Cisco.300-730.v2022-07-13.q63

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：	63
バージョン：	v2022-07-13
ページの閲覧量：	504
問題集の閲覧量：	4498

https://www.jpnshiken.com/shiken/Cisco.300-730.v2022-07-13.q63.html

質問: **1**

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. IKEv2 AnyConnect

B. クライアントレス

C. SSL AnyConnect

D. クリプトマップ
正解: **(**正解を表示します**)**

質問: **2**

```
IKEv2:(SESSION ID = 17,SA ID = 1):Processing IKE_AUTH message
IKEv2:IPSec policy validate request sent for profile CloudOne with psh index 1.

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

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

IKEv2:(SESSION ID = 17,SA ID = 1):Sending Packet [To 68.72.250.251:500/From 68.72.250.250:500/VRF i0:f0]
Initiator SPI : 3D527B1D50DBEEF4 - Responder SPI : 8C693F77F2656636 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 ENCR
```

展示を参照してください。デバッグ出力に基づいて、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

正解: **B (**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

Explanation:

レスポンダーのポリシーで、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は、TS_UNACCEPTABLE通知メッセージで応答します。

質問: **3**

展示を参照してください。

```
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
```

SSLクライアントがASAヘッドエンドに接続しています。 接続の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、セッションが失敗します。パケットの処理方法に基づいて、どのフェーズが障害を引き起こしていますか？

A. フェーズ4 :アクセスリスト

B. フェーズ3 :UN-NAT

C. フェーズ5 :NAT

D. フェーズ9 :rpf-check

正解: **(**正解を表示します**)**

質問: **4**

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. トンネルグループ（一般属性）
B. トンネルグループ（webvpn-attributes）
C. webvpn（グループポリシー）
D. webvpn（グローバル構成）
正解: **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: **5**

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: **B** (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: **6**

```
*Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D5684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
*Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
 VID Next payload: IDr, reserved: 0x0, length: 20
 IDr Next payload: AUTH, reserved: 0x0, length: 12
   Id type: IPv4 address, Reserved: 0x0 0x0
 AUTH Next payload: SA, reserved: 0x0, length: 28
   Auth method PSK, reserved: 0x0, reserved: 0x0
 SA Next payload: TSi, reserved: 0x0, length: 40
  last proposal: 0x0, reserved: 0x0, length: 35
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
   type: 1, reserved: 0x0, id: 3DES
   last transform: 0x3, reserved: 0x0: length: 8
   type: 3, reserved: 0x0, id: SHA96
   last transform: 0x0, reserved: 0x0: length: 8
   type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 30.30.30.0, end addr: 30.30.30.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 20.20.20.0, end addr: 20.20.20.255
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
   Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
```

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. ピアID

C. 変換セット

D. ikev2プロポーザル

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: **7**

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SSLVPN接続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

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/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config / vpn_clientless_ssl.html＃29951

質問: **8**
DMVPNフェーズ3の実装に固有の2つのNHRP機能はどれですか。（2つ選択してください。）
A. 登録返信
B. リダイレクト
C. 解決リクエスト
D. 解決応答
E. 登録リクエスト
正解: **B,D (**コメントを発表する**)**

質問: **9**
正しいコマンドを夜から左側のコード内の空白にドラッグアンドドロップして、動的なスポーク間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

