Fortinet.FCSS_SASE_AD-24.v2026-04-14.q51

試験コード:	FCSS_SASE_AD-24
試験名称:	FCSS - FortiSASE 24 Administrator
認定資格:	Fortinet
無料問題数:	51
バージョン:	v2026-04-14
アクセス数:	127
ページビュー数:	510
https://www.jpnpdf.com/Fortinet.FCSS_SASE_AD-24.v2026-04-14.q51-mondaishu.html	

最新問題: **1**
FortiSASE でダッシュボード ビューをカスタマイズする利点は何ですか?
応答：
A. インターフェースの外観をカスタマイズする
B. セキュリティ調査に関連する特定の指標に焦点を当てる
C. 無関係なビジネス指標を表示する
D. 保存されるデータの量を減らす
Answer: B (メーッセージを残す**)**

最新問題: **2**
個々のエンドポイント構成を最小限に抑えるセキュア インターネット アクセス (SIA) ユースケースはどれですか?
A. サイトベースのリモートユーザーインターネットアクセス
B. エージェントレスリモートユーザーインターネットアクセス
C. SSL VPNリモートユーザー用のSIA
D. ZTNA を使用した SIA
Answer: B (メーッセージを残す**)**
エージェントレスのリモートユーザーインターネットアクセスユースケースは、個々のエンドポイント設定を最小限に抑えるように設計されています。このシナリオでは、FortiSASEはエンドポイントデバイスにエージェントをインストールすることなく、安全なインターネットアクセスを提供します。このアプローチは、各エンドポイントで複雑な設定を行う必要がないため、管理対象外のデバイスや一時的なユーザーが存在する環境に特に有効です。セキュリティポリシーはネットワークレベルで適用され、エンドポイント固有のソフトウェアに依存することなく、一貫した保護を実現します。
他のオプションが間違っている理由は次のとおりです。

* A. サイトベースのリモートユーザーによるインターネットアクセス :このユースケースでは、特定のサイトまたは場所のユーザーのインターネットアクセスを、通常はゲートウェイまたはファイアウォールを介して保護します。このユースケースでは、そのサイトの全ユーザーの設定が簡素化されますが、リモートユーザーの個々のエンドポイント設定が特に簡素化されるわけではありません。
* C. SSL VPNリモートユーザー向けSIA :SSL VPNでは、ユーザーはクライアントまたはブラウザベースのインターフェースを介して企業ネットワークに接続する必要があります。このアプローチでは、SSL VPNクライアントのインストールや設定など、エンドポイント側での追加設定が必要になることがよくあります。
* D. ZTNAを使用したSIA :ゼロトラストネットワークアクセス（ZTNA）は、リソースへのアクセスを許可する前に、デバイスのIDとポスチャを検証することに重点を置いています。ZTNAはセキュリティを強化しますが、エンドポイントエージェントやポスチャチェックが必要になる場合があり、ある程度のエンドポイント設定が必要になります。
参考文献:
Fortinet FCSS FortiSASE ドキュメント - セキュアインターネットアクセス (SIA) ユースケース
FortiSASE 管理ガイド - エージェントレスリモートユーザーアクセス

最新問題: **3**
セキュリティ プロファイル内でコンテンツ検査を最適化するには、どのような手法を実装する必要がありますか?
（2つ選択）
応答：
A. AIベースの分析ツールの応用
B. テストのための最小限のデータセットの使用
C. 検査対象コンテンツの継続的な監視
D. 検査アルゴリズムの定期的な更新
Answer: C,D (メーッセージを残す**)**

最新問題: **4**
FortiSASE を使用して SD-WAN を導入すると、組織にはどのようなメリットがもたらされますか?
（3つ選択してください）
応答：
A. ネットワークデバイスの物理的なセキュリティ強化
B. 運用コストの削減
C. アプリケーションパフォーマンスの向上
D. ネットワークの俊敏性の向上
Answer: B,C,D (メーッセージを残す**)**

最新問題: **5**

FortiSASE 内のゼロ トラスト ネットワーク アクセス (ZTNA) は、ユーザー ID とデバイスの状態に基づいてアプリケーションへのアクセスを制限します。
応答：
A. 偽
B. 真
Answer: B (メーッセージを残す)

最新問題**: 6**
FortiSASE ポータルに初めてアクセスする場合、管理者はどの 3 つの FortiSASE コンポーネントのデータセンターの場所を選択する必要がありますか? (3 つ選択してください。)
A. エンドポイント管理
B. プレゼンスポイント
C. SD-WANハブ
D. ログ記録
E. 認証
Answer: (解答を表示する)
FortiSASE ポータルに初めてアクセスする場合、管理者は次の FortiSASE コンポーネントのデータセンターの場所を選択する必要があります。
* エンドポイント管理:
* エンドポイント管理のデータ センターの場所により、エンドポイント データとポリシーが選択した地理的領域内で管理および保存されることが保証されます。
* プレゼンスポイント（PoP）：
* Point of Presence (PoP) は、FortiSASE サービスがユーザーに提供される場所です。
PoP の場所を選択すると、ユーザーの地理的な分布に基づいて最適なパフォーマンスと接続性が確保されます。
* ログ記録:
* ログデータの保存場所と管理場所が、ログデータを保存するデータセンターの所在地によって決まります。これは、コンプライアンスと規制要件の遵守、そして効率的なログ分析とレポート作成にとって非常に重要です。
参考文献:
FortiOS 7.2 管理ガイド: FortiSASE の初期セットアップと構成手順の詳細。
FortiSASE 23.2 ドキュメント: さまざまな FortiSASE コンポーネントのデータ センターの場所を選択することの重要性について説明します。

最新問題**: 7**
FortiSASE のリアルタイム セキュリティ イベントに関するレポートを生成するために FortiOS で使用されるコマンドはどれですか?
応答：
A. システムステータスを取得する
B. セキュリティイベントレポートを取得する

C. レポート生成を実行する
D. システムセキュリティイベントレポートの診断
Answer: (解答を表示する**)**

最新問題**: 8**
FortiSASE にゼロ トラスト ネットワーク アクセス (ZTNA) を実装する主な目的は何ですか?
応答：
A. ネットワーク構成を簡素化するため
B. 既存のセキュリティ対策をすべて置き換える
C. IDとコンテキストに基づいて最小権限のアクセスを強制する
D. すべてのネットワークリソースへの包括的なアクセスを提供する
Answer: C (メーッセージを残す**)**

最新問題**: 9**
FortiSASE でのリアルタイム監視ではどのログを優先する必要がありますか?
（該当するものをすべて選択してください）
応答：
A. ユーザー認証ログ
B. セキュリティイベントログ
C. 帯域幅使用ログ
D. 電力消費ログ
Answer: A,B,C (メーッセージを残す**)**

最新問題**: 10**
マイクロ ブランチ展開で FortiAP が FortiSASE と通信するために使用するアクセス ポイント通信プロトコルは何ですか?
A. 軽量アクセスポイントプロトコル (LWAPP)
B. 無線アクセスポイントの制御とプロビジョニング (CAPWAP)
C. ワイヤレス アプリケーション プロトコル (WAP)
D. アクセスポイント間プロトコル (IAPP)
Answer: B (メーッセージを残す**)**

