Cisco.300-730J.v2021-08-09.q35

試験コード： 300-730J
試験名称： Implementing Secure Solutions with Virtual Private Networks (300-730日本語版)
認証ベンダー： Cisco
無料問題の数： 35
バージョン： v2021-08-09
ページの閲覧量 :482
問題集の閲覧量 :6023
https://www.jpnshiken.com/shiken/Cisco.300-730J.v2021-08-09.q35.html

質問: **1**
Cisco AnyConnectクライアントは、本社の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ーがエンタープライズ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. 高度なエンドポイント評価
B. Cisco Secure Desktop
C. 基本ホストスキャン
D. エンドポイント評価
正解: **A (**コメントを発表する**)**

質問: **2**
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 が使用されていますか?
A. Cisco AnyConnect SSL VPN
B. clientless SSL VPN
C. Cisco Easy VPN
D. GETVPN
正解: **(**正解を表示します**)**

質問: **3**
展示を参照してください。

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

お客様は、2つのCisco ASAデバイス間にIKEv2サイト間VPNトンネルを確立できません。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Cisco ASAの最大SA制限を減らします。

B. リモートCisco ASAの最大SA制限を削除します。

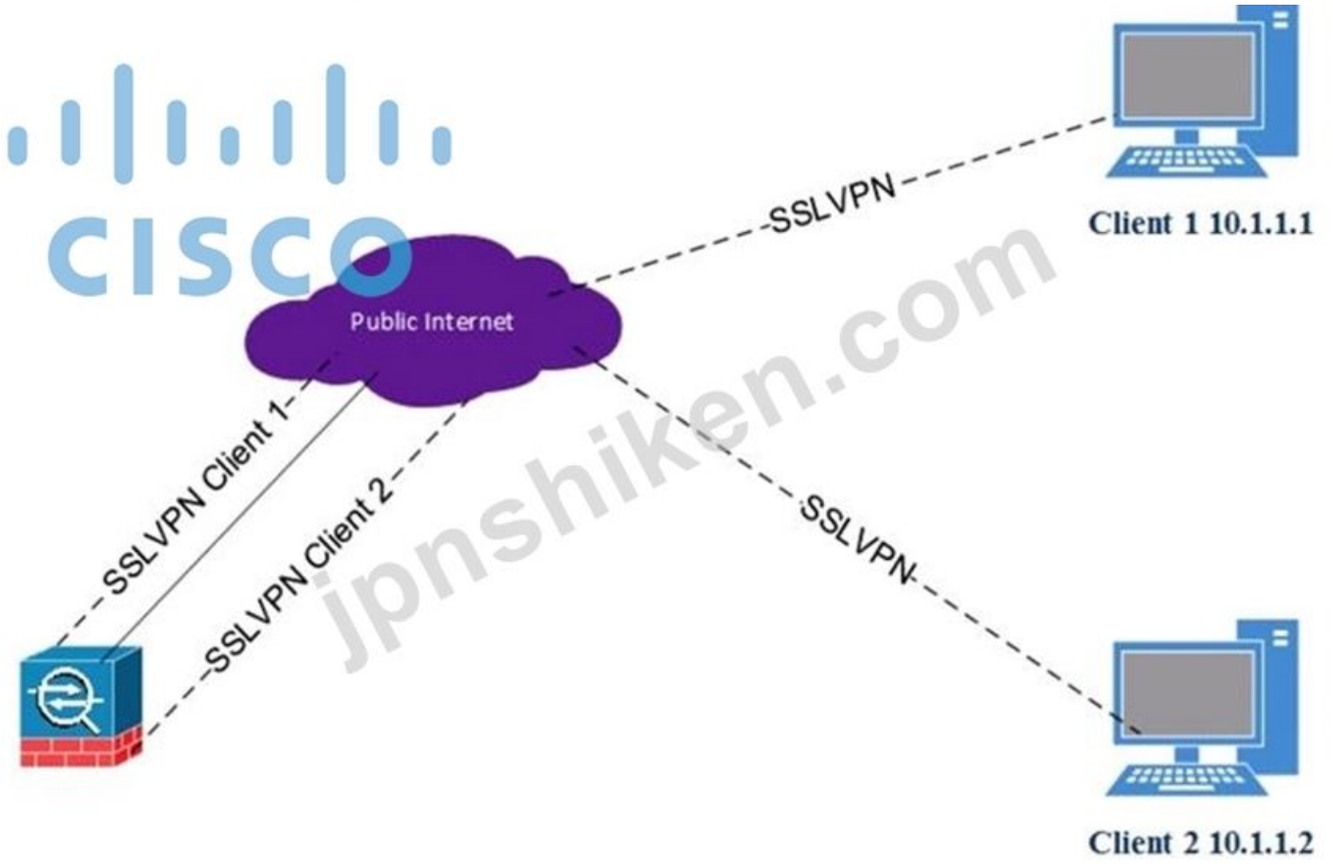
C. 両方のCisco ASAデバイスの暗号化アクセスリストを修正します。

D. ローカルCisco ASAの交渉中のSAの最大数を増やします。

正解: **D** (コメントを発表する)

質問: **4**

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Cisco AnyConnectを使用しており、ハブASAへの正常なSSL VPN接続を確立しています。ASAのどのコマンドが欠落していますか？

