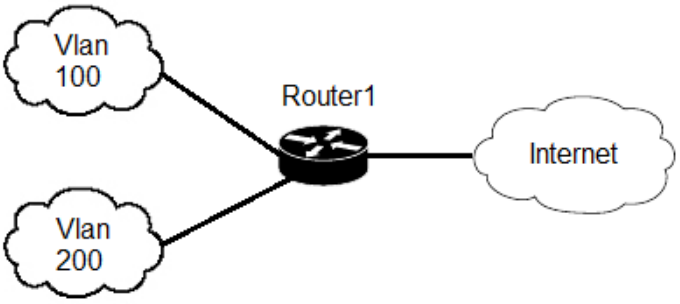



```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 209.165.200.225 255.255.255.224
Router1(config-if)#ip nat outside
Router1(config)# interface GigabitEthernet0/1
Router1(config-if)#ip nat inside
Router1(config)# interface GigabitEthernet0/1.100
Router1(config-if)#encapsulation dot1Q 100
Router1(config-if)#ip address 10.10.10.1 255.255.255.0
Router1(config)#interface GigabitEthernet0/1.200
Router1(config-if)#encapsulation dot1Q.200
Router1(config-if)#ip address 10.10.20.1 255.255.255.0
Router1(config)#ip access-list standard NAT_INSIDE_RANGES
Router1(config-std-nac)#permit 10.10.10.0 0.0.0.255
Router1(config)#ip nat inside source list NAT_INSIDE_RANGES interface GigabitEthernet0/0 overload
```

展示を参照してください。既存の VLAN 100 上のユーザーは、インターネット上のサイトにアクセスできます。VLAN 200 のユーザーがインターネットへの接続を確立するには、管理者はどのような操作を実行する必要がありますか?

A. ルーター上で NAT プールを定義します。

B. VLAN 200 の別のインターフェイスで ip natOutside コマンドを設定します。

C. VLAN 200 の静的 NAT 変換を構成します。

D. NAT_INSIDE_RANGES ACL を更新します。

問題 602

組織は、従業員のスマートフォンの認証アプリを使用した多要素認証でネットワークを保護しています。ユーザーのスマートフォンが紛失または盗難された場合、アプリケーションはどのように保護されますか?

A. アプリケーションでは、2 番目の要素を提供する前に、ユーザーが PIN を入力する必要があります。

B. 設定された間隔の後にアプリケーションを再アクティブ化するには、管理者パスワードが必要です

C. アプリケーションは、2 番目の要素を提供する前に、ユーザーが特定の場所にいるかどうかを確認します。

D. アプリケーションは、スマートフォンの再起動時に再アクティブ化するために管理者パ

スワードを要求することでユーザーに要求を出します。

問題 603
トラフィックのステートフル検査を実行するデバイスはどれですか?
A. スイッチ
B. ファイアウォール
C. アクセスポイント
D. ワイヤレスコントローラー

問題 604
ネットワーク管理者が、プリンタに接続されているスイッチ インターフェイスでポートセキュリティを有効にしました。ポートがプリンターの MAC アドレスを学習してテーブルに自動的に挿入できるようにするための次の構成アクションは何ですか?
A. 動的 MAC アドレス学習を有効にする
B. 静的 MAC アドレス指定を実装する
C. スティッキー MAC アドレス指定を有効にする
D. 自動 MAC アドレス学習を実装する

問題 605

```
Switch(config)#hostname R1
R1(config)#interface FastEthernet0/1
R1(config-if)#no switchport
R1(config-if)#ip address 10.100.20.42 255.255.255.0
R1(config-if)#line vty 0 4
R1(config-line)#login
```

展示を参照してください。エンジニアは新しいスイッチを起動し、コンソール ポート経由でこの設定を適用しました。管理者がローカルのユーザー名とパスワードを使用して Telnet 経由で特権モードを有効にするために直接認証できるようにするには、どの追加構成を適用する必要がありますか?
A. R1(config)#username admin R1(config-if)#line vty 0 4 R1(config-line)#password p@ss1234 R1(config-line)#transport input telnet
B. R1(config)#username admin privilege 15 secret p@ss1234 R1(config-if)#line vty 0 4 R1(config-line)#login local
C. R1(config)#username admin secret p@ss1234 R1(config-if)#line vty 0 4 R1(config-line)#login local R1(config)#enable secret p@ss1234
D. R1(config)#username admin R1(config-if)#line vty 0 4 R1(config-

line)#password p@ss1234

問題 606
aaa new-model コンフィギュレーション コマンドにはどのような効果がありますか?
A. デバイス上で AAA サービスを有効にします。
B. AAA の RADIUS サーバーに接続するようにデバイスを設定します。
C. RADIUS サーバーをグループに関連付けます。
D. デバイス上でローカル ユーザーを構成します。

問題 607
展示を参照してください。インターフェイスがセキュア MAC アドレスの最大数を学習した後に不明な送信元アドレスからのパケットが到着した場合、インターフェイス上で発生する 2 つのイベントはどれですか? (2 つお選びください。)

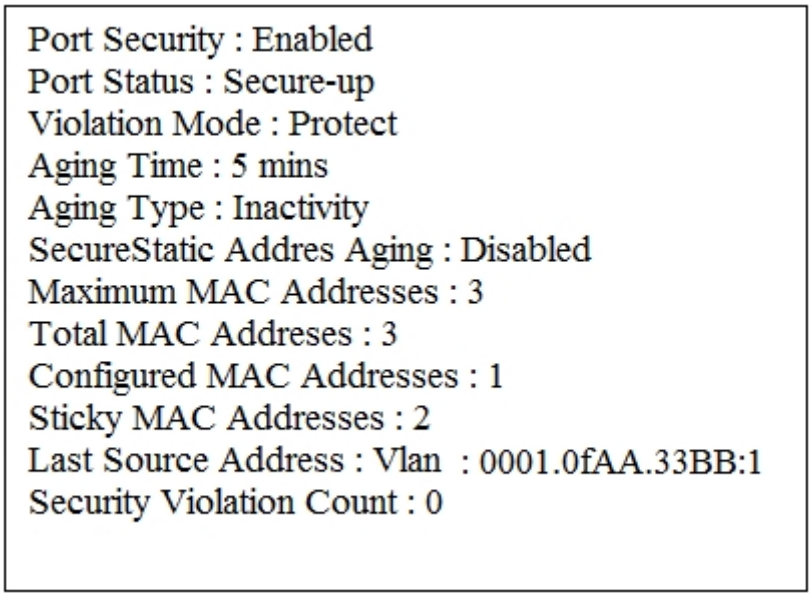
```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 4
Total MAC Addresses : 3
Configured MAC Addresses: 1
Sticky MAC Addresses : 2
Last Source Address:Vlan : 0001:0fAA.33BB:1
Security Vioaltion Count : 0
```

A. セキュリティ違反カウンターは増加しません。
B. ポート LED が消灯する
C. インターフェイスがエラーディセーブルになっている
D. syslog メッセージが生成される
E. インターフェイスが不明な MAC アドレスからのトラフィックをドロップする

問題 608
最高のセキュリティでネットワーク デバイス監視を構成するには、どのテクノロジーを実装する必要がありますか?
A. IP SLA
B. syslog

C. NetFlow
D. SNMPv3

問題 609
展示を参照してください。出力を生成したインターフェイスに関する 2 つのステートメントのうち、正しいものはどれですか? (2 つお選びください。)




A. 学習された MAC アドレスは、非アクティブ状態が 5 分間続くと削除されます。
B. パケットが新しい未知の送信元アドレスから到着した場合、インターフェイスはエラーディセーブルになります
C. 2 つのセキュア MAC アドレスを動的に学習している
D. 3 つのセキュア MAC アドレスを動的に学習している
E. パケットが新しい不明な送信元アドレスから到着すると、セキュリティ違反カウンターが増加します

問題 610
展示を参照してください。出力を生成したインターフェースに関するどのステートメントが真実ですか?

```
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 5
Total MAC Addresses          : 1
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 0
Last Source Address : Vlan   : 0001.0fAA.33BB:1
Security Violation Count     : 0
```

A. 違反が発生すると、syslog メッセージが生成されます。
B. 1 つのセキュア MAC アドレスがインターフェイス上に手動で設定されます。
C. 1 つのセキュア MAC アドレスがインターフェイス上で動的に学習されます。
D. 5 つのセキュア MAC アドレスがインターフェイス上で動的に学習されます。

問題 611

```
ip arp inspection vlan 2
interface fastethernet 0/1
        switchport mode access
        switchport access vlan 2
```

展示を参照してください。この構成の効果は何ですか?
A. インターフェイスが別のスイッチに接続されるまで、スイッチ ポートは管理上ダウンしたままになります。
B. ARP ACL が欠落しているため、ダイナミック ARP インスペクションが無効になっています。
C. スイッチ ポート インターフェイスの信頼状態が非信頼になります。
D. スイッチ ポートは、受信パケットを信頼するか信頼しないように設定されるまでダウンしたままになります。

