HostEntry>
```

D.

```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.200.225</HostAddress>
</HostEntry>
```

A. オプションA
B. オプションD
C. オプションB
D. オプションC
正解: **(**正解を表示します**)**

質問: **45**
展示を参照してください。

2つのサイト間のサイト間トンネルは発生していません。デバッグに基づいて、この問題の原因は何ですか？

A. ピアからのUDP4500トラフィックがルータに到達しません。

B. リモートピアで認証失敗が発生しました。

C. ルータで認証エラーが発生しました。

D. 証明書の断片化の問題が両側で発生します。

正解: **(**正解を表示します**)**

質問: **46**

展示を参照してください。

2つのルータ間のIKEv2サイト間VPNトンネルがダウンしています。デバッグ出力に基づいて、どのタイプの不一致が問題ですか？

A. 事前共有キー

B. 変換セット

C. ikev2プロポーザル

D. ピアID

正解: **(**正解を表示します**)**

質問: **47**

スマートトンネルが正しく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は管理者アクセス権を持っている必要があります。

正解: **A** (コメントを発表する)
セクション：安全な通信アーキテクチャ
説明/リファレンス :https ://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00。html

質問: **48**
外部SSOサーバなしでCiscoASAで使用できるSSO機能の2つのタイプはどれですか。2つ選択してください。）
A. HTTPベーシック
B. SAML
C. OAuth 2.0
D. Kerberos
E. NTLM
正解: **A,E** (コメントを発表する)

質問: **49**
ASAのVPNロードバランシングはどのVPNをサポートしていますか。
A. VTI
B. IPsecサイト間トンネル
C. L2TP over IPsec
D. Cisco AnyConnect
正解: (正解を表示します)
セクション：安全な通信アーキテクチャ

質問: **50**
FlexVPNトンネルで使用する必要がある構成構成はどれですか。
A. IKEv2プロファイル
B. EAP構成
C. マルチポイントGREトンネルインターフェース
D. IKEv1ポリシー
正解: (正解を表示します)

質問: **51**
FlexVPNサーバに接続するCiscoAnyConnectセキュアモビリティクライアントにローカル認証を使用するには、どの要件が必要ですか。
A. ユーザー名とパスワードの代わりに証明書を使用する
B. EAP-AnyConnect
C. EAPクエリID
D. AnyConnectプロファイル
正解: (正解を表示します)

セクション :リモートアクセスVPN
説明
説明/リファレンス :https ://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2- Remote-Access.html

質問: **52**
展示を参照してください。

```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy Cisc012345678 internal
group-policy Cisc012345678 attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```


グループCisc012345678に表示されるCiscoVPNのタイプはどれですか。
A. GETVPN
B. クライアントレスSSLVPN
C. DMVPN
D. CiscoAnyConnectクライアントVPN
正解: **D (**コメントを発表する**)**

質問: **53**
FlexVPN展開では、スポークはハブに正常に接続されますが、スポークツースポークトンネルは形成されません。どのトラブルシューティング手順で問題が解決しますか？
A. スポーク構成を確認して、NHRPリダイレクトが有効になっているかどうかを確認します。
B. スポークがリダイレクトメッセージを受信し、解決要求を送信することを確認します。
C. ハブ構成を確認して、NHRPショートカットが有効になっているかどうかを確認します。
D. トンネルインターフェイスがVRF内に含まれていることを確認します。
正解: **(**正解を表示します**)**
セクション :ASDMとCLIを使用したトラブルシューティング
説明/リファレンス :https ://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec- conn-dmvpn-15-mt-book / sec-conn-dmvpn-summ-maps.pdf

質問: **54**

```
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)
```

展示を参照してください。エンジニアが新しいGREoverIPsecトンネルのトラブルシューティングを行っています。トンネルは確立されていますが、エンジニアはスポーク1からスポーク2にpingを実行できません。どのタイプのトラフィックがブロックされていますか？

A. spoke2からspoke1へのESPパケット

B. spoke2からspoke1へのISAKMPパケット

C. spoke1からspoke2へのESPパケット

D. spoke1からspoke2へのISAKMPパケット

正解: **A (**コメントを発表する**)**

セクション :ASDMとCLIを使用したトラブルシューティング

質問: **55**

Cisco AnyConnectクライアントは、VPNセッションを介して大きなファイルを転送する必要があります。どのプロトコルが最高のスループットを提供しますか？

A. SSL / TLS

B. L2TP

C. DTLS

D. IPsec IKEv1

正解: **(**正解を表示します**)**

セクション：安全な通信アーキテクチャ

質問: **56**

展示を参照してください。従業員トンネルグループに接続するユーザーに許可されているVPNテクノロジーはどれですか？

A. SSL AnyConnect

B. IKEv2 AnyConnect

C. クリプトマップ

D. クライアントレス

正解: **(**正解を表示します**)**

セクション :リモートアクセスVPN

質問: **57**

クライアントレスSSLVPNユーザが使用できるようにするには、どのセクションでブックマークまたはURLリストをCiscoASAに設定する必要がありますか。

A. webvpn グループポリシー）

B. トンネルグループ（一般属性）

C. トンネルグループ（webvpn-attributes）

D. webvpn グローバル構成）

正解: **(**正解を表示します**)**

質問: **58**

GETVPNのどの機能がDMVPNと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の要件はありません

B. パブリックまたはプライベートWANで使用するための設計

C. スケーラブルなリプレイチェックを可能にするシーケンス番号

D. ESPまたはAHの使用を有効にしました

正解: (正解を表示します)

質問: **59**
IOSルータのフラッシュにアップロードされたCiscoAnyConnectプロファイルを識別するコマンドはどれですか。
A. webvpn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. svc import profile SSL_profile flash :simos-profile.xml
D. crypto vpn anyconnect profile SSL_profile flash :simos-profile.xml
正解: **D** (コメントを発表する)

質問: **60**
FlexVPNのどの利点がIKEv1を使用するDMVPNの制限ですか？
A. GREカプセル化により、非IPトラフィックの転送が可能になります。
B. IKE実装は、ルーティングテーブルにルートをインストールできます。
C. NHRP認証はセキュリティを強化します。
D. 動的ルーティングプロトコルを構成できます。
正解: (正解を表示します)
セクション：安全な通信アーキテクチャ

質問: **61**
FlexVPN展開では、スポークはハブに正常に接続されますが、スポークツースポークトンネルは形成されません。どのトラブルシューティング手順で問題が解決しますか？
A. スポーク構成を確認して、NHRPリダイレクトが有効になっているかどうかを確認します。
B. スポークがリダイレクトメッセージを受信し、解決要求を送信することを確認します。
C. ハブ構成を確認して、NHRPショートカットが有効になっているかどうかを確認します。
D. トンネルインターフェイスがVRF内に含まれていることを確認します。
正解: **B** (コメントを発表する)
リファレンス：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn- dmvpn-15-mt-book / sec-conn- dmvpn-summ-maps.pdf

質問: **62**

```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:02:09, expire 00:00:01
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:13:25, 01:46:34
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 3.3.3.1
```

展示を参照してください。DMVPNトンネルはランダムにドロップしており、トンネル保護は設定されていません。どのスポーク構成がトンネルドロップを軽減しますか？

A.

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

B.

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

C.

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 20
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```


D.

正解: (正解を表示します)

セクション :ルーターとファイアウォール上のサイト間仮想プライベートネットワーク