TESTPASSPORT

練 習 問 題



高 品 質 な 学 習 リ ソ ー ス

https://www.testpassport.jp

1年間無料アップデート

Exam : **642-637J**

Title : Securing Networks with Cisco Routers and Switches (SECURE) v1.0

Version : V13.02

1. 展示を参照してください。

```
Router# debug crypto isakmp
*ISAKMP (1009): received packet from 192.168.2.2 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1009): processing ID payload. message ID = 0
ISAKMP (1009): ID payload
        next-payload : 8
        type         : 1
        address      : 192.168.2.2
        protocol     : 17
        port         : 500
        length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1009): processing HASH payload. message ID = 0
ISAKMP:(1009):SA authentication status:         authenticated
ISAKMP:(1009):SA has been authenticated with 192.168.2.2
```

debug コマンドの出力の一部を考えると、何を決定することができますか？

A. などのメッセージ ID =0 で示されるパケットに ID ペイロードは存在しません。

B. ピアは、任意提供のプロファイルを一致していません。

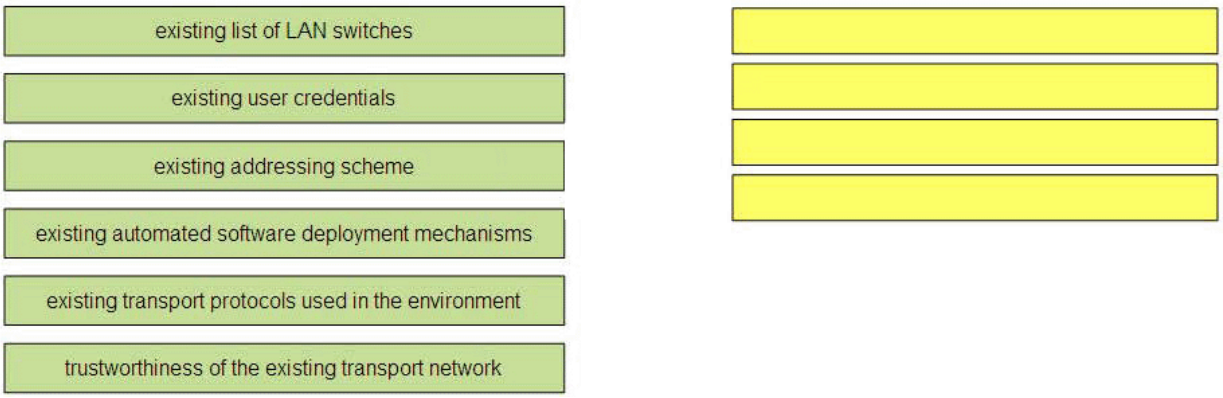
C. これは、IKE クイックモードネゴシエーションです。

D. これは成功したフェーズ 1 の IKE 交換の通常の出力です。

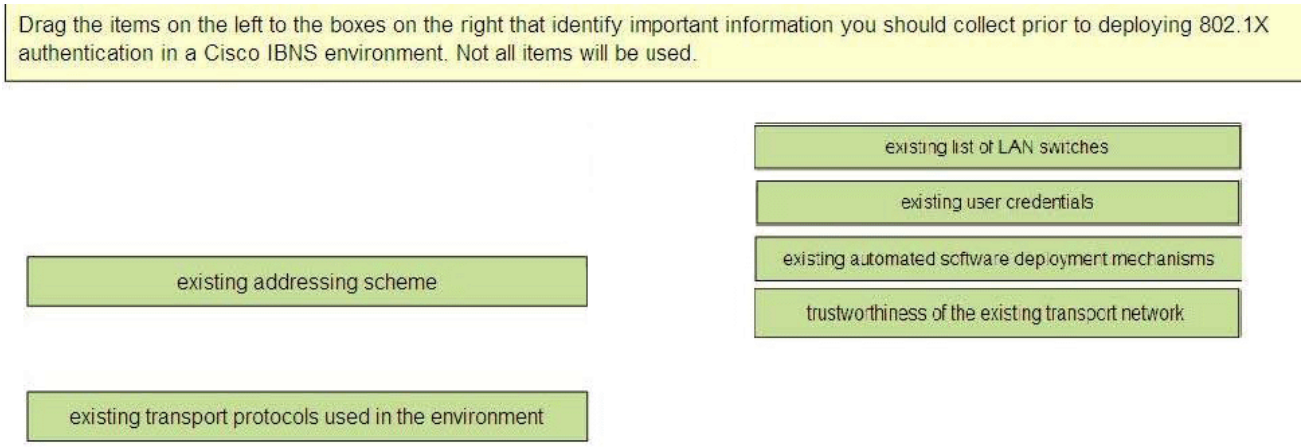
Answer: D

2. DROP をドラッグ

Drag the items on the left to the boxes on the right that identify important information you should collect prior to deploying 802.1X authentication in a Cisco IBNS environment. Not all items will be used.