最新問題**: 11**
エンドポイント コンプライアンスに利用できる FortiSASE コンポーネントはどれですか?
応答：
A. セキュアウェブゲートウェイ (SWG)
B. ゼロトラストネットワークアクセス (ZTNA)
C. クラウド アクセス セキュリティ ブローカー (CASB)
D. サービスとしてのファイアウォール (FWaaS)
Answer: B (メーッセージを残す**)**

最新問題: **12**
FortiSASE の FortiView をどのように活用してネットワーク セキュリティを強化できますか?
応答：
A. セキュリティアップデートをブロードキャストすることで
B. 非準拠デバイスを無効にすることで
C. ユーザーのアクティビティをリアルタイムで表示することで
D. ネットワークトラフィックの詳細な情報を提供することで
Answer: (解答を表示する**)**

最新問題: **13**
FortiSASE SSL VPN ユーザーの作成をキャプチャするイベント ログ サブタイプはどれですか?
A. エンドポイントイベント
B. VPNイベント
C. ユーザーイベント
D. 管理者イベント
Answer: (解答を表示する**)**
FortiSASE SSL VPNユーザーの作成を記録するイベントログのサブタイプは、ユーザーイベントです。このサブタイプは、ユーザーアカウントの作成、変更、削除など、ユーザー管理に関連するアクティビティを記録するために特別に設計されています。SSL VPNユーザーの作成は、システムに新しいユーザーを追加するため、このカテゴリに分類されます。
他のオプションが間違っている理由は次のとおりです。
A. エンドポイントイベント :これらのログは、デバイス登録、コンプライアンスチェック、セキュリティポスチャ評価など、エンドポイントデバイスに関連するアクティビティに関するものです。SSL VPNユーザーの作成はエンドポイントイベントとは無関係です。
B. VPNイベント :これらのログは、セッションの確立、終了、エラーなど、VPN接続に関連するアクティビティを記録します。SSL VPNの使用はVPNイベントを生成しますが、ユーザーアカウントの作成自体はこのサブタイプでは記録されません。
D . 管理者イベント :これらのログは、設定変更やポリシー更新など、管理者が実行したアクションを追跡します。管理者はSSL VPNユーザーを作成する場合がありますが、ユーザー作成という具体的なイベントは管理者イベントではなくユーザーイベントに分類されます。
参照：
Fortinet FCSS FortiSASE ドキュメント - イベントログとサブタイプ
FortiSASE 管理ガイド - 監視とログ記録

最新問題: **14**
自動スクリプトによる一括ユーザー登録は、FortiSASE での個別ユーザー登録よりも安全性が低くなります。
応答：
A. 真

B. 偽
Answer: B (メーッセージを残す**)**

最新問題**: 15**
FortiSASE で設定されたログ設定を表示するには、どの FortiOS コマンドを使用しますか?
応答：
A. ログ設定を取得する
B. システムログ設定を取得する
C. 構成ログ設定ビュー
D. デバッグログを診断する
Answer: B (メーッセージを残す**)**

最新問題**: 16**
リモートユーザーは、日常業務を遂行するために、プライベートWebサーバー上でホストされているTCPベースのアプリケーションにアクセスする必要があります。リモートユーザーの要件を満たす最も効率的かつ安全な方法は、FortiSASEの導入事例の中でどれでしょうか？
A. SD-WAN プライベートアクセス
B. インラインCASB
C. ゼロトラストネットワークアクセス (ZTNA) プライベートアクセス
D. 次世代ファイアウォール (NGFW)
Answer: C (メーッセージを残す**)**
ゼロトラストネットワークアクセス（ZTNA）プライベートアクセスは、リモートユーザーがプライベートWebサーバーでホストされているTCPベースのアプリケーションにアクセスするための、最も効率的かつ安全な方法を提供します。ZTNAは、事前定義されたポリシーに基づいて、認証および承認されたユーザーのみが特定のアプリケーションにアクセスできるようにすることで、セキュリティとアクセス制御を強化します。
* ゼロトラストネットワークアクセス (ZTNA):
* ZTNA は、「決して信頼せず、常に検証する」という原則に基づいて動作し、アクセスを許可する前にユーザーの ID とデバイスのセキュリティ状態を継続的に検証します。
* 特定のアプリケーションへの安全できめ細かなアクセスを提供し、リモート ユーザーがプライベート Web サーバーでホストされている TCP ベースのアプリケーションに安全にアクセスできるようにします。
* 安全で効率的なアクセス:
* ZTNA プライベート アクセスにより、リモート ユーザーは完全な VPN トンネルを必要とせずにアプリケーションに直接接続できるため、遅延が短縮され、パフォーマンスが向上します。
* 許可されたユーザーのみがアプリケーションにアクセスできるようにすることで、強力なセキュリティ制御を実現します。
参考文献:
FortiOS 7.2 管理ガイド: ZTNA とその展開ユースケースに関する詳細情報を提供します。

FortiSASE 23.2 ドキュメント: ZTNA を使用してリモート ユーザーにプライベート アプリケーションへの安全なアクセスを提供する方法について説明します。

最新問題: **17**
FortiSASE でログ設定を構成する際に、効果的なセキュリティ分析のためにキャプチャする必要があるものは何ですか?
応答：
A. 印刷されたすべての文書のログ
B. セキュリティインシデントに関連するエラーおよびイベントログ
C. サーバールームの連続ビデオログ
D. 日常的な操作のデバッグレベルのログ
Answer: B (メーッセージを残す**)**

