Fortinet.FCSS_LED_AR-7.6.v2026-06-16.q43

試験コード:	FCSS_LED_AR-7.6
試験名称:	FCSS - LAN Edge 7.6 Architect
認定資格:	Fortinet
無料問題数:	43
バージョン:	v2026-06-16
アクセス数:	113
ページビュー数:	430
https://www.jpnpdf.com/Fortinet.FCSS_LED_AR-7.6.v2026-06-16.q43-mondaishu.html	

最新問題: **1**
FortiAuthenticator を使用して RSSO を完全に有効にするには、FortiGate で何を行う必要がありますか?
応答：
A. ユーザーグループでRSSOを有効にする
B. Syslogフィルタを追加する
C. RADIUSクライアントIPを設定する
D. RSSO属性を無効にする
Answer: A (メーッセージを残す**)**

最新問題: **2**
大規模キャンパス環境で FortiAIOps を使用する利点は次のどれですか?
（2つ選択してください）
応答：
A. ログ保持期間の延長
B. ライセンスプール
C. 予測アラートと診断
D. 平均解決時間（MTTR）の短縮
Answer: C,D (メーッセージを残す**)**

最新問題: **3**
FortiLink 経由で接続した後、FortiSwitch が FortiGate 管理インターフェースに表示されません。
トラブルシューティングの最初の手順は何でしょうか?
A. FortiGate セキュリティ ポリシーが FortiSwitch からのトラフィックを許可していることを確認します。
B. FortiSwitch に静的 IP を手動で割り当てます。
C. FortiGate デバイスの DHCP サーバーが FortiSwitch に IP を割り当てていることを確認します。
D. FortiSwitch がインターネットにアクセスできることを確認します。
Answer: (解答を表示する**)**

FortiLinkトポロジでは、管理対象FortiSwitchは通常、FortiLinkインターフェース上のDHCPサーバーから管理IPを自動的に取得します。スイッチがIPを取得できない場合は、以下の手順を実行してください。
* FortiLink CAPWAP/DTLS 制御チャネルを形成できません。
* そのため、WiFi & Switch Controller > FortiSwitch には表示されません。
FortiOS のドキュメントには、FortiLink がスイッチのオンボーディングに FortiLink インターフェース上の組み込み DHCP サーバーを使用することが記載されています。
したがって、最初のトラブルシューティング手順は次のことを確認することです。
* FortiLink DHCP サーバーが有効になっています。
* リースは FortiSwitch MAC に配布されています。
その他のオプション:
* A: セキュリティ ポリシーは L2 FortiLink 制御チャネルには影響しません。
* B: 静的 IP を使用することもできますが、通常の最初のステップではありません。
* D: FortiGate がスイッチを認識するためにインターネット アクセスは必要ありません。

最新問題**: 4**
ワイヤレス展開における VLAN プーリングの主な利点は何ですか?
応答：
A. DHCP枯渇を軽減し、負荷分散を改善します
B. クライアントにMACアドレス経由で接続するよう強制する
C. 不正AP検出を無効にする
D. VLAN間のNATを有効にする
Answer: A (メーッセージを残す**)**

最新問題**: 5**
FortiSwitch 管理のために FortiGate のポート 1 で FortiLink を有効にする CLI コマンドはどれですか。
応答：
A. 上記のすべて
B. Fortilink を有効にする
C. ポート1を編集
D. 設定システムインターフェース
Answer: A (メーッセージを残す**)**

最新問題**: 6**
展示品を参照してください。

WTP profile configuration

```
config wireless-controller wtp-profile
    edit "S231F"
        config platform
            set type 231F
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country US
        config radio-1
            set band 802.11n-2G
            set wids-profile "default-wids-apscan-enabled"
            set vap-all manual
            set vaps "Student01"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac-5G
            set channel-bonding 40MHz
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set arrp-profile "arrp-default"
            set vap-all manual
            set vaps "Student01"
            set channel "36" "44" "52"
        end
        config radio-3
            set mode disabled
        end
    next
end
```

これは WTP プロファイル構成を示しています。
AP プロファイルは、オープン プラン エリアに設置された 2 つの FAP-231F AP に割り当てられます。
最初の AP には、5 GHz 無線に関連付けられた 32 個のクライアントと、2.4 GHz 無線に関連付けられた 22 個のクライアントがあります。
2 番目の AP には、5 GHz 無線に関連付けられたクライアントが 12 台と、2.4 GHz 無線に関連付けられたクライアントが 20 台あります。
デュアルバンド対応クライアントが最初のAP付近のエリアに入ると、最初のAPは新しいクライアントの信号強度を-3. 3dBmと測定します。2番目のAPは新しいクライアントの信号強度を-43dBmと測定します。
新しいクライアントが学生 01 ワイヤレス ネットワークに接続しようとすると、クライアントはどの AP 無線に関連付けられますか?
A. 最初の AP 2.4 GHz インターフェイスはより強力な信号を提供するため、クライアントはこれを優先することがよくあります。
B. 信号がより強いため、最初の AP 5 GHz インターフェースを選択します。
C. 2 番目の AP 5 GHz インターフェイスにはクライアントが少ないため、信号が弱いにもかかわらずパフォーマンスが向上します。
D. 2 番目の AP 2.4 GHz インターフェイスは、速度が向上し干渉が少なくなるため、5 GHz よりも優先されます。
Answer: C (メーッセージを残す**)**
WTPプロフィールより:
ハンドオフRSSIを30に設定
ハンドオフスタしきい値を30に設定する
無線1の設定
バンド802.11n-2Gの設定
ベイプセット Student01」
無線2の設定