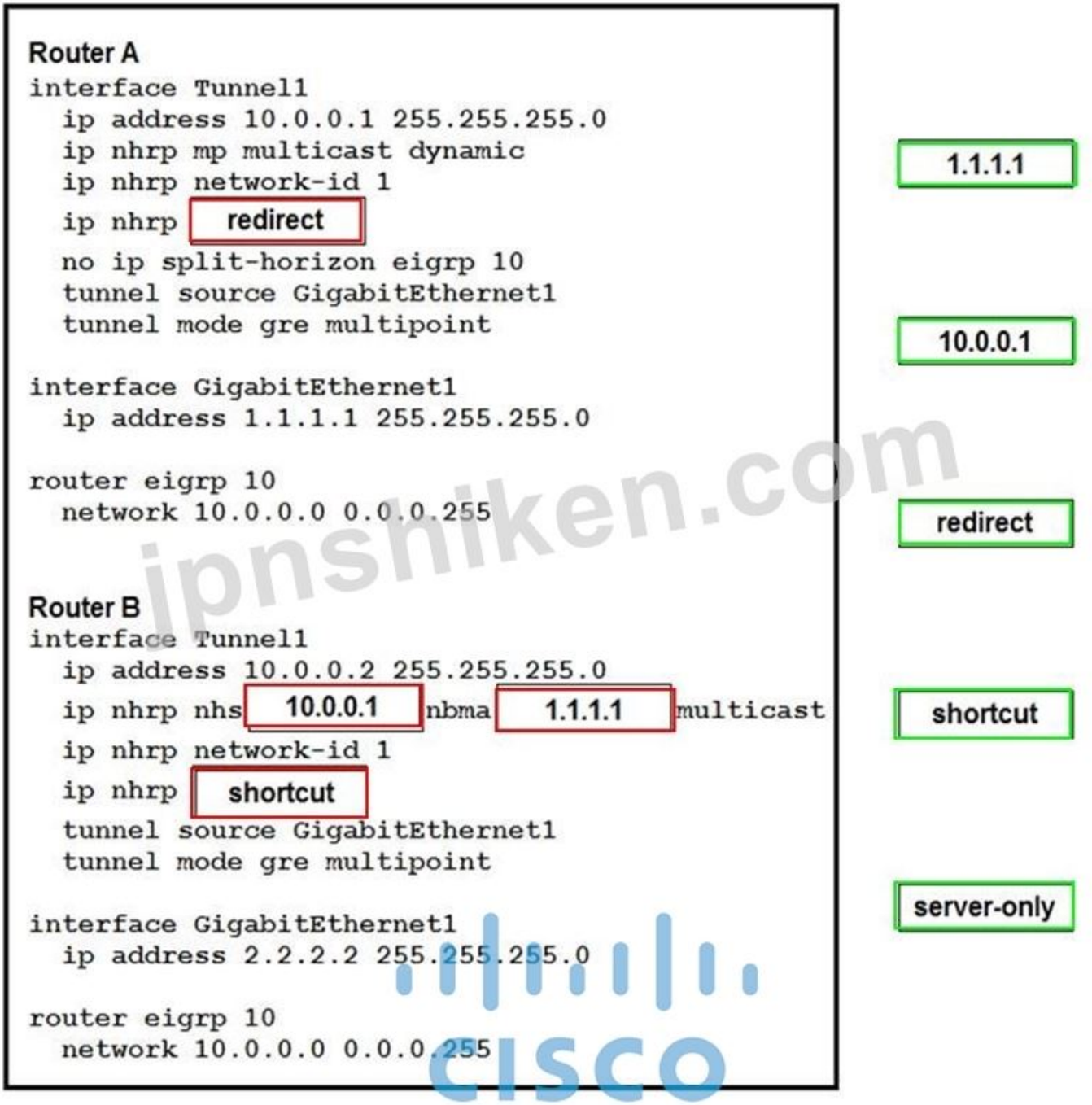
redirect

shortcut

server-only

正解:

Answer Area



質問: **10**

```
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トンネルがランダムにドロップしており、トンネル保護が構成されていません。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
```

```
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
```

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 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

D.

正解: **D** (コメントを発表する)

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: **11**

ECDHとECDSAの2つの機能は何ですか？ 2つ選択してください。）

A. 否認防止
B. 鍵交換
C. 失効
D. 暗号化
E. デジタル署名
正解: **B,E** (コメントを発表する)

質問: **12**
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: **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

質問: **13**
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トンネルを終了できるようにするために必要なコマンドはどれですか。
A. インターフェーストンネル
B. インターフェース仮想アクセス
C. ipnhrpリダイレクト
D. インターフェイス仮想テンプレート
正解: (正解を表示します)

質問: **14**
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. ESPまたはAHの使用を有効にする
D. 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
正解: (正解を表示します)

質問: **15**
IPv6 FlexVPNスポークからハブへの接続障害のトラブルシューティングに使用されるコマンドはどれですか？
A. show crypto ikev2 sa
B. show crypto isakmp sa
C. show crypto gkm
D. 暗号IDを表示する

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/support/docs/security/flexvpn/116413-configure-flexvpn-00.pdf

質問: **16**
エンジニアがCiscoIOSルータの新しいDMVPNセットアップのトラブルシューティングを行っています。show crypto isakmp saコマンドが発行された後、「MM_NO_STATE」の応答が返されます。なぜこの障害が発生するのですか？
A. ISAKMPポリシーの優先度の値が無効です。
B. ESPトラフィックがドロップされています。
C. フェーズ1ポリシーは両方のデバイスで一致しません。
D. トンネル保護はDMVPNトンネルに適用されません。
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: **17**
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. コードバージョン
B. 最高のIPアドレス
C. 最も優先度の高い値
D. 最小のIPアドレス
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/リファレンス :https ://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

質問: **18**
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**)**
参照：
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2- Remote-Access.html

質問: **19**

展示を参照してください。展示に基づいて、なぜユーザーはCCNP Webサーバーブックマークにアクセスできないのですか？
A. URLはWebACLによってブロックされています。
B. ASAはURLを解決できません。
C. ブックマークが無効になっています。
D. ユーザーはURLにアクセスできません。
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: **20**
展示を参照してください。

```
interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

 protected vrf: (none)
 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 current_peer 192.168.0.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 16228, #pkts encrypt: 16228, #pkts digest: 16228
  #pkts decaps: 26773, #pkts decrypt: 26773, #pkts verify: 26773
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
  #pkts invalid prot (recv) 0, #pkts verify failed: 0
  #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
  ##pkts replay failed (rcv): 23751
  #pkts tagged (send): 0, #pkts untagged (rcv): 0
  #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (recv) 0

  local crypto endpt.: 10.10.10.1, remote crypto endpt.: 192.168.0.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
  current outbound spi: 0x48998999(1218021785)
  PFS (Y/N): N, DH group: none
```

2つのサイト間にトンネルを設定すると、ユーザーはVPNを介したアプリケーションへの接続が一貫して機能していないと不満を漏らしています。show crypto ipsec saの出力は、VPNデバイスの1つで収集されました。この出力に基づいて、この問題を修正するにはどうすればよいですか？

A. トンネルMTUを下げます。

B. 完全転送秘密を有効にします。

C. リモートIDでアプリケーションネットワークを指定します。

D. IPSec再生ウィンドウを調整します。

正解: **A** (コメントを発表する)

質問: **21**

ECDHとECDSAの2つの機能は何ですか？ 2つ選択してください。）

A. 否認防止

B. 失効

C. デジタル署名

D. 鍵交換

E. 暗号化

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/リファレンス：

https ://tools.cisco.com/security/center/resources/next_generation_cryptography

質問: **22**
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. 仮想テンプレート
B. IKEv2認証ポリシー
C. グループポリシー
D. webvpnコンテキスト
正解: **(**正解を表示します**)**

質問: **23**
正しいコマンドを夜から左側のコード内の空白にドラッグアンドドロップして、動的なスポーク間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

