Cisco.300-730.v2023-12-12.q90

試験コード:	300-730
試験名称:	Implementing Secure Solutions with Virtual Private Networks
認定資格:	Cisco
無料問題数:	90
バージョン:	v2023-12-12
アクセス数:	873
ページビュー数:	900
https://www.jpnpdf.com/Cisco.300-730.v2023-12-12.q90-mondaishu.html	

最新問題: **1**
DMVPN フェーズ 3 クラウド内のすべてのルーターで一致する必要があるパラメータはどれですか?
A. GRE トンネルキー
B. トンネル VRF
C. NHRPネットワークID
D. EIGRP スプリットホライズン設定
Answer: (解答を表示する)

最新問題: **2**
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>
```

jpnpdf.com

顧客は、XML プロファイルを使用せずに Cisco AnyConnect 接続を確立できます。AnyConnect ドロップダウンでホスト "Ikev2"が選択されると、接続は失敗します。この問題の原因は何ですか?

A. プライマリ プロトコルは SSL である必要があります。
B. UserGroup は接続プロファイルと一致する必要があります。
C. IPアドレスが間違っています。
D. ホスト名が間違っています。
Answer: B (メーッセージを残す**)**

最新問題**: 3**
展示を参照してください。

```
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
```

この構成の結果はどうなるのでしょうか?

A. リモート認証方法が間違っているため、スポーク 2 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. 認証方法が間違っているため、スポーク 1 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。
Answer: C (メーッセージを残す**)**

最新問題**: 4**
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
```

jpnpdf.com

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. IPv6 外部 AAA を使用してグループを認可する FlexVPN サーバ
C. IPv6 dVTI セッション用の FlexVPN サーバー
D. EAP を使用して IPv6 ピアを認証する FlexVPN サーバ
Answer: A (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-フレックスclnt.html

最新問題**: 5**
ある企業は、支社からの接続を受け入れるために、本社の Cisco ASA に動的暗号マップを設定しています。ブランチ オフィス間に IP サブネットの重複はありませんが、エンジニアはブランチ オフィスによってどの暗号化ドメインが要求されるかわかりません。さらに、会社のセキュリティ ポリシーでは、ルーティング プロトコルのトラフィックが本社ネットワークから出てはいけないと規定されています。最小限の管理労力でトラフィックを Cisco ASA からブランチにルーティングするにはどのソリューションを使用する必要がありますか?
A. すべてのブランチ ルータで、tunneled キーワードを使用してデフォルト ルートを設定します。
B. EIGRP を使用してスナップショット ルーティングを設定し、帯域外ルーティング アップデートを送信します。
C. リモート サブネットの静的ルートを構成します。
D. ダイナミック クリプト マップでリバース ルート インジェクションを設定します。
Answer: D (メーッセージを残す)

最新問題**: 6**
GETVPNの特徴は何ですか?
A. 対象のトラフィックを定義する ACL を設定し、クリプト マップに適用する必要があります。
B. すべてのピアには、インバウンド通信とアウトバウンド通信用に 1 つの IPsec SPI があります。
C. IPsec SA の作成にはクイック モードが使用されます。
D. IPsec セッションのリモート ピアは暗号マップの一部として設定されます。
Answer: C (メーッセージを残す)

最新問題**: 7**
Cisco ASA クライアントレス SSL VPN 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つお選びください。)
A. HTTP
B. ICA (シトリックス)
C. VNC
D. RDP
E. CIFS
Answer: A,E (メーッセージを残す)
HTTP (ハイパーテキスト転送プロトコル) は、Web ページや HTML ドキュメントなどの Web リソースをインターネット経由で転送するために使用されます。CIFS (Common Internet File System) は、ネットワーク上のコンピュータ間でファイルとプリンタを共有するために使用されます。ICA (Citrix)、VNC (仮想

ネットワーク コンピューティング)、および RDP (リモート デスクトップ プロトコル) は、Cisco ASA クライアントレス SSL VPN ポータルではデフォルトでは有効になっていません。
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/webvpn-configure-gateway.html

最新問題: **8**
IPsec トンネルが起動した後でも NHRP 登録プロセスが完了しない理由を特定するのに役立つ 2 つのコマンドはどれですか? (2つお選びください。)
A. 暗号 isakmp sa を表示します。
B. IP トラフィックを表示
C. 暗号化 ipsec sa を表示します。
D. ip nhrp トラフィックを表示します。
E. dmvpn の詳細を表示
Answer: A,D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

最新問題: **9**
エンジニアは、Cisco ASA 上で Windows Vista ワークステーションに設定されたクライアントレス SSL VPN を介して、オフサイト管理者用のリモート デスクトップ接続を設定する必要があります。要求されたアクセスを提供する 2 つの構成はどれですか? (2つお選びください。)
A. ICA プラグイン経由の Citrix ブックマーク
B. SSH プラグイン経由の SSH ブックマーク
C. Telnet プラグインによる Telnet ブックマーク
D. RDP2 プラグイン経由の RDP2 ブックマーク
E. VNC プラグイン経由の VNC ブックマーク
Answer: B,D (メーッセージを残す**)**

最新問題: **10**
Cisco ASA はアクティブ/スタンバイ モードで設定されます。Cisco AnyConnect ユーザがフェールオーバー イベント後に確実に接続できるようにするには何が必要ですか?
A. AnyConnect イメージは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 を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: A (メーッセージを残す**)**
セクション: 安全な通信アーキテクチャ
説明/参照: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html

最新問題: **11**
IPsec VPN トンネル設定のどのパラメータがオプションですか?
A. 完全前方秘匿性
B. 寿命
C. ハッシュ

D. 暗号化
Answer: A (メーッセージを残す**)**

最新問題**: 12**
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 に VPN を設定しています。セキュリティ制限のため、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上での実行がブロックされています。これらのユーザーが RDP サーバーにアクセスできるようにするには、管理者はどの VPN 機能を実装する必要がありますか?
A. スマート トンネリング
B. クライアントレス プロキシ
C. クライアントレスプラグイン
D. クライアントレス リライター
Answer: C (メーッセージを残す**)**

最新問題**: 13**
Cisco AnyConnect クライアントは、企業オフィスの ASA との SSL VPN 接続を確立します。エンジニアは、クライアント コンピュータが企業のセキュリティ ポリシーを満たしていることを確認する必要があります。企業のセキュリティ ポリシーを満たすようにクライアントを更新できる機能はどれですか?
A. エンドポイント評価
B. Cisco セキュア デスクトップ
C. 基本的なホスト スキャン
D. 高度なエンドポイント評価
Answer: D (メーッセージを残す**)**
セクション: リモート アクセス VPN

最新問題**: 14**
Cisco ASA クライアントレス SSL VPN ソリューションに関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
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. リライター機能はデフォルトで無効になっているため、グローバル webvpn 設定で rewriter Enable コマンドを使用すると、リライター機能が有効になります。
C. Cisco ASA は、クライアントレス SSL VPN 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、安全なネットワークへのレイヤー 3 接続を提供します。
Answer: C,D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/webvpn.html

最新問題**: 15**
Cisco ASA はアクティブ/スタンバイ モードで設定されます。Cisco AnyConnect ユーザがフェールオーバー イベント後に確実に接続できるようにするには何が必要ですか?
A. AnyConnect イメージは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 を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: (解答を表示する**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html

最新問題**: 16**

展示を参照してください。顧客は、XML プロファイルを使用せずに Cisco AnyConnect 接続を確立できます。
AnyConnect ドロップダウンでホスト 「ikev2」が選択されると、接続は失敗します。この問題の原因は何ですか?
A. ホスト名が間違っています。
B. IPアドレスが間違っています。
C. プライマリ プロトコルは SSL である必要があります。
D. ユーザーグループは接続プロファイルと一致する必要があります。
Answer: (解答を表示する**)**
セクション: ASDM および 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

有効な **300-730** 問題集は GoShiken.com が提供された合格しやすい 300-730 試験問題集！ GoShiken.com が最新の **300-730** 試験問題集を提供しています。GoShiken.com 300-730 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-730 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240**30%OFF**問題集溶と正解付きで 30%ｗ特別割引コード: Freepdfdumps**)

最新問題**: 17**
FlexVPN トンネルではどの構成構造を使用する必要がありますか?
A. EAP 設定

B. マルチポイント GRE トンネル インターフェイス
C. IKEv1 ポリシー
D. IKEv2 プロファイル
Answer: D (メーッセージを残す)
セクション: リモート アクセス VPN

最新問題**: 18**
プライベート WAN 上でマルチキャスト トラフィックを暗号化するときに、VPN パフォーマンスへの影響を最小限に抑える VPN テクノロジーはどれですか?
A. FlexVPN
B. IPsec VPN
C. DMVPN
D. GETVPN
Answer: D (メーッセージを残す)

最新問題**: 19**
ネットワーク エンジニアは、500 人の同時ユーザをサポートし、クライアントからのすべてのトラフィックが ASA を通過することを保証し、ユーザが内部インターフェイス サブネット（192.168.0.0/24）上のすべてのデバイスにアクセスできるようにする SSLVPN Cisco AnyConnect ソリューションを実装する必要があります。他のすべての構成が適切に設定されていると仮定すると、どの構成がこのソリューションを実装しますか?