バンド802.11ac-5Gの設定
darrpを有効にする
arrp-profile を "arrp-default" に設定する
ベイプセット 「Student01」
要点:
* 同じ SSID (Student01) が両方の AP と両方の帯域 (2.4 GHz と 5 GHz) でブロードキャストされます。
* handoff-sta-thresh 30 は AP 間のクライアント負荷分散を有効にします。
* AP 無線に関連付けられたクライアントが 30 台を超える場合、クライアントが代わりに近隣の AP に接続するように、新しい関連付けを拒否し始めます (RSSI が許容できる限り)。
* 現在のクライアント数:
* AP1:5GHzで32クライアント、2.4GHzで22クライアント
* AP2: 5 GHz で 12 クライアント、2.4 GHz で 20 クライアント
5GHzでは次のようになります。
* AP1 の 5 GHz 無線が 30 クライアントのしきい値を超えています (32 > 30)。# 新しいクライアントを押し出そうとします。
* AP2 の 5 GHz 無線はしきい値 (12 クライアント) をはるかに下回っており、新しいクライアントを問題なく受け入れます。
新しいデュアルバンド クライアントは次の場所で確認できます。
* AP1による-33dBm
* AP2による-43dBm
AP1の信号はより強いものの、設定されたしきい値に基づいて5GHz帯の無線がすでに過負荷状態にあるため、AP1はAP1クライアントからのアソシエーション試行を拒否します。その後、クライアントはAP2の5GHz帯の無線に接続します。AP2のアソシエーション試行では、以下のようになります。
* クライアントが少ない（デバイスあたりの通信時間が長い）
* 依然として許容できる信号があります (-43 dBm は 5 GHz で容易に使用できます)。
これはオプションCと完全に一致します。
その他のオプションは、設定されたクライアント負荷分散しきい値を無視し、純粋に RSSI に基づいて関連付けを想定するか、このプロファイルが調整されている目的ではない 2.4 GHz を優先するため、正しくありません。

最新問題**: 7**
デジタル証明書の使用に関する次の 2 つの記述のうち正しいものはどれですか。
（2つ選択してください。）
応答：
A. 中間 CA によって署名された証明書は、依然として信頼されたチェーンの一部です。
B. 証明書失効リスト (CRL) は、失効した証明書をすべてのシステムからリアルタイムで自動的に削除します。
C. CRL は自己署名証明書にのみ必要です。
D. 中間 CA は階層的な信頼チェーンの確立に役立ちます。
Answer: A,D (メーッセージを残す**)**

最新問題: **8**
FortiLink ではなく FortiManager を使用して FortiSwitch を管理する利点は何ですか?
（2つ選択してください）
応答：
A. すべてのスイッチのCLIのみの制御
B. 別途FortiAnalyzerが必要
C. 一元化されたポリシーとテンプレートの展開
D. バックアップ構成のバージョン管理
Answer: C,D (メーッセージを残す**)**

最新問題: **9**
FortiAuthenticator を LDAP サーバーと統合する場合、ユーザー検索を実行するためにどのパラメータを正しく定義する必要がありますか?
応答：
A. グループ名
B. 共有秘密
C. Syslogフィルター
D. DN（識別名）
Answer: D (メーッセージを残す**)**

最新問題: **10**
ユーザー認証用の RADIUS サーバーとして FortiAuthenticator を構成するために必要な手順は次のどれですか。
（2つ選択してください）
応答：
A. FortiGateでRSSOを有効にする
B. ローカルユーザーグループまたはリモートユーザーグループを作成する
C. 共有秘密鍵を持つRADIUSクライアントを定義する
D. FortiGateでLDAPクエリを設定する
Answer: B,C (メーッセージを残す**)**

最新問題: **11**
FortiSwitch を管理するために FortiManager で FortiLink を構成する場合、次の手順のうち必須のものはどれですか。
（2つ選択してください）
応答：
A. FortiGateでFortiLinkインターフェースを有効にする
B. FortiAPにプロビジョニングテンプレートを適用する
C. FortiGateポリシーでスイッチコントローラを構成する
D. FortiSwitch構成テンプレートをFortiManagerにインポートする
Answer: A,D (メーッセージを残す**)**

最新問題: **12**
FortiAuthenticator が RSSO グループの割り当てに使用する RADIUS アカウンティング メッセージのフィールドはどれですか?
応答：
A. ユーザーパスワード
B. 発信局ID
C. フィルターID
D. NAS識別子
Answer: C (メーッセージを残す**)**

最新問題: **13**
FortiGate を使用したゲスト アクセス ワークフローにおいて、FortiAuthenticator はどのような役割を果たしますか?
応答：
A. DHCPサーバーとして機能する
B. SMSまたは電子メールでゲストユーザーを認証します
C. トラフィックログをキャプチャします
D. クライアントにファームウェアを展開する
Answer: B (メーッセージを残す**)**

最新問題: **14**
訪問者にWi-Fiアクセスを提供するためのキャプティブポータルを設定しています。プロセスを簡素化するため、チームは訪問者が新しいアカウントを作成したり、手動で認証情報を入力したりするのではなく、既存のソーシャルメディアアカウントを使用して認証できるようにしたいと考えています。
この機能を有効にするために必要な 2 つのアクションはどれですか? (2 つ選択してください。)
A. FortiAuthenticator内部データベースをユーザー認証情報のプライマリソースとして設定します
B. 認証タイプとしてアカウント ログインを有効にし、リモート LDAP サーバーを構成します。
C. 選択したソーシャル メディア プラットフォームごとにリモート オープン認証 (OAuth) サーバーを設定します。
D. サポートされているプラットフォームのソーシャル ログイン プロファイルを構成します。
E. キャプティブ ポータルではソーシャル メディア ログインを使用できないため、電子メール ログイン オプションのみを構成します。
Answer: (解答を表示する**)**