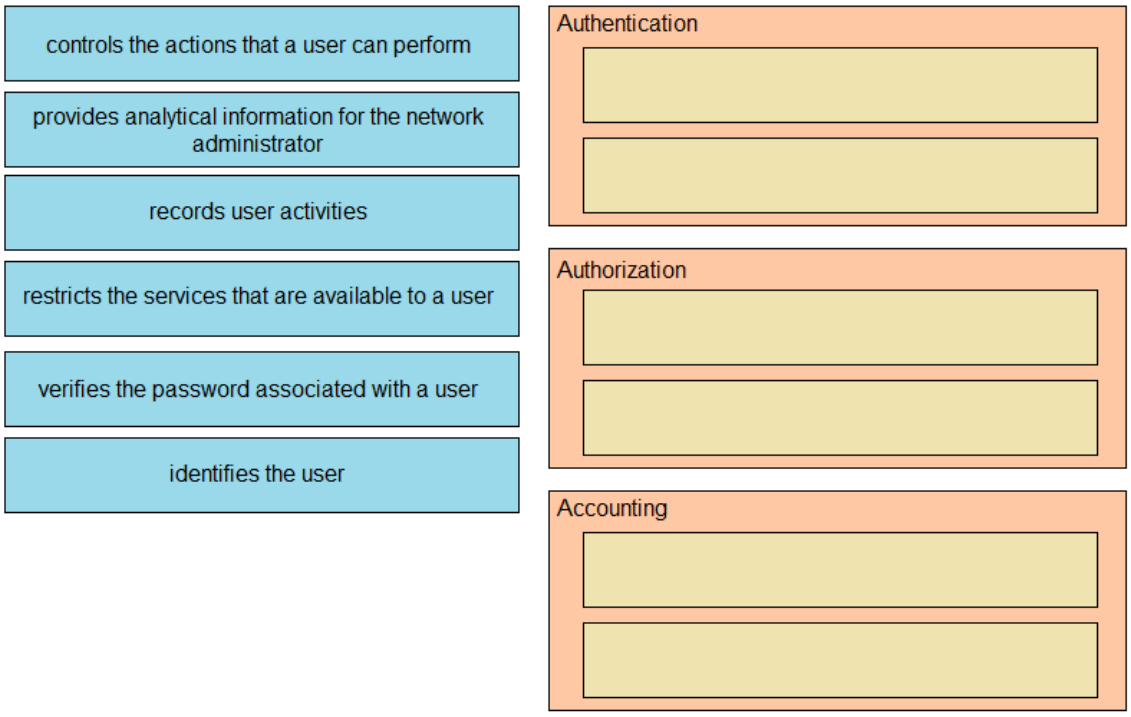
問題 612
AAA 認証と認可の違いは何ですか?
A. 認証はシステムにアクセスしようとしているユーザーを識別して検証し、認可はユーザ

ーが実行するタスクを制御します。
B. 認証はユーザーがアクセスするシステムプロセスを制御し、認可はユーザーが開始したアクティビティをログに記録します。
C. 認証ではユーザー名とパスワードが検証され、認可では認証エージェントとユーザーデータベース間の通信が処理されます。
D. 認証はシステムにアクセスしようとしているユーザーを識別し、認可はユーザーのパスワードを検証します。

問題 613
Cisco ワイヤレス LAN コントローラ GUI で WPA2 PSK を使用して WLAN を設定する場合、選択できる 2 つの形式はどれですか? (2 つお選びください。)
A. decimal
B. ASCII
C. hexadecimal
D. binary
E. base64

問題 614
DRAG DROP -
左側の AAA 機能を右側の適切な AAA サービスにドラッグ アンド ドロップします。
選択して配置します:

**Answer Area**




問題 615

エンジニアは、スイッチ上のデフォルト VLAN に設定されている未使用のポートを保護するように求められます。どの 2 つの手順でリクエストが満たされますか? (2 つお選びください。)

A. ポートをトランク ポートとして設定します。

B. Cisco Discovery Protocol を有効にします。

C. ポート タイプをアクセスとして設定し、VLAN 99 に配置します。

D. ポートを管理的にシャットダウンします。

E. EtherChannel でポートを設定します。

問題 616

電子メール ユーザーが、会社のセキュリティ組織から送信された電子メール内のリンクをクリックするように誘導されました。開いた Web ページでは安全であると報告されていますが、リンクには悪意のあるコードが含まれている可能性があります。

どのタイプのセキュリティ プログラムが導入されていますか?

A. ユーザーの意識

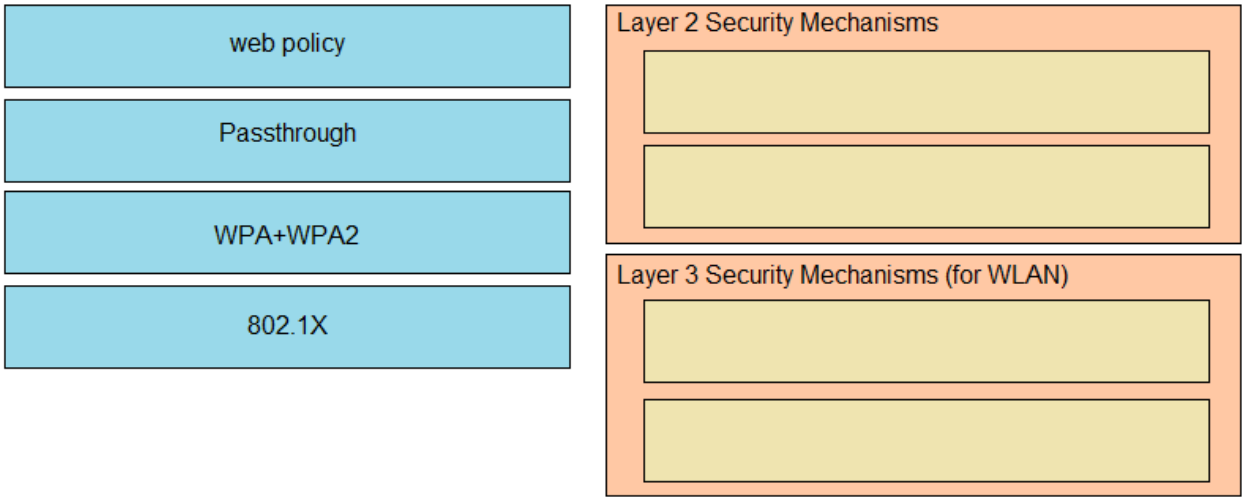
B. ブルートフォース攻撃

C. 物理的アクセス制御

D. ソーシャル エンジニアリング攻撃

問題 617
DRAG DROP -
Cisco ワイヤレス LAN コントローラのセキュリティ設定を左側から右側の適切なセキュリティ メカニズム カテゴリにドラッグ アンド ドロップします。
選択して配置します:

**Answer Area**

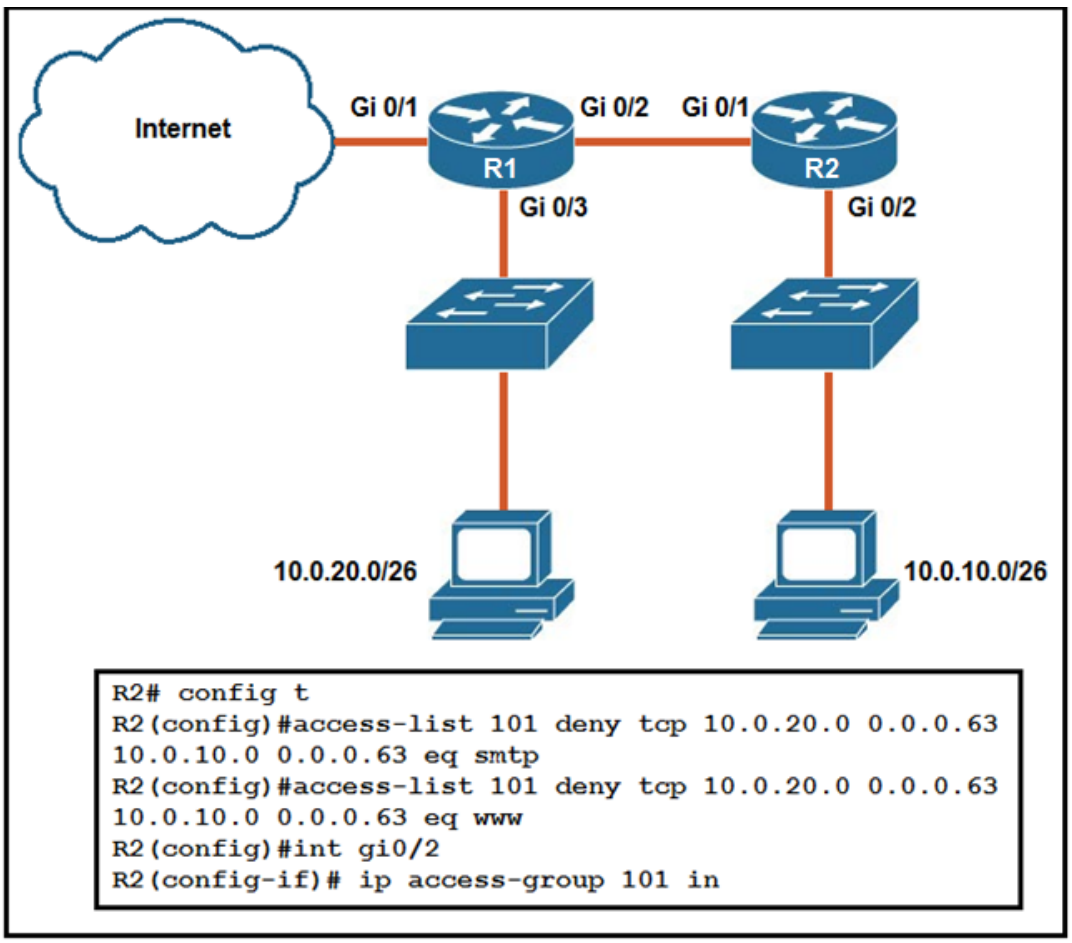



問題 618
Cisco ワイヤレス LAN コントローラのどの機能を有効にすると、特定のネットワークからの管理アクセスが制限されますか?
A. TACACS
B. CPU ACL
C. Flex ACL
D. RADIUS

問題 619
多要素認証の要件を満たす一連のアクションはどれですか?
A. ユーザーはユーザー名とパスワードを入力し、2 番目の画面で資格情報を再入力します。
B. ユーザーがキーフォブをスワイプし、電子メールのリンクをクリックします。
C. ユーザーはユーザー名とパスワードを入力し、モバイル デバイス上の認証アプリで通知をクリックします。
D. ユーザーは RSA トークンに PIN を入力し、表示された RSA キーをログイン画面に

入力します。

問題 620
ルーター上で SSH 用の RSA キーを生成するにはどの設定が必要ですか?
A. VTY アクセスを設定します。
B. SSH のバージョンを設定します。
C. DNS ドメイン名を割り当てます。
D. パスワードを持つユーザーを作成します。