○ A.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

○ B.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

○ C.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

○ D.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

ipr.pdf.com

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
Answer: A (メーッセージを残す**)**

最新問題**: 20**
本社のユーザーは、L2L IPsec VPN で接続されているブランチ サイトのネットワーク共有にアクセスするのに問題を抱えています。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。この問題を解決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 デバイス上のルーティングを調整して、トンネル経由でトラフィックを戻すようにします。
B. 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 に送り返します。
C. 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。
D. 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。
Answer: A (メーッセージを残す**)**

最新問題**: 21**
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
```

itnpdf.com

グループ Cisc012345678 にはどのタイプの Cisco VPN が表示されますか?
A. Cisco AnyConnect クライアント VPN
B. クライアントレス SSLVPN
C. DMVPN
D. GETVPN

Answer: A (メーッセージを残す)

最新問題**: 22**
サイト間 VPN 経由でマルチキャスト トラフィックを送信するために使用されるテクノロジーはどれですか?
A. FTD 上の IPsec トンネル
B. ASA 上の GRE トンネル
C. FTD 上の GRE over IPsec
D. IOS ルータ上の GRE over IPsec
Answer: C (メーッセージを残す)

最新問題**: 23**
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
```

IPsec VPN トンネルの問題の原因となっている不一致のタイプはどれですか?
A. 暗号アクセスリスト
B. フェーズ 1 ポリシー
C. トランスフォーム セット
D. 事前共有キー
Answer: D (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike

最新問題**: 24**
展示を参照してください。

```
tunnel-group client general-attributes
address-pool MYPOOL
authentication-server-group RADIUS
tunnel-group client ipsec-attributes
pre-shared-key test123
```

どのタイプの VPN が使用されますか?
A. Cisco AnyConnect SSL VPN
B. GETVPN
C. クライアントレス SSL VPN

D. Cisco Easy VPN
Answer: D (メーッセージを残す**)**

最新問題**: 25**
リモート トンネル エンドポイントのネットワーク ルートを動的にインストールする方法はどれですか?
A. ポリシーベースのルーティング
B. CEF
C. 逆ルート注入
D. ルートフィルタリング
Answer: C (メーッセージを残す**)**
参照：
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn-availability-12-4t-book/sec-rev -rte-inject.html>

最新問題**: 26**
展示を参照してください。

```
interface Ethernet0
 nameif outside
 security-level0
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.0.1 255.255.255.0
!
object network InsideNet
subnet 10.7.7.0 255.255.255.0
!
object network RemoteNet
subnet 10.8.8.0 255.255.255.0
!
nat (inside,outside) source static InsideNet InsideNet destination static RemoteNet RemoteNet
!
access-list cmap10 extended permit ip object InsideNet object RemoteNet
!
route outside 0.0.0.0 0.0.0.0 172.16.1.1
!
crypto ipsec ikev1 transform-set AES256 esp-aes-256 esp-sha-hmac
!
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
!
crypto map cmap 10 match address cmap10
crypto map cmap 10 set peer 172.17.1.1
crypto map cmap 10 set ikev1 transform-set AES256
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key Cisco123
```

cisco
ionpdf.com

エンジニアはピア Cisco ASA への IKEv1 トンネルを構築していますが、トンネルに障害が発生します。展示内の設定に基づいて、VPN トンネルを起動できるようにするにはどのアクションを実行する必要がありますか?

A. 外部インターフェイスで IKEv1 を有効にします。

B. IKEv1 ポリシー番号を 256 以上に変更します。

C. トランスフォーム セット モードをトランスポートに変更します。

D. 10.7.7.0/24 ネットワークのルートを追加して、外部インターフェイスから出力します。

Answer: (解答を表示する)

最新問題: **27**
ASA にクライアントレス SSLVPN を実装するときに、ネットワーク エンジニアがデフォルトの X.509 証明書の使用を避けなければならないのはなぜですか?
A. 証明書はローカル CA によって管理される必要があります。
B. 証明書は再起動するたびに再生成されます。
C. デフォルトの X.509 証明書は SSLVPN ではサポートされていません。
D. 証明書が弱すぎるため、適切なセキュリティを提供できません。
Answer: B (メーッセージを残す)
デフォルトでは、ASA は起動時に自己署名 X.509 証明書を生成します。この証明書は、デフォルトでクライアント接続を提供するために使用されます。この証明書の信頼性はブラウザでは検証できないため、この証明書を使用することはお勧めできません。さらに、この証明書は再起動のたびに再生成されるため、再起動のたびに変更されます。https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html

最新問題: **28**
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. crypto vpn anyconnect 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 インポート 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: (解答を表示する)

最新問題: **29**
FlexVPN を設定する場合、IKEv2 用に設定する必要がある 2 つのコンポーネントはどれですか? (2つお選びください。)
A. メソッド
B. 持続性
C. プロファイル
D. 提案
E. 好み
Answer: C,D (メーッセージを残す)

最新問題: **30**
展示を参照してください。

```
KEv2:IPSec policy validate request sent for profile CloudOne with psh index 1.

KEv2:(SESSION ID = 17,SA ID = 1):
KEv2:(SA ID = 1):[IPsec -> IKEv2] Callback received for the validate proposal - FAILED.

KEv2-ERROR:(SESSION ID = 17,SA ID = 1):: There was no IPSEC policy found for received TS
KEv2:(SESSION ID = 17,SA ID = 1):Sending TS unacceptable notify
KEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
KEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
KEv2:(SESSION ID = 17,SA ID = 1):Get peer's preshared key for 68.72.250.251
KEv2:(SESSION ID = 17,SA ID = 1):Generate my authentication data
KEv2:(SESSION ID = 17,SA ID = 1):Use preshared key for id 68.72.250.250, key len 5
KEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
KEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
KEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
KEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
KEv2:(SESSION ID = 17,SA ID = 1):Generating IKE_AUTH message
KEv2:(SESSION ID = 17,SA ID = 1):Constructing IDr payload: '68.72.250.250' of type 'IPv4 address'
KEv2:(SESSION ID = 17,SA ID = 1):Building packet for encryption.
ayload contents:
VID IDr AUTH NOTIFY(TS_UNACCEPTABLE)

KEv2:(SESSION ID = 17,SA ID = 1):Sending Packet [To 68.72.250.251:500/From 68.72.250.250:500/VRF i0:f0]
nitiator SPI : 3D527B1D50DBEEF4 - Responder SPI : 8C693F77F2656636 Message id: 1
KEv2 IKE_AUTH Exchange RESPONSE
ayload contents:
ENCR
```

デバッグ出力に基づくと、VPN の起動を妨げているのはどのタイプの不一致ですか?

A. 興味深いトラフィック

B. 生涯

C. 事前共有キー

D. PFS

Answer: (解答を表示する**)**

2 つの TS ペイロードのうちの最初のペイロードは、TSi (Traffic Selector-initiator) として知られています。2 つ目は TSr (トラフィック セレクター レスポンダー) として知られています。TSi は、子 SA ペアのイニシエーターから転送されるトラフィックの送信元アドレス (または、子 SA ペアのイニシエーターに転送されるトラフィックの宛先アドレス) を指定します。https://www.rfc-editor.org/rfc/rfc5996#page-40 応答側のポリシーにより、提案されたトラフィック セレクターの一部を受け入れることが許可されていない場合、応答側は TS_UNACCEPTABLE 通知メッセージで応答します。

最新問題**: 31**

```
Ciscoasa# sh cap o trace packet-number 4

737 packets captured

     4: 08:19:36.054181    10.99.117.195.56485 > 10.31.124.31.443: $ 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow


1 packet shown
```

展示を参照してください。SSL クライアントが ASA ヘッドエンドに接続しています。セッションが失敗し、次のメッセージが表示される
「接続試行がタイムアウトしました。インターネット接続を確認してください。」パケットの処理方法に基づいて、どのフェーズが障害の原因となっているのか?

A. フェーズ 9: rpf-check

B. フェーズ 5: NAT

C. フェーズ 4: アクセスリスト

D. フェーズ 3: UN-NAT

Answer: D (メーッセージを残す**)**

セクション: ASDM および CLI を使用したトラブルシューティング

有効な **300-730** 問題集は GoShiken.com が提供された合格しやすい 300-730 試験問題集！ GoShiken.com が最新の **300-730** 試験問題集を提供しています。GoShiken.com 300-730 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-730 問題集をゲットする人はこちら: https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **32**
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. Java または ActiveX がクライアント マシンで有効になっている必要があります。
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てはなりません。
D. クライアント マシン上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。
Answer: A (メーッセージを残す**)**
セクション: 安全な通信アーキテクチャ
説明/参照: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00。html

最新問題: **33**
展示を参照してください。

XML profile

```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

お客様は RDP マシンで Cisco AnyConnect を起動する必要があります。このタスクを実行できる IOS 構成はどれですか?

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
```

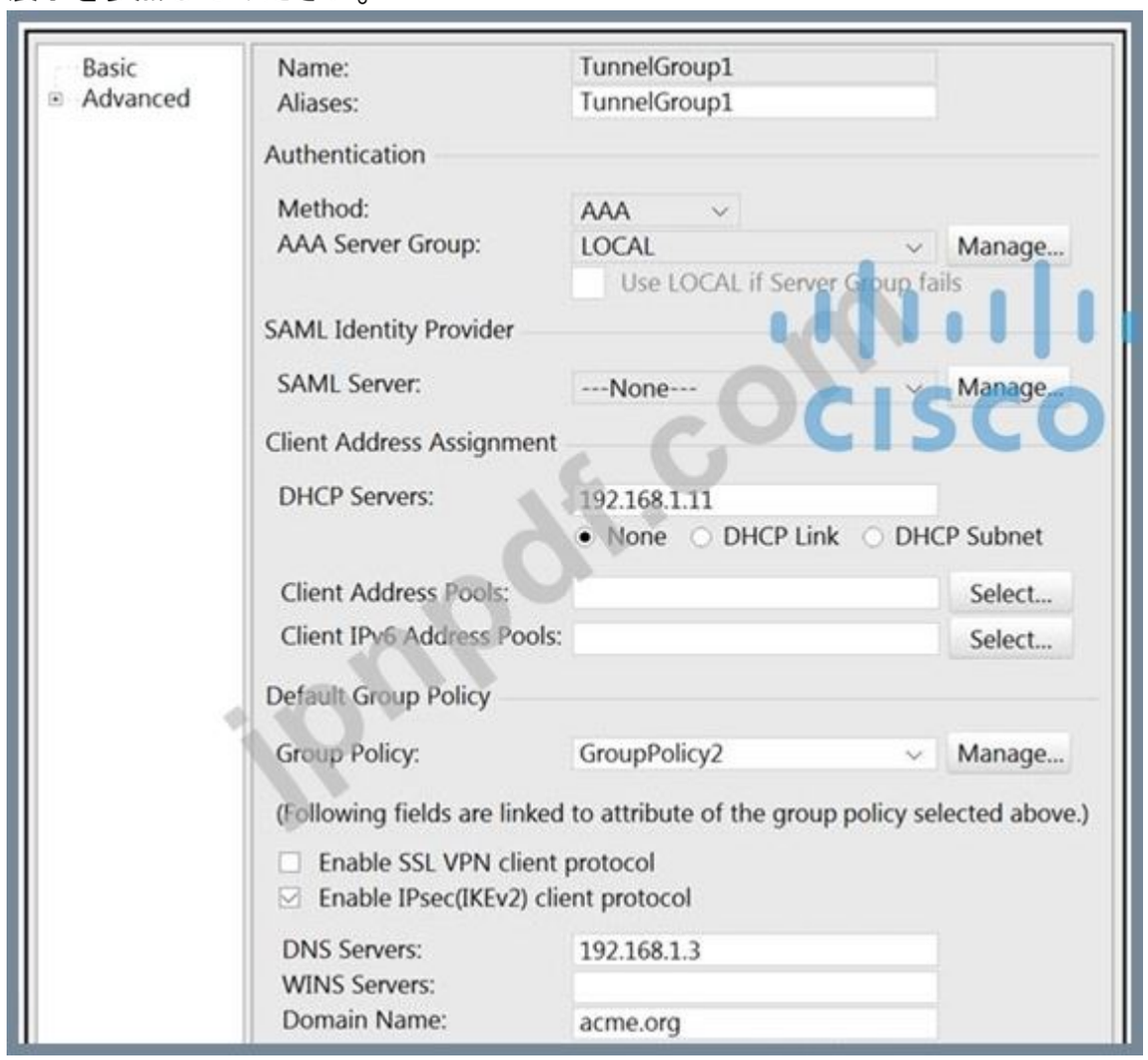
C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