最新問題: **15**
チームは、自動化ステッチを使用してデバイスを自動的に隔離するFortiGateワイヤレスネットワークの構成を計画しています。IOCイベントの検出時にワイヤレスクライアントを正常に隔離するには、どの2つの構成が必要ですか？（2つ選択してください。）
応答：
A. インターフェース レベルでデバイス検出を有効にします。
B. FortiAnalyzer には有効な脅威検出サービス ライセンスが必要です。
C. FortiGate を Security Fabric グループのメンバーとして設定します。

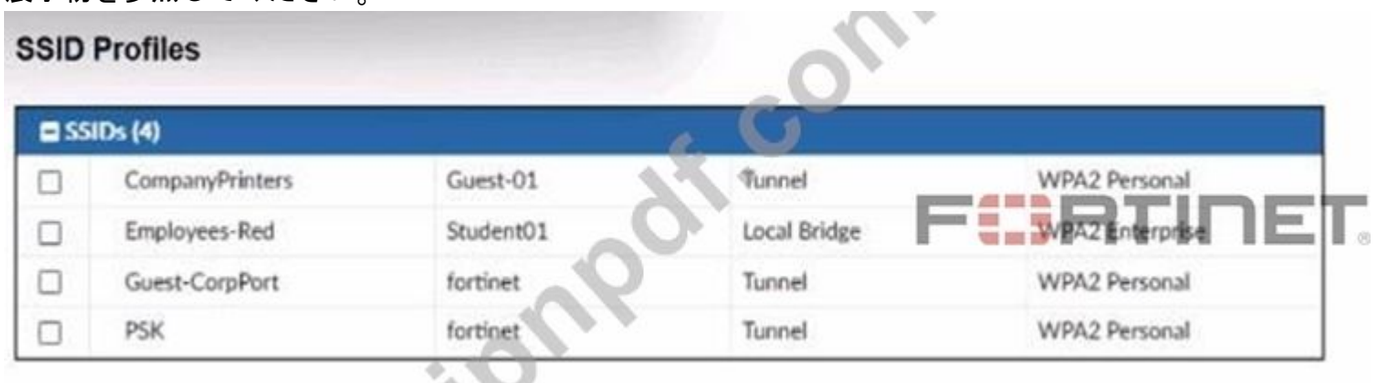
D. SSID はブリッジ モードで設定する必要があります。
Answer: (解答を表示する**)**

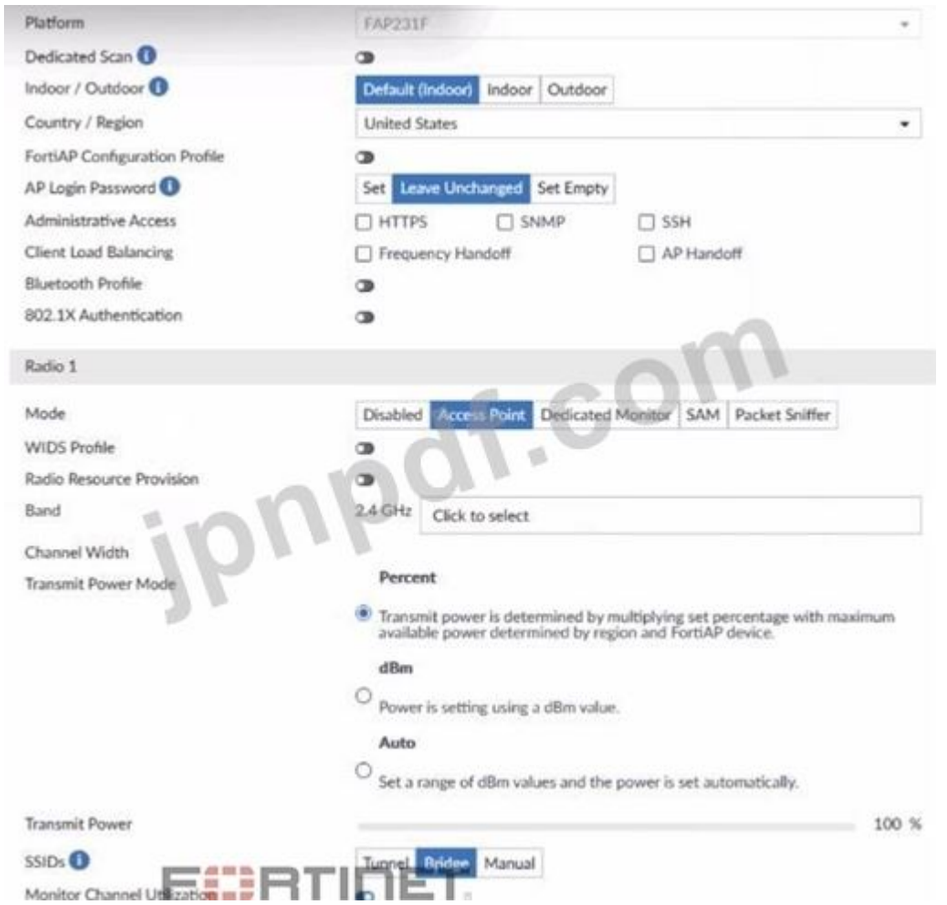
最新問題**: 16**
CER 証明書の証明書署名要求 (CSR) の生成に関する正しい記述はどれですか。
A. CSR 内のフィールドが不正確であったり欠落していると、CA が要求を検証できず、証明書が拒否され、展開プロセスが遅延する可能性があります。
B. 共通名 (CN) や組織 (O) などの重要なフィールドが正しくない場合でも、証明機関 (CA) は証明書を発行しますが、検証に正確なフィールド情報を必要とする特定のアプリケーションやシステムでは、その証明書が信頼されない可能性があります。
C. CSR フィールドは主に要求元組織による内部記録保存に使用され、証明書の署名を正常に行うには CSR 内の公開キーのみが正確である必要があります。
D. CSR 内のフィールドは主に文書化を目的としています。不足している情報や不正確な情報は、署名プロセス中に CA によって自動的に修正されます。
Answer: (解答を表示する**)**
FortiOS のドキュメントでは、証明書の署名に使用される CSR には、特に次の正確で有効なフィールドが含まれている必要があることが明示的に記載されています。
一般名（CN）
組織（O）
国（C）
公開鍵パラメータ
FortiGate 証明書セクションによると:
CSR フィールド情報が正しくない場合、CA が要求を拒否する可能性があります。
理由は次のとおりです:
CA は ID と組織情報を検証します。
データが欠落しているか不正な形式である場合、PKI 要件は無効になります。
CSR は CA によって自動的に修正されません。
したがって：
#Aが正解です。
オプション BD は PKI の原則に反します:
B は誤りです。CA は、パブリック トラストの ID フィールドが一致しない証明書を発行しません。
C は誤りです。CSR フィールドは内部使用のためだけのものではなく、証明書の ID を定義します。
D は誤りです: CA は CSR フィールドを自動修正しません。