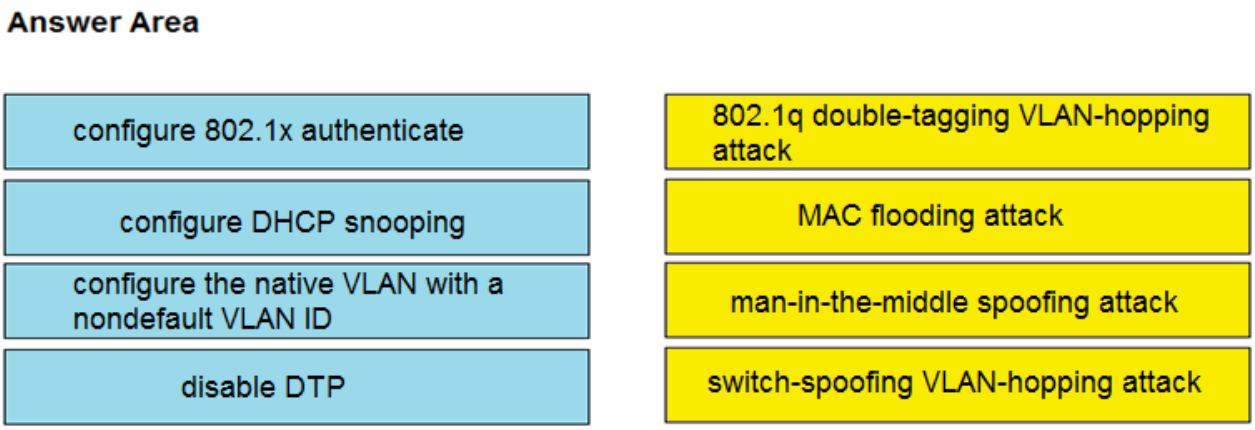
問題 621


展示を参照してください。拡張 ACL が設定され、ルータ R2 に適用されています。構成が意図したとおりに機能しませんでした。
他のすべてのトラフィックを許可しながら、10.0.10.0/26 サブネットから 10.0.20.0/26 への TCP ポート 25 および 80 の送信トラフィックを停止する 2 つの変更はどれですか? (2 つお選びください。)
A. 許可されたトラフィックの ACL 101 の末尾に「permit ip any any」ステートメントを追加します。

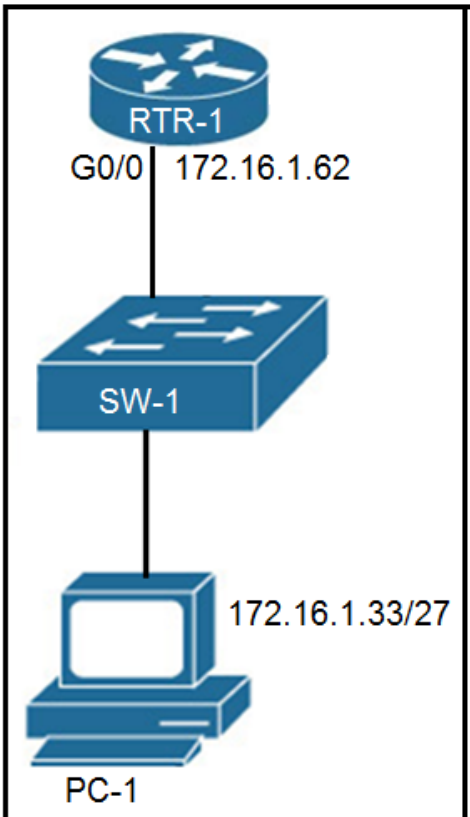
B. 許可されたトラフィックの ACL 101 の先頭に「permit ip any any」ステートメントを追加します。
C. ACL は、R2 の送信 Gi0/1 インターフェイスに移動する必要があります。
D. 送信元 IP と宛先 IP は ACL 101 で交換する必要があります。
E. ACL は、R1 の受信 Gi0/2 インターフェイスに設定する必要があります。

問題 622
エンジニアは、WPA2-PSK の最も強力な暗号化タイプを使用して WLAN を設定する必要があります。どの暗号が構成要件を満たしますか?
A. WEP
B. AES
C. RC4
D. TKIP

問題 623
ドラッグ ドロップ -
左側の攻撃軽減テクニックを、右側の軽減対象となる攻撃の種類にドラッグ アンド ドロップします。
選択して配置します:




問題 624
展示を参照してください。RTR-1 のどの設定が PC-1 から RTR-1 インターフェイスへの SSH アクセスを拒否し、他のすべてのトラフィックを許可しますか?




```
RTR-1
interface Loopback1
ip address 192.168.1.1 255.255.255.0
!
interface Loopback2
ip address 192.168.2.1 255.255.255.0
!
interface Loopback3
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0
ip address 172.16.1.62 255.255.255.224
```

A.
```
access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any

interface GigabitEthernet0/0
ip access-group 100 in
```

B.
```
access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any

line vty 0 15
access-class 100 in
```

C.
```
access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any

interface GigabitEthernet0/0
ip access-group 100 in
```

D.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any

line vty 0 15
access-class 100 in
```

問題 625
ネットワーク上の過剰なトラフィックを調べていると、IPv4 ACL がインターフェイスに適用されているにもかかわらず、インターフェイス上のすべての受信パケットが許可されているように見えることがわかります。この動作を引き起こす 2 つの構成ミスはどれですか? (2 つお選びください。)
A. ACL が空です
B. 一致する許可ステートメントの定義が広すぎる
C. パケットがどの許可ステートメントとも一致しない
D. 一致する拒否ステートメントがアクセス リストの上位にありすぎる
E. 一致する許可ステートメントがアクセス リストの上位にありすぎます。

問題 626
servicepassword-encryption コマンドはルータで入力されます。この構成の効果は何ですか?
A. 権限のないユーザーが実行コンフィギュレーション内のクリアテキスト パスワードを表示できないように制限します。
B. ネットワーク管理者がクリアテキストのパスワードを設定できないようにする
C. スイッチ上の無許可の PC 接続から VLAN データベースを保護します。
D. VPN トンネルの確立時のパスワード交換を暗号化する

問題 627
Wi-Fi ネットワーク上のトラフィックを閲覧するハッカーから保護する WPA3 の拡張機能はどれですか?
A. SAE 暗号化
B. TKIP 暗号化
C. スクランブルされた暗号化キー
D. AES 暗号化

問題 628
展示を参照してください。ネットワーク環境が正常に動作している場合、インターフェイス

fastethernet 0/1 にはどのタイプのデバイスを接続する必要がありますか?

```
ip arp inspection vlan 2-10
interface fastethernet 0/1
        ip arp inspection trust
```

A. DHCP client

B. access point

C. router

D. PC

問題 629

展示を参照してください。管理者は、暗号化ハッシュとして保存されたパスワードを使用して、ローカル認証用に 4 つのスイッチを構成します。4 つのスイッチは、管理者がネットワーク インフラストラクチャを管理するための SSH アクセスもサポートする必要があります。これらの要件を満たすように正しく構成されているスイッチはどれですか?

```
SW1(config-line) #line vty 0 15
SW1(config-line) #no login local
SW1(config-line) #password cisco

SW2(config) #username admin1 password abcd1234
SW2(config) #username admin2 password abcd1234
SW2(config-line) #line vty 0 15
SW2(config-line) #login local

SW3(config) #username admin1 secret abcd1234
SW3(config) #username admin2 secret abcd1234
SW3(config-line) #line vty 0 15
SW3(config-line) #login local

SW4(config) #username admin1 secret abcd1234
SW4(config) #username admin2 secret abcd1234
SW4(config-line) #line console 0
SW4(config-line) #login local
```

A. SW1

B. SW2

C. SW3

D. SW4

問題 630

```
ip arp inspection vlan 5-10
interface fastethernet 0/1
   switchport mode access
   switchport access vlan 5
```

展示を参照してください。この構成の効果は何ですか?

A. スイッチは、無効な MAC-to-IP アドレス バインディングを持つすべての入力 ARP トラフィックを破棄します。

B. すべての ARP パケットがスイッチによってドロップされます。

C. 出力トラフィックは、宛先が DHCP サーバーの場合にのみ渡されます。

D. インターフェイスが信頼できないため、すべての入力トラフィックと出力トラフィックがドロップされます。

問題 631

サイト間 VPN が使用される場合、ユーザー データの転送はどのプロトコルが担当しますか?

A. IPsec

B. IKEv1

C. MD5

D. IKEv2

問題 632

事前共有キー モードの WPA2 にはどのタイプのワイヤレス暗号化が使用されますか?

A. AES-128

B. RC4 を使用した TKIP

C. AES-256

D. RC4

問題 633

ドラッグ ドロップ -

左側の脅威軽減テクニックを、右側の軽減する脅威または攻撃の種類にドラッグ アンドドロップします。

選択して配置します:

**Answer Area**

| | |
|---|---|
| Configure BPDU guard. | 802.1q double tagging |
| Configure dynamic ARP inspection. | ARP spoofing |
| Configure root guard. | unwanted superior BPDUs |
| Configure VACL. | unwanted BPDUs on PortFast-enabled interfaces |

問題 634

パスワードがルーターまたはスイッチの設定にプレーン テキストとして保存されるのを防ぐコマンドはどれですか?

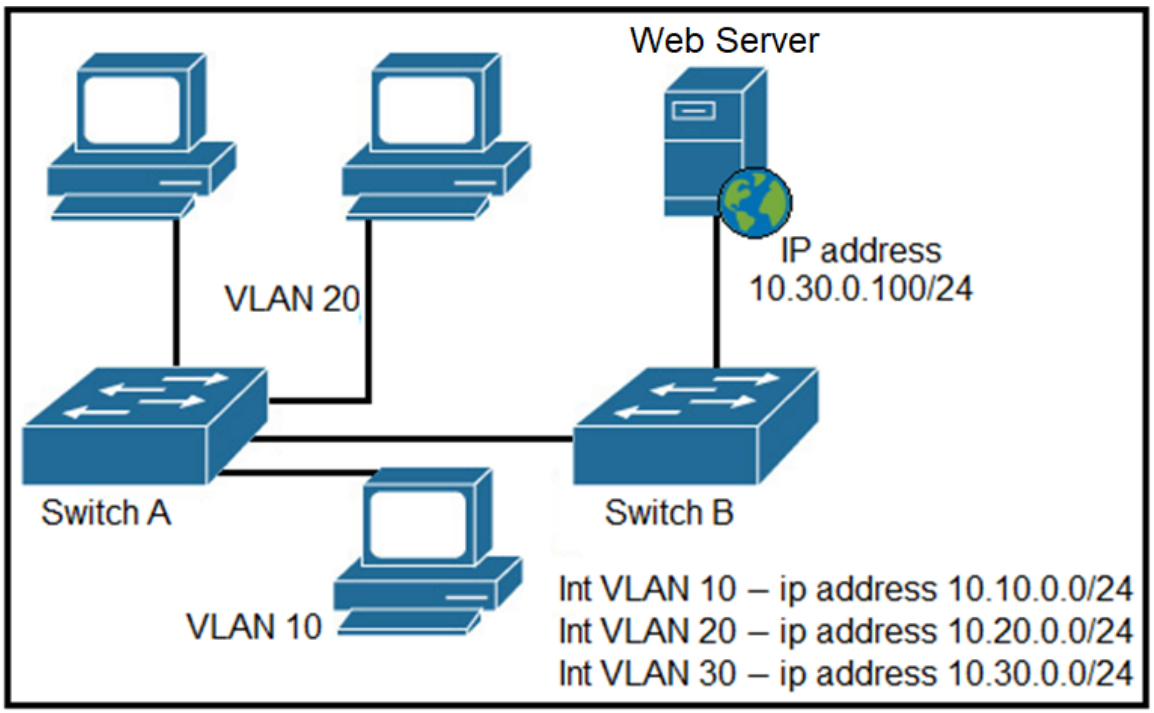
A. シークレットを有効にする

B. パスワードを有効にする

C. サービスのパスワード暗号化

D. ユーザー名 cisco パスワード暗号化

問題 635



展示を参照してください。ネットワーク エンジニアは、VLAN 20 上のすべてのコンピュータによる HTTP 経由の Web サーバーへのアクセスをブロックする必要があります。他のすべてのコンピュータは Web サーバーにアクセスできる必要があります。どの設定をスイッチ A に適用するとタスクが完了しますか?

A.
```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 20
ip access-group wwwblock in
```

B.
```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 30
ip access-group wwwblock in
```

C.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 10
ip access-group wwwblock in
```