Answer:



3. 展示を参照してください。

```
webvpn context MY-WEBVPN
 policy group GROUP-POLICY
   functions svc-enabled
   svc keep-client-installed
   svc address-pool MY-POOL
   svc default-domain cisco.com
   svc dns-server primary 10.10.1.1
   svc split dns domain.com
   svc split include 10.0.0.0 255.0.0.0
   filter tunnel FILTER-ACL
```

どの台の Cisco IOS の WebVPN 機能が部分的な設定が示されて有効になっていますか？（二つ選択してください。）

A. エンドユーザの Cisco AnyConnect の VPN ソフトウェアは、エンドシステムにインストールされたままになります。

B. Cisco AnyConnect の VPN ソフトウェアは、エンドユーザの PC にインストールに失敗した場合、エンドユーザーは、他のモードを使用することができません。

C. クライアントベースのフルトンネルアクセスが有効になっています。

D. 10.0.0.0/ 8 のネットワーク宛てのトラフィックは、スプリットトンネルを経由してのアクセスをトンネル化されず、許可されます。

E. クライアントは 10.10.0.0/16 の範囲内の IP アドレスが割り当てられます。

Answer: A,D

4. どのこれらの二つは、透過モードでのゾーンベースのポリシーファイアウォールを実装する利点はなんでしょうか？（二つ選択してください。）
A. より少ないファイアウォール管理が必要であります。。
B. それは簡単に既存のネットワークに導入することができます。
C. IP 再アドレッシングは必要ありません。
D. これは、ステートフルに非 IP トラフィックを検査する機能を追加します。
E. これは、データ・フローに影響がすくないです。
Answer: B,C

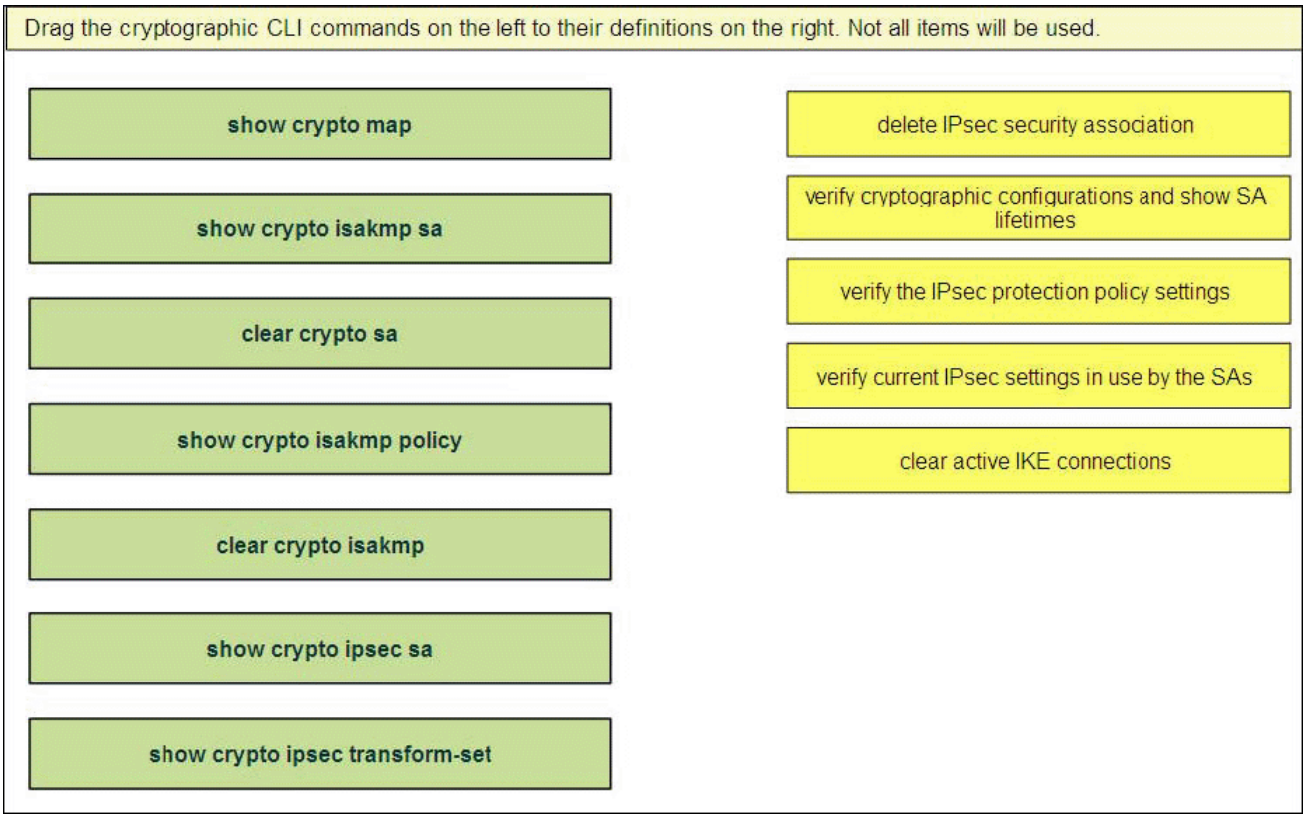
5. あなたはゾーンの可能性のあるペアの任意のゾーンのペアを指定しない場合、ゾーンベースのポリシーファイアウォールを設定するときは、何が結果として行動でしょうか？
A. すべてのセッションは、検査されずにゾーンを通過します。
B. すべてのセッションは、デフォルトではこれら二つのゾーン間で拒否されます。
C. すべてのセッションは、宛先ゾーンに渡す許可される前に検査のためのルータ"自己ゾーン"を通過する必要があります。
D. この構成では、ステートレスパケットを宛先ゾーンに送達することができます。
Answer: B