最新問題: 17
FortiLink NAC がネットワーク アクセス制御を実施するために使用できる 3 つの条件は何ですか?
（3つ選択してください）
応答：
A. デバイスタイプ
B. MACアドレス
C. スイッチスタックの優先度
D. ユーザーID
E. インターフェースMTU
Answer: A,B,D (メーッセージを残す)

最新問題: 18
FortiAnalyzer は、Fortinet セキュリティ ファブリックのデバイス隔離アクションにどのように貢献しますか?
応答：
A. 影響を受けるFortiSwitchポートを再起動します
B. FortiAIOps修復をトリガーします
C. ログベースのイベントトリガーをFortiGateに送信します
D. エンドポイントの自動切断を提供します
Answer: C (メーッセージを残す)

最新問題: 19
展示物を参照してください。





FortiManagerでSSIDプロファイルのセットが設定され、FortiGateで管理されているAPグループにAPプロファイルが割り当てられています。しかし、指定されたSSIDはいずれもこれらのAPからブロードキャストされていません。
AP がこれらの SSID を意図どおりにブロードキャストするには、どのような構成変更が必要ですか?
A. AP プロファイルを調整して、すべての SSID がブリッジまたはトンネルのいずれかのサポートされているモードに設定され、両方の混在がないようにする。
B. 設定された SSID の組み合わせをサポートするプラットフォームを使用するように AP プロファイルを変更します。
C. SSID 設定で [手動] を選択し、ブロードキャストする SSID を選択します。
D. 送信電力モードを自動に設定します。
Answer: C (メーッセージを残す**)**
展示品より:
* AP プロファイルには次の内容が表示されます:
* SSID: トンネル | ブリッジ | 手動
* 現在の設定は 「手動」ではなく 「ブリッジ」です。
* [ブリッジまたはトンネル] を選択した場合、対応する VAP が AP プロファイルで明示的にマップされていない限り、AP プロファイルは SSID を自動的にブロードキャストしません。
* FortiManager SSID プロファイルは作成されますが、手動 SSID 選択で明示的に適用されない限り、AP は SSID をブロードキャストしません。
Fortinet のドキュメントには次のように記載されています。

APがブロードキャストするSSIDを制御するには、APプロファイルでSSIDを手動に設定し、必要なSSIDを選択する必要があります。したがって、APが意図したSSIDをブロードキャストするには、次の手順を実行します。
#SSID 設定を手動に切り替えて、SSID (CompanyPrinters、Student01、Guest-CorpPort、PSK) を手動で選択する必要があります。
他のオプションが間違っている理由:
* A. ブリッジ/トンネルの混在を避けるようにAPプロファイルを調整してください。混在モードはサポートされています。問題ではありません。
* B. プラットフォームの変更プラットフォーム (FAP231F) はすでにリストされているすべての SSID をサポートしています。
* D. 送信電力モードを自動に設定する電力設定は SSID ブロードキャストとは関係ありません。

最新問題**: 20**
各ユーザー証明書では、サブジェクトフィールド、有効期限、ユーザープリンシパル名（UPN）、CRLダウンロードURL、OCSP URLを定義できます。これらの属性の詳細な設定は、証明書にどのような影響を与えますか？
A. 自動チェックの必要性が減るため、証明書を手動で取り消すことが容易になります。
B. 証明書の有効性が特定のデバイスとアプリケーションに制限されるため、証明書の一般的な有用性が低下します。
C. ユーザーの正確な識別を可能にし、証明書失効チェックをタイムリーに実行できるようにします。
D. 証明書の普遍的な有効性を保証することで、幅広いアプリケーションやサービスとの互換性を実現します。
Answer: (解答を表示する**)**
FortiGate / FortiAuthenticator / SSL-VPN / 802.1X で使用されるユーザー証明書では、次の属性が重要です。
* 件名フィールドとUPN
* ユーザーに一意の ID (CN および/または UPN) を提供します。
* FortiGate は、LDAP 統合証明書認証に SAN/UPN フィールドを使用できます。
* 有効期限
* 証明書の有効期間を制限し、ライフサイクルとローテーションを強制します。
* CRL URL と OCSP URL
* 証明書が失効しているかどうかを確認する場所を FortiGate (または任意の証明書利用者) に伝えます。
* 有効期限のみに頼るのではなく、OCSP または定期的な CRL ダウンロードを使用して、ほぼリアルタイムの失効を可能にします。
これらのフィールドを慎重に構成することで、次のことが可能になります。
* 証明書はユーザーを一意かつ正確に識別します。
* 依存システムは正確かつタイムリーな失効チェックを実行できるため、セキュリティが向上します。
他の選択肢が間違っている理由:
* 回答: その逆です。CRL/OCSP は手動による失効ではなく、自動化を強化します。
* B: これらの属性は、本質的に証明書を特定のデバイスに制限するものではありません。これは、キーの使用法、EKU、またはデバイス証明書によって行われます。
* D: これらは 普遍的な有効性を保証する」ものではなく、証明書を強制可能な有効期間と失効を持つ 1 つの ID に正確にバインドするものです。