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 D
B. オプション A
C. オプション B

D. オプション C
Answer: D (メーッセージを残す**)**

最新問題**: 34**
展示を参照してください。



ネットワーク エンジニアがリモート アクセス SSLVPN を構成していますが、ローカル資格情報を使用して接続を完了できません。この問題を解決するには何をしなければなりませんか?
A. 認証方法をローカルに変更します。
B. Cisco AnyConnect プロファイルでクライアント プロトコルを有効にします。
C. クライアントを認証するための AAA サーバー グループを設定します。
D. ローカル認証を強制するようにグループ ポリシーを構成します。
Answer: B (メーッセージを残す**)**

最新問題**: 35**
Cisco AnyConnect セキュア モビリティ クライアントは、あるユーザ グループには IKEv2 を使用し、別のグループには SSL を使用するように設定されています。管理者が Cisco ASA 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のリリース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か?
A. XML プロファイルが影響を受けるユーザーに対して正しく構成されていません。

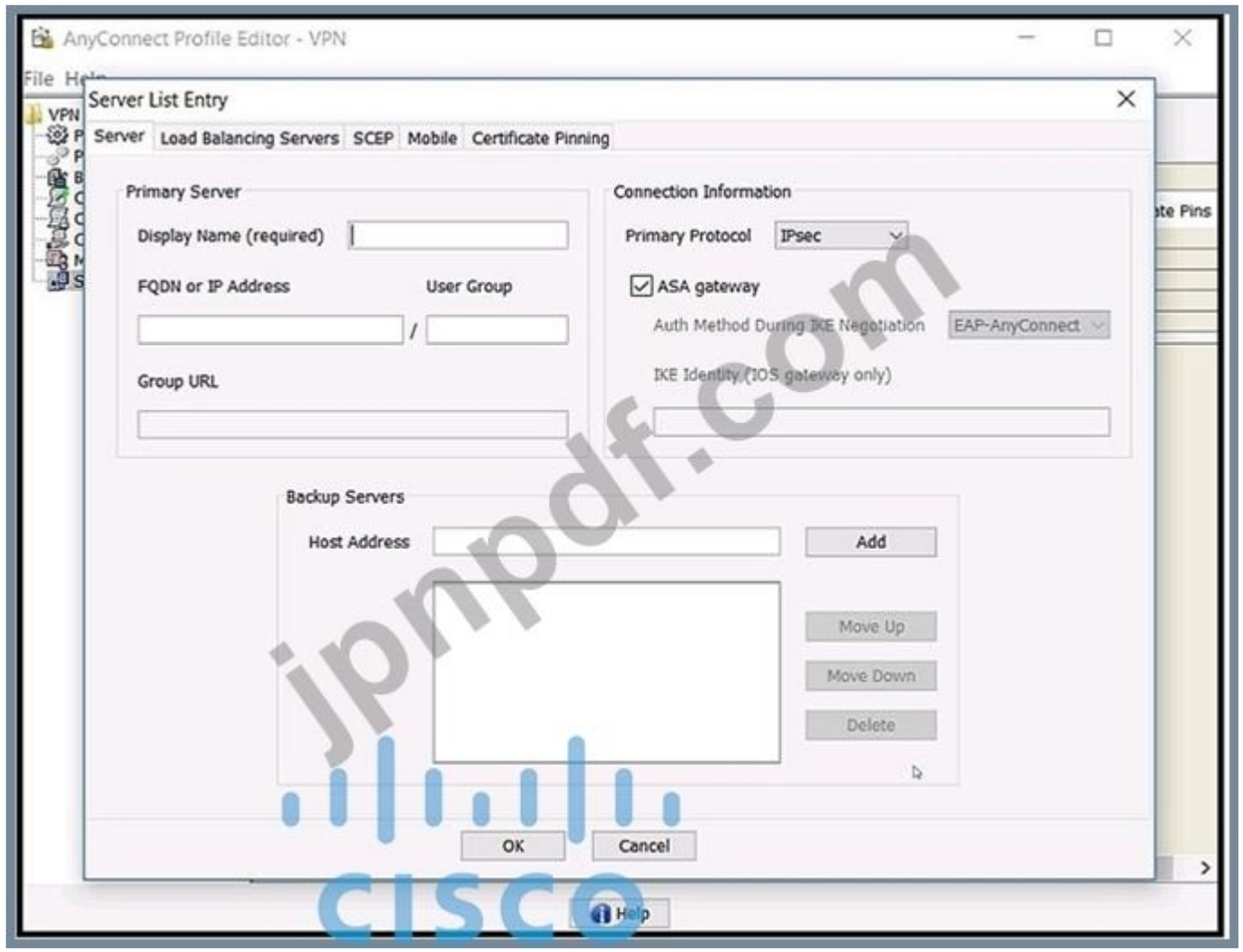
B. 新しいクライアント イメージは、現在のイメージと同じメジャー リリースを使用していません。
C. クライアント サービスが有効になっていません。
D. クライアント ソフトウェアの更新は IKEv2 ではサポートされていません。
Answer: C (メーッセージを残す**)**

最新問題**: 36**
展示を参照してください。

```
crypto gdoi group GDOI-GROUP1
server local
 address ipv4 10.0.0.1
 redundancy
  local priority 250
  peer address ipv4 10.0.6.1
```

部分的な構成スニペットに基づいて、どのタイプの VPN が構成されていますか?
A. FlexVPN ロードバランサ
B. デュアル グループ メンバーによる VPN の取得
C. FlexVPN バックアップ ゲートウェイ
D. COOP キーサーバーを使用して VPN を取得する
Answer: D (メーッセージを残す**)**

最新問題**: 37**
展示を参照してください。



IPsec をプライマリ プロトコルとして 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ときに、[User Group] フィールドで設定する必要がある値はどれですか?

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: D (メーッセージを残す**)**

ユーザー グループはホスト アドレスと組み合わせて使用され、グループベースの URL を形成します。プライマリ プロトコルを IPsec として指定する場合、ユーザー グループは接続プロファイル (トンネル グループ) の正確な名前である必要があります。SSL の場合、ユーザー グループは接続プロファイルのグループ URL で

す。https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-profile-editor.html#ID-1430-0000026c