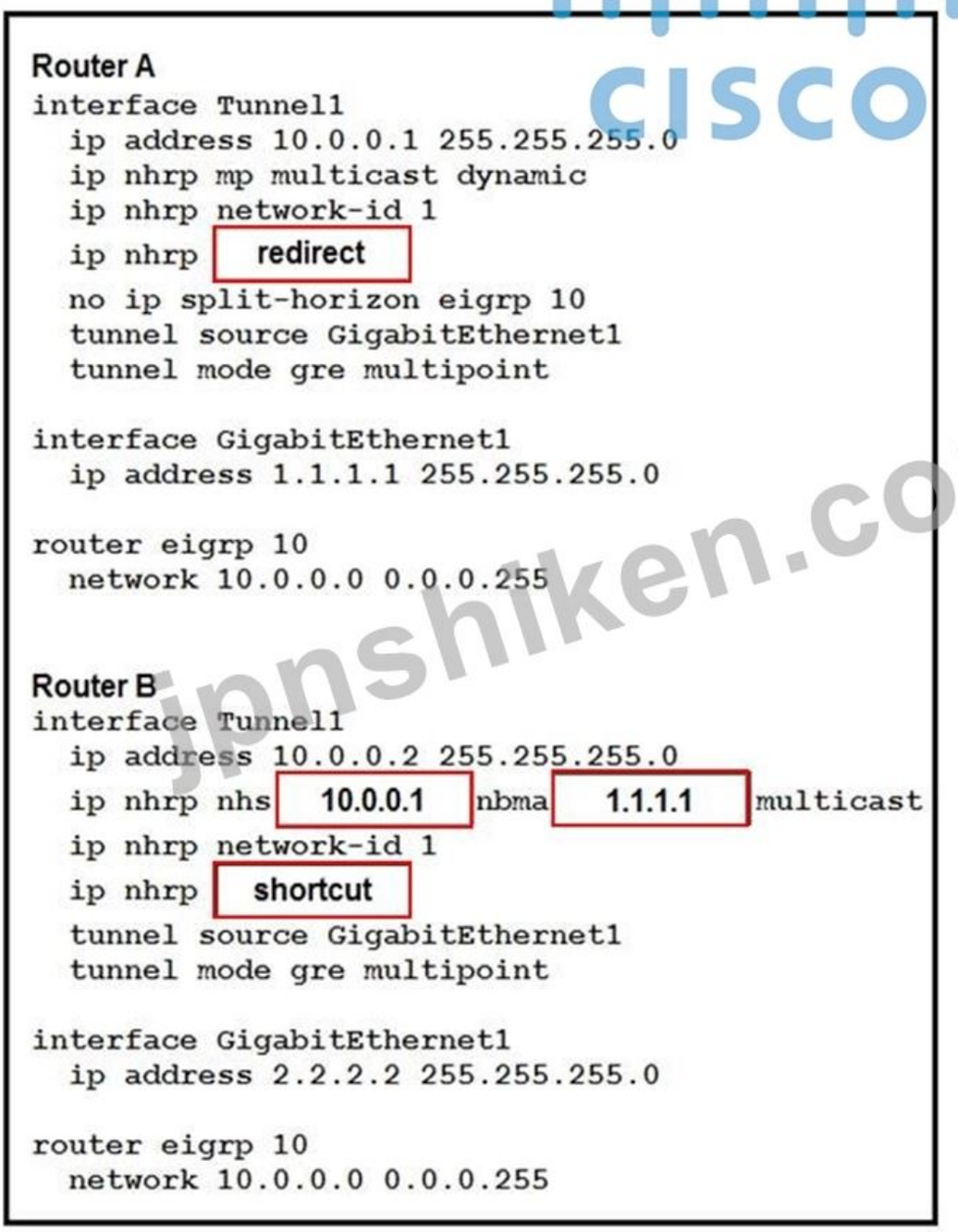
redirect

shortcut

server-only

正解:

Answer Area



1.1.1.1

10.0.0.1

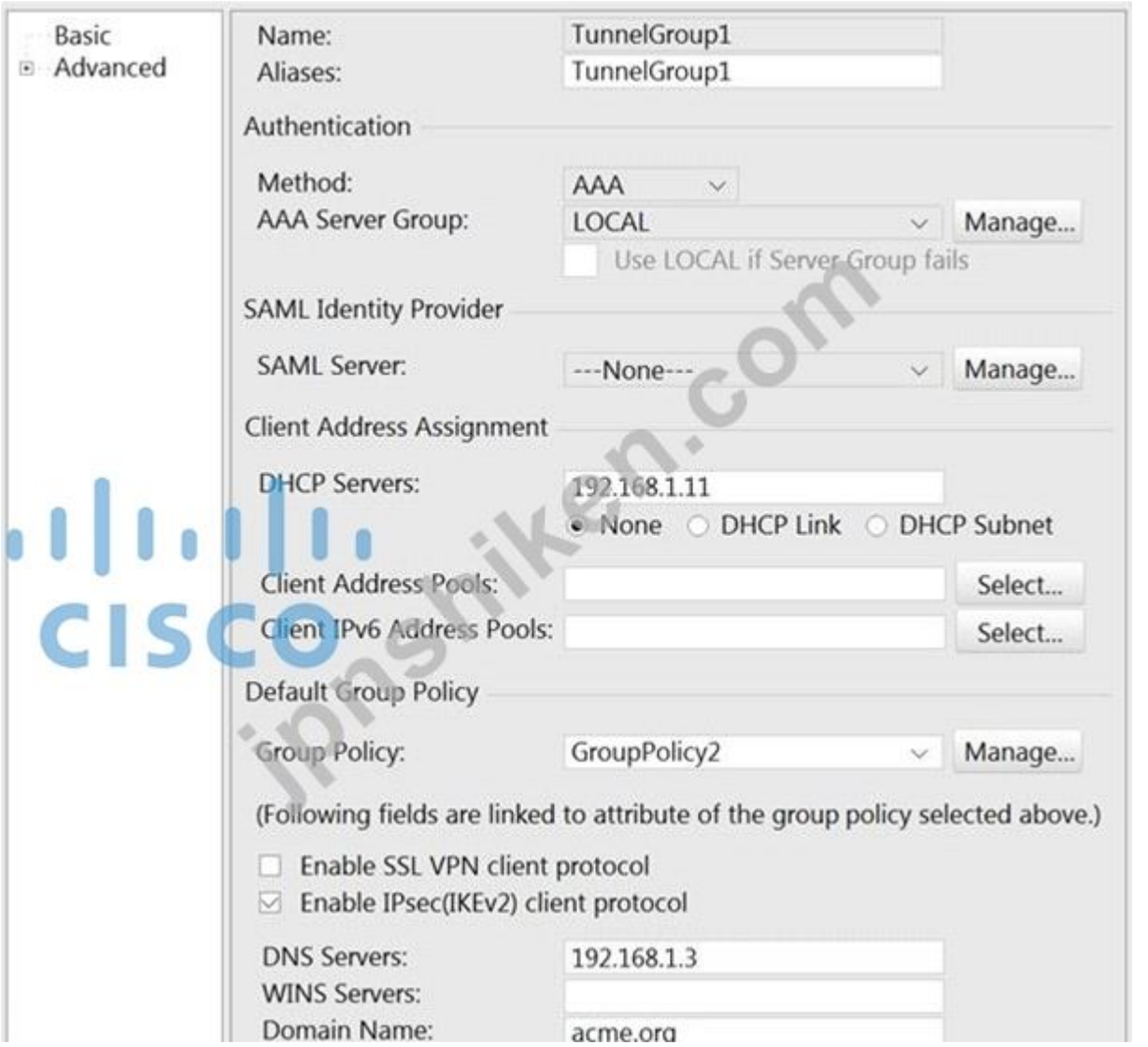
redirect

shortcut

server-only

参照：
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: **24**
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を設定していて、ローカルクレデンシャルを使用して接続を完了できません。この問題を修正するには何をする必要がありますか？

A. 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。

B. 認証方法をローカルに変更します。

C. クライアントを認証するようにAAAサーバグループを設定します。

D. CiscoAnyConnect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。

正解: **(**正解を表示します**)**

質問: **25**

サイト間VPNを介して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. IOSルーター上のGRE over IPsec