A. same-security-traffic permit inter-interface

B. same-security-traffic permit intra-interface

C. dns-server value 10.1.1.3

D. dns-server value 10.1.1.2

正解: **B** (コメントを発表する)

質問: **5**
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. 自動開始
D. 自動アップグレード
正解: **(**正解を表示します**)**

質問: **6**
エンジニアがCisco IOSルータでの新しい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ると、「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. フェーズ1ポリシーが両方のデバイスで一致しません。
B. トンネル保護はDMVPNトンネルに適用されません。
C. ESPトラフィックがドロップされています。
D. ISAKMPポリシーの優先度の値が無効です。
正解: **(**正解を表示します**)**

質問: **7**
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 next-hop-selfを無効にします。
B. ハブにNHRPショートカットを追加します。
C. ハブでEIGRP next-hop-selfを有効にします。
D. ハブにNHRPリダイレクトを追加します。
E. スポークにNHRPリダイレクトを追加します。
正解: **A,D (**コメントを発表する**)**

質問: **8**
エンジニアは、従業員がリモートで接続している間、すべてのトラフィックが企業ネットワークにルーティングされていることに気付きました。在宅勤務時にリモート クライアントがインターネット アクセスにローカル プロバイダーを使用できるようにするスプリット トンネル ポリシーはどれですか?
A. 除外指定
B. すべてを除外
C. トンネル指定
D. トンネルオール
正解: **(**正解を表示します**)**

質問: **9**

展示を参照してください。



```
*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
```

2つのルーター間の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、どのタイプのミスマッチが問題ですか？