最新問題**: 38**

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
```

IPsec VPN トンネルの問題の原因となっている不一致のタイプはどれですか?

A. 事前共有キー

B. フェーズ 1 ポリシー

C. 暗号アクセスリスト

D. トランスフォーム セット

Answer: A (メーッセージを残す**)**

最新問題**: 39**

GETVPN を使用して企業オフィス間のネットワークを通過する 2 つの利点は何ですか? (2つお選びください。)

A. これは、拡張性の高い任意のメッシュ トポロジです。

B. マルチキャストに対応しています。

C. QoS サポートがあります。

D. ハブアンドスポーク トポロジをサポートします。

E. セキュリティを向上させるための固有のセッション キーがあります。

Answer: A,B (メーッセージを残す**)**

最新問題**: 40**

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 IKE ID を受信することを想定していますか?

A. *$SecureMobilityClient$*

B. *$AnyConnectClient$*

C. *$RemoteAccessVpnClient$*

D. *$DfltIkeIdentityS*

Answer: B (メーッセージを残す**)**

セクション: リモート アクセス VPN

説明/参照: https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

最新問題**: 41**

ドラッグドロップ

夜の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デザインを実装します。すべてのコメントが使用されるわけではありません。

選択して配置します:

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

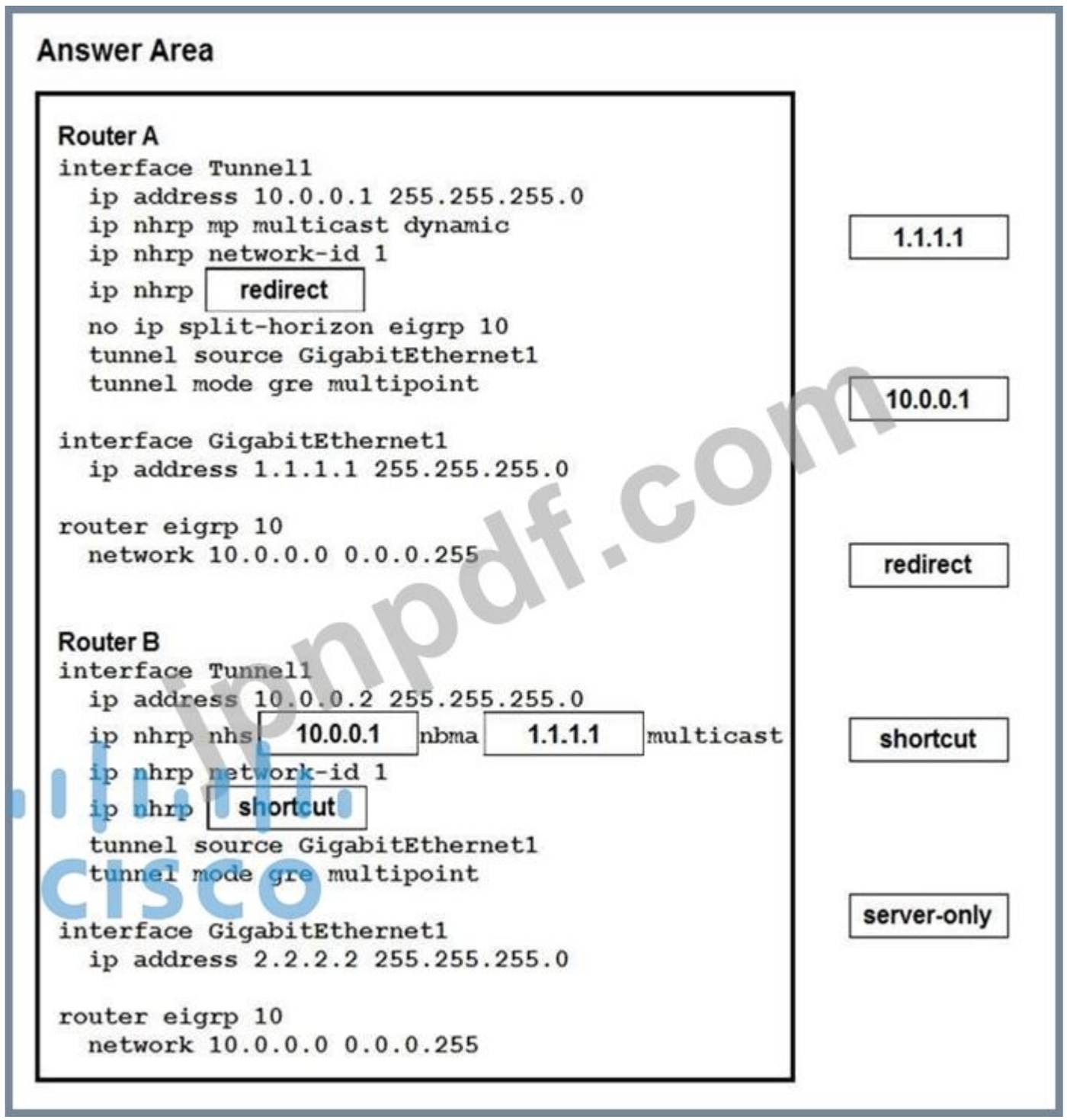
redirect

shortcut

server-only

pdf.com

Answer:



セクション :ルータおよび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 説明/参照先 :https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe- 16/秒-conn-dmvpn-xe-16-book/sec-conn-dmvpn-summ-maps. html

最新問題: **42**
展示を参照してください。

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CCNP
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 172.18.10.2
 tunnel protection ipsec profile CCNP
```

展示ではどの VPN テクノロジーが使用されていますか?

A. DVTI

B. VTI

C. DMVPN

D. グレー

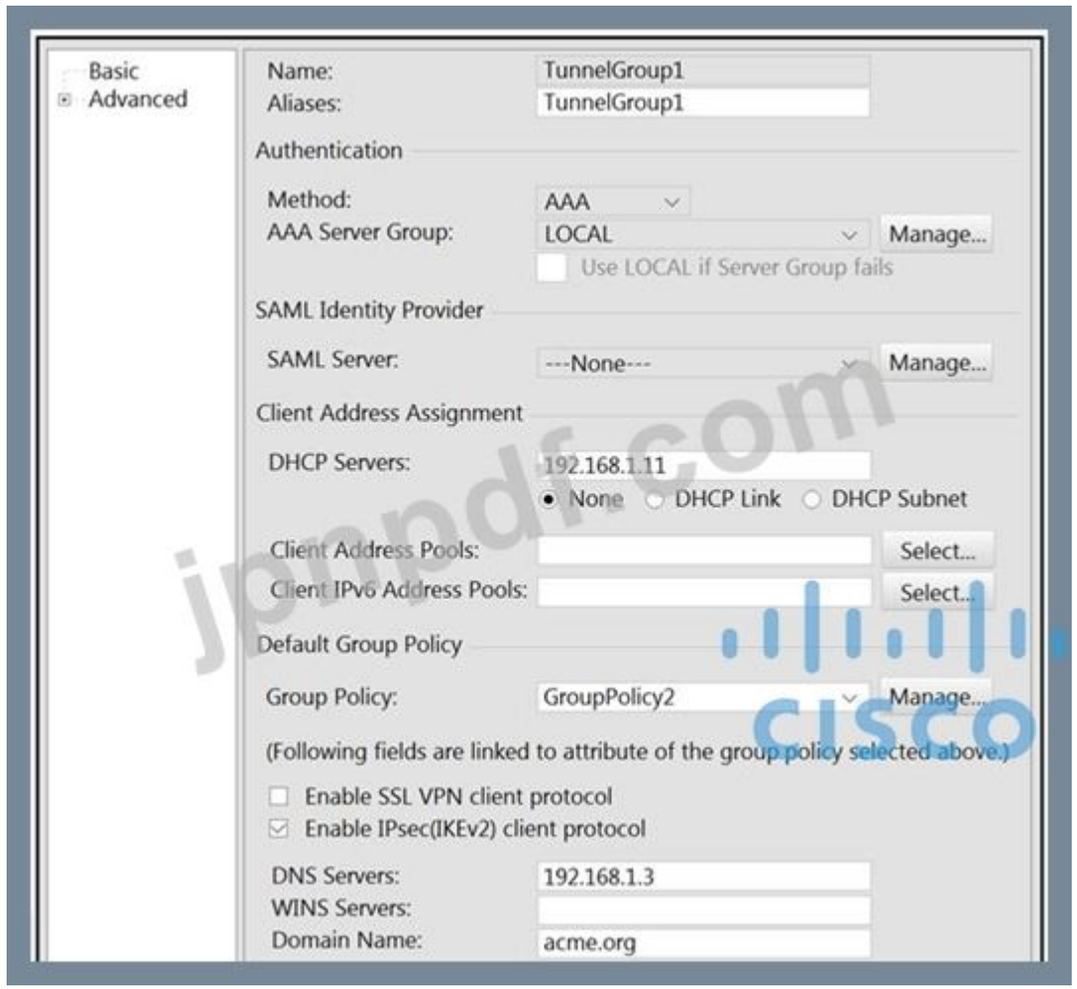
Answer: B (メーッセージを残す**)**

参照：

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

最新問題**: 43**

展示を参照してください。



ネットワーク エンジニアがリモート アクセス SSLVPN を構成していますが、ローカル資格情報を使用して接続を完了できません。この問題を解決するには何をしなければなりませんか?

A. クライアントを認証するための AAA サーバー グループを設定します。

B. ローカル認証を強制するようにグループ ポリシーを構成します。

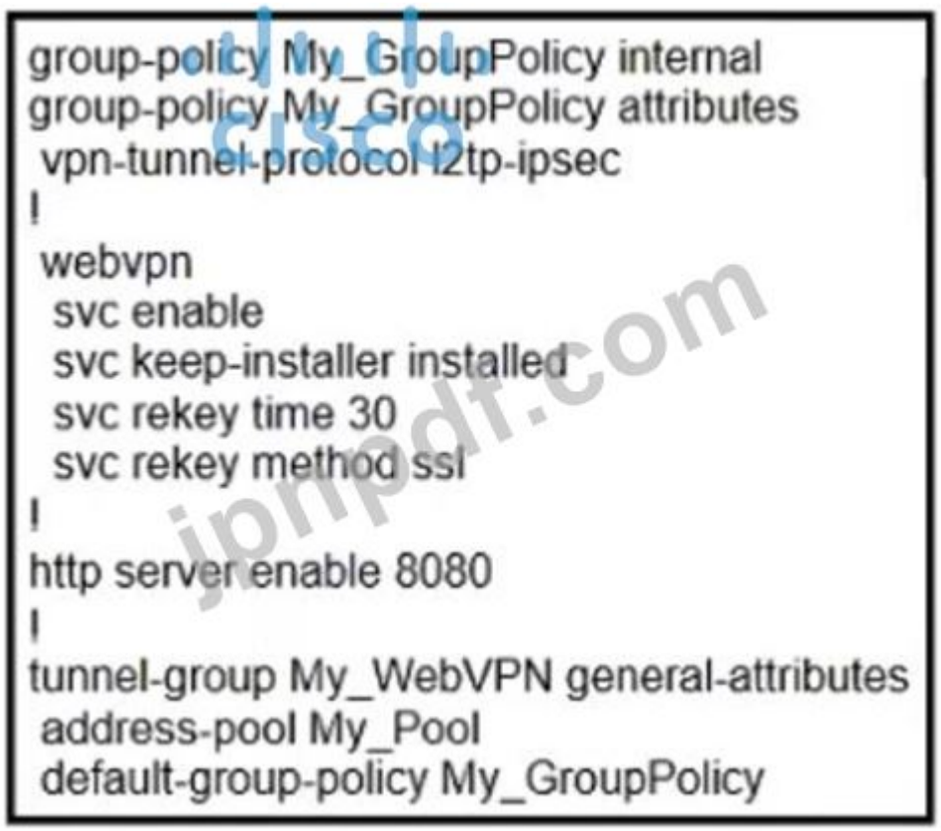
C. Cisco AnyConnect プロファイルでクライアント プロトコルを有効にします。

D. 認証方法をローカルに変更します。

Answer: (解答を表示する**)**

最新問題**: 44**

展示を参照してください。



ユーザは AnyConnect SSLVPN 経由で接続できません。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. ポート 443 でリッスンするように HTTP サーバーを構成します。

B. IPsec 事前共有キーをグループ ポリシーに追加します。

C. DHCP サーバとして機能するように ASA を設定します。

D. VPN プロトコルの許可リストに ssl クライアントを追加します。

Answer: D (メーッセージを残す**)**

最新問題**: 45**

キーサーバーのグループから主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はどれですか?