B. ASAのGREトンネル

C. FTDのIPsecトンネル

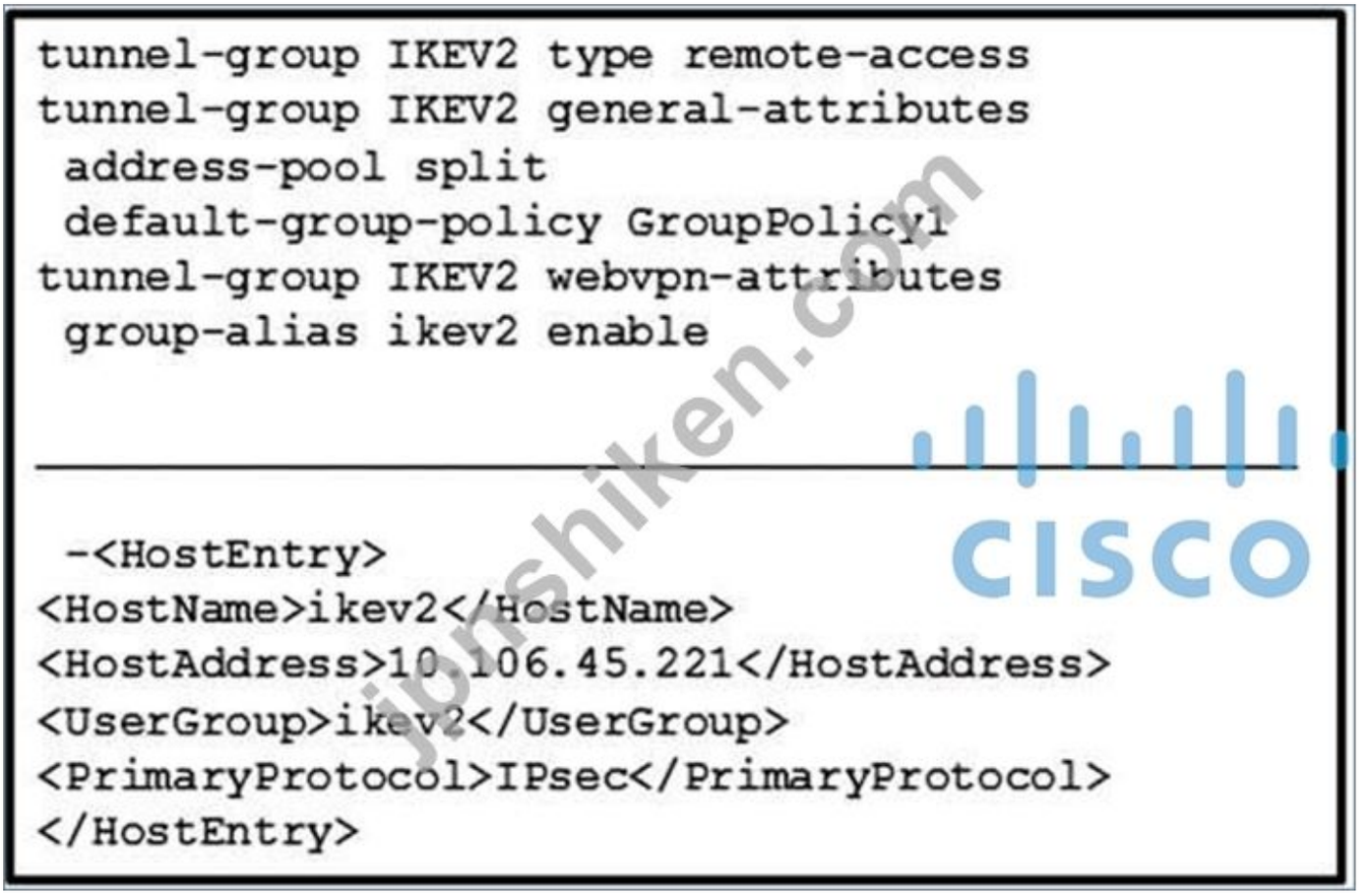
D. FTDでのGRE over IPsec

正解: **(**正解を表示します**)**

質問: **26**
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: **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: **27**
ECDHとECDSAの2つの機能は何ですか？ （2つ選択してください。）
A. 否認防止
B. 失効
C. デジタル署名
D. 鍵交換
E. 暗号化
正解: **C,D (コメントを発表する)**
参照：
https://tools.cisco.com/security/center/resources/next_generation_cryptography

質問: **28**



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。

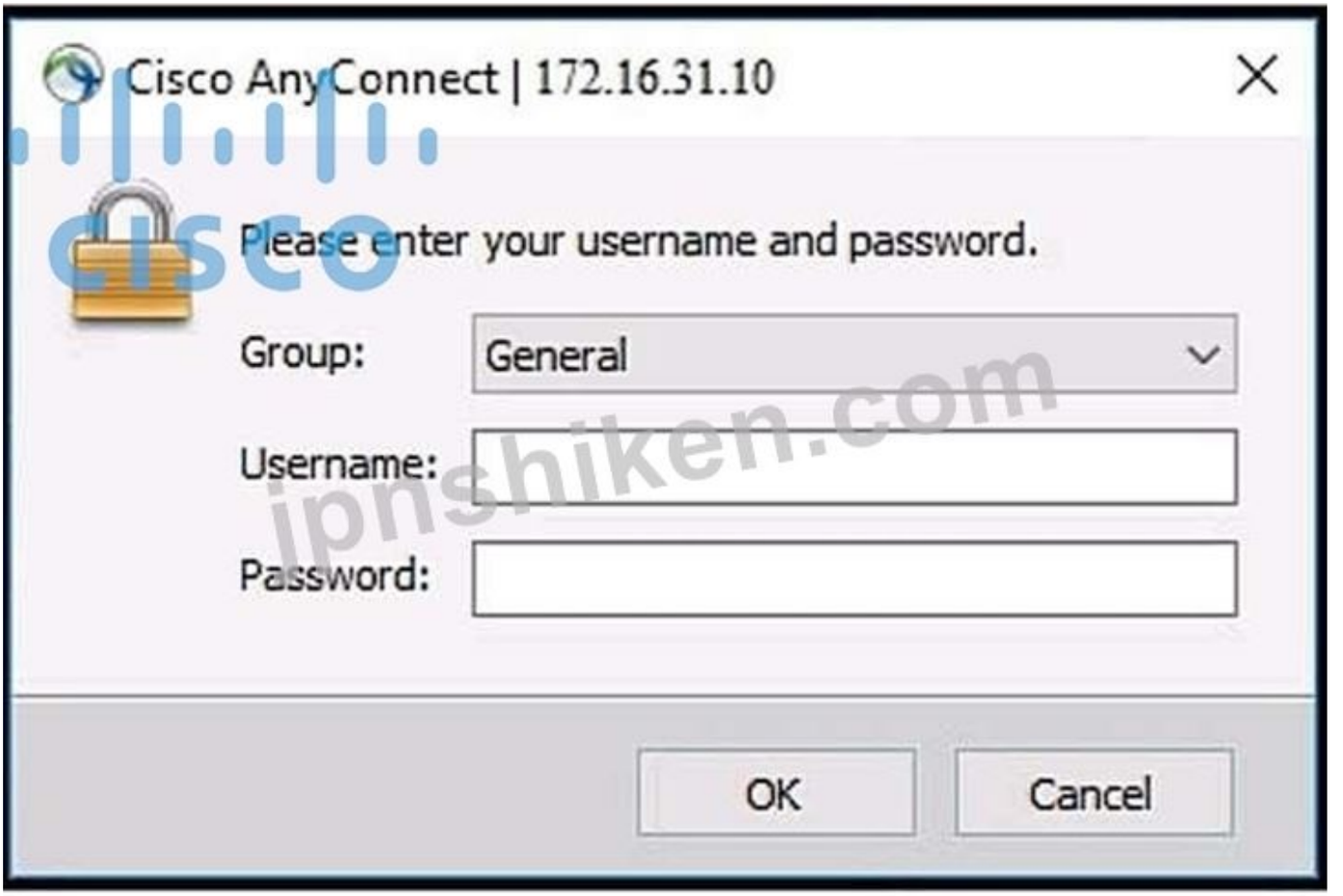
D. UserGroupは接続プロファイルと一致する必要があります。

正解: **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 ://community.cisco.com/t5/security-documents/anyconnect-xml-settings/ta-p/3157891

質問: **29**



展示を参照してください。tunnel-group webvpn-attributesの下にある2つのコマンドのうち、CiscoAnyConnectユーザが展示でAnyConnectプロンプトを受信する結果となるのはどれですか。（2つ選択してください。）