最新問題**: 21**
FortiGate で FortiSwitch のステータスが 管理対象 (切断)」になっているのはどういう意味ですか?
応答：
A. 登録されていません
B. 構成の更新やハートビートを受信しなくなりました
C. 管理対象スイッチグループから削除されました
D. スタンドアロンモードです
Answer: B (メーッセージを残す**)**

最新問題**: 22**
ゼロタッチプロビジョニング (ZTP) 展開では、通常どのデバイスが FortiManager への接続を開始しますか?
応答：
A. FortiAuthenticator
B. FortiSwitch
C. FortiAP
D. フォーティゲート
Answer: D (メーッセージを残す**)**

最新問題**: 23**
FortiGate から管理対象 FortiSwitch のステータスを表示する CLI コマンドはどれですか?
応答：
A. システムインターフェースを取得する
B. スイッチコントローラの診断、接続ステータスの取得
C. スイッチコントローラのグローバル表示
D. スイッチコントローラ管理スイッチを取得する
Answer: (解答を表示する**)**

最新問題**: 24**
APはIPsecネットワーク経由でFortiGateに接続するように手動で設定されており、FortiGateはAPを正常に検出して認証します。しかし、FortiGateがAPとCAPWAPトンネルを確立できないため、APは管理対象外のままです。
どのような構成変更によってこの問題が解決され、FortiGate が IPsec 接続を介して CAPWAP トンネルを確立できるようになるのでしょうか?
A. IPsec トンネル経由で AP に到達できるように、FortiGate で静的ルートを設定します。
B. set mpls-connection オプションを有効にして、リモート AP にカスタム AP プロファイルを割り当てます。
C. 断片化を防ぐために、AP の CAPWAP トンネル MTU サイズを減らします。
D. FortiAP ファームウェア イメージをアップグレードして、FortiOS バージョンとの互換性を確保します。
Answer: B (メーッセージを残す**)**
FortiAP が FortiGate overIPsec トンネルに接続する場合、これは WAN/MPLS 展開と同様に処理されます。
このようなシナリオでは、FortiGate は CAPWAP が anon-L2 トランスポートを通過する必要があることを認識する必要があります。

FortiAP プロファイルには次のものが含まれます。
mpls接続を有効にする
この設定は次の理由で必要です:
* FortiGateはCAPWAPをトランスポートトンネル内にカプセル化できる
* リモートFortiAPは、ルーティング/IPsecネットワークの背後にある場合でもCAPWAPを確立できます。このオプションがない場合、FortiGateはAPを検出しますが、CAPWAPをUPにすることができず、APは
「検出済み/未承認」または「オフライン」状態。
他人が間違っている理由
* A. 静的ルート# 検出はすでに成功しているので、ルーティングは問題ではありません。
* C. MTU# を減らす IPsec には役立つ場合もありますが、CAPWAP の確立には必要ありません。
* D. ファームウェアのアップグレード# ファームウェアの不一致は、CAPWAP トンネルの障害ではなく、「管理対象(アップグレードが必要)」と表示されます。
したがって、mpls-connection enable を設定することが必要です。

最新問題**: 25**
FortiManager は FortiAP 上でどの機能を集中制御できますか?
（2つ選択してください）
応答：
A. 無線プロファイル
B. SSIDブロードキャスト
C. セルラーモデムルーティング
D. IPsecトンネルの作成
Answer: A,B (メーッセージを残す**)**

最新問題**: 26**
FortiAuthenticator が syslog サーバーにログを送信するように構成するには、どの 2 つのアクションを実行する必要がありますか?
（2つ選択してください）
応答：
A. syslogサーバのIPとポートを指定する
B. SNMPトラップを設定する
C. Syslog機能を選択
D. LDAPデバッグを有効にする
Answer: A,C (メーッセージを残す**)**

最新問題**: 27**
FortiManagerで「CORP」という名前のSSIDを作成し、FortiAPに割り当てたいのですが、どのような手順が必要ですか？
（3つ選択してください）
応答：

A. FortiGateに構成をプッシュする
B. FortiAPにプロファイルを割り当てる
C. APを再起動する
D. APプロファイルでSSIDを定義する
Answer: A,B,D (メーッセージを残す**)**

最新問題**: 28**
FortiSwitch でサポートされているデフォルトのトランキング プロトコルは何ですか?
応答：
A. STP
B. 802.1Q
C. VTP
D. LACP
Answer: B (メーッセージを残す**)**

最新問題**: 29**
展示物を参照してください。

Fortilink interface settings in FortiGate

```
FortiGate (fortilink) # show
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.0.13.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4"
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
        set snmp-index 14
        set auto-auth-extension-device enable
        set ip-managed-by-fortiipam disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
        set lacp-mode static
    next
end
```

DHCP server setting for fortilink

```
config system dhcp server
    edit 1
        set dns-service default
        set ntp-service local
        set default-gateway 10.0.13.254
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.0.13.1
                set end-ip 10.0.13.253
            next
        end
        set vci-match enable
        set vci-string "FortiExtender"
    next
end
```

管理のためにFortiGateに新しいFortiSwitchを追加しています。FortiGateでは必要な設定はすべて完了していますが、FortiSwitchはオフラインのままです。ケーブル接続は検証済みで、正しく接続されています。
FortiGate が FortiSwitch を検出できない原因となっている可能性のある誤った構成はどれですか?