D.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
permit ip any any
int vlan 20
ip access-group wwwblock in
```

問題 636

パスワード マネージャーは、ハッカーがユーザーのパスワードを盗む可能性を減らす 2 つの方法のうちどれですか? (2 つお選びください。)

A. ユーザーがより強力なパスワードを作成することを奨励します。

B. 内部ファイアウォールを使用してパスワード リポジトリを不正アクセスから保護します

C. ウイルス対策およびマルウェア対策機能が組み込まれたローカル ワークステーションにパスワード リポジトリを保存します。

D. 元のユーザーが知らない 2 番目の認証要素を自動的に提供します。

E. 侵害されたデバイスまたは Web サイトでのキーストロークのログ記録から保護します。

問題 637
ネットワーク上にプライベート IPv4 アドレス指定を実装することで達成される目標はどれですか?
A. インターネットへの露出に対する追加レベルの保護を提供します
B. ネットワークルーター上の転送テーブルのサイズを削減します。
C. インターネットを介して他のプライベート ネットワークへの通信を許可する
D. サーバーとワークステーションがパブリック ネットワークの境界を越えて通信できるようにする

問題 638
動的 ARP インスペクションによって軽減されるのはどのタイプの攻撃ですか?
A. DDoS
B. マルウェア
C. 中間者
D. ワーム

問題 639
リモート アクセス VPN の機能とは何ですか?
A. 2 つのブランチ サイト間に安全なトンネルを確立します。
B. 暗号化トンネリングを使用して、複数のユーザーのデータのプライバシーを同時に保護します。
C. ユーザーが企業の内部ネットワークに接続している場合にのみ使用されます。
D. ユーザーが安全なトンネルを通じて社内ネットワーク リソースにアクセスできるようにする

問題 640
IT クローゼットの外のオフィス スペースにネットワーク ポートが配置されている場合に、ネットワーク ポートが悪用されないように保護するための 2 つの推奨事項は何ですか? (2 つお選びください。)
A. ポートで PortFast 機能を有効にする
B. 静的 ARP エントリを構成する
C. ポートを固定速度に設定する
D. ポートベースの認証を実装する
E. 未使用のポートをシャットダウンする

問題 641

```
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
ip access-group 2699 in
!
access-list 2699 deny icmp any 10.10.1.0 0.0.0.255 echo
access-list 2699 deny ip any 10.20.1.0 0.0.0.255
access-list 2699 permit ip any 10.10.1.0 0.0.0.255
access-list 2699 permit tcp any 10.20.1.0 0.0.0.127 eq 22
```

展示を参照してください。ネットワーク管理者は、ネットワーク内のルーターをリモートで管理するために SSH アクセスを許可する必要があります。運用チームは 10.20.1.0/25 ネットワークに常駐しています。このタスクを実行できるコマンドはどれですか?

A. access-list 2699 permit udp 10.20.1.0 0.0.0.255

B. no access-list 2699 deny tcp any 10.20.1.0 0.0.0.127 eq 22

C. access-list 2699 permit tcp any 10.20.1.0 0.0.0.255 eq 22

D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255

問題 642

最大 MAC アドレス数を超えたため、スイッチ ポートでポート セキュリティ違反が発生しました。セキュリティ違反カウントを増加させ、SNMP トラップを転送するには、どのコマンドを設定する必要がありますか?

A. switchport port-security violation access

B. switchport port-security violation protect

C. switchport port-security violation restrict

D. switchport port-security violation shutdown

問題 643

VLAN ホッピング攻撃からネットワークを保護する方法は何ですか?

A. 動的 ARP 検査を有効にする

B. トラフィックが VLAN を変更しないように ACL を設定する

C. ネイティブ VLAN を未使用の VLAN ID に変更する

D. インターネットに接続された VLAN にポート セキュリティを実装する

問題 644

スイッチは DHCP スヌーピング情報をどこに保持しますか?

A. CAM テーブル内

B. フレーム転送データベース内

C. MAC アドレス テーブル内
D. バインディング データベース内

問題 645
ネットワーク管理者は、ルーター R1 へのリモート アクセス用に SSH を設定する必要があります。要件は、公開キーと秘密キーのペアを使用して、接続クライアントとの間の管理トラフィックを暗号化することです。どの構成を適用すると要件を満たしますか?
A. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate ec keysize 1024
B. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate ec keysize 2048
C. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key encrypt rsa name myKey
D. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate rsa modulus 1024

問題 646
WPA2 PSK を使用した WLAN がワイヤレス LAN コントローラ GUI で設定されている場合、どの形式がサポートされますか?
A. decimal
B. ASCII
C. unicode
D. base64

問題 647

```
access-list 101 permit ospf any any
 access-list 101 permit tcp any any eq 179
 access-list 101 permit tcp any eq 179 any
 access-list 101 permit gre any any
 access-list 101 permit esp any any

access-list 101 deny ospf any any
 access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 500
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 4500
 access-list 101 deny ip any any log