A. group-url https://172.16.31.10/General enable

B. グループポリシー一般内部

C. 認証aaa

D. 認証証明書

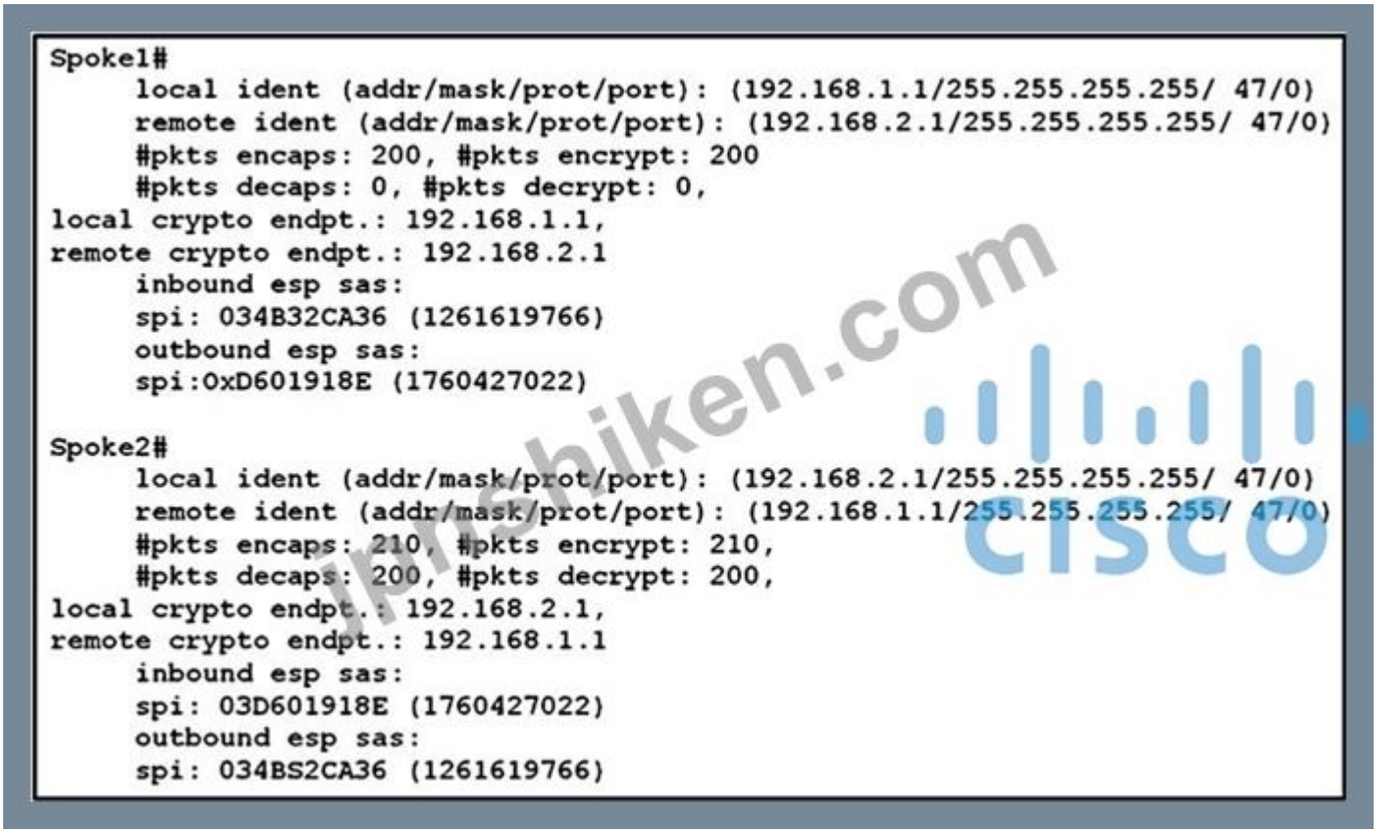
E. group-alias General enable

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: **30**

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. spoke1からspoke2へのISAKMPパケット

B. spoke2からspoke1へのISAKMPパケット

C. spoke2からspoke1へのESPパケット

D. spoke1からspoke2へのESPパケット

正解: **C** (コメントを発表する)

質問: **31**

Cisco ASAは、アクティブ/スタンバイモードで設定されています。Cisco AnyConnectユーザがフェールオーバーイベント後に接続できるようにするには、何が必要ですか。

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

B. vpnsession-db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アドレスを指している必要があります。

正解: (正解を表示します)

参照：

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html

質問: **32**
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. コードバージョン
D. 最高のIPアドレス
正解: **A** (コメントを発表する)

質問: **33**
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)
参照：
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ike

質問: **34**
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. IPv6外部AAAを使用してグループを承認するFlexVPNサーバー

C. IPv6dVTI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サーバー
正解: **(**正解を表示します**)**
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- flex-clnt.html

質問: **35**
特定の内部サブネット内のデバイスにポート443を使用してのみアクセスできるようにするCiscoAnyConnectコンポーネントはどれですか。
A. ルーティング
B. WebACL
C. スプリットトンネル
D. VPNフィルター
正解: **(**正解を表示します**)**

質問: **36**
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: **37**
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. ルートフィルタリング
B. CEF
C. リバースルートインジェクション
D. ポリシーベースのルーティング
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実装が表示されますか？

A. IKEv2再接続

B. IKEv2ロードバランサー

C. IKEv2バックアップゲートウェイ

D. IKEv1クラスター

正解: **(**正解を表示します**)**

質問: **39**

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SSLVPN接続で正しく表示できるようにする機能はどれですか。

A. WebType ACL

B. シングルサインオン

C. プラグイン

D. スマートトンネル

正解: **(**正解を表示します**)**

質問: **40**

EIGRPが設定されている場合にDMVPNフェーズ2からフェーズ3に移行するには、どの2つの変更を行う必要がありますか。2つ選択してください。）

A. ハブでEIGRPネクストホップセルフをディセーブルにします。

B. ハブにNHRPショートカットを追加します。

C. スポークにNHRPリダイレクトを追加します。

D. ハブにNHRPリダイレクトを追加します。
E. ハブでEIGRPネクストホップセルフを有効にします。
正解: **A,D** (コメントを発表する)

質問: **41**

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: **42**
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: (正解を表示します)
セクション :リモートアクセスVPN