A. Fortilink インターフェース設定 ip-managed-by-fortiipam を有効にする必要があります。

B. Fortilink インターフェースに間違ったインターフェース メンバーがあります。

C. Fortilink インターフェース設定サイクルは物理である必要があります。

D. DHCP サーバー設定の vci-string が正しく構成されていません。

Answer: (解答を表示する**)**

FortiLinkでは、FortiGateに内蔵されたDHCPサーバーがFortiSwitchにIPアドレスを割り当て、管理下に置くことができます。FortiSwitchの自動オンボーディングでは、通常、DHCPサーバーは以下のように設定されます。
VCIマッチを有効にする
vci文字列「FortiSwitch」「FortiExtender」を設定します
展示では、Fortilink の DHCP サーバーには次のものが含まれています。
VCIマッチを有効にする
VCI文字列「FortiExtender」を設定する

VCI文字列に「FortiSwitch」が含まれていないため、DHCPオファーはベンダークラス識別子がFortiExtenderと一致するクライアントにのみ送信されます。FortiSwitchはIPアドレスを取得できないため、オフライン状態のままとなります。
* オプションBは間違っています: メンバー「port4」はトポロジ内の物理ケーブルと一致します。
* オプション C は適切です: FortiLink は、物理的なインターフェイスだけでなく、集約インターフェイスにもなります。
* オプションA(ip-managed-by-fortiipam) は無関係です。ここでは FortiIPAM は必要ありません。

最新問題: **30**
FortiAuthenticator でデジタル証明書ベースの 2 要素認証を有効にするための 2 つの要件は何ですか? （2つ選択してください）
応答：
A. インポートされたユーザー証明書
B. Syslogサーバーの設定
C. FortiAnalyzer統合
D. 証明機関（CA）のセットアップ
Answer: A,D (メーッセージを残す**)**

最新問題: **31**
EAP-TLSを使用して2FAを設定しています。ユーザー名と一致させるには、証明書にどのフィールドを含める必要がありますか？
応答：
A. シリアル番号
B. 発行者DN
C. サブジェクト別名
D. 有効期限
Answer: C (メーッセージを残す**)**

最新問題: **32**
展示物を参照してください。

FortiManager configuration

FortiGate CLI output

```
FortiGate# diagnose switch-controller switch-info mac-table S224EPTF19005867
vdom: root

Managed Switch : S224EPTF19005867 0

MAC: 00:0c:29:e6:ea:d2 VLAN: 4089 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 1 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native I

MAC: 00:0c:29:e6:ea:d2 VLAN: 4093 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 4094 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 70:88:6b:8c:4a:ce VLAN: 4089 Port: port2(port-id 2)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 04:d5:90:3e:e7:80 VLAN: 1 Port: port1(port-id 1)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 00:0c:29:06:ea:d2 VLAN: 4088 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 10 Trunk:  GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

Total Displayed: 8

FortiGate# diagnose switch-controller mac-device nac onboarding
vdom: root
VLAN        MAC                 LAST-SEEN    TYPE    LOCATION
4089        70:88:6b:8c:4a:ce   4            SW      S224EPTF19005867      port2

FortiGate# diagnose switch-controller mac-device nac known
vdom: root
MAC        LAST-KNOWN-SWITCH     LAST-KNOWN-PORT       MATCHED-NAC-POLICY MAC-POLICY-ACTION   FSW-ID  COMMENTS
```


図に示されている FortiManager 構成と FortiGate CLI 出力を調べます。

管理対象FortiSwitch S224SPTF19005867のポート2に接続されたデバイスでNAC機能をテストしています。ポート2にはNACポリシーが適用されており、テストデバイスからトラフィックが生成されました。しかし、テストデバイスからのトラフィックはNACポリシーと一致しず、オンボーディングVLANに留まります。
テスト デバイスが NAC ポリシーによって正しく分類されない理由として考えられる 2 つの理由は何ですか? (2つ選択してください。)
A. VLAN 4089 でデバイス検出が有効になっていません。
B. FortiGate によって検出されたデバイスのオペレーティング システムは Linux ではありません。
C. FortiGate と FortiSwitch 間の管理通信がダウンしています。
D. NAC ポリシーに設定されている MAC アドレスが正しくありません。
Answer: A,B (メーッセージを残す)
FortiManager NAC ポリシーから:
* カテゴリ = デバイス
* 一致基準にはMACアドレスとオペレーティングシステム = Linuxが含まれます
* アクション = VLAN 「学生」を割り当てる
FortiGate CLI から:
スイッチ コントローラの診断、スイッチ情報、MAC テーブル...
MAC: 70:88:6b:8c:4a:ce VLAN: 4089 ポート: port2
スイッチコントローラのMacデバイスの診断、Macオンボーディング
VLAN 4089 MAC 70:88:6b:8c:4a:ce
そのため、デバイスはオンボーディングVLANであるVLAN 4089に固定され、一致するNACポリシーがありません。
NAC ポリシーを一致させるには、FortiGate に、VLAN/FortiLink インターフェース上のデバイス検出から得られるデバイス ID 情報と、ポリシーが期待する属性 (OS、MAC など) が必要です。
* A. VLAN 4089 ではデバイス検出が有効になっていません。
* エンドポイントが存在するインターフェース/VLAN でデバイス検出が無効になっている場合、FortiGate は OS/デバイス情報を学習できません。
* これがないと、NAC エンジンは NAC ポリシー (OS やその他の属性に依存) と比較できないため、デバイスはオンボーディング VLAN 内に残ります。#これが有効な根本原因です。
* B. FortiGate によって検出されたデバイスのオペレーティング システムは Linux ではありません。
* NAC ポリシーでは、オペレーティング システム = Linux が明示的に要求されます。
* エンドポイントが実際には Windows/macOS である場合、または OS フィンガープリントがまだ「不明」である場合、ポリシーは一致せず、デバイスはオンボーディング状態のままになります。#これも正当な理由です。
* C. FortiGate と FortiSwitch 間の管理通信がダウンしています。
* CLI 出力 (switch-info mac-table および mac-device) は、FortiGate がスイッチと通信しており、MAC/VLAN/ポート情報を確認していることを証明します。#有効な理由ではありません。
* D. NAC ポリシーに設定されている MAC アドレスが正しくありません。
* 図は、NAC ポリシー内の MAC が MAC テーブルに表示される MAC と一致していることを示しています。
#原因はここにはありません。