interface Ethernet0/0
  ip address 10.1.1.25 255.255.255.0
  ip access-group 101 in
```

展示を参照してください。ネットワーク管理者は、ルーターへの VTY アクセスを保護するという任務を負っています。どのアクセス リスト エントリがこのタスクを実行しますか?
A. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet
B. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq scp
C. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq https
D. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq ssh

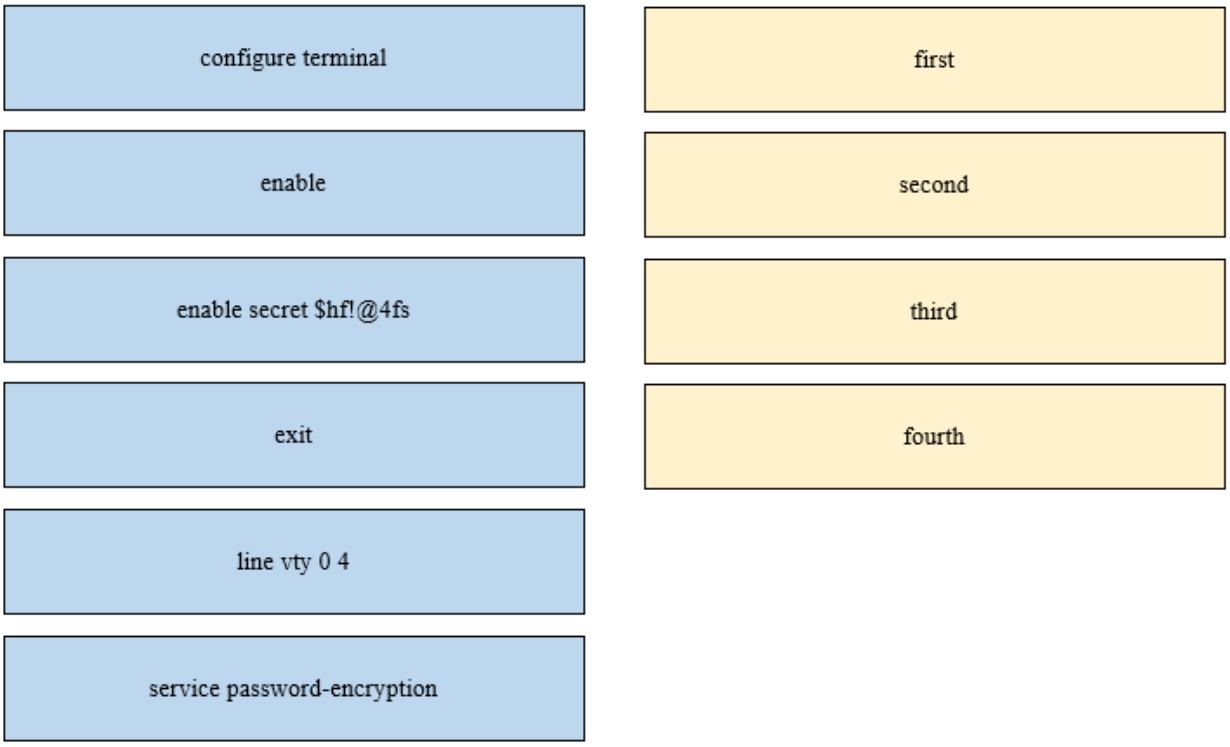
問題 648
ワイヤレス LAN コントローラへの管理接続のセキュリティを強化するには、どの 2 つのプロトコルを無効にする必要がありますか? (2 つお選びください。)
A. HTTPS
B. SSH
C. HTTP
D. Telnet
E. TFTP

問題 649
データセンターのドアにバッジ リーダーを設置して、従業員が職務に基づいて出入りできるようにすることを含むセキュリティ プログラムの要素はどれですか?
A. 物理的アクセス制御
B. 生体認証
C. 役割ベースのアクセス制御
D. 多要素認証

問題 650
DHCP スヌーピングによってどの機能が実行されますか?
A. パケット転送のためにマルチキャスト トラフィックをリッスンします。
B. 特定のトラフィックをレート制限する
C. スイッチ間で VLAN 情報を伝達する
D. DDoS 軽減策を提供する

問題 651
DRAG DROP -
エンジニアは、ローカル ユーザ データベースがすでに設定されているルータ上で、enable コマンドの暗号化されたパスワードを設定しています。設定コマンドを左側から右側の正しい順序にドラッグ アンド ドロップします。すべてのコマンドが使用されるわけではあ

りません。
選択して配置します:




問題 652
安全なリモート CLI アクセスにはどのプロトコルが使用されますか?
A. Telnet
B. HTTP
C. HTTPS
D. SSH

問題 653
ワイヤレス環境に最も強力な暗号化の組み合わせを提供する実装はどれですか?
A.WEP _
B. WPA + TKIP
C. WPA + AES
D. WPA2 + AES

問題 654
物理的アクセス制御は何を規制しますか?
A. ネットワーク機器および施設へのアクセス

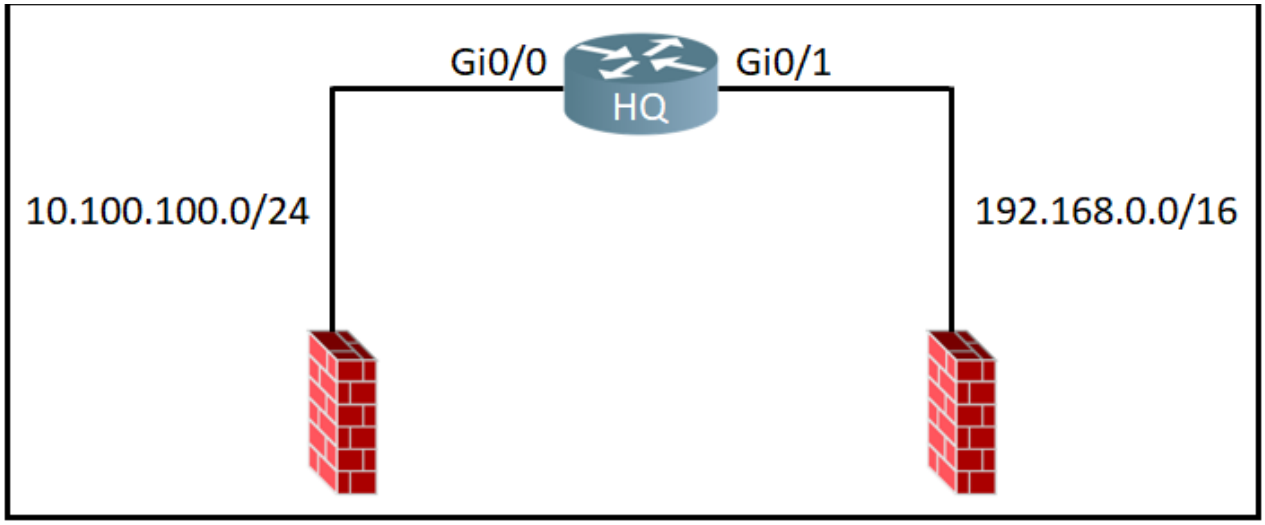
B. 悪意のある活動を防ぐためのサーバーへのアクセス
C. ビジネス機能に基づいた特定のネットワークへのアクセス
D. コンピュータネットワークおよびファイルシステムへのアクセス

問題 655
ネットワーク エンジニアは、新しい実装のために VLAN 2、3、および 4 を構成するように求められます。一部のポートは、未使用のポートを残したまま新しい VLAN に割り当てる必要があります。未使用のポートに対してどのようなアクションを実行する必要がありますか?
A. デフォルト以外のネイティブ VLAN で設定する
B. ネイティブ VLAN でポートを構成する
C. ブラックホール VLAN でポートを構成する
D. ポートをアクセス ポートとして設定する

問題 656
WPA2-PSK WLAN がワイヤレス LAN コントローラーで設定されている場合、ASCII 形式で必要な最小文字数は何ですか?
A. 6
B. 8
C. 12
D. 18

問題 657
リモート サイト間でマルチキャスト トラフィックを伝送し、暗号化をサポートするメカニズムは何ですか?
A. ISATAP
B. IPsec over ISATAP
C. GRE
D. GRE over Ipsec

問題 658




展示を参照してください。インターフェイス Gi0/0 上の任意のホストからのトラフィックを許可し、インターフェイス Gi0/1 からのトラフィックを拒否するには、アクセス リストが必要です。どのアクセス リストを適用する必要がありますか?

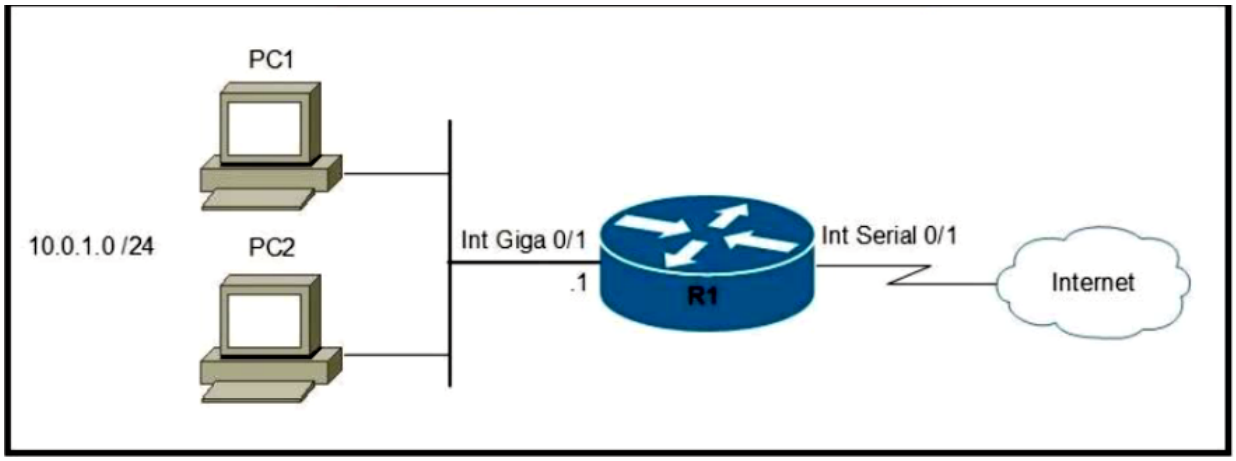
A. ip access-list standard 99 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.0.255.255

B. ip access-list standard 99 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.255.255.255

C. ip access-list standard 199 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.255.255.255

D. ip access-list standard 199 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.0.255.255

問題 659




展示を参照してください。ルータが安全なリモート アクセス接続を受け入れることができるようにするには、ルータ R1 で設定する必要がある 2 つのコマンドはどれですか? (2 つお選びください。)

A. ip ssh pubkey-chain
B. username cisco password 0 cisco
C. crypto key generate rsa
D. transport input telnet
E. login console

問題 660
WLC への管理アクセスを提供するために RADIUS が選択されている場合、どのサービスが欠落していますか?
A. authorization
B. authentication
C. accounting
D. confidentiality