A. コードバージョン

B. 最大の IP アドレス

C. 最も優先度の高い値

D. 最小の IP アドレス

Answer: C (メーッセージを残す**)**

参照：

https://www.cisco.com/c/en/us/products/colternate/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

最新問題**: 46**

FlexVPN トンネルではどの構成構造を使用する必要がありますか?

A. IKEv1 ポリシー

B. EAP 設定

C. IKEv2 プロファイル

D. マルチポイント GRE トンネル インターフェイス

Answer: C (メーッセージを残す)

有効な **300-730** 問題集は GoShiken.com が提供された合格しやすい 300-730 試験問題集！ GoShiken.com が最新の **300-730** 試験問題集を提供しています。GoShiken.com 300-730 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-730 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 47**
IPsec ステートレス フェイルオーバーが機能するには、どの冗長プロトコルを実装する必要がありますか?
A. SSO
B. GLBP
C. HSRP
D. VRRP
Answer: C (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/17826-ipsec-feat.html

最新問題**: 48**
ネットワーク エンジニアは、リモート ユーザーが内部 HTTP サーバーにアクセスできるようにするクライアントレス VPN のセットアップをほぼ完了しました。ユーザーはユーザー名とパスワードを 2 回入力する必要があります。1 回目はクライアントレス VPN Web ポータルで、もう 1 回目は内部 HTTP サーバーにログインします。Cisco ASA と HTTP サーバは、同じ Active Directory サーバを使用してユーザを認証します。ユーザーがパスワードを 1 回だけ入力できるようにするには、次のどの手順を実行する必要がありますか?
A. HTTP サーバーのスマート トンネルを作成します。
B. NTLM 認証を使用した自動サインオンを構成します。
C. SAML 2.0 IDP 経由でユーザーを認証するように Cisco ASA をセットアップします。
D. LDAPS を使用し、クライアントレス トンネル グループにパスワード管理を追加します。
Answer: B (メーッセージを残す)

最新問題**: 49**
右側のコード スニペットを設定内の空白にドラッグ アンド ドロップして、FlexVPN を実装します。すべてのスニペットが使用されるわけではありません。

```
aaa new-model
aaa authentication login AuthC local
aaa authorization network AuthZ local

crypto ikev2 authorization policy Flex_Author
 pool Flex_Pool
 netmask 255.255.255.0
 route set remote ipv4 192.168.0.0 255.255.255.0

crypto ikev2 proposal Flex_Prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Flex_Policy
 proposal Flex_Prop

crypto ikev2 keyring Flex_Key
 peer any
  address 0.0.0.0
  pre-shared-key cisco

crypto ikev2 profile Flex_Profile
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local Flex_Key
 aaa authorization group psk list [          ] [          ]
 virtual-template 1

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile Flex_Ipsec
 set transform-set TS
 set ikev2-profile Flex_Profile

interface Virtual-Template1 type [          ]
 ip unnumbered Loopback1
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flex_IPsec

ip local pool Flex_Pool 10.10.10.5 10.10.10.10
```

AuthZ

AuthC

Flex_Policy

Flex_Author

0.0.0.0

tunnel

Answer:

```
aaa new-model
aaa authentication login AuthC local
aaa authorization network AuthZ local

crypto ikev2 authorization policy Flex_Author
 pool Flex_Pool
 netmask 255.255.255.0
 route set remote ipv4 192.168.0.0 255.255.255.0

crypto ikev2 proposal Flex_Prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Flex_Policy
 proposal Flex_Prop

crypto ikev2 keyring Flex_Key
 peer any
  address 0.0.0.0
  pre-shared-key cisco

crypto ikev2 profile Flex_Profile
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local Flex_Key
 aaa authorization group psk list AuthZ Flex_Author
 virtual-template 1

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile Flex_Ipsec
 set transform-set TS
 set ikev2-profile Flex_Profile

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flex_IPsec

ip local pool Flex_Pool 10.10.10.5 10.10.10.10
```

AuthZ

AuthC

Flex_Policy

Flex_Author

0.0.0.0

tunnel

topdf.com

最新問題: **50**

展示を参照してください。

Hub

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 2

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 0.0.0.0

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 no ip split-horizon
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.1 255.255.255.0
```

Spoke

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 2

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 172.16.18.1

interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1 nbma 172.16.18.1 multicast
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.2 255.255.255.0
```

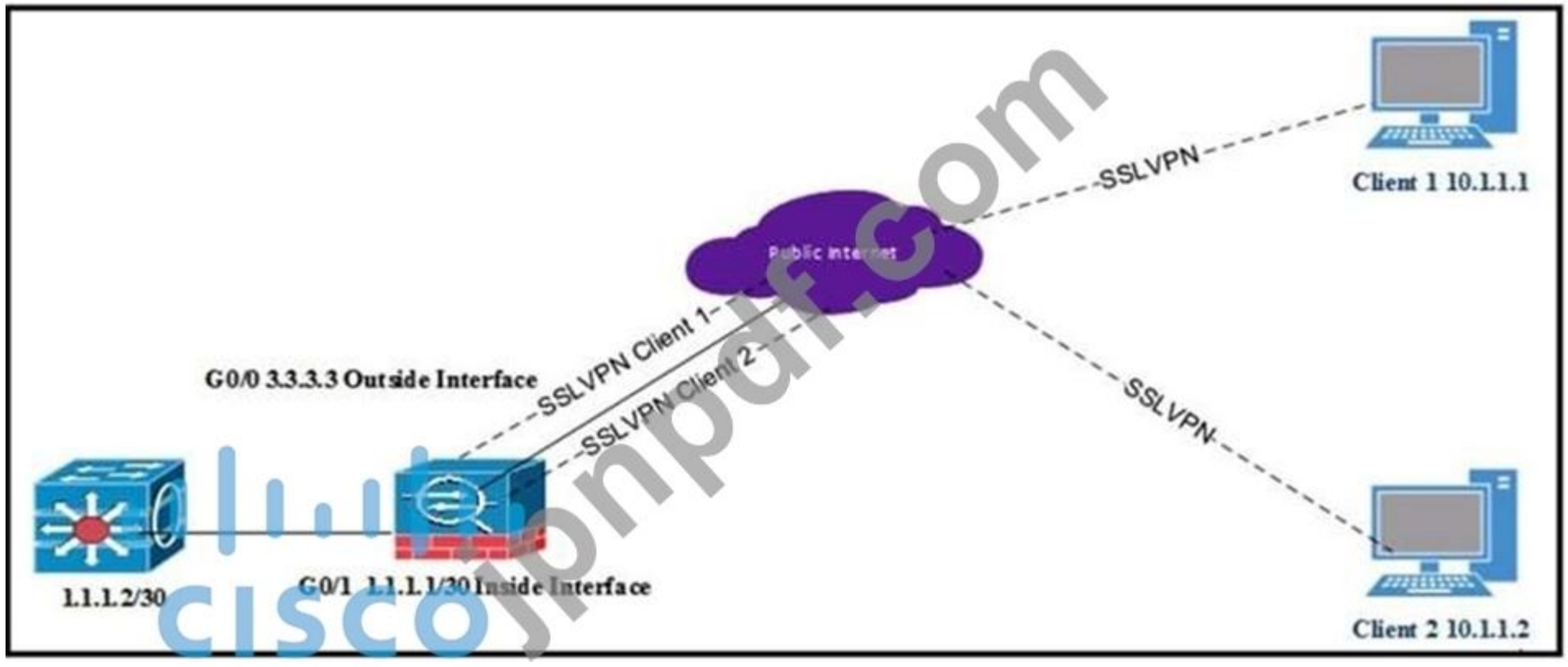
jpnpdf.com

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 2 つのアクションはどれですか? (2つお選びください。)

A. トランスフォーム セットをモード トンネルに変更します。
B. スポーク nhs を 172.16.18.1 に、nbma を 10.0.0.1 に変更します。
C. スポークの nhrp 認証キーを cisco123 に変更します。
D. スポーク上の ISAKMP ポリシー認証を事前共有に変更します。
E. スポーク上の ISAKMP キー アドレスを 0.0.0.0 に変更します。
Answer: C,D (メーッセージを残す)

最新問題**: 51**
TBAR を使用する VPN ソリューションはどれですか?
A. GETVPN
B. VTI
C. DMVPN
D. Cisco AnyConnect
Answer: A (メーッセージを残す)
参照：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get- vpn-xe-3s-book/sec-get- vpn.html

最新問題**: 52**
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のポート アドレスは、IP アドレス 3.3.3.3 を持つパブリック外部インターフェイスに変換されます。クライアント 1 とクライアント 2 は、ASA への SSL VPN 接続を正常に確立しました。
ブラウザの IP アドレス検索で 「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 ポリシーに基づく同一セキュリティ トラフィック許可のインターフェイス間
B. グループ ポリシーで以下のネットワーク リストを除外します
C. グループ ポリシーですべてのネットワークをトンネルする
D. グループ ポリシーの下のトンネル ネットワーク リスト
Answer: (解答を表示する**)**
IP アドレスのブラウザ検索で 「3.3.3.3」が返されるようにするには、グループ ポリシーで [以下のトンネル ネットワーク リスト] オプションを使用して ASA を設定する必要があります。これにより、ASA の背後にあるすべての内部クライアントのポート アドレスが、IP アドレス 3.3.3.3 のパブリック外部インターフェイスに変換されるようになります。これにより、ブラウザの検索から正しい IP アドレスが返されるようになります。

最新問題**: 53**
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、Cisco ASA でブックマークまたは URL リストをどのセクションで設定する必要がありますか?
A. webvpn (グローバル設定)
B. トンネルグループ (一般属性)
C. webvpn (グループポリシー)
D. トンネルグループ (webvpn 属性)
Answer: A (メーッセージを残す**)**

最新問題**: 54**
企業の遠隔地は MPLS 経由でデータセンターに接続します。新しいリクエストでは、リモートの場所に送信されるユニキャスト トラフィックとマルチキャスト 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、どの非トンネル技術を使用する必要がありますか?