質問: **43**
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: **(**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: **44**
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. 自動アップグレード
B. 自動接続
C. 自動起動
D. 自動実行
正解: **(**正解を表示します**)**
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

質問: **45**
エンジニアがクライアントレスSSLVPNを設定しています。財務部門には、自分だけ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、営業部門はそれにアクセスできます。財務部門と営業部門は、別々のグループポリシーとして構成されています。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. トンネルグループロック
B. ポートフォワーディング
C. ウェブタイプACL
D. スマートトンネル
正解: **A (**コメントを発表する**)**

質問: **46**
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. ECDSA
B. ECDHE
C. AES-GCM
D. SHA
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
説明/参照 :https ://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

質問: **47**
エンジニアが新しいDMVPNを統合し、CiscoIOSルータを使用してインターネット経由でリモートオフィスをリンクしました。リモートサイトに接続すると、pingと音声データが適切に流れているように見え、すべてのトンネル統計がそれらが稼働していることを示します。ただし、RDPを使用してリモートサーバーに接続しようとすると、接続は失敗します。この問題を解決するアクションはどれですか？
A. RDPサーバーの証明書を置き換えます。
B. DMVPNタイムアウト値を変更します。
C. ルーター内のMTUサイズを調整します。
D. 拡張ACLにRDPポートを追加します。
正解: **(**正解を表示します**)**

質問: **48**
ネットワークエンジニアは、企業向けのクライアントレスVPNソリューションを設計する必要があります。VPNユーザーは、複数の内部Webサーバーにアクセスできる必要があります。これらのWebサーバへの到達可能性をテストしたところ、1つのWebサイトがASAによって正しく書き換えられていないことがわかりました。
クライアントレスVPNセットアップを可能にしながら、この問題の潜在的な解決策は何ですか？
A. WebサーバのIPアドレスを持つスプリットトンネルを使用してCiscoAnyConnectを設定します。
B. ポート80でASAパブリックアドレスをWebサーバプライベートアドレスに変換するNATルールを設定します。
C. WebサーバーのIPアドレスを使用してスマートトンネルを設定します。
D. WebサーバーのIPアドレスを許可するようにWebACLを設定します。
正解: **C (**コメントを発表する**)**

質問: **49**
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. トンネルグループ（一般属性）
B. トンネルグループ（webvpn-attributes）

C. webvpn グループポリシー）
D. webvpn グローバル構成）
正解: **D (**コメントを発表する**)**
セクション :リモートアクセスVPN
説明/参照：

質問: **50**

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. リモートピアで認証失敗が発生しました。
B. 証明書の断片化の問題が両側で発生します。
C. ピアからのUDP4500トラフィックがルータに到達しません。
D. ルーターで認証エラーが発生しました。
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: **51**
IPsecステートレスフェールオーバーを機能させるには、どの冗長プロトコルを実装する必要がありますか？
A. GLBP
B. VRRP

C. HSRP
D. SSO
正解: **(**正解を表示します**)**

質問: **52**
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. ECDSA
B. ECDHE
C. AES-GCM
D. SHA
正解: **B (**コメントを発表する**)**
参照：
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

質問: **53**
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. プライマリプロトコルはSSLである必要があります。
B. IPアドレスが正しくありません。
C. UserGroupは接続プロファイルと一致する必要があります。

D. ホスト名が正しくありません。
正解: **(**正解を表示します**)**

質問: **54**
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. 証明書の断片化の問題が両側で発生します。
B. リモートピアで認証失敗が発生しました。
C. ピアからのUDP4500トラフィックがルータに到達しません。
D. ルーターで認証エラーが発生しました。
正解: **(**正解を表示します**)**

質問: **55**
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トンネルがランダムにドロップしており、トンネル保護が構成されていません。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
```

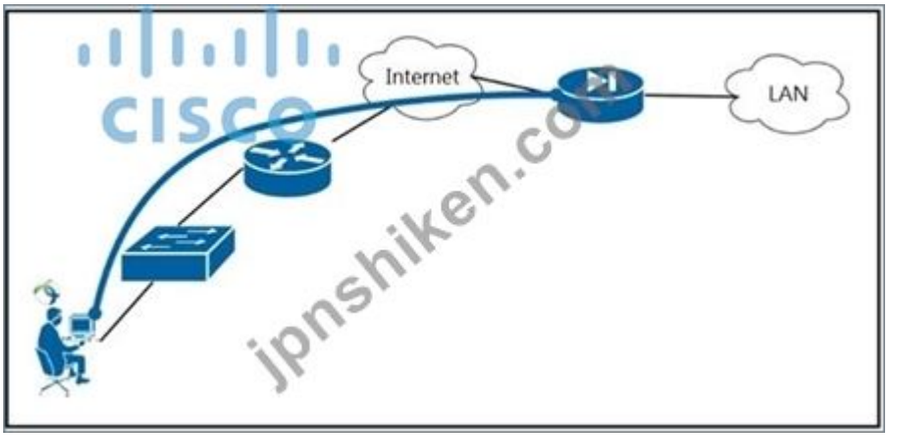

D.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode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

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

質問: **56**
DMVPNフェーズ3クラウドのすべてのルーターで一致する必要があるパラメーターはどれですか。
A. トンネルVRF
B. NHRPネットワークID
C. GREトンネルキー
D. EIGRPスプリットホライズン設定
正解: **C (**コメントを発表する**)**

質問: **57**

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>
```