問題 661
組織のセキュリティ プログラムの一部として物理的アクセス制御を実装するアクションはどれですか?
A. 主要なインフラストラクチャを監視するための IP カメラの設定
B. コンソールポートのパスワードの設定
C. リモートの場所での syslog のバックアップ
D. ネットワークデバイスでのイネーブルパスワードの設定

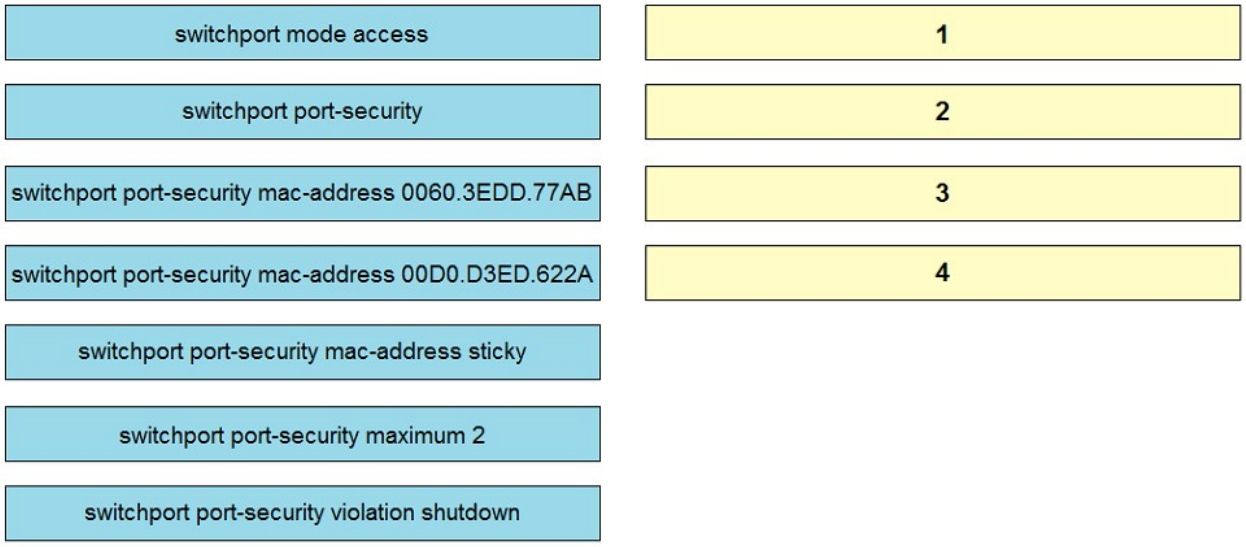
問題 662
アクセス要求パケット内のどのフィールドが RADIUS によって暗号化されますか?
A. 認可されたサービス
B. パスワード
C. 認証者
D. ユーザー名

問題 663
シスコのエンジニアは、次の 3 つのパスワードを使用して工場出荷時のデフォルト ルータを設定しています。
☞ コンソール アクセス用のユーザ EXEC パスワードは、p4ssw0rd1 です。
☞ Telnet アクセス用のユーザー EXEC パスワードは s3cr3t2 です。
☞ 特権 EXEC モードのパスワードは、priv4t3p4ss です。
エンジニアはどのコマンド シーケンスを設定する必要がありますか?

A. enable secret priv4t3p4ss ! line con 0 password p4ssw0rd1 ! line vty 0 15 password s3cr3t2
B. enable secret priv4t3p4ss ! line con 0 password p4ssw0rd1 login ! line vty 0 15 password s3cr3t2 login
C. enable secret priv4t3p4ss ! line con 0 password login p4ssw0rd1 ! line vty 0 15 password login s3cr3t2 login
D. enable secret privilege 15 priv4t3p4ss ! line con 0 password p4ssw0rd1 login ! line vty 0 15 password s3cr3t2 login

問題 665
DRAG DROP -
エンジニアは、ユニキャスト、マルチキャスト、およびブロードキャストを転送するデバイスがポートをフラッディングできないようにするために、ポート セキュリティを備えたスイッチを構成する任務を負っています。ポートは、一度に 2 つのランダムな MAC アドレスのみを許可するように設定する必要があります。必要な設定コマンドを左側から右側のシーケンスにドラッグ アンド ドロップします。すべてのコマンド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**

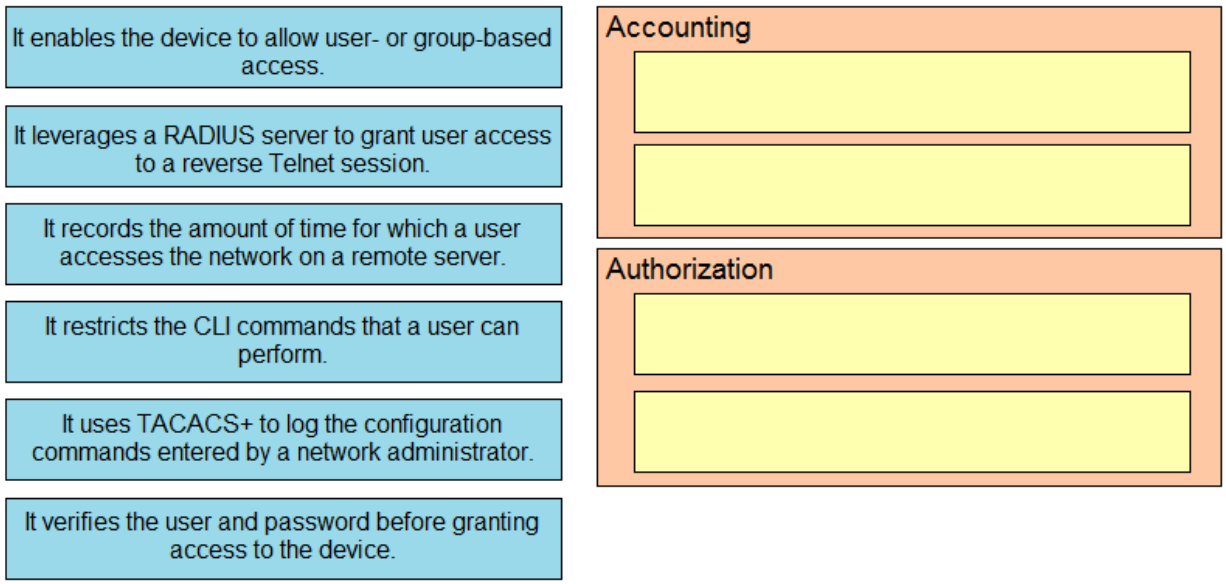



問題 666
環境における Opportunistic Wireless Encryption の機能は何ですか?
A. 認証を提供する
B. オープンネットワーク上のトラフィックを保護する

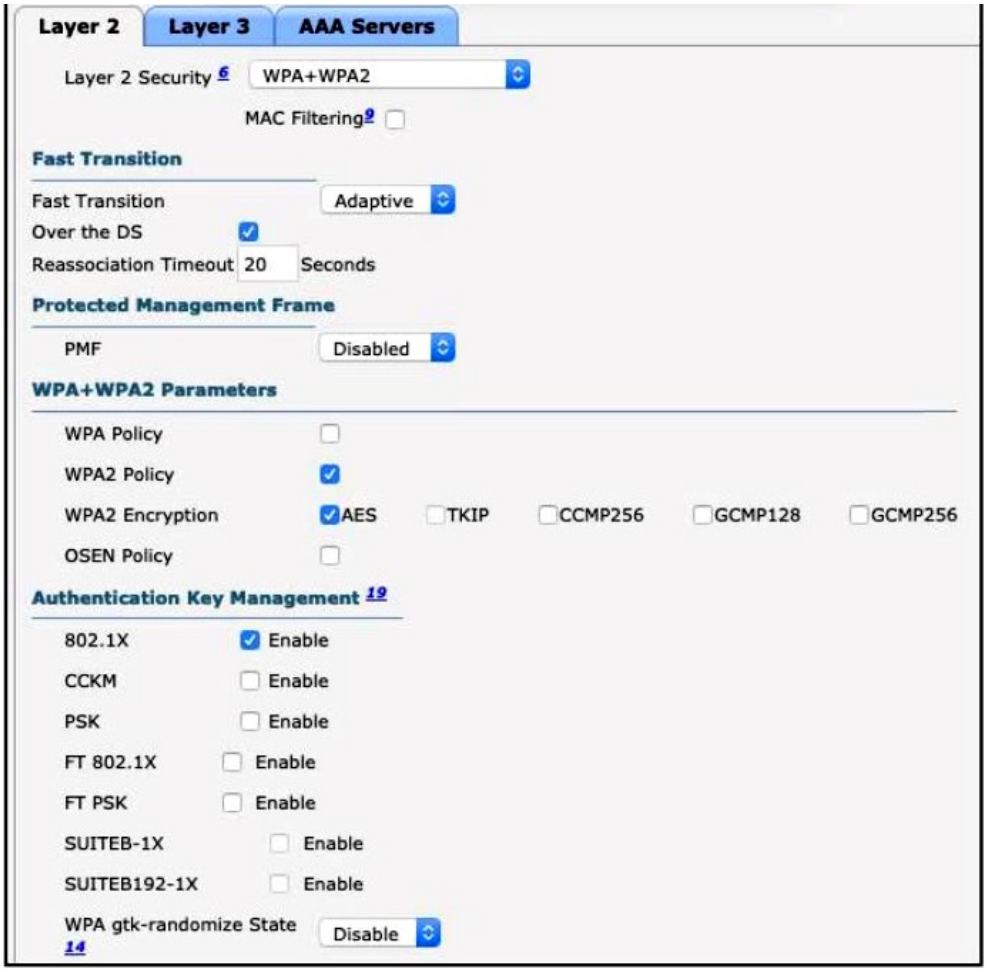
C. 圧縮を提供する
D. WEP 接続を使用してセキュリティを強化する

問題 667
ドラッグ ドロップ -
左側の AAA 機能を右側の対応する AAA セキュリティ サービスにドラッグ アンド ドロップします。すべてのオプション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**




問題 668




展示を参照してください。WLAN 上のクライアントは 802.11r を使用する必要があります。要件を満たすためにはどのような措置を講じる必要がありますか?

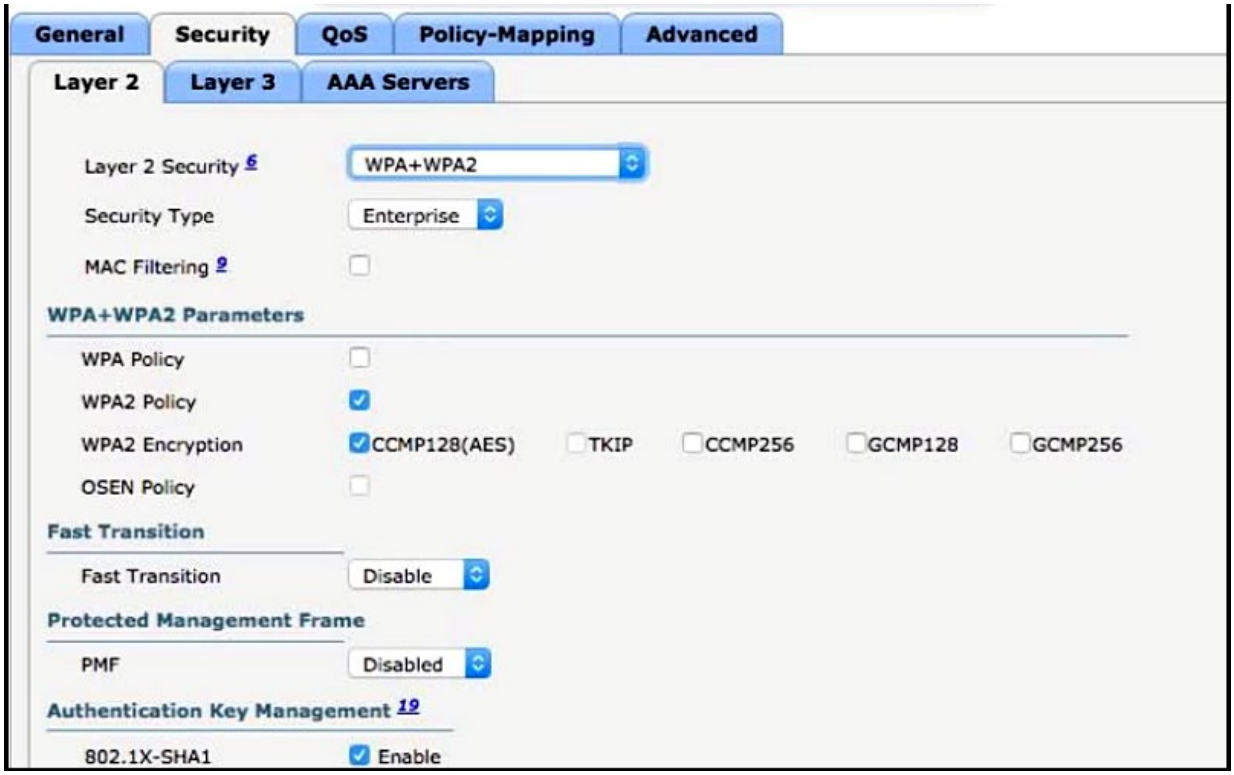
A. [保護された管理フレーム] で、PMF オプションを [必須] に設定します。

B. 「認証キー管理」で CCKM を有効にします。

C. Fast Transition オプションと WPA gtk-randomize State を無効に設定します。

D. [高速移行] オプションを [有効] に設定し、[認証キー管理] で FT 802.1X を有効にします。

問題 669




展示を参照してください。WLAN で 802.11w を有効にするには何を設定する必要がありますか?

A. 高速遷移を有効に設定します。

B. WPA ポリシーを有効にします。

C. PMF を必須に設定します。

D. MAC フィルタリングを有効にする。

問題 670

WPA3 ではどの暗号化方式が使用されていますか?

A. TKIP

B. AES

C. SAE

D. PSK

問題 671

純粋な IPsec で送信されるトラフィックのタイプはどれですか?

A. あるサイトのサーバーから別の場所のホストへのマルチキャスト トラフィック

B. 複数のリモート サイトの 1 つで MAC アドレスを見つけようとするスイッチからのブロードキャスト パケット

C. リモートサイトのホストから本社のサーバーへのユニキャストメッセージ

D. 2 つの異なるサイトにあるスイッチ間のスパニングツリー更新

問題 672
認証と認可はどう違うのですか?
A. 認証はユーザーがアクセスするリソースを記録するために使用され、認可はユーザーがアクセスできるリソースを決定するために使用されます。
B. 認証はネットワークにアクセスする人の身元を確認し、認可はユーザーがアクセスできるリソースを決定します。
C. 認証は、ユーザーがどのリソースにアクセスできるかを決定するために使用され、認可は、どの機器がネットワークへのアクセスを許可されているかを追跡するために使用されます。
D. 認証は個人の身元を確認するために使用され、承認はログイン用の syslog メッセージを作成するために使用されます。

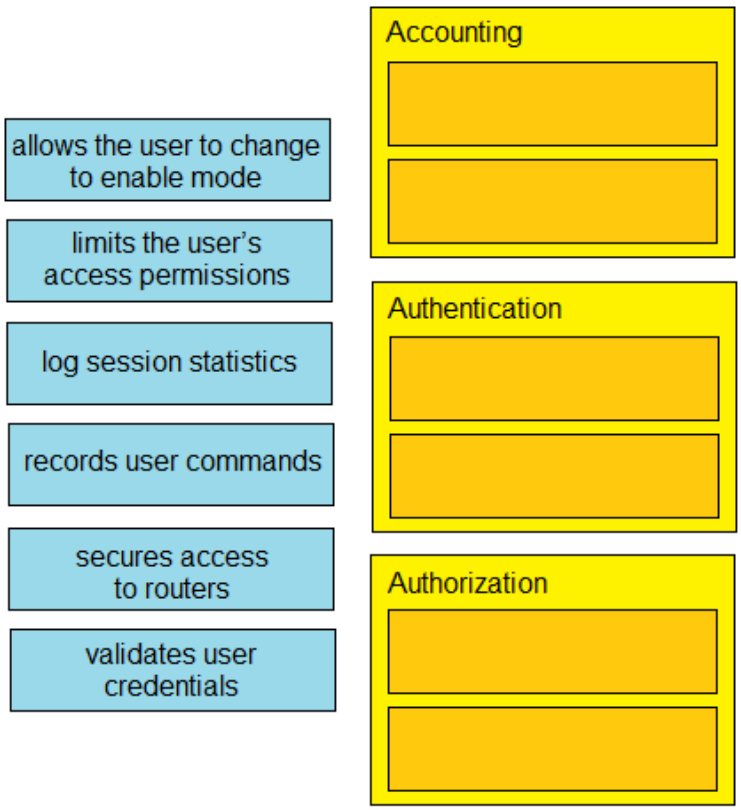
問題 673
エンジニアは、ローカル ルーター上でドメイン名、ユーザー名、およびパスワードを設定しました。Secure Shell アクセス RSA キーの構成を完了するには、次の手順は何ですか?