A. FlexVPN
B. GETVPN
C. SSL
D. DMVPN
Answer: B (メーッセージを残す**)**

最新問題**: 55**
リモート トンネル エンドポイントのネットワーク ルートを動的にインストールする方法はどれですか?
A. ポリシーベースのルーティング
B. CEF
C. 逆ルート注入
D. ルートフィルタリング
Answer: C (メーッセージを残す**)**
セクション :ルータおよび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 説明/参照先 :https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12- 4t/sec-vpn-availability-12-4t-book/sec-rev-rte-inject.html

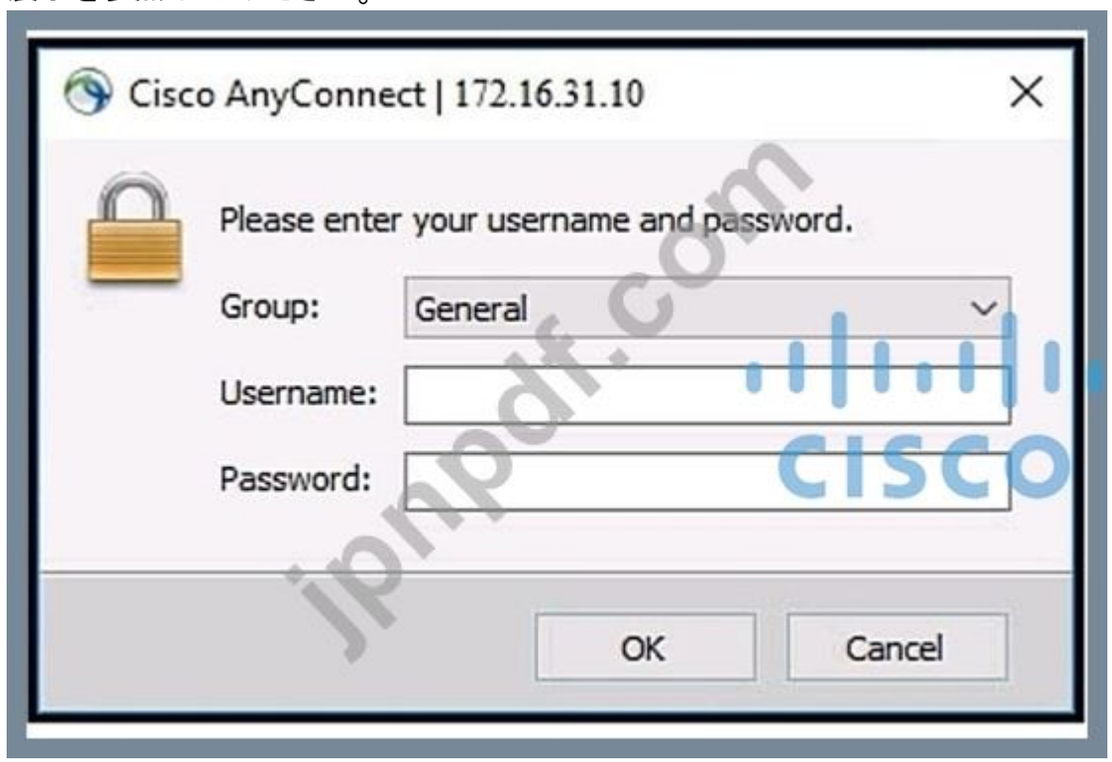
最新問題**: 56**
ASA が非標準のアプリケーションと Web リソースを処理して、クライアントレス SSL VPN 接続上で正しく表示できるようにする機能はどれですか?
A. シングルサインオン
B. スマート トンネル
C. WebType ACL
D. プラグイン
Answer: B (メーッセージを残す**)**
参照：
https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_clientless_ssl.html#29951

最新問題**: 57**
FlexVPN サーバに接続する Cisco AnyConnect 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. EAP-AnyConnect
C. AnyConnect プロファイル
D. ユーザー名とパスワードの代わりに証明書を使用する
Answer: C (メーッセージを残す**)**

最新問題**: 58**
VPN ヘッドエンドがさまざまな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ようにするテクノロジーと VPN コンポーネントはどれですか?
A. ISAKMP を使用した DMVPN
B. ISAKMP を使用した GETVPN
C. NHRP を使用した GETVPN

D. NHRP を使用した DMVPN
Answer: (解答を表示する**)**

最新問題**: 59**
展示を参照してください。



展示内の AnyConnect プロンプトを Cisco AnyConnect ユーザが受信することになる、tunnel-group webvpn-attributes の 2 つのコマンドはどれですか? (2つお選びください。)
A. グループ URL https://172.16.31.10/一般有効
B. グループ ポリシー 一般内部
C. 認証 aaa
D. 認証証明書
E. グループエイリアス 一般有効化
Answer: C,E (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

最新問題**: 60**
展示を参照してください。

```
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)
```

エンジニアが新しい GRE over IPsec 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 を送信できません。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. スポーク 2 からスポーク 1 への ESP パケット
B. スポーク 1 からスポーク 2 への ESP パケット
C. スポーク 1 からスポーク 2 への ISAKMP パケット
D. スポーク 2 からスポーク 1 への ISAKMP パケット
Answer: A (メーッセージを残す**)**

最新問題: **61**
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 で設定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、同社はネットワークに出入りする断片化したトラフィックをドロップするセキュリティ ポリシーを持っています。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 を通過しない場合、最大 IP パケット サイズは 1500 になります。暗号化されたペイロードによって 90 バイトが追加されると仮定すると、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 IP MTU を 1400 に設定します。
C. トンネルの TCP 調整-mss を 1460 に設定します。
D. トンネルの TCP 調整-mss を 1360 に設定します。
Answer: D (メーッセージを残す**)**

有効な **300-730** 問題集は GoShiken.com が提供された合格しやすい 300-730 試験問題集！ GoShiken.com が最新の **300-730** 試験問題集を提供しています。GoShiken.com 300-730 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-730 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **62**
ルーターがハブ経由で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. DMVPN フェーズ 2
B. GETVPN
C. DMVPN フェーズ 3
D. FlexVPN
Answer: (解答を表示する**)**

最新問題: **63**
エンジニアは、トラブルシューティング中に、show crypto isakmp sa コマンドがトンネルの最後の状態が MM_KEY_EXCH であることを示していることを発見しました。この問題を解決するには次のステップは何でしょうか?
A. ISAKMP プロポーザルが一致することを確認します。
B. 両方のデバイスで事前共有キーが一致していることを確認します。
C. クリプト マップ上のピアの IP アドレスを修正します。
D. UDP 500 がデバイス間でブロックされていないことを確認します。
Answer: (解答を表示する**)**

最新問題: **64**
エンジニアは、他のすべてのトラフィックがインターネットに送信されている間に、Cisco AnyConnect ユーザが 10.10.0.0/16 サブネット内のサーバにアクセスできるようにしたいと考えています。このタスクを実行できるのはどの IPsec 構成ですか?

```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```

```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

```
crypto ikev1 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

```
crypto ikev2 authorization policy Local_Authz_01
 route set remote ipv4 10.10.0.0 0.0.255.255
```

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
Answer: D (メーッセージを残す)

最新問題: **65**
Cisco ASA クライアントレス SSL VPN ソリューションに関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
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. 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。
C. リライター機能はデフォルトで無効になっているため、グローバル Webvpn 設定で rewriter Enable コマンドを使用すると、リライター機能が有効になります。
D. クライアントレス SSLVPN は、安全なネットワークへのレイヤー 3 接続を提供します。
E. Cisco ASA は、クライアントレス SSL VPN 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。
Answer: (解答を表示する**)**

最新問題: **66**
展示を参照してください。

```
Ciscoasa# sh cap c trace packet-number 4

737 packets captured

     4: 08:19:36.054181    10.99.117.195.56485 > 10.31.124.31.443: S 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow


1 packet shown
```

SSL クライアントが ASA ヘッドエンドに接続しています。セッションは失敗し、接続試行がタイムアウトしました。インターネット接続を確認してください。」というメッセージが表示されます。パケットの処理方法に基づいて、どのフェーズが障害の原因となっているのか?

A. フェーズ 9: rpf チェック

B. フェーズ 3: UN-NAT

C. フェーズ 5: NAT

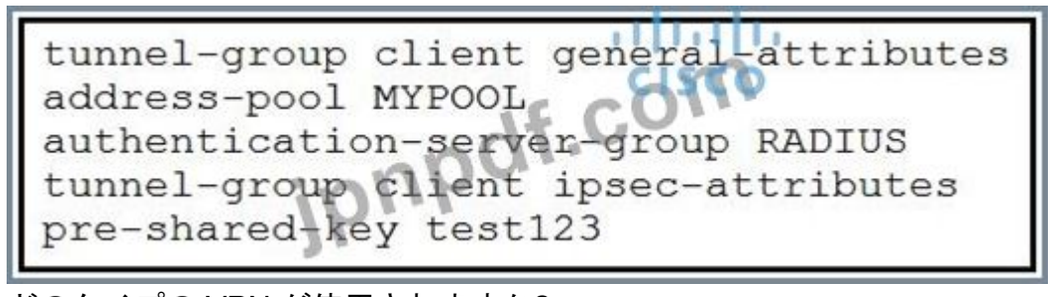
D. フェーズ 4: アクセスリスト

Answer: B (メーッセージを残す**)**

最新問題**: 67**

展示を参照してください。

jpnpdf.com



どのタイプの VPN が使用されますか?

A. GETVPN

B. クライアントレス SSL VPN

C. Cisco Easy VPN

D. Cisco AnyConnect SSL VPN

Answer: (解答を表示する**)**

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-easyvpn.html

最新問題**: 68**

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
```

jpnpdf.com

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. IPv6 外部 AAA を使用してグループを認可する FlexVPN サーバ

C. IPv6 dVTI セッション用の FlexVPN サーバー
D. EAP を使用して IPv6 ピアを認証する FlexVPN サーバ
Answer: C (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116528-config-flexvpn-00.html

最新問題**: 69**
FlexVPN で AAA 属性リストを使用できるようにするには、どの 2 つのタスクを実行する必要がありますか? (2つお選びください。)
A. 最大セグメントサイズを設定します。
B. RADIUS サーバーを定義します。
C. AAA サーバーを定義します。
D. クライアントが正しい認可ポリシーを使用していることを確認します。
E. リストを認可ポリシーに割り当てます。
Answer: D,E (メーッセージを残す**)**

最新問題**: 70**
展示を参照してください。

お客様は RDP マシンで Cisco AnyConnect を起動する必要があります。このタスクを実行できる IOS 構成はどれですか?