A. peer identity

B. transform set

C. preshared key

D. ikev2 proposal

正解: **A (**コメントを発表する**)**

質問: **10**

夜間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

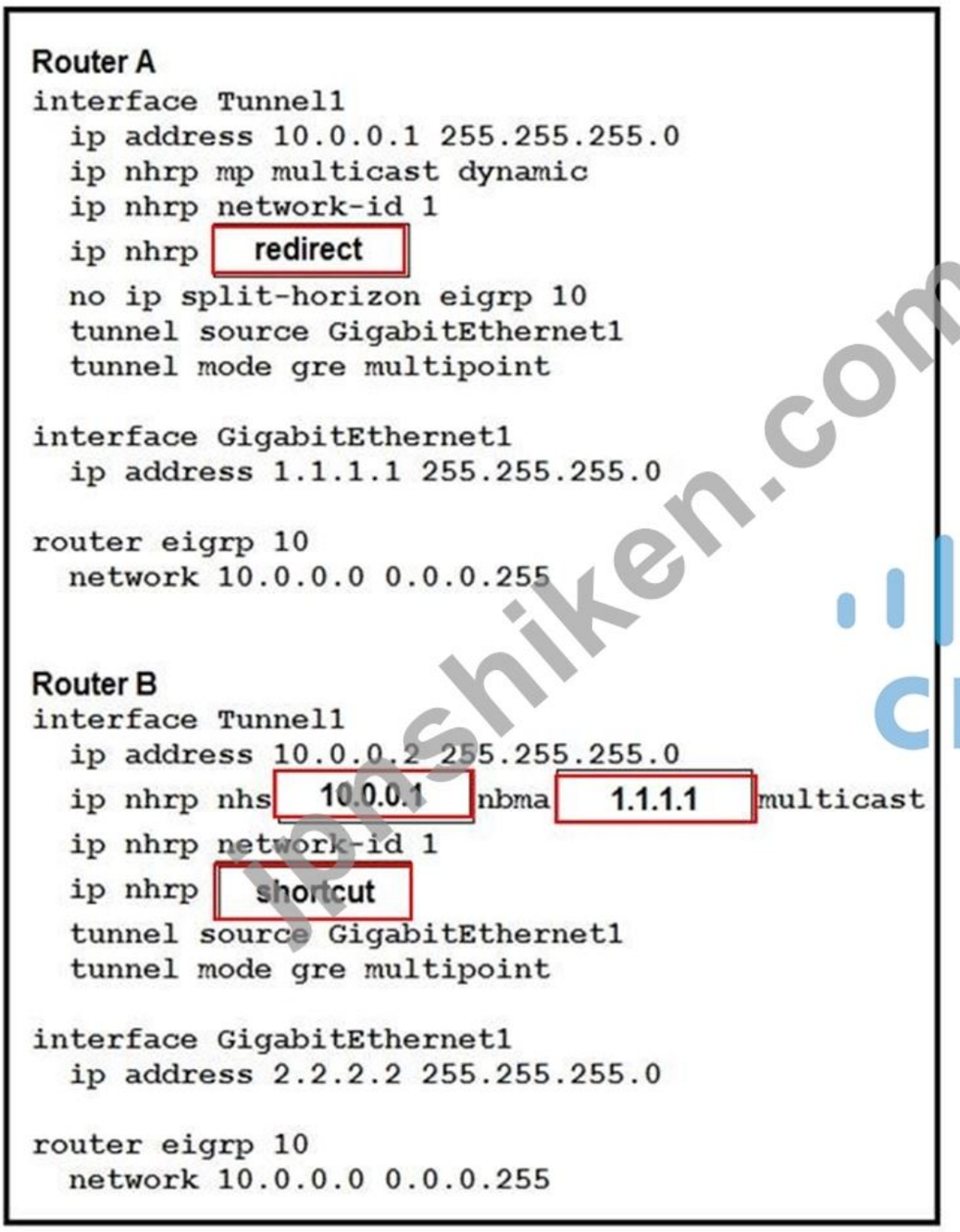
shortcut

server-only

jpnshiken.com

正解:

Answer Area



1.1.1.1

10.0.0.1

redirect

shortcut

server-only

10shiken.com

質問: **11**

展示を参照してください。



展示に基づいて、ユーザーがCCNP Webサーバーのブックマークにアクセスできないのはなぜですか？

A. ブックマークが無効になっています。

B. URLはWebACLによってブロックされています。

C. ユーザーはURLにアクセスできません。

D. ASAはURLを解決できません。

正解: **A** (コメントを発表する)

質問: **12**

IPsecステートレスフェイ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. SSO

B. VRRP

C. HSRP

D. GLBP

正解: **C** (コメントを発表する)

質問: **13**

展示を参照してください。

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-clientless
 split-tunnel-policy tunnelall

tunnel-group Admins type remote-access
tunnel-group Admins general-attributes
 default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes
 group-alias Admins enable

tunnel-group Employee type remote-access
tunnel-group Employee webvpn-attributes
 group-alias Employee enable

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

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. crypto map

B. IKEv2 AnyConnect

C. clientless

D. SSL AnyConnect

正解: (正解を表示します)

質問: **14**

ネットワーク エンジニアは、SSL VPN を構成して、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することを任されています。企業の IP 範囲を宛先とするトラフィックはトンネルを通過し、他のすべてのトラフィックは直接インターネットに向かう必要があります。これを実現するには、どの機能を構成する必要がありますか?

A. ヘアピニング

B. デュアルホーミング

C. Uターン

D. スプリットトンネル

正解: **D** (コメントを発表する)

質問: **15**

IPsec プロファイルのスマートなデフォルト設定を表示するコマンドはどれですか?