A. crypto key import rsa pem
B. crypto key generate rsa
C. crypto key zeroize rsa
D. crypto key pubkey-chain rsa

問題 674
ネットワーク攻撃が、ターゲットのハーフオープン TCP リソースが使い果たされるまでポートに複数のパケットを送信することによってターゲット サーバーを圧倒する場合、どのタイプですか?
A. SYN flood
B. reflection
C. teardrop
D. amplification

問題 675
PKI の一部を構成する 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. 接続を認証する事前共有キー
B. 1 つ以上の CRL
C. RSA トークン

D. 証明書を付与する CA
E. 接続を認証するクリアテキストのパスワード

問題 676
DRAG DROP -
AAA サービスの説明を左側から右側の対応するサービスにドラッグ アンド ドロップします。
選択して配置します:




問題 677
最近のセキュリティ違反と RADIUS 障害の後、エンジニアはローカルのユーザー名とパスワードを使用して各エンタープライズ ルーターのコンソール ポートを保護する必要があります。
このタスクを達成するには、エンジニアはどの構成を適用する必要がありますか?
A. aaa new-model line con 0 password plaintextpassword privilege level 15
B. aaa new-model aaa authorization exec default local aaa authentication login default radius username localuser privilege 15 secret plaintextpassword
C. username localuser secret plaintextpassword line con 0 no login local privilege level 15

D. username localuser secret plaintextpassword line con 0 login authentication default privilege level 15

問題 678
Perfect Forward Secrecy に依存するワイヤレス セキュリティ プロトコルはどれですか?
A. WEP
B. WPA2
C. WPA
D. WPA3

問題 679
ゼロデイエクスプロイトとは何ですか?
A. ネットワークが悪意のあるトラフィックで飽和し、リソースと帯域幅に過負荷がかかる場合です。
B. 攻撃者が SQL サーバーに悪意のあるコードを挿入した場合です。
C. 修正が利用可能になる前に、新しいネットワークの脆弱性が発見された場合です。
D. 加害者が 2 者間の会話に介入し、データをキャプチャまたは改ざんする場合です。

問題 680
ネットワーク エンジニアは、マネージド サービス クライアントに属するスイッチを新しい Cisco Catalyst スイッチに交換しています。新しいスイッチは、交換を含む最新のセキュリティ標準に合わせて構成されます。
暗号化された接続とモジュラス サイズが 1024 から 2 倍になった Telnet サービス。エンジニアが新しいスイッチで設定する必要がある 2 つのコマンドはどれですか?
(2 つお選びください。)
A. transport input ssh
B. transport input all
C. crypto key generate rsa modulus 2048
D. crypto key generate rsa general-keys modulus 1024
E. crypto key generate rsa usage-keys

問題 681
多要素認証の 2 つの例は何ですか? (2 つお選びください。)
A. シングルサインオン
B. ソフトトークン

C. 有効期限が切れたパスワード
D. 共有パスワードリポジトリ
E. 独自のユーザー知識

問題 682
認証の概念を認可やアカウンティングと区別する特徴は何ですか?
A. 従量課金制
B. 本人確認
C. ユーザーアクティビティのログ記録
D. サービスの制限

問題 683
次世代 IPS 向け Cisco Advanced Malware Protection の機能は何ですか?
A. 特定のファイルとファイル タイプのマルウェアを検査する
B. 侵害される可能性のあるワイヤレス トラフィックを許可する
C. エンドユーザーの認証
D. URL フィルタリング

問題 684
WPA の機能は何ですか?
A. TKIP/MIC 暗号化
B. 小型 Wi-Fi アプリケーション
C. 事前共有キー
D. 802.1x 認証

問題 685
ネットワーク内で許容可能なセキュリティ体制を実現するには、どの 2 つの実践が推奨されますか? (2 つお選びください。)
A. 暗号化キーチェーンを使用してネットワーク デバイスを認証します。
B. 内部電子メール サーバーとファイル サーバーを指定された DMZ に配置します。
C. 安全に取得できるように、デバイス構成を暗号化された USB ドライブにバックアップします。
D. 未使用または不要なポート、インターフェイス、およびサービスを無効にします。
E. ネットワーク機器を安全な場所に保管します。

問題 686

WPA3 はどのようにセキュリティを向上させますか?

A. 認証には SAE を使用します。

B. 暗号化に RC4 を使用します。

C. 暗号化に TKIP を使用します。

D. 認証に 4 ウェイ ハンドシェイクを使用します。

問題 687

次世代 IPS の機能とは何ですか?

A. ユーザーアクティビティとネットワークイベントを相関させる

B. コントローラーベースのネットワーク内でコントローラーとして機能する

C. RADIUS サーバーと統合して、レイヤー 2 デバイス認証ルールを適用します