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
```

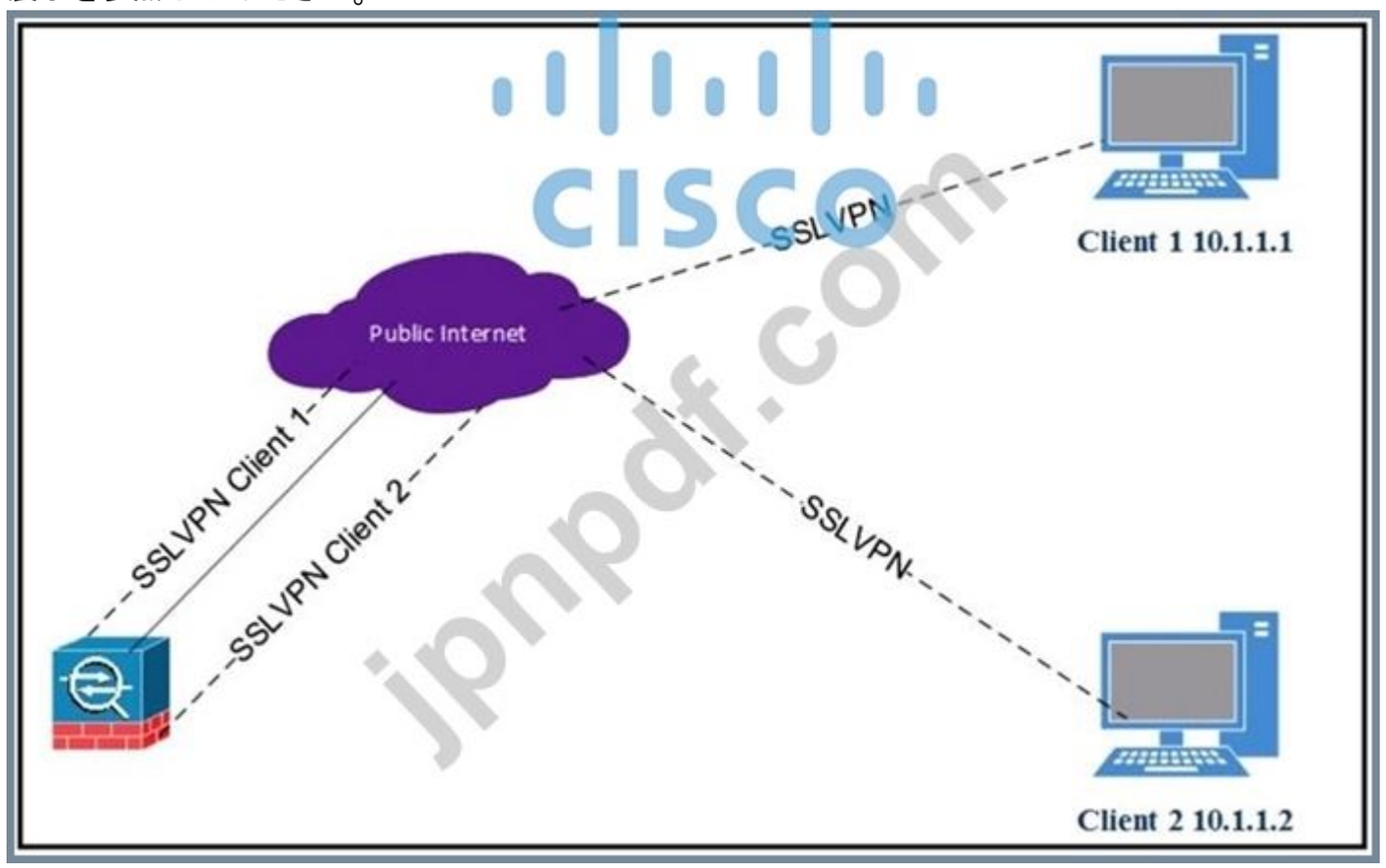
C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

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 B
C. オプション C
D. オプション D
Answer: C (メーッセージを残す**)**

参照：
https://community.cisco.com/t5/vpn/starting-anyconnect-vpn-through-rdp-session-on-cisco-891/td-p/2128284

最新問題**: 71**
展示を参照してください。



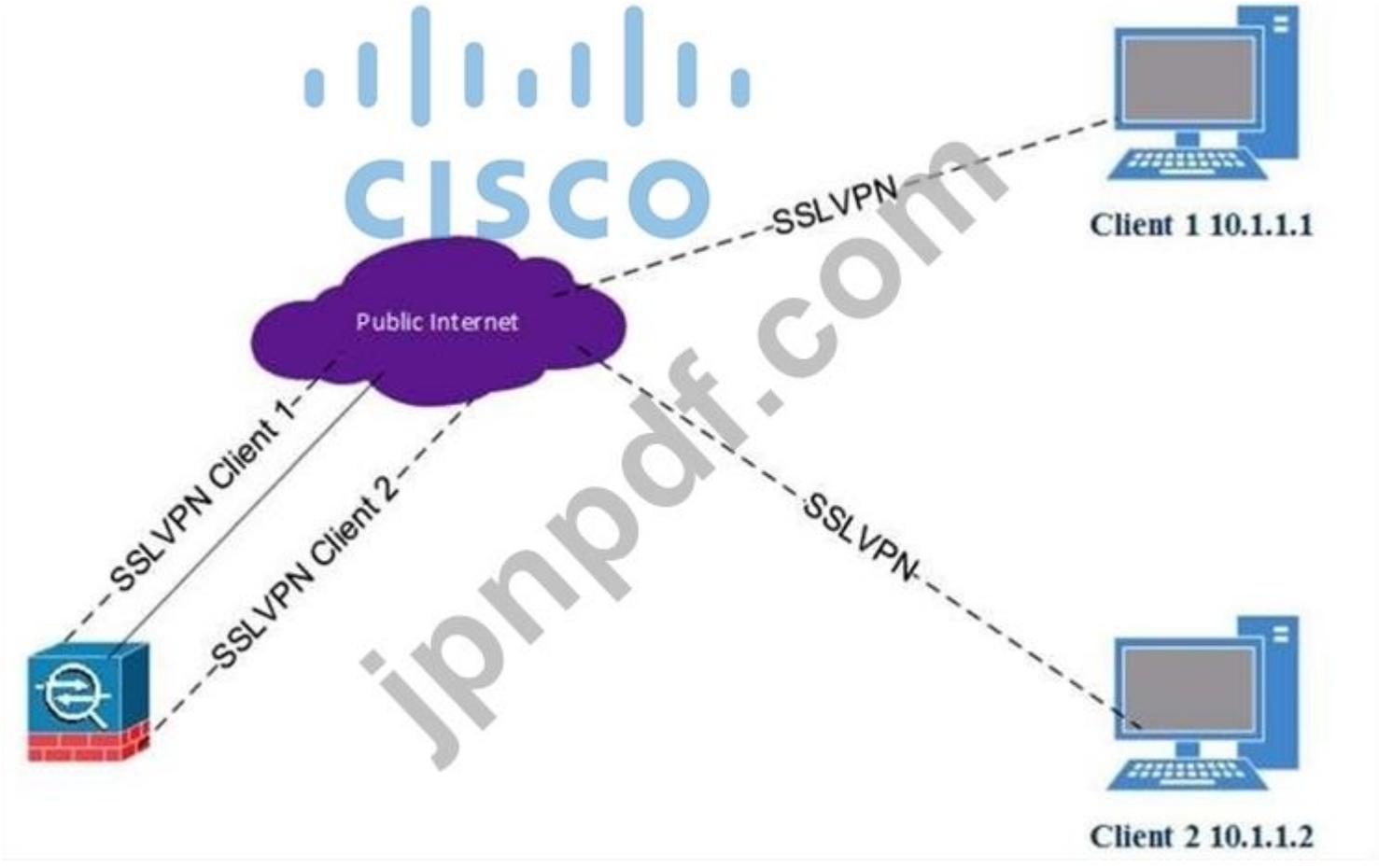
クライアント 1 はクライアント 2 と通信できません。両方のクライアントは Cisco AnyConnect を使用しており、ハブ ASA への SSL VPN 接続を正常に確立しています。
ASA で欠落しているコマンドはどれですか?
A. 同一セキュリティトラフィック許可インターフェイス間
B. dns-server 値 10.1.1.3
C. 同じセキュリティトラフィックのインターフェイス内許可
D. DNS サーバー値 10.1.1.2
Answer: (解答を表示する**)**

最新問題**: 72**
ユーザが WebVPN ポータル ページにログインすると、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. 自動アップグレード
B. 自動接続
C. 自動起動
D. 自動実行
Answer: C (メーッセージを残す**)**
参照：

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

最新問題: **73**
ネットワーク エンジニアは、リモート ユーザーが企業ネットワークにアクセスできるように SSL VPN を構成する任務を負っています。エンタープライズ IP 範囲宛てのトラフィックはトンネルを通過し、その他のトラフィックはすべてインターネットに直接送信される必要があります。これを実現するにはどの機能を設定する必要がありますか?
A. Uターン
B. デュアルホーミング
C. ヘアピニング
D. スプリットトンネル
Answer: (解答を表示する**)**

最新問題: **74**



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は Cisco AnyConnect を使用しており、ハブ ASA への SSL VPN 接続を正常に確立しています。ASA で欠落しているコマンドはどれですか?
A. DNS サーバー値 10.1.1.2
B. 同一セキュリティ トラフィック許可イントラインターフェイス
C. 同一セキュリティ トラフィック許可インターフェイス間
D. DNS サーバー値 10.1.1.3
Answer: B (メーッセージを残す**)**
セクション: ASDM および CLI を使用したトラブルシューティング

最新問題: **75**
トラフィック セレクターの 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 IKE_SA_INIT
B. IKEv2 情報
C. IKEv2 CREATE_CHILD_SA
D. IKEv2 IKE_AUTH
Answer: C (メーッセージを残す**)**
IKEv2 CREATE_CHILD_SA パケットは、2 つのピア間に新しいセキュリティ アソシエーション (SA) を確立するために使用されます。このパケットには、トラフィック セレクター、使用される暗号アルゴリズムとキー、その他の関連情報を含む交換の詳細が含まれています。

最新問題: **76**
トンネル グループ リストを使用せずに VPN セッションをトンネル グループにマッピングするのに役立つ 2 つのパラメータはどれですか? (2つお選びください。)
A. グループエイリアス
B. 証明書マップ
C. 最適なゲートウェイの選択
D. グループ URL
E. AnyConnect クライアントのバージョン
Answer: A,D (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

有効な **300-730** 問題集は GoShiken.com が提供された合格しやすい 300-730 試験問題集！ GoShiken.com が最新の **300-730** 試験問題集を提供しています。GoShiken.com 300-730 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 300-730 問題集をゲットする人はこちら:
https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **77**
Cisco ASA クライアントレス SSL VPN 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つお選びください。)
A. ICA (シトリックス)
B. VNC
C. CIFS
D. RDP
E. HTTP
Answer: C,D (メーッセージを残す**)**

最新問題: **78**
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 IKE ID を受信することを想定していますか?

A. *$DfltIkeIdentityS*
B. *$RemoteAccessVpnClient$*
C. *$AnyConnectClient$*
D. *$SecureMobilityClient$*
Answer: C (メーッセージを残す)

最新問題**: 79**
GETVPN のどの機能が DMVPN および FlexVPN の制限となっていますか?
A. ESP または AH の使用を有効にします
B. 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
C. パブリックまたはプライベート WAN 経由で使用するための設計
D. オーバーレイ ルーティング プロトコルの要件なし
Answer: D (メーッセージを残す)

最新問題**: 80**
展示を参照してください。