A. show run all crypto ipsec profile

B. クリプト ipsec プロファイルのデフォルトを表示

C. ipsec プロファイルにはスマートなデフォルト設定がありません

D. スマートデフォルトの ipsec プロファイルを表示

正解: (正解を表示します)

質問: **16**

展示を参照してください。

```
KEv2:(SESSION ID = 17,SA ID = 1):Processing IKE_AUTH message
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いて、どのタイプのミスマッチがVPNの起動を妨げていますか？

A. 興味深いトラフィック

B. 寿命

C. 事前共有キー

D. PFS

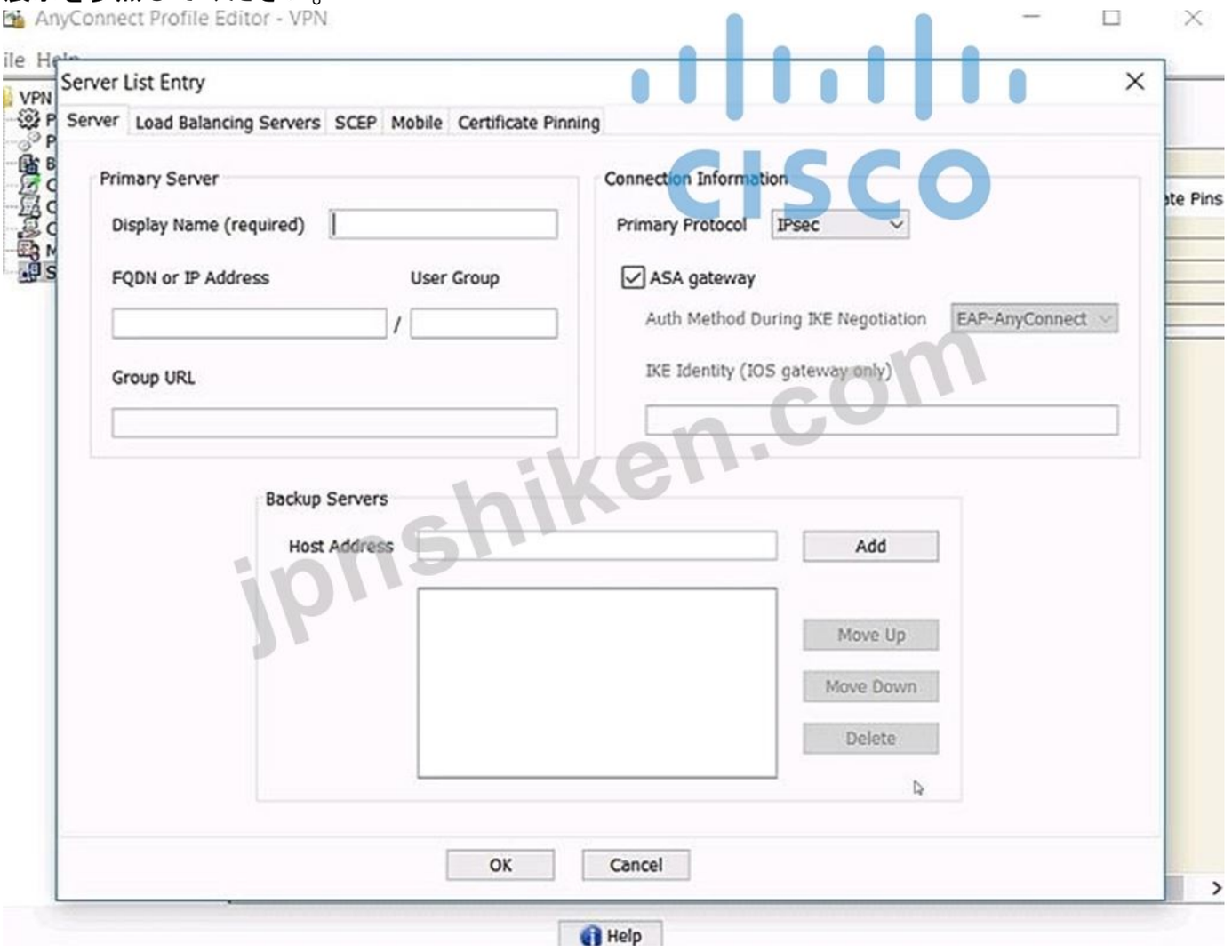
正解: **B** (コメントを発表する)

If the responder's policy does not allow it to accept any part of the proposed Traffic Selectors, it responds with a TS_UNACCEPTABLE Notify message.

有効的な**300-730J**問題集はJPNTest.com提供され、**300-730J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-730J**試験問題集を提供します。JPNTest.com 300-730J試験問題集はもう更新されました。ここで**300-730J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-730J-mondaishu　**240**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
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接続を介して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. Smart Tunnel
C. single sign-on
D. plug-ins
正解: **(**正解を表示します**)**

質問: **18**
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]フィールドに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