6. 展示を参照してください。
この show コマンドの出力から決定することができますか？

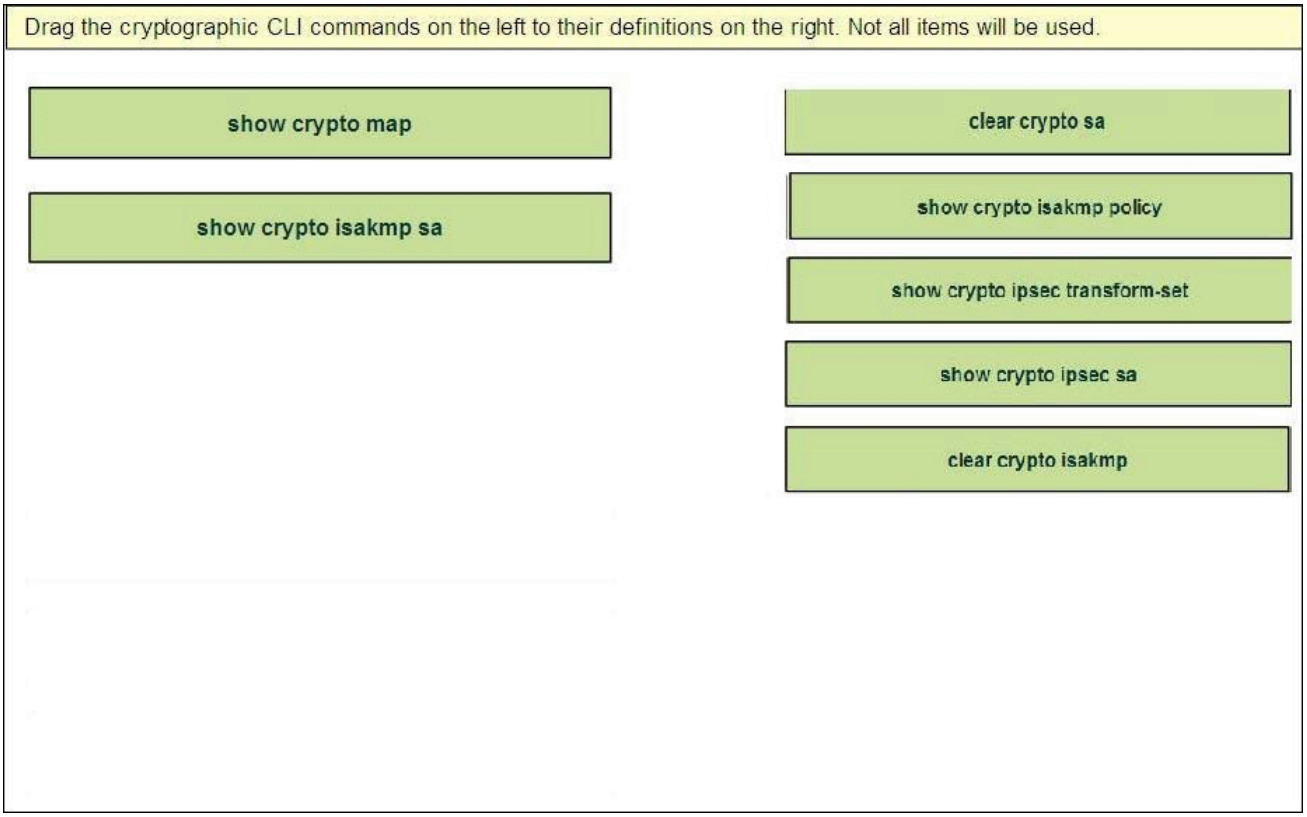
```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.1     192.168.2.1      QM_IDLE           1002 ACTIVE
```