```
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
```

この構成の結果はどうなるのでしょうか?

A. リモート認証方法が間違っているため、スポーク 2 は認証に失敗します。

B. 認証方法が間違っているため、スポーク 1 は認証に失敗します。

C. 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。

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。

Answer: B (メーッセージを残す)

最新問題: **81**
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
```

cisco
npdf.com

グループ Cisc012345678 にはどのタイプの Cisco VPN が表示されますか?
A. クライアントレス SSLVPN
B. Cisco AnyConnect クライアント VPN
C. GETVPN
D. DMVPN
Answer: (解答を表示する**)**

最新問題: **82**
楕円曲線鍵交換アルゴリズムを使用するものは何ですか?
A. SHA
B. ECDHE
C. ECDSA
D. AES-GCM
Answer: (解答を表示する**)**

最新問題: **83**
FlexVPN 導入では、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、解決要求を送信していることを確認します。
B. スポーク設定を検証して、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。

C. ハブの設定を確認して、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。
Answer: A (メーッセージを残す**)**

最新問題: **84**
展示を参照してください。

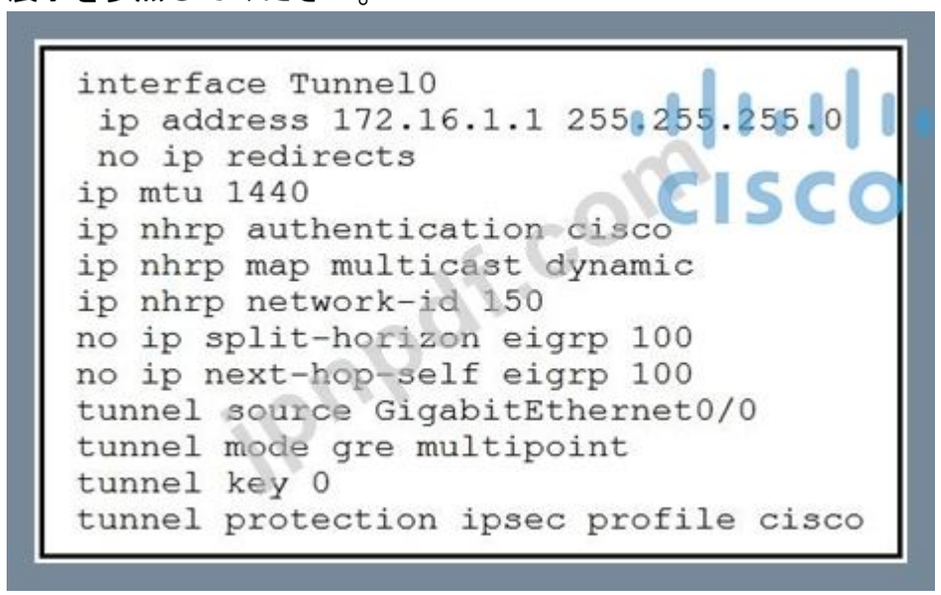
```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy 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期間中にクライアントレス SSLVPN を再構成し、新しい構成をテストした後、接続を確立できません。この問題を解決するには何をしなければなりませんか?
A. グループ ポリシーで DTLS を有効にします。
B. 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。
C. 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。
D. 外部インターフェイスでクライアント サービスを有効にします。
Answer: (解答を表示する**)**

最新問題: **85**
ネットワーク エンジニアは、複数の FlexVPN クライアントを終了するために FlexVPN サーバーをセットアップしました。VPN トンネルは問題なく確立されます。ただし、RADIUS サーバによって認可の変更が発行された場合、FlexVPN サーバは接続されている FlexVPN クライアントの認可を更新しません。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. RADIUS サーバーと FlexVPN サーバー間の RADIUS キーの不一致を修正します。
B. FlexVPN クライアントに aaaserverradiusdynamic-author コマンドを追加します。
C. RADIUS サーバーと FlexVPN クライアントの間の RADIUS キーの不一致を修正します。

D. FlexVPN サーバに aaaserverradiusdynamic-author コマンドを追加します。
Answer: (解答を表示する**)**

最新問題**: 86**
展示を参照してください。



DMVPN フェーズ 2 設定から導き出される結論は次の 2 つのうちどれですか? (2つお選びください。)
A. ダイナミック ルーティング プロトコルとして EIGRP が使用されます。
B. Next-hop-self は必須です。
C. スポークツースポーク通信が許可されます。
D. EIGRP ルートの再配布は許可されません。
E. EIGRP ネイバー隣接関係は失敗します。
Answer: (解答を表示する**)**

最新問題**: 87**
展示を参照してください。

エンジニアは、FlexVPN ハブに接続するようにスポークを設定しました。トンネルは稼働していますが、エンジニアがスポークの背後にあるホスト 192.168.200.10 に到達しようとすると ping が失敗し、トラフィックの送信元は FlexVPN サーバの背後にあるホスト 192.168.100.3 になります。エンジニアは、パケット キャプチャに基づいて、ホスト 192.168.200.10 が icmp エコーを受信し、スポークの内部インターフェイスに到達する icmp 応答を送信していることを発見しました。エンジニアがスポーク上でキャプチャした展示内の出力に基づいて、どのアクションがこの問題を解決しますか?

A. aaa authorization group cert listdefault コマンドをハブ ikev2 プロファイルに追加します。

B. aaa authorization group cert listdefault コマンドをスポーク ikev2 プロファイルに追加します。

C. ハブ認可ポリシーに、route set remote ipv4 192.168.200.0 255.255.255.0 コマンドを追加します。

D. ルート設定リモート ipv4 192.168.100.0 255.255.255.0 コマンドをスポーク認可ポリシーに追加します。

Answer: D (メーッセージを残す)

最新問題**: 88**

FlexVPN サーバに接続する Cisco AnyConnect 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
Answer: B (メーッセージを残す**)**
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.pdf

最新問題**: 89**
エンジニアがクライアントレス SSL VPN を構成しています。財務部門には財務部門のみがアクセスできるデータベース サーバーがありますが、現在は営業部門もアクセスできます。財務部門と営業部門は、別個のグループ ポリシーとして構成されます。営業部門のユーザーが財務部門のサーバーにアクセスできないようにするには、構成に何を追加する必要がありますか?
A. トンネルグループブロック
B. スマートトンネル
C. ポートフォワーディング
D. Web タイプ ACL
Answer: (解答を表示する**)**
https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/acl-webtype.pdf

最新問題**: 90**
IPsec ステートレス フェイルオーバーが機能するには、どの冗長プロトコルを実装する必要がありますか?
A. SSO
B. GLBP
C. HSRP
D. VRRP
Answer: C (メーッセージを残す**)**
セクション: 安全な通信アーキテクチャ
説明/参照: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/17826-ipsec-feat.html

Valid 300-730 Dumps shared by GoShiken.com for Helping Passing 300-730 Exam! GoShiken.com now offer the **newest 300-730 exam dumps**, the GoShiken.com 300-730 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 300-730 dumps with Test Engine here: https://www.goshiken.com/Cisco/300-730-mondaishu.html (**240** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)