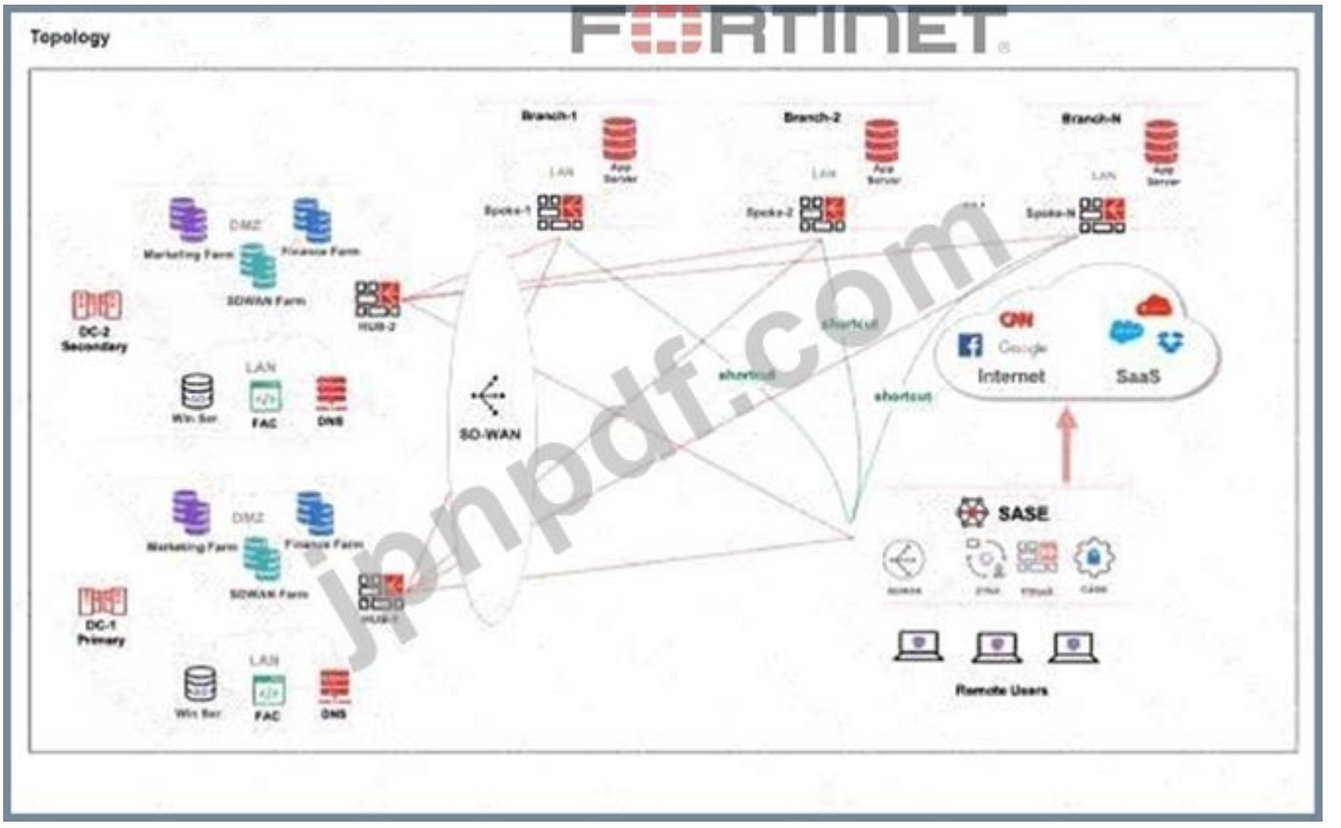
最新問題: **18**
FortiSASE の Digital Experience Monitor (DEM) 機能を最もよく表す記述はどれですか?
A. すべての FortiSASE セキュリティ PoP から特定の SaaS アプリケーションまでのエンドツーエンドのネットワーク可視性を提供します。
B. FortiGuard チームにエンドポイントの詳細な分析を依頼するために使用できます。
C. FortiSASE ポータルから別の DEM エージェントをダウンロードし、エンドポイントにインストールする必要があります。
D. IT チームとセキュリティ チームがリモート ユーザーに対して一貫したセキュリティ監視を確実に実行するのに役立ちます。
Answer: A (メーッセージを残す**)**
FortiSASEのデジタルエクスペリエンスモニター（DEM）機能は、FortiSASEセキュリティPoP（Point of Presence）と特定のSaaSアプリケーション間の接続のパフォーマンスと健全性を監視することで、エンドツーエンドのネットワーク可視性を提供するように設計されています。これにより、管理者は、クラウドベースのサービスへのアクセス時にユーザーエクスペリエンスに影響を与える可能性のある、レイテンシ、ジッタ、パケットロスなどのネットワークパフォーマンス指標に関連する問題を特定し、トラブルシューティングを行うことができます。

最新問題: **19**

FortiSASE でログ設定を構成する際に考慮すべき点は何ですか?
（該当するものをすべて選択してください）
応答：
A. 日常的な操作のデバッグレベルのログ
B. ログローテーション頻度
C. エラーとイベントログ
D. 機密情報のプライバシー設定
Answer: (解答を表示する**)**

最新問題**: 20**
従来の VPN ソリューションと異なる ZTNA の主な機能は何ですか?
応答：
A. デバイスの姿勢チェック
B. ネットワークレベルの暗号化
C. アプリケーションレベルのアクセス制御
D. 永続的なセッション接続
Answer: A,C (メーッセージを残す**)**

最新問題**: 21**
展示物を参照してください。



FortiSASE に接続しているリモート ユーザーが Branch-2 の内部リソースにアクセスする必要がある場合、トラフィックはどのようにルーティングされますか?

A. FortiSASE は SD-WAN 機能を使用して、トラフィックが HUB-2 に送信されるよう決定します。その後、トラフィックは Branch-2 にルーティングされます。

B. FortiSASEはAD VPNプロトコルを使用し、トラフィックが動的ルートを使用してBranch-2に直接送信されることを決定します。

C. FortiSASEはAD VPNプロトコルを使用し、トラフィックが静的ルートを使用してBranch-2に直接送信されることを決定します。

D. FortiSASE は SD-WAN 機能を使用して、トラフィックが HUB-1 に送信されることを決定し、HUB-1 はトラフィックを Branch-2 にルーティングします。

Answer: B (メーッセージを残す**)**

最新問題**: 22**

FortiSASE のどの側面によって、インターネットにアクセスする際にリモート ユーザーのデータが安全に保たれることが保証されますか?