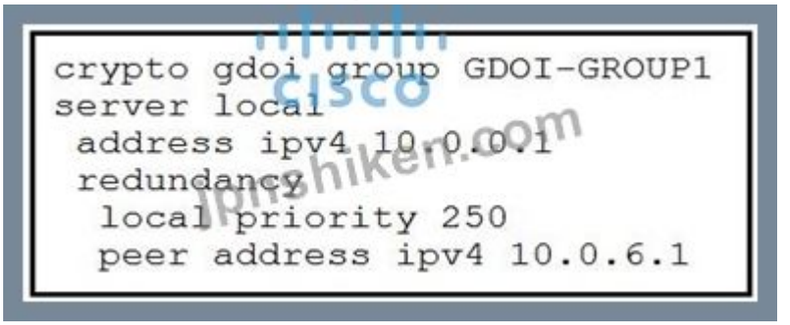
C.
```
<HostEntry>
  <HostName>RAVPN</HostName>
  <HostAddress>209.165.202.129</HostAddress>
</HostEntry>
```

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: **58**
展示を参照してください。



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バックアップゲートウェイ
B. デュアルグループメンバーでVPNを取得
C. COOPキーサーバーでVPNを取得
D. FlexVPNロードバランサー
正解: **(**正解を表示します**)**

質問: **59**
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. ICA（Citrix）
B. VNC
C. CIFS
D. RDP
E. HTTP
正解: **(**正解を表示します**)**

質問: **60**
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. IPsecサイト間トンネル
B. Cisco AnyConnect
C. L2TP over IPsec
D. VTI
正解: **B (**コメントを発表する**)**

質問: **61**

```
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。

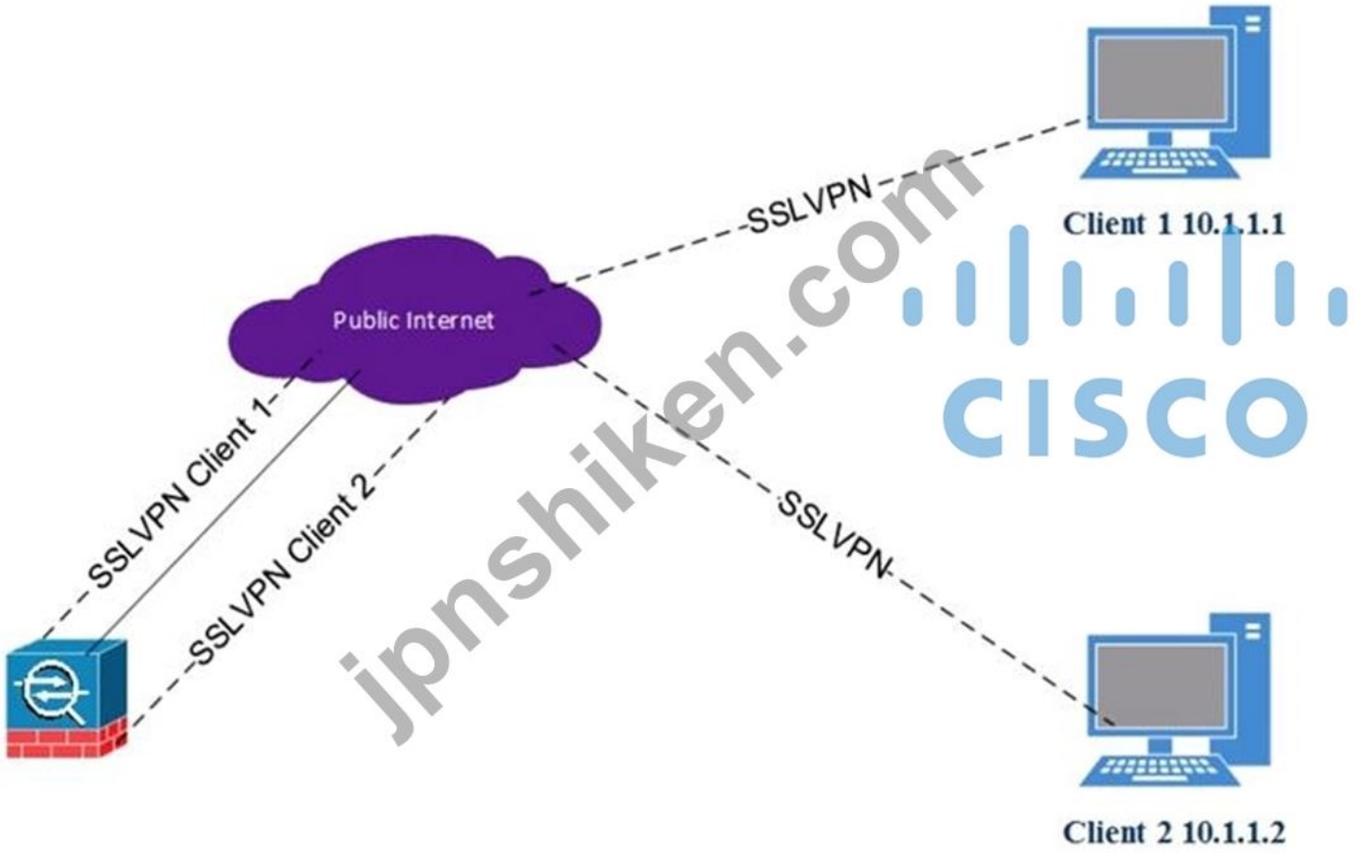
D. スポーク1は認証をハブに渡し、フェーズ2に正常に進みます。

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: **62**
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. 自動起動
B. 自動実行
C. 自動接続
D. 自動アップグレード
正解: **A** (コメントを発表する)

質問: **63**
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. same-security-traffic permit intra-interface
B. dns-server value 10.1.1.3
C. same-security-traffic permitinter-interface
D. dns-server value 10.1.1.2
正解: **(**正解を表示します**)**