最新問題**: 33**

FortiAuthenticator の syslog 設定で認証ログをキャプチャするには、どのログ カテゴリを選択する必要がありますか?
応答：
A. 認証
B. ポリシー
C. システムイベント
D. デバッグ
Answer: A (メーッセージを残す)

最新問題**: 34**
FortiGate と FortiSwitch 間の通信を回復するには、どの手順を実行すればよいですか?
（2つ選択してください）
応答：
A. FortiLinkインターフェースのステータスを確認する
B. スイッチの役割を 「ルートブリッジ」に設定する
C. DHCPオプション138を確認する
D. FortiSwitchのSNMPエージェントを再起動します
Answer: A,C (メーッセージを残す)

最新問題**: 35**
会議センターの無線ネットワークでは、キャプティブポータルを介したゲストアクセスが提供されており、未登録のユーザーがセルフ登録してネットワークに接続できます。ITチームは、既存の設定を更新し、安全なHTTPS接続を介したキャプティブポータル認証を強制する任務を負っています。この変更を実施するために、管理者が実行すべき2つの手順はどれですか？ （2つ選択してください。）
A. ユーザー認証設定で HTTP リダイレクトを有効にします。
B. HTTPS キャプティブ ポータル URL を使用して新しい SSID を作成します。
C. HTTPS 接続を強制するには、ゲスト SSID での HTTP 管理アクセスを無効にします。
D. FortiGate および FortiAuthenticator で HTTPS を使用するようにキャプティブ ポータル URL を更新します。
Answer: A,D (メーッセージを残す)
目標: ゲストに対して HTTPS 経由のキャプティブ ポータル認証を強制します。
FortiGate/FortiAuthenticator キャプティブ ポータルの設定の場合:
* HTTP リダイレクトは、ゲストが任意の HTTP サイトを参照するときに、そのリクエストがポータル URL にリダイレクトされるようにするために使用されます。
* 安全なログイン ページが必要な場合は、ポータル URL 自体が HTTPS である必要があります。
FortiOS キャプティブ ポータルおよびファイアウォール認証ガイドラインでは、次のことが推奨されています。
* HTTP リダイレクトを有効にすると、認証されていない HTTP トラフィックが透過的にポータルに送信されます。
* ポータル URL を HTTPS で構成し、多くの場合、FortiGate または FortiAuthenticator の証明書を参照します。
したがって：
* A. ユーザー認証設定で HTTP リダイレクトを有効にします。#これにより、認証されていない HTTP 要求が (現在は HTTPS) ポータルにリダイレクトされるようになります。

* D. FortiGate および FortiAuthenticator で HTTPS を使用するようにキャプティブ ポータル URL を更新します。#これにより、ログイン自体が安全になります (TLS で保護されます)。
正しくない：
* B- 新しい SSID は必要ありません。同じ SSID で HTTPS ポータルを使用できます。
* C- SSID で HTTP 管理者アクセスを無効にしても、キャプティブ ポータル スキームは制御されません。HTTPS の適用は、管理者アクセス フラグではなく、ポータル構成とリダイレクトによって行われます。

最新問題: **36**
デバイスの MAC アドレスが FortiSwitch で隔離されると、その出力トラフィックはどうなりますか?
A. トラフィックはアクセス VLAN に送信されます。
B. トラフィックはネイティブ VLAN に割り当てられます。
C. トラフィックはタグなしトラフィックとして送信されます。
D. トラフィックは許可された VLAN に送信されます。
Answer: A (メーッセージを残す**)**
デバイスの MAC アドレスが FortiSwitch で（FortiLink NAC、ファブリック自動化、または手動隔離を介して）隔離されると、FortiSwitch は隔離 VLAN（FortiSwitch NAC 操作内ではアクセス VLAN とも呼ばれます）を使用して隔離を実施します。
FortiSwitch の動作は、LAN Edge ドキュメントで定義されています。
* 隔離されたデバイスは、分離用に予約された「アクセス VLAN」に移動されます。
* この VLAN は FortiGate NAC ポリシーで静的に定義されており、スイッチ ポートは隔離された MAC をその VLAN に動的に再割り当てします。
* 隔離された MAC からのすべての出力トラフィックはこの VLAN に強制的に送信され、実稼働ネットワークへのアクセスが防止されます。
したがって、正しい説明は次のようになります。
#トラフィックはアクセスVLANに送信されます。
オプション B、C、および D は次の理由で不正解です。
* 検疫はネイティブ VLAN に再割り当てされません。
* タグなしトラフィックを恣意的に送信しません。
* 許可されたVLANにトラフィックを転送しません

最新問題: **37**
キャプティブ ポータルの問題をトラブルシューティングする場合、リダイレクトされた HTTPS 要求のどの POST パラメータを使用してユーザーのセッションを追跡し、要求が有効であることを確認できますか。
A. ユーザー名
B. 実行
C. 魔法
D. メール
Answer: C (メーッセージを残す**)**
FortiGate キャプティブ ポータル ワークフロー (ローカルまたは外部) の場合:

* クライアントは、キャプティブ ポータルが有効になっている SSID/インターフェイスに接続します。
* クライアントが HTTP/HTTPS リクエストを行います。
* FortiGate はインターセプトしてログイン ページ (ローカルまたは外部 URL) にリダイレクトします。
* ポータル フォームは POST 経由で FortiGate に送信されます。
改ざんを防止し、POST を正しいユーザー セッションに結び付けるために、FortiGate はリダイレクトに特別な隠しパラメータを含め、POST でそれを期待します。
* パラメータの名前はmagicです。
魔法の値:
* キャプティブポータルセッションごとに生成される一意のトークンです。
* ユーザーの IP、インターフェース、セッション情報をエンコード/セッションリンクします。
* FortiGate により次のことが保証されます:
* POST は元のリクエストを開始したユーザーから送信されます。
* リクエストはランダムまたは再送信されたものではありません。
トラブルシューティングを行う場合:
* 外部ポータルがマジック パラメータを受信したとおりに保持して FortiGate に再送信しない場合、認証は失敗し、「セッションが見つかりません」や「マジックが無効です」などのエラーが表示されます。
他のフィールドがこの目的に使用されない理由
* A. ユーザー名 - ログイン ID のみ。複数のユーザーが異なる場所から同じユーザー名を使用できるため、ブラウザー セッションを一意に追跡することはできません。
* B. redir - ユーザーが最初に要求したURLが格納されており、ログイン後にそのURLにリダイレクトされます。セッション整合性トークンではありません。
* D. email - 一部のゲスト/登録フローで使用されるオプション フィールド。セッション検証とは無関係です。

最新問題**: 38**
LAN エッジ展開における FortiAIOps の主な機能は何ですか?
応答：
A. ファームウェアアップデートを展開する
B. アプリケーション層ファイアウォールを監視する
C. AIを使用して運用データを相関させて分析する
D. NetFlowデータを収集する
Answer: C (メーッセージを残す**)**

最新問題**: 39**
FortiSwitch ポートに VLAN を割り当てるには、どの構成要素が必要ですか?
（2つ選択してください）
応答：
A. FortiGateでVLAN IDを定義する
B. VLANでDHCPリレーを有効にする
C. スイッチポートプロファイルにVLANを割り当てる
D. 静的ルートを作成する

Answer: (解答を表示する**)**

最新問題**: 40**
FortiAuthenticator は、証明機関 (CA) として機能するときにどのような機能をサポートしますか?
応答：
A. デジタル証明書の発行と失効を行う自己署名者として機能できます。
B. サードパーティの証明機関と統合して外部証明書を検証できます。
C. デジタル証明書を発行および失効できますが、OCSP サーバーとして機能することはできません。
D. CRL リポジトリとしてのみ機能し、証明書署名要求 (CSR) はサポートされません。
Answer: A (メーッセージを残す**)**

最新問題**: 41**
デバイスが 802.1X をサポートしていないが、MAC アドレスを使用してネットワークにアクセスする必要がある場合、どの認証方法がトリガーされますか?
応答：
A. RADIUS EAP チェーン
B. EAP-TLS
C. MAC認証バイパス（MAB）
D. LDAPベースのログイン
Answer: C (メーッセージを残す**)**

最新問題**: 42**

```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
```


FortiLinkインターフェースを設定し、DHCPサーバーがデフォルトで有効になっています。その結果得られるDHCPサーバー設定は図に示されています。この設定におけるvci-string設定の役割は何ですか？
A. FortiSwitch および FortiExtender デバイスからの DHCP 要求を無視します。
B. ホスト名として FortiSwitch または FortiExtender を持つデバイスへの IP アドレスの割り当てを制限します。

C. 接続するには、デバイスが VCI 文字列と一致する必要があります。一致しない場合は、IP アドレスを受信しません。
D. FortiSwitch および FortiExtender デバイスの IP アドレスを予約します。
Answer: C (メーッセージを残す**)**
DHCP 構成には次のように表示されます。
VCIマッチを有効にする
vci文字列 「FortiSwitch」 「FortiExtender」を設定します
これが意味するもの
VCI = ベンダークラス識別子（DHCPオプション60）
vci-match を有効にすると、DHCP サーバーは、設定されたベンダー ID と一致する VCI 文字列を持つクライアントからの DHCP 要求にのみ応答します。
FortiSwitch と FortiExtender はどちらも、次の内容の DHCP オプション 60 を送信します。
「FortiSwitch」
「FortiExtender」
これは FortiLink の展開で使用されるため、これらのデバイスのみが FortiLink ネットワーク上の IP アドレスを受け取ります。
したがって：
C) 接続するには、デバイスが VCI 文字列と一致する必要があります。一致しない場合は、IP アドレスを取得できません。
#正しい。
これは、FortiGate FortiLink DHCP の動作と完全に一致します。
誤った選択肢の要約
A - FortiSwitch/FortiExtenderを無視する
#反対の動作。
B - ホスト名に基づいて制限する
#VCI はホスト名をチェックしません。
D - IPを予約する
#予約は行われません。予約ではなくフィルタリングが行われます。

最新問題**: 43**
ネットワーク管理者は新しい FortiGate をネットワークに接続し、FortiManager で自動的に検出して登録できるようにします。
FortiGate が FortiManager アドレスを取得した後、何が起こりますか?
A. FortiGate は、TCP ポート 541 を介して FortiManager への安全なトンネルを確立します。
B. デバイスは FortiManager で手動で認証する必要があります。
C. FortiGate は、FortiManager からの DHCP 応答に基づいてインターフェース設定を構成します。
D. FortiGate は、UDP ポート 1068 を使用して、ローカル ネットワーク上のすべてのデバイスに検出要求を送信します。
Answer: (解答を表示する**)**

FortiGate がゼロ タッチ プロビジョニング (ZTP) または自動検出を使用して導入される場合:
* FortiGate は FortiManager IP アドレスを取得します (DHCP オプション 240、FortiCloud/ZTNA プロビジョニング、または手動設定から)。
* 次のステップは UI 認証や DHCP の変更ではなく、すぐに FGFM (FortiGate-FortiManager) トンネルの形成を試みます。
* FGFM プロトコルは、TCP ポート 541 を使用して安全な管理チャネルを確立します。
FortiManager では引き続き FortiManager 内でのデバイスの手動認証が必要ですが、これはトンネルが確立された後に行われます。
したがって、FMG アドレスを取得した後の最初の自動アクションは、TCP/541 上に安全な FGFM トンネルを作成することです。