A. IPsec 接続がアイドル状態であります。
B. IKE 協会が設定されている過程にあります。
C. IKE ステータスは認証されます。
D. ISAKMP ステートは、IPsec パラメータがピア間で渡される前に認証するためにクイックモードの状態を待っています。
E. IKE クイックモードは、IKE フェーズ 1 に問題があることを示している、アイドル状態になっています。
Answer: C

7.DRAG DROP



Answer:



8. あなたのエッジルータで Cisco IOS IPS ソフトウェアを実行している。新しい脅威が問題となっています。Cisco IOS IPS ソフトウェアは、新たな脅威に対処することができ、署名を持っていますが、以前

に署名を引退した。あなたが希望する保護レベルを取り戻すために、その署名をリタイアすることにします。
どのようにあなたの決定に行動しなければなりませんか？
A. 引退した署名は、ルータのメモリ内に存在しない。あなたが引退した署名を取り戻すために新しいシグニチャのパッケージをダウンロードする必要があります。
B. シグニチャを再度有効にして、新しい脅威の兆候のトラフィックを検査開始する必要があります。
C. 署名を Unretiring するルータは一時的にパフォーマンスに影響を与える可能性シグネチャデータベースをコンパイルするようになります。
D. あなたが署名をリタイアすることはできません。新しいシグニチャのパッケージをダウンロードして、ルータをリロードできるようになるまでトラフィックフローの中断を回避するために、カスタム署名を作成するのが最善です。
Answer: C

9. どのステートメントは、NAT ポリシーベースの内側に最善を説明?
A. ポリシーNAT ルールはアドレスが企業のセキュリティポリシーに基づいて変換する必要があるかを判断するものであります。
B. ポリシーNAT は、内部エンドポイントと通信しようとする外部の情報源に基づいてポリシールールで構成されています。
C. これらのルールは、翻訳政策の決定として、送信元アドレスを使用しています。
D. これらの規則は、すべての通信のエンドポイントに敏感です。
Answer: A

10. 展示を参照してください。

```
ip ips signature-category
 category all
  enabled false
  retired true
 category os ios
  enabled true
  retired false
  event-action produce-alert reset-tcp-connection
```

IPS カテゴリ構成が示さについて決定することができますか？
A. すべてのカテゴリは無効になっています。
B. すべてのカテゴリは廃止されています。
C. 他のすべてのカテゴリが無効になっていた後、名前のカスタムカテゴリは、 "OS の IOS"が作成されました。
D. 予防措置での Cisco IOS システム結果にのみ攻撃です。
Answer: D

11. Cisco IOS IPS は、イベント通知用 SDEE を使用するように設定されている場合、イベントがどのよ

うに管理されていますか？
A. 彼らはルータのイベントストアに保存され、認証されたリモートシステムがイベント・ストアからイベントをプルすることができます。
B. すべてのイベントが即時にリモート SDEE サーバに送信されます。
C. イベントはセキュア SSUTLS 通信チャネル上の syslog を介して送信されます。
D. イベント・ストアは、イベント通知の最大構成された数に達すると、保存されたイベントは、リモート認証サーバに SDEE を経由して送信され、新しいイベントストアが作成されます。
Answer: A

12. どのこれらの二次の構成パラメータで正規表現にマッチするのでしょうか? [a-zA-Z][0-9][a-z]（二つ選択してください。）
A. Q3h
B. B4Mn
C. aaB132AA
D. c7lm
E. BBpjnrIT
Answer: A,D

13. これらのどれが攻撃がクリティカルなルータのリソースを使い果たししようと､正しく予防コントロールはバイパスされたりした場合は動作していない場合、通知をトリガ設定可能な Cisco IOS の機能ですか？
A. コントロールプレーン保護
B. 管理プレーン保護
C. CPU およびメモリしきい値
D. SNMPv3
Answer: C

14. Cisco IOS IPS 機能は、一つまたはそれ以上の攻撃、および/またはターゲットアドレスの基準に基づいてすべてのアクティブなシグネチャからアクションだけでなく、イベントリスク評価基準を削除することを可能にしますか？
A. シグニチャイベントアクションフィルタ
B. シグニチャイベントアクションオーバーライド
C. シグネチャ攻撃深刻度
D. シグニチャイベントのリスク評価
Answer: A

15. あなたは、IPsec VPN 接続を経由して本社にアクセスしているリモートユーザから報告された接続の問題をトラブルシューティングします。
何がこれらの問題をトラブルシューティングする最初のステップとなるでしょうか？
A. トンネルエンドポイントのマッチングポリシーを確認するには、show crypto isakmp policy コマンドを発行する
B. トンネルのエンドポイントを ping する
C. トンネルのパスを確認するために traceroute を実行する
D. 接続プロセスをデバッグし、トンネルの確立にすべてのエラーメッセージを探する

Answer: B

16. これらのうち、仮想アクセスインターフェイスの設定に関する正しいですか？
A. これらは、スタートアップコンフィギュレーションに保存することができません。
B. あなたは、トンネル内部のスタティックルートを使用する必要があります。
C. DVTI インターフェイスは、固有の IP アドレスの範囲を割り当てる必要があります。
D. 仮想アクセス一つインターフェイスは管理上アップ/アップの状態で有効にする必要があります。
Answer: A

17. 展示を参照してください。

```
ip access-list extended INTRA_ZONE_ACL
  permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq ssh
!
class-map type Inspect INTRAZONE_CLASS
  match access-group name INTRA_ZONE_ACL
!
policy-map type inspect INTRAZONE_POLICY
  class type inspect INTRAZONE_CLASS
   inspect
  class class-default
   drop log
!
zone-pair security INTRAZONE source INSIDE destination INSIDE
 service-policy type inspect INTRAZONE_POLICY
```

INSIDE ゾーンが設定され、2 つの別々のルータインターフェイスに割り当てられている。他のすべてのゾーンとのインターフェイスが適切に設定されている。
示す構成例を考えると、何を決定することができますか？
A. INSIDE ゾーン内のホストは、10.10.10.0/24 ネットワーク内のアドレスでは、SSH プロトコルを使用して、10.10.10.0/24 ネットワーク内の任意のホストにアクセスすることができます。
B. INSIDE ゾーン内のホストが内部ゾーン内の別のインターフェイス上の別のホストで SSH を介して通信しようとすると、通信はイントラゾーンポリシーを使用してルータのセルフゾーンを通過しなければなりません。
C. これは違法な構成です。あなたは、同じソースと宛先ゾーンを持つことはできません。
D. このポリシー設定は、同じゾーン内のトラフィックがデフォルトで通過させ、不要であります。
Answer: A

18. コマンドプライベート VLAN アソシエーション 100,200 どの行動を取るのでしょうか？
A. それらを構成 VLAN の 100 と 200 とコミュニティとして関連付けます。
B. プライマリ VLAN に関連付けは、VLAN100 および 200 をします。
C. VLAN 100 と VLAN 200 の指定を持つ 2 つのプライベート VLAN を作成します。
D. プライベート VLAN の関連付けとしての VLAN100 および 200 を割り当てます。
Answer: B

19. これらのどれを使用すると、個別にそれぞれの署名を設定しなくても、全体的に各イベントのリスク評価に基づいて、イベントアクションを追加することができますか？
A. イベントアクションの要約

B. イベントアクションフィルタ
C. イベントアクションオーバーライド
D. シグニチャイベントアクションプロセッサ
Answer: C

20. シスコの Easy VPN を使用する場合、Cisco Easy VPN リモートルータからの VPN 接続を確立するための XAUTH ユーザー名とパスワードを入力するための 3 つのオプションは何ですか？（三つ選択してください。）
A. 外部 AAA サーバを使用する
B. 特権 EXEC モードでルータ暗号の IPSec クライアント EZVPN 接続の CLI コマンドを使用して情報を入力する
C. ルータのローカルユーザデータベースを使用する
D. ブラウザを介して、PC から情報を入力する
E. ルータのコンフィギュレーションファイルに XAUTH クレデンシャルを格納する
Answer: B,D,E