応答：

A. データ損失防止 (DLP)

B. データ損失防止 (DLP)

C. セキュア Web ゲートウェイ (SWG)

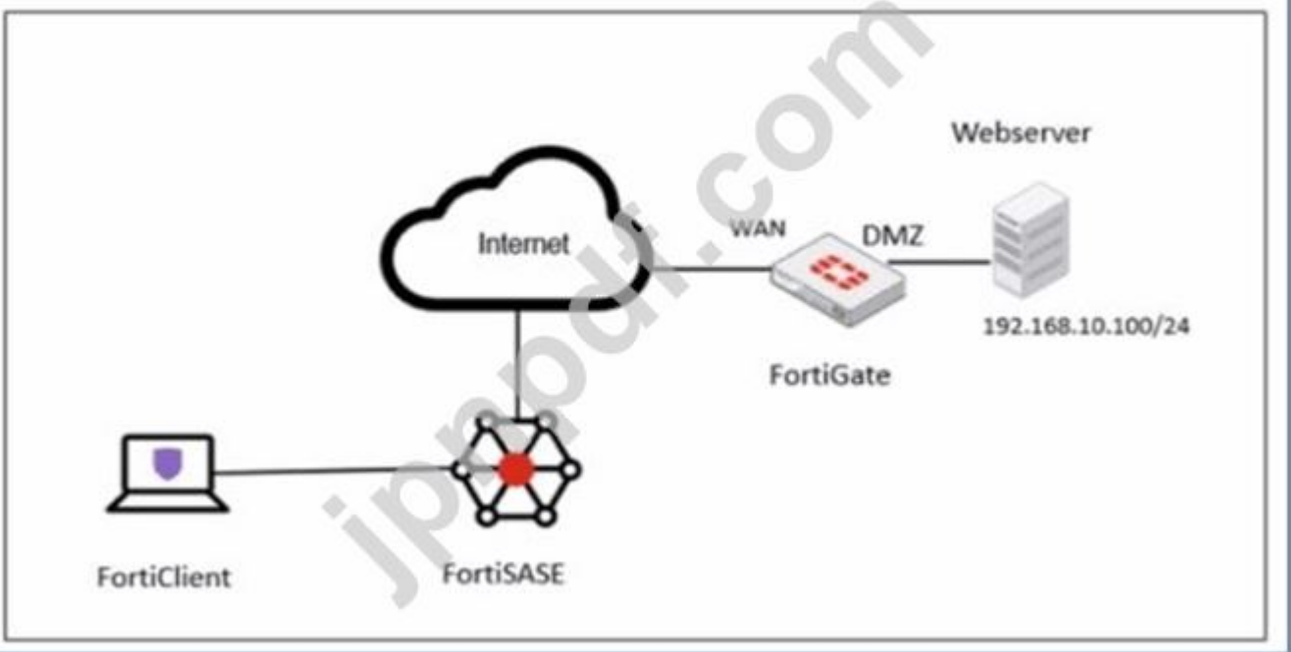
D. セキュアなSD-WAN

Answer: (解答を表示する**)**

最新問題**: 23**

展示物を参照してください。

Network diagram



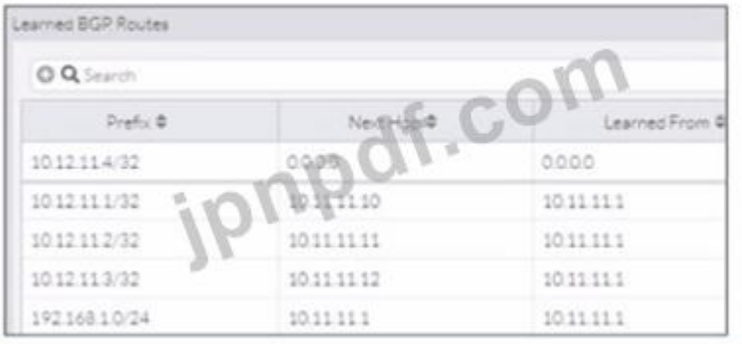
VPN tunnel diagnose output on FortiGate Hub

```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rfc
d=100

parent=SASE index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=s/1
stat: rxp=1667 txp=4583 rxb=278576 txb=108695
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=64916
fec: egress=0 ingress=0
proxyid=SASE proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42025/0B replaywin=1024
       seqno=11cf esn=0 replaywin_lastseq=00000680 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=603df878 esp=aes key=16 2e8932988987c1fdeed9242673bc76f5
       ah=sha1 key=20 01b6c2a13e6cff22796e428c5fb4e4c5262b1a71
  enc: spi=f16ce4a1 esp=aes key=16 90dce5d608caf2714a4f84cff482b557
       ah=sha1 key=20 b60cd0c39489a9f509fe720c0c8e36bb9206f824
  dec:pkts/bytes=3/120, enc:pkts/bytes=2509/285776
  npu_flag=03 npu_rgwy=172.16.10.1 npu_lgwy=172.16.10.101 npu_selid=11 dec_npuid=1 enc_npuid=1
```

Secure Private Access policy on FortiSASE

BGP route information on FortiSASE



Firewall policies on FortiGate Hub

```
# show firewall policy | grep -f SASE
config firewall policy
    edit 5
        set name "vpn_SASE_spoke2hub_0"
        set uuid 01ba85f2-d45c-51ee-5ff9-2035aa36cb3f
        set srcintf "SASE"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "SASE_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 9
        set name "vpn_SASE_spoke2spoke_0"
        set uuid 01eb72ca-d45c-51ee-bd83-bd2feb606cb6
        set srcintf "SASE"
        set dstintf "SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 10
        set name "SASE Health Check"
        set uuid b9573f5c-d45c-51ee-bc11-d5a3143f082a
        set srcintf "SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```


FortiSASE管理者は、FortiSASEをFortiGateハブへのスポークとして設定しようとしています。トンネルはFortiGaleハブまで接続されていますが、管理者はFortiGateハブの背後でホストされているWebサーバーにpingを送信できません。

出力に基づいて、ping 失敗の理由は何ですか?

A. BGPルートが受信されません。

B. スポークツーハブ ポリシーでネットワーク アドレス変換 (NAT) が有効になっていません。

C. Secure Private Access (SPA) ポリシーで PING サービスを許可する必要があります。

D. クイック モード セレクターによってサブネットが制限されています。

Answer: A (メーッセージを残す**)**

最新問題: **24**

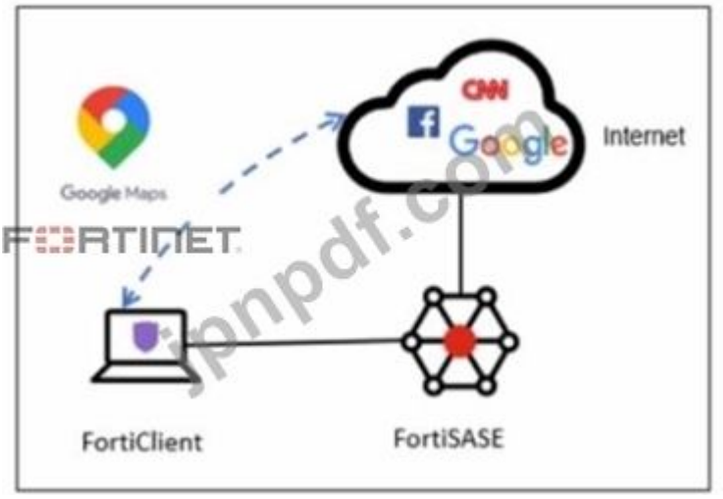
FortiSASE でユーザー デバイスのコンプライアンス チェックのステータスを確認するには、どのコマンドを使用しますか?
応答：
A. デバッグコンプライアンスを診断する
B. コンプライアンス検証を実行する
C. システムのコンプライアンスステータスを取得する
D. コンプライアンスチェックを診断する
Answer: (解答を表示する**)**

最新問題**: 25**
FortiSASE は、ログを表示および分析するときに、どのようにしてユーザー情報を非表示にするのでしょうか?
A. Blowfishを使用してデータをハッシュする
B. ソルトを使ってデータをハッシュ化することで
C. セキュアハッシュアルゴリズム256ビット $HA-256）を使用してデータを暗号化することにより
D. 高度な暗号化規格 (AES) を使用してデータを暗号化することにより
Answer: (解答を表示する**)**
FortiSASEは、ソルトを使用してデータをハッシュ化することで、ログの表示および分析時にユーザー情報を隠蔽します。このアプローチにより、機密性の高いユーザー情報が難読化され、プライバシーとセキュリティが強化されます。
* ソルトを使ったデータのハッシュ化:
* データをハッシュするには、データを固定サイズの文字列 (通常はハッシュ値) に変換します。
* ソルトはハッシュ関数の入力にランダムなデータを追加し、同一の入力であっても異なるハッシュ値が生成されるようにします。
* この方式では、ハッシュ値から元のデータをリバースエンジニアリングすることが困難になるため、セキュリティが強化されます。
* セキュリティとプライバシー:
* ソルト付きハッシュを使用すると、ログに保存または分析されるときにユーザー情報が安全かつプライベートに保たれます。
* この技術は、機密データを不正アクセスから保護するためのセキュリティ システムで広く使用されています。
参考文献:
FortiOS 7.2 管理ガイド: ログ管理とデータ保護技術に関する情報を提供します。
FortiSASE 23.2 ドキュメント: FortiSASE がデータ ハッシュとソルティングを実装してログ内のユーザー情報を保護するための詳細について説明します。

最新問題**: 26**
FortiSASE が企業の非 Web アプリケーションにセキュア プライベート アクセス (SPA) を提供する 3 つの方法はどれですか (3 つ選択してください)。

A. セキュアWebゲートウェイ（SWG）の使用
B. SD-WANテクノロジーの使用
C. デジタルエクスペリエンスモニタリングの使用
D. 次世代ファイアウォール (NGFW) の使用
E. ゼロトラストネットワークアクセス（ZTNA）テクノロジーの使用
Answer: B,D,E (メーッセージを残す**)**

最新問題**: 27**
展示品を参照してください。



ある企業では、FortiSASE 上のすべてのエンドポイント インターネット トラフィックを検査し、FortiSASE VPN トンネルから Google マップ トラフィックを除外してエンドポイントの物理インターフェイスにリダイレクトする必要があります。
この要件を満たすにはどの構成を適用する必要がありますか?
A. エンドポイント システムのプロキシ設定から Google マップの FQDN を除外します。
B. エンドポイントでGoogle Maps FQDNを使用して静的ルートを設定し、トラフィックをリダイレクトします。
C. FortiSASE エンドポイント プロファイルで、Google マップの FQDN をスプリット トンネリングの宛先として設定します。
D. エンドポイント システムの DNS を使用するように、FortiSASE のデフォルトの DNS サーバー構成を変更します。
Answer: C (メーッセージを残す**)**
FortiSASE上のすべてのエンドポイントのインターネットトラフィックを検査しながら、Google マップのトラフィックをFortiSASE VPNトンネルから除外し、エンドポイントの物理インターフェースにリダイレクトするという要件を満たすには、スプリットトンネリングを設定する必要があります。スプリットトンネリングにより、特定のトラフィックがVPNトンネルをバイパスし、エンドポイントのローカルインターフェースに直接ルーティングされます。
スプリットトンネリング構成:
スプリット トンネリングにより、選択したトラフィックを VPN トンネルの外部にルーティングできるようになります。

Google マップの完全修飾ドメイン名 (FQDN) をスプリット トンネリングの宛先として構成すると、Google マップへのトラフィックが VPN トンネルをバイパスし、代わりにエンドポイントのローカル インターフェースを使用するようになります。
実装手順:
FortiSASE エンドポイント プロファイル構成にアクセスします。
Google マップの FQDN をスプリット トンネリングの宛先リストに追加します。
この構成により、Google マップ向けのトラフィックが VPN トンネルをバイパスし、エンドポイントの物理ネットワーク インターフェースを介して直接ルーティングされるようになります。
参照：
FortiOS 7.2 管理ガイド: スプリット トンネリング構成の詳細について説明します。
FortiSASE 23.2 ドキュメント: 特定の宛先に対してスプリット トンネリングを設定および管理する方法について説明します。

最新問題**: 28**
FortiSASE 管理者は、企業の FortiGate とエンドポイント情報を共有するために、Secure Private Access (SPA) ソリューションを構成しています。
このソリューションを実現するには、どの 3 つの構成アクションを実行すればよいですか (3 つ選択してください)。
A. FortiSASE のセキュア プライベート アクセス構成に FortiGate IP アドレスを追加します。
B. 企業のFortiGate上のFortiClient EMSクラウドコネクタを使用してFortiSASEに接続します。
C. FortiGate と FortiSASE を同じ FortiCloud アカウントに登録します。
D. FortiSASE 上の企業 FortiGate を ZTNA アクセス プロキシとして承認します。
E. 企業の FortiGate に FortiSASE ゼロ トラスト ネットワーク アクセス (ZTNA) ライセンスを適用します。
Answer: B,C,D (メーッセージを残す**)**
FortiClient EMS クラウド コネクタ: FortiGate 上のこのコンポーネントにより、FortiSASE と通信し、エンドポイント情報を受信できるようになります。
FortiCloud アカウント: FortiGate と FortiSASE の両方を同じアカウントに登録すると、データを共有し、セキュリティ ポリシーを調整できるようになります。
ZTNA アクセス プロキシ: FortiGate を ZTNA アクセス プロキシとして承認すると、エンドポイント接続の仲介役として機能できるようになり、セキュリティと制御が強化されます。

最新問題**: 29**
FortiSASE ログを分析すると、規制基準への準拠にどのように役立ちますか?
応答：
A. 1日あたりに送信されたメールの数を追跡することで
B. すべてのユーザーのログイン時間と期間を記録することで
C. 娯楽目的のインターネットの使用をすべて記録することで
D. 積極的な脅威検出と対応の証拠を提供することにより
Answer: D (メーッセージを残す**)**

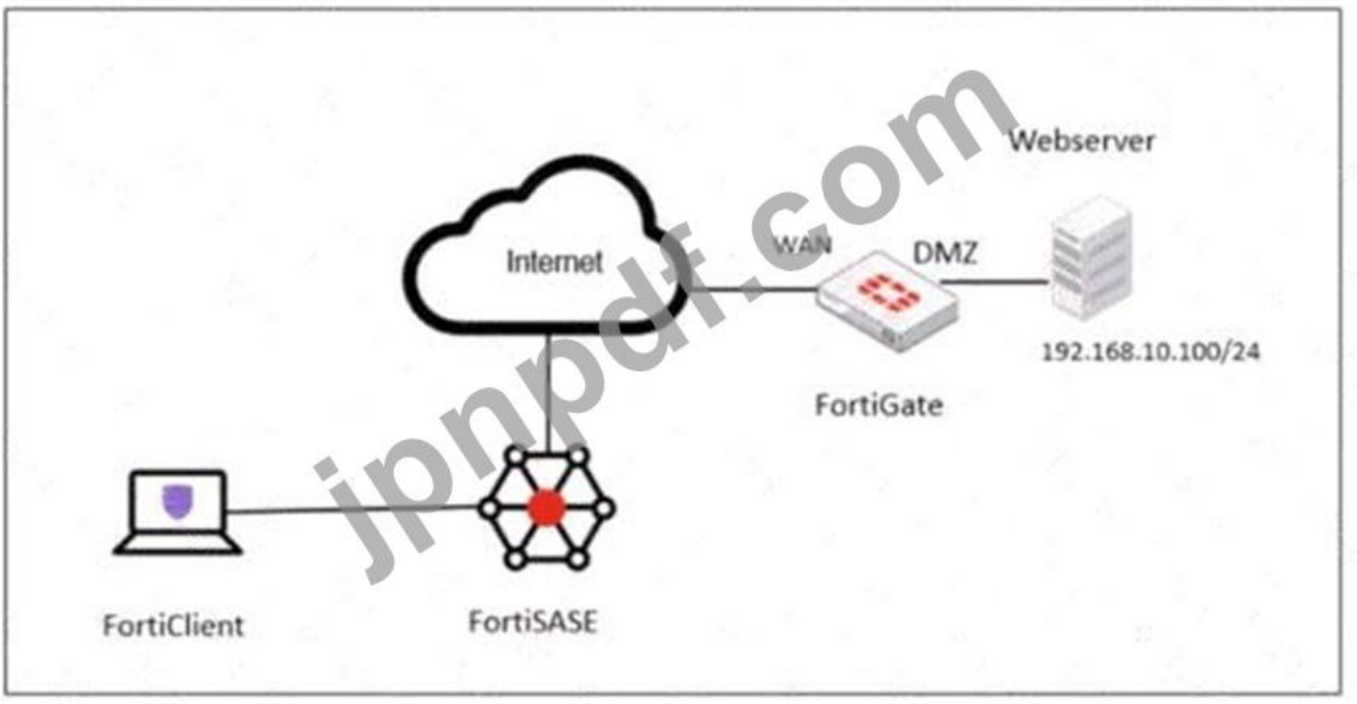
最新問題: **30**
現代のエンタープライズ ネットワークに ZTNA を導入する主な目的は何ですか?
（3つ選択してください）
応答：
A. 安全なリモートアクセスを確保するため
B. ユーザー認証を簡素化するため
C. 攻撃対象領域を最小限に抑える
D. 送信通信のみを監視する
Answer: A,B,C (メーッセージを残す**)**

最新問題: **31**
ゼロトラスト タグを使用する 2 つの利点は何ですか? (2 つ選択してください。)
A. ゼロトラストタグは、ネットワークリソースへのアクセスを許可または拒否するために使用できます。
B. ゼロトラスト タグは、エンドポイントのセキュリティ体制を判断できます。
C. ゼロトラストタグを使用すると、異なるエンドポイントに適用できる複数のエンドポイントプロファイルを作成できます。
D. ゼロトラストタグはセキュアWebゲートウェイ（SWG）アクセスを許可するために使用できます。
Answer: A,B (メーッセージを残す**)**
ゼロトラストタグは、ゼロトラストネットワークアクセス（ZTNA）ポリシーの実装に不可欠です。
ゼロトラストタグを使用する主なメリットは以下の2つです。
アクセス制御（許可または拒否）:
ゼロトラスト タグを使用すると、ユーザーまたはデバイスに関連付けられたタグに基づいて、特定のネットワーク リソースへのアクセスを許可または拒否するポリシーを定義できます。
このきめ細かな制御により、適切なタグを持つ承認されたユーザーまたはデバイスのみが機密リソースにアクセスできるようになるため、セキュリティが強化されます。
セキュリティ態勢の決定:
ゼロトラスト タグは、エンドポイントのセキュリティ体制を評価および判断するために利用できます。
割り当てられたタグに基づいて、FortiSASE は、ウイルス対策ステータス、パッチ レベル、構成設定などのセキュリティ ポリシーに対するデバイスのコンプライアンスを評価できます。
必要なセキュリティ体制を満たしていないデバイスは、ネットワークへのアクセスを制限されたり、アクセスが制限されたりすることがあります。
参照：
FortiOS 7.2 管理ガイド: アクセス制御とセキュリティ態勢評価のためのゼロトラスト タグの構成と使用に関する詳細情報を提供します。
FortiSASE 23.2 ドキュメント: セキュリティとコンプライアンスを強化するために、ゼロ トラスト タグを FortiSASE 環境内で実装および使用する方法について説明します。

最新問題: **32**

展示物を参照してください。

Network diagram



VPN tunnel diagnose output on FortiGate Hub

```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rfc
d=100

parent=SASE index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=s/1
stat: rxp=1667 txp=4583 rxb=278576 txb=108695
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=64916
fec: egress=0 ingress=0
proxyid=SASE proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42025/0B replaywin=1024
       seqno=11cf esn=0 replaywin_lastseq=00000680 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=683df878 esp=aes key=16 2e8932908987c1fdeed9242673bc76f5
       ah=sha1 key=20 01b6c2a13e6cff22796e428c5fb4e4c5262b1a71
  enc: spi=f16ce4a1 esp=aes key=16 90dce5d608caf2714a4f84cff482b557
       ah=sha1 key=20 b60cd0c39489a9f509fe720c0c8e36bb9206f824
  dec:pkts/bytes=3/120, enc:pkts/bytes=2509/285776
  npu_flag=03 npu_rgwy=172.16.10.1 npu_lgwy=172.16.10.101 npu_selid=11 dec_npuid=1 enc_npuid=1
```

Secure Private Access policy on FortiSASE

BGP route information on FortiSASE

Learned BGP Routes

Search

Prefix	Next Hop	Learned From
10.12.114.32	0.0.0.0	0.0.0.0
10.12.111.32	10.11.1.10	10.11.111
10.12.112.32	10.11.11.11	10.11.111
10.12.113.32	10.11.11.12	10.11.111
192.168.10.24	10.11.111	10.11.111

Firewall policies on FortiGate Hub

```
# show firewall policy | grep -f SASE
config firewall policy
    edit 5
        set name "vpn_SASE_spoke2hub_0"
        set uuid 01ba85f2-d45c-51ee-5ff9-2035aa36cb3f
        set srcintf "SASE"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "SASE_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 9
        set name "vpn_SASE_spoke2spoke_0"
        set uuid 01eb72ca-d45c-51ee-bd83-bd2feb606cb6
        set srcintf "SASE"
        set dstintf "SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 10
        set name "SASE Health Check"
        set uuid b9573f5c-d45c-51ee-bc11-d5a3143f082a
        set srcintf "SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

FortiSASE管理者は、FortiSASEをFortiGateハブへのスポークとして設定しようとしています。トンネルはFortiGaleハブまで接続されていますが、管理者はFortiGateハブの背後でホストされているWebサーバーにpingを送信できません。
出力に基づいて、ping 失敗の理由は何ですか?
A. スポークツーハブ ポリシーでネットワーク アドレス変換 (NAT) が有効になっていません。
B. BGPルートが受信されません。
C. クイック モード セレクターによってサブネットが制限されています。
D. Secure Private Access (SPA) ポリシーで PING サービスを許可する必要があります。
Answer: (解答を表示する**)**

最新問題**: 33**
お客様は、保護対象サーバーへのアクセス時にリモートエンドポイントのデバイスポスチャチェックを実装する必要があります。また、リモートエンドポイントと保護対象サーバー間のTCPトラフィックをFortiGateで処理することも希望しています。
このシナリオでは、どの 3 つの設定が上記の要件を満たしますか? (3 つ選択してください。)
A. FortiGate で ZTNA サーバーと ZTNA ポリシーを構成します。
B. ZTNA を使用して FortiSASE でプライベート アクセス ポリシーを構成します。
C. FortiGate で ZTNA タグを設定します。
D. FortiGate をゼロ トラスト ネットワーク アクセス (ZTNA) アクセス プロキシとして構成します。
E. ZTNA タグを FortiSASE から FortiGate に同期します。
Answer: A,D,E (メーッセージを残す**)**
参考文献:
Fortinet FCSS FortiSASE ドキュメント - ゼロトラストネットワークアクセス (ZTNA) の導入
FortiGate 管理ガイド - ZTNA 構成

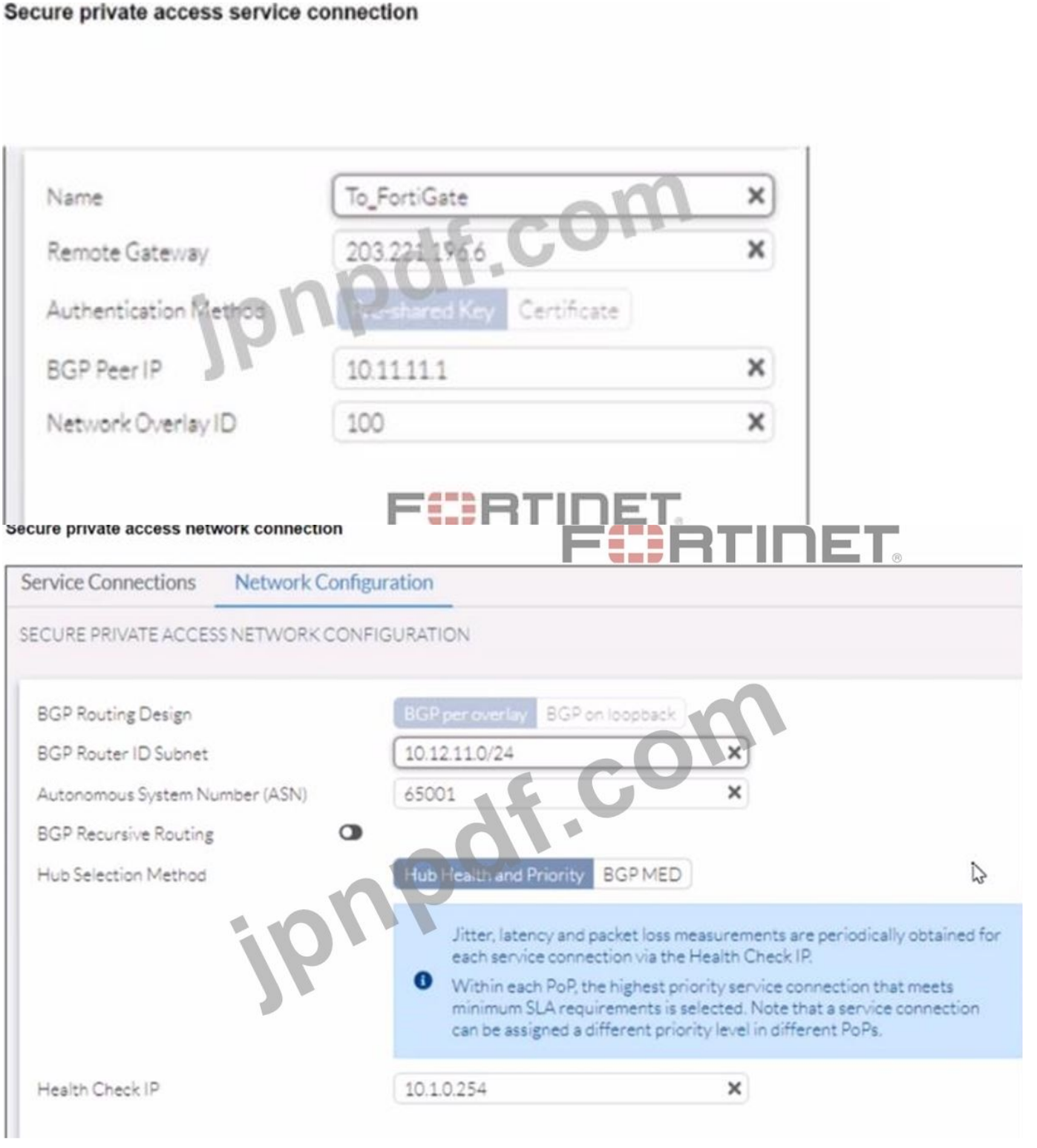
最新問題**: 34**
FortiSASEはゼロトラストネットワークアクセス（ZTNA）の原則をサポートする上でどのような役割を果たしますか？9
A. ネットワークセグメンテーション用のハードウェアベースのファイアウォールを提供します。
B. ソフトウェア定義ネットワーク (SDN) ソリューションと統合します。
C. セキュリティ ポスチャ チェックのためにエンドポイント上の属性を識別できます。
D. リモート従業員の VPN 接続を有効にします。
Answer: C (メーッセージを残す**)**
FortiSASEは、セキュリティポスチャチェックのためにエンドポイントの属性を識別することで、ゼロトラストネットワークアクセス（ZTNA）の原則をサポートします。ZTNAの原則では、ネットワークリソースへのアクセスを許可する前に、ユーザーとデバイスの認証情報、およびセキュリティポスチャを継続的に検証することが求められます。
* セキュリティ態勢チェック:

* FortiSASE は、ウイルス対策ステータス、パッチ レベル、構成設定などのセキュリティ ポリシーへの準拠をチェックすることで、エンドポイントのセキュリティ状況を評価できます。
* これにより、準拠した安全なデバイスのみがネットワークへのアクセスを許可されるようになります。
* ゼロトラストネットワークアクセス (ZTNA):
* ZTNA は、「決して信頼せず、常に検証する」という原則に基づいており、ユーザーとデバイスの信頼性を継続的に評価する必要があります。
* FortiSASE は、これらのセキュリティ ポスチャ チェックを実行し、アクセス制御ポリシーを適用することで、ZTNA の実装に重要な役割を果たします。
参考文献:
FortiOS 7.2 管理ガイド: ZTNA およびエンドポイント セキュリティ ポスチャ チェックに関する情報を提供します。
FortiSASE 23.2 ドキュメント: FortiSASE が ZTNA 原則を実装する方法の詳細。

最新問題**: 35**
FortiSASEによって生成された日次サマリーレポートを閲覧した際、管理者はレポートにデータが非常に少ないことに気付きました。このほとんど空のレポートの原因は何でしょうか？
A. デジタル エクスペリエンス モニタリングが構成されていません。
B. すべてのポリシーで、許可されたトラフィックのログがセキュリティ イベントに設定されています。
C. Webフィルタセキュリティプロファイルが監視に設定されていません
D. すべてのポリシーに適用されているセキュリティ プロファイル グループはありません。
Answer: B (メーッセージを残す**)**
FortiSASEによって生成される日次サマリーレポートにデータが非常に少ない場合、「許可されたトラフィックのログ」設定が、すべてのポリシーにおいて「セキュリティイベント」のみを記録するように設定されていることが考えられます。この設定では、セキュリティイベントのみが記録され、通常の許可されたトラフィックは記録されないため、記録されるデータの量が制限されます。
* 許可されたトラフィックのログ設定:
* 「許可されたトラフィックをログに記録する」設定により、ログに記録されるトラフィックの種類が決まります。
* 「セキュリティ イベント」に設定すると、セキュリティ イベント (脅威の検出やポリシー違反など) をトリガーするトラフィックのみが記録されます。
* レポートデータへの影響:
* ログ設定で定期的に許可されるトラフィックを除外すると、キャプチャおよびレポートされるデータの量が大幅に削減されます。
* セキュリティ関連のイベントのみが含まれるため、レポートには最小限のデータが含まれた状態になります。
参考文献:
FortiOS 7.2 管理ガイド: トラフィック ポリシーのログ設定の構成に関する詳細を説明します。

FortiSASE 23.2 ドキュメント: ログ記録構成がレポート生成とデータの可視性に与える影響を説明します。

最新問題: **36**
展示物を参照してください。



Firewall policy configuration

```
config firewall policy
    edit 5
        set name "Spoke-to-Spoke"
        set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
        set srcintf "To_SASE"
        set dstintf "To_SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
    edit 6
        set name "Lo-BGP-HC"
        set uuid f5a12c92-216b-51ee-4802-8ccd013d6acf
        set srcintf "To_SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
    edit 9
        set name "Spoke-to-Hub"
        set uuid 617b81ee-cc64-51ee-8da6-6cdff3ca2cca
        set dstintf "internal3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

```
# show vpn ipsec phase1-interface To_SASE
 config vpn ipsec phase1-interface
    edit "To_SASE"
        set type dynamic
        set interface "wan1"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: To_SASE (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable
        set ipv4-start-ip 10.11.11.10
        set ipv4-end-ip 10.11.11.200
        set ipv4-netmask 255.255.255.0
        set unity-support disable
        set psksecret ENC SblOigpvIFFYSpRZ/hyxQVUXv9NZm7uqltD9v+BViPd+7RWizmUA3ZINn0zbsxq70F
  iYkPLkxaNwIo7VLlipkye1xt84NAwEfm5jTqqf1dMj/phYvBI3hzU0yXq==
    next
 end

# show vpn ipsec phase2-interface To_SASE
config vpn ipsec phase2-interface
    edit "To_SASE"
        set phase1name "To_SASE"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
 end
```

BGP protocol configuration

```
#config router bgp
     set as 65001
     set router-id 10.1.0.254
     config neighbor
         edit "10.10.1.3"
             set advertisement-interval 1
             set ebgp-enforce-multihop enable
             set link-down-failover enable
             set remote-as 65001
             set route-reflector-client enable
         next
     end
     config neighbor-group
         edit "To_SASE"
             set capability-graceful-restart enable
             set link-down-failover enable
             set next-hop-self enable
             set interface "To_SASE"
             set remote-as 65001
             set additional-path both
             set adv-additional-path 4
             set route-reflector-client enable
         next
     end
     config neighbor-range
         edit 1
             set prefix 10.11.11.0 255.255.255.0
             set neighbor-group "To_SASE"
         next
     end
     config network
         edit 1
             set prefix 10.190.190.0 255.255.255.0
         next
     end
```

FortiSASE管理者がFortiSASEをFortiGateハブへのスポークとして設定しようとしています。VPNトンネルが確立されません。提供された設定に基づいて、トンネルを確立するにはどのような設定を変更する必要がありますか？

A. FortiSASE スポーク デバイスはモード構成をサポートしていません。

B. Spoke-to-Hub ファイアウォール ポリシーで NAT を有効にする必要があります。

C. ハブでは、IPsec フェーズ 1 設定で IKEv2 を有効にする必要があります。

D. BGP ルーター ID は、ハブと FortiSASE で一致する必要があります。

Answer: C (メーッセージを残す**)**

最新問題**: 37**

FortiSASE のどの機能を使用して、Software-as-a-Service (SaaS) アプリケーションのリストと、FortiSASE インスタンス用にプロビジョニングされた地理的なプレゼンス ポイント (PoP) と

これらの SaaS アプリケーション間のファースト マイル接続のヘルスチェック メトリックを表示できますか。
応答：
A. イベントログ
B. セキュリティログ
C. フォルティビュー
D. デジタルエクスペリエンスモニタリングDEM
Answer: D (メーッセージを残す**)**

最新問題**: 38**
セキュア Web ゲートウェイ (SWG) エンドポイントのオンボーディングに含まれる 2 つのコンポーネントはどれですか (2 つ選択してください)。
A. FortiSASE CA証明書
B. プロキシ自動構成 (PAC) ファイル
C. FortiSASE招待コード
D. FortiClientインストーラー
Answer: A,B (メーッセージを残す**)**
セキュアWebゲートウェイ（SWG）エンドポイントのオンボーディングには、FortiSASEとの安全かつ効果的な統合を確保するための複数のコンポーネントが含まれます。主要なコンポーネントは、FortiSASE CA証明書とプロキシ自動構成（PAC）ファイルです。
* FortiSASE CA 証明書:
* FortiSASE CA 証明書は、エンドポイントと FortiSASE インフラストラクチャ間の信頼を確立するために不可欠です。
* エンドポイントがFortiSASEサービスと安全に通信し、SSLを検査できることを保証します。/TLS トラフィック。
* プロキシ自動構成 (PAC) ファイル:
* PAC ファイルは、Web トラフィックを FortiSASE プロキシ経由で送信するようにエンドポイントを構成するために使用されます。
* トラフィックをルーティングする方法に関する指示を提供し、すべての Web 要求が FortiSASE によって適切に検査およびフィルタリングされるようにします。
参考文献:
FortiOS 7.2 管理ガイド: エンドポイントのオンボーディングと SWG の構成の詳細。
FortiSASE 23.2 ドキュメント: エンドポイントを FortiSASE と統合するために必要なコンポーネントと、CA 証明書および PAC ファイルを展開するプロセスについて説明します。

最新問題**: 39**
セキュア プライベート アクセス (SPA) のユースケースでは、FortiSASE のどの 2 つの機能が企業アプリケーションへのアクセスを容易にしますか (2 つ選択してください)。
A. SD-WAN
B. ゼロトラストネットワークアクセス (ZTNA)

C. 細いエッジ
D. クラウド アクセス セキュリティ ブローカー (CASB)
Answer: A,B (メーッセージを残す**)**

最新問題**: 40**
エンドポイント検出および応答 (EDR) システムを SASE に統合すると、セキュリティ体制にどのように貢献しますか?
応答：
A. ネットワークをインターネットから分離します
B. エンドポイントでリアルタイムの脅威検出と対応を提供します
C. プライマリファイアウォールとして機能します
D. ユーザーインターフェースのデザインを強化します
Answer: B (メーッセージを残す**)**

最新問題**: 41**
現在、貴社ではサイバーセキュリティ対策としてFortiSASEを使用しています。最近、本社オフィスで勤務する契約社員を雇用しましたが、WebベースのPOSシステム導入のため、一時的なインターネットアクセスが必要になりました。
請負業者にインターネット アクセスを提供するための推奨される方法は何ですか?
A. エンドポイントで FortiClient を使用してインターネット アクセスを管理します。
B. プロキシ自動構成 (PAC) ファイルを使用し、明示的な Web プロキシとしてセキュア Web ゲートウェイ (SWG) サービスを提供します。
C. ゼロ トラスト ネットワーク アクセス (ZTNA) を使用し、クライアントを管理対象外エンドポイントとしてタグ付けします。
D. インターネットへのアクセスを提供するために、FortiSASE で VPN ポリシーを構成します。
Answer: C (メーッセージを残す**)**
請負業者に一時的なインターネットアクセスを提供する推奨方法は、ゼロトラストネットワークアクセス（ZTNA）を使用し、クライアントを管理対象外エンドポイントとしてタグ付けすることです。ZTNAは、すべてのエンドポイントをデフォルトで信頼できないものとして扱いながら、承認されたユーザーとデバイスのみが特定のリソースにアクセスできるようにします。請負業者のデバイスを管理対象外エンドポイントとしてタグ付けすることで、厳格なアクセス制御を適用し、請負業者が必要なリソース（例WebベースのPOSシステム）のみにアクセスできるように制限することで、社内ネットワークを不必要なリスクにさらすことなく、アクセスを制限できます。
他のオプションがあまり