正解: **(**正解を表示します**)**

質問: **19**
管理者は、パートナーの Cisco 以外の VPN ソリューションを使用して VPN を設計しています。パートナーの VPN デバイスは、サブネット 192.168.0.0/24 から 10.0.0.0/24 のみを暗号化する IKEv2 トンネルをネゴシエートします。これらの要件を満たすには、どのテクノロジーを使用する必要がありますか?
A. DMVPN
B. VTI
C. クリプトマップ
D. GETVPN
正解: **(**正解を表示します**)**

質問: **20**
DMVPN フェーズ 3 の実装に固有の 2 つの NHRP 機能はどれですか? (2つ選んでください。)
A. 解決依頼
B. 登録要求
C. 解決返信
D. 登録応答
E. リダイレクト
正解: **(**正解を表示します**)**

質問: **21**
スポークツースポークトンネルが許可されていないFlexVPNハブアンドスポークトポロジで、ハブがFlexVPNトンネルを終端できるようにするには、どのコマンドが必要ですか？
A. インターフェース仮想テンプレート
B. ip nhrpリダイレクト
C. インターフェース仮想アクセス
D. インターフェーストンネル
正解: **(**正解を表示します**)**

質問: **22**
Cisco IOS GETVPN のキー サーバの 2 つの目的は何ですか? (2つ選んでください。)
A. 暗号化キーをダウンロードする

B. ルーティング情報を配布する
C. グループメンバーの認証
D. 暗号化ポリシーを維持するため
E. データ トラフィックを暗号化する
正解: **(**正解を表示します**)**

質問: **23**
展示を参照してください。

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.0.1

   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 192.168.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.1, remote crypto endpt.: 192.168.0.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0x3D05D003(1023791107)
     PFS (Y/N): N, DH group: none
```

展示で見られるshow crypto ipsec sa出力を生成するトンネルタイプはどれですか。 2つ選択してください。）
A. VTI
B. crypto map
C. FlexVPN
D. DMVPN
E. GRE
正解: **(**正解を表示します**)**

質問: **24**
エンジニアは、新しい DMVPN を統合して、Cisco IOS ルータを使用してインターネット全体でリモート オフィスをリンクしました。リモート サイトに接続すると、ping と音声データが適切に流れているように見え、すべてのトンネル統計はそれらが稼働していることを示しています。ただし、RDP を使用してリモート サーバーに接続しようとすると、接続に失敗します。この問題を解決するアクションはどれですか?
A. RDP サーバー上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. RDP ポートを拡張 ACL に追加します。
D. ルーター内の MTU サイズを調整します。

正解: **D** (コメントを発表する)

質問: **25**
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つのパラメーターはどれですか。 2つ選択してください。）
A. グループのURL
B. AnyConnectクライアントのバージョン
C. グループエイリアス
D. 証明書マップ
E. 最適なゲートウェイの選択
正解: **A,D** (コメントを発表する)

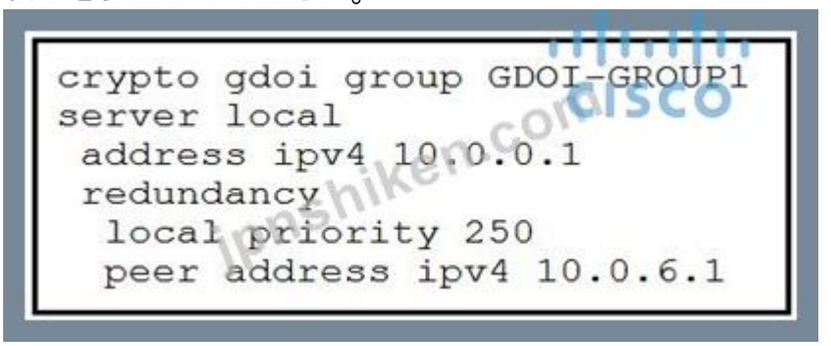
質問: **26**
ECDHとECDSAの2つの機能は何ですか？ 2つ選択してください。）
A. デジタル署名
B. 鍵交換
C. 否認防止
D. 取り消し
E. 暗号化
正解: (正解を表示します)

質問: **27**
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. webvpnインポートプロファイルSSL_profile flash :simos-profile.xml
B. svcインポートプロファイルSSL_profile flash :simos-profile.xml
C. 暗号vpn anyconnectプロファイルSSL_profile flash :simos-profile.xml
D. anyconnectプロファイルSSL_profile flash :simos-profile.xml
正解: (正解を表示します)

質問: **28**
トラブルシューティング中に、エンジニアは 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ために取るべき次のステップは何ですか?
A. 事前共有キーが両方のデバイスで一致することを確認します。
B. デバイス間で UDP 500 がブロックされていないことを確認します。
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. ISAKMP プロポーザルが一致することを確認します。
正解: (正解を表示します)

質問: **29**

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. FlexVPN ロード バランサー

C. デュアル グループ メンバーで VPN を取得

D. COOPキーサーバーでVPNをGET

正解: **(**正解を表示します**)**

質問: **30**

ネットワーク エンジニアは、500 人の同時ユーザーをサポートし、クライアントからのすべてのトラフィックが確実に ASA を通過し、ユーザー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、このソリューションを実装する構成はどれですか?

○ 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
```

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: **A** (コメントを発表する)

質問: **31**
ユーザがブックマーク リストを使用して接続プロファイルを設定し、クライアントレス SSLVPN 接続をテストすると、すべてのブックマークがグレー表示されます。この動作を修正するには何をしなければなりませんか?
A. ブックマークの下にある Web サーバーの正しいポートを指定します。
B. Cisco ASA で DNS サーバーを構成し、Web サーバーのレコードがあることを確認します。
C. Cisco ASA と Web サーバー間の HTTP/HTTPS 接続を確認します。
D. ブックマークを正しいグループ ポリシーに適用します。
正解: (正解を表示します)

有効的な**300-730J**問題集はJPNTest.com提供され、**300-730J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-730J**試験問題集を提供します。JPNTest.com 300-730J試験問題集はもう更新されました。ここで**300-730J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-730J-mondaishu　**240**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
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のは、どのタイプのミスマッチですか。
A. preshared key
B. Phase 1 policy
C. crypto access list
D. transform set
正解: **A** (コメントを発表する)

質問: **33**
CiscoルータのIKEv2リモートアクセスクライアントに分割トンネリングはどこに定義されていますか？
A. webvpnコンテキスト
B. IKEv2許可ポリシー
C. グループポリシー
D. 仮想テンプレート
正解: (正解を表示します)

質問: **34**
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. Cisco AnyConnect
B. L2TP over IPsec
C. IPsecサイト間トンネル
D. VTI
正解: **A** (コメントを発表する)

質問: **35**
展示を参照してください。



```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):       encryption AES-CBC
ISAKMP: (0):       keylength of 256
ISAKMP: (0):       hash SHA256
ISAKMP: (0):       default group 14
ISAKMP: (0):       auth pre-share
ISAKMP: (0):       life type in seconds
ISAKMP: (0):       life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

2つのサイト間のサイト間トンネルは確立されません。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エラーが発生しました。

C. ルーターで認証エラーが発生しました。

D. ピアからのUDP 4500トラフィックがルーターに到達しません。

正解: **(**正解を表示します**)**

有効的な**300-730J**問題集はJPNTest.com提供され、**300-730J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-730J**試験問題集を提供します。JPNTest.com 300-730J試験問題集はもう更新されました。ここで**300-730J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-730J-mondaishu　**240**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」