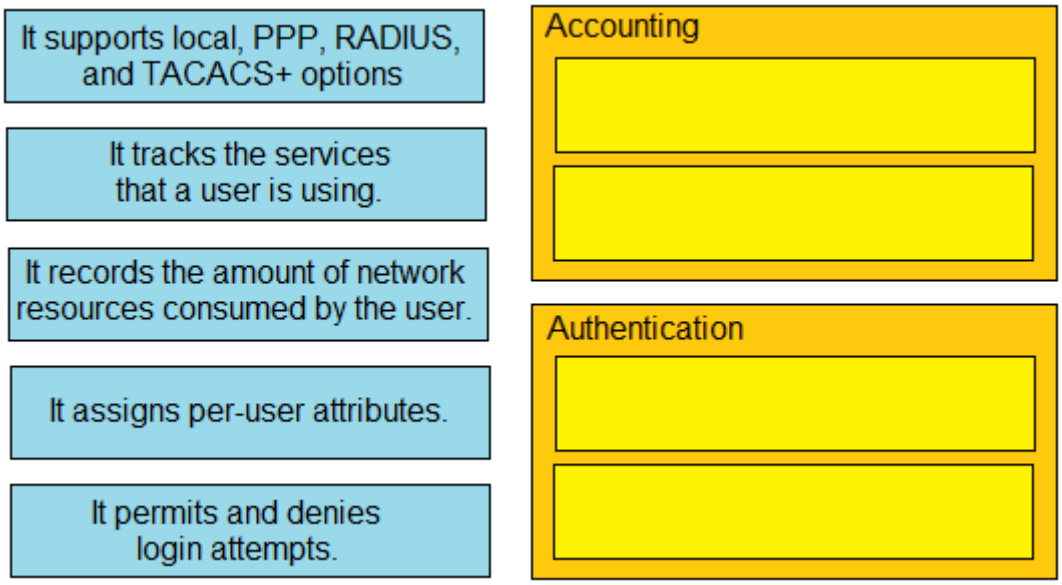
D. 学習した MAC アドレスに基づいて転送を決定します。

問題 688

DRAG DROP -

AAA に関するステートメントを左側から右側の対応する AAA サービスにドラッグ アンド ドロップします。すべてのオプションが使用されるわけではありません。

選択して配置します:

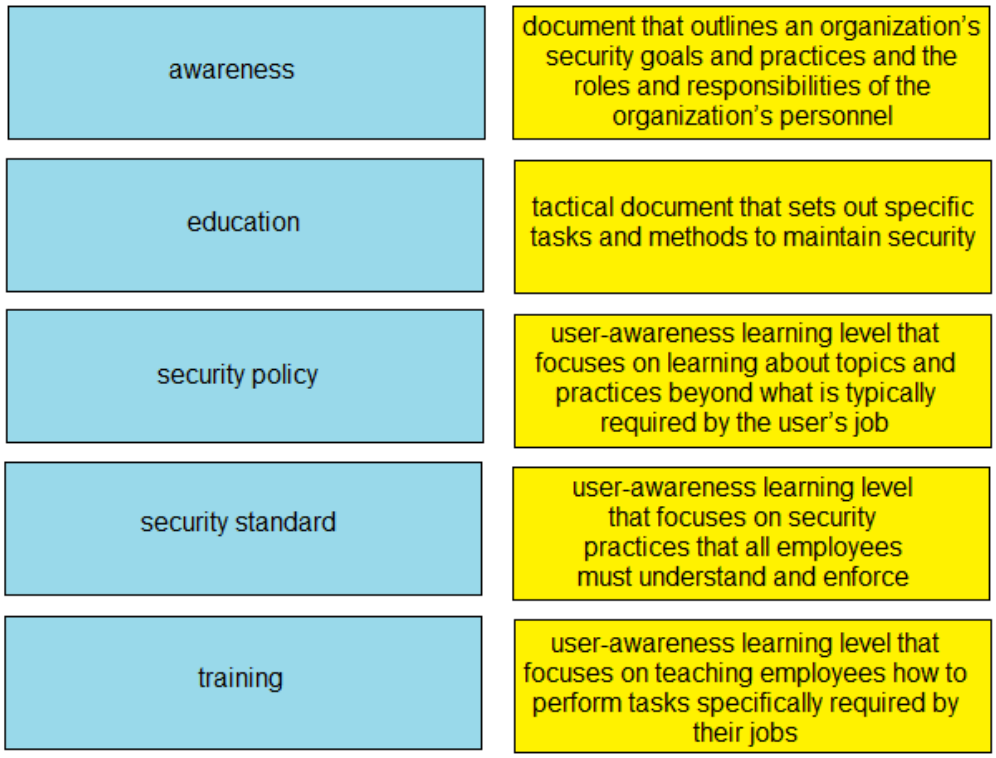



問題 689

DRAG DROP -

セキュリティ プログラムの要素を左側から右側の対応する説明にドラッグ アンド ドロップします。

選択して配置します:




問題 690

IP ヘッダーとペイロードを暗号化する IPsec トランスポート モードはどれですか?

A. pipe

B. transport

C. control

D. tunnel

問題 691

トランク リンク上のデフォルトのポート セキュリティ動作は何ですか?

A. 複数の MAC アドレスを学習すると、ポートは err-disabled 状態になります。

B. 違反が発生するとネットワークループが発生します。

C. ポート セキュリティが有効になるとすぐに、ネイティブ VLAN 設定が無効になります。

D. 10 個の MAC アドレスが静的に設定された後、ポートが err-disabled 状態になります。

問題 692

ネットワークをセキュリティ ドメインごとに分離するデバイスはどれですか?

A. 侵入防御システム

B. ファイアウォール

C. ワイヤレスコントローラー
D. アクセスポイント

問題 693
VLAN ホッピング攻撃はどのように軽減されますか?
A. トランク ポートを手動で実装し、DTP を無効にする
B. 拡張 VLAN を構成する
C. すべてのポートをアクティブにし、デフォルトの VLAN に配置します。
D. 動的 ARP 検査を有効にする

問題 694
WPA3 の一部として実装された機能強化はどれですか?
A. 安全な初期キー交換のためのパーソナル モードでの前方秘匿性と SAE
B. 802.1x 認証と AES-128 暗号化
C. パーソナル モードの AES-64 およびエンタープライズ モードの AES-128
D. TKIP 暗号化による WEP およびパケットごとのキーイングの改善

問題 695
サイト間 VPN が構成されている場合、元の IP パケット全体のカプセル化と暗号化を提供する IPsec モードはどれですか?
A. AH を使用した IPsec トランスポート モード
B. AH を使用した IPsec トンネル モード
C. ESP を使用した IPsec トランスポート モード
D. ESP を使用した IPsec トンネル モード

問題 696
エンジニアは、IP サブネット 10.139.58.0/28 からルーターへのリモート アクセスを構成しています。ドメイン名、暗号キー、SSH が設定されました。宛先ルーターでトラフィックを有効にする設定はどれですか?
A. line vty 0 15 access-class 120 in ! ip access-list extended 120 permit tcp 10.139.58.0 0.0.0.15 any eq 22
B. interface FastEthernet0/0 ip address 10.122.49.1 255.255.255.252 ip access-group 10 in ! ip access-list standard 10 permit udp 10.139.58.0 0.0.0.7 host 10.122.49.1 eq 22
C. interface FastEthernet0/0 ip address 10.122.49.1 255.255.255.252 ip access-group 110 in ! ip access-list standard 110 permit tcp 10.139.58.0 0.0.0.15 eq 22

host 10.122.49.1
D. line vty 0 15 access-group 120 in ! ip access-list extended 120 permit tcp 10.139.58.0 0.0.0.15 any eq 22

問題 697
SDN アーキテクチャでは、ネットワーク ノードのどの機能がコントローラに集中されますか?
A. IP ルーティング テーブルを作成します。
B. フィルタリングによりメッセージを破棄する
C. ルーティングを決定する
D. リモート アクセス デバイスにプロトコル アクセスを提供する

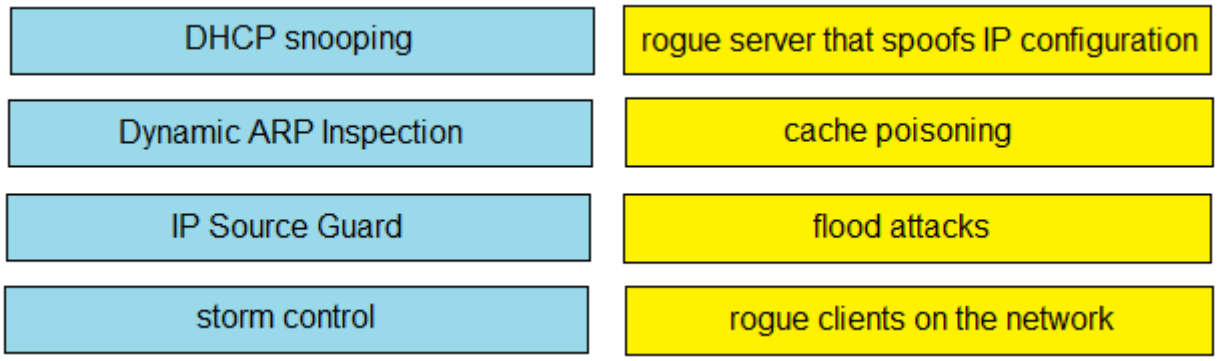
問題 698
ユーザーがユーザー名とパスワードを使用してネットワーク デバイスにログインすると、どの管理セキュリティ プロセスが呼び出されますか?
A. authentication
B. auditing
C. accounting
D. authorization

問題 699


展示を参照してください。LDAP のドメイン資格情報を使用して最高の暗号化と認証を提供するためにエンジニアが実行する必要がある 2 つの手順は何ですか?
(2 つお選びください。)
A. [認証キー管理] で [PSK] を選択します。
B. レイヤ 2 セキュリティで Static-WEP + 802.1X を選択します。
C. [レイヤー 2 セキュリティ] で [WPA+WPA2] を選択します。
D. [認証キー管理] から [802.1X] を選択します。
E. [TKIP 暗号化を使用した WPA ポリシー] を選択します。

問題 700
WPA3 にはどの拡張機能が実装されていますか?
A. PKI を使用してアクセス ポイントを識別する
B. 802.1x 認証を適用する
C. TKIP を使用する
D. ブルートフォース攻撃から保護する

問題 701
DRAG DROP -
Cisco IOS 攻撃軽減機能を左側から右側の軽減するネットワーク攻撃の種類にドラッグアンド ドロップします。
選択して配置します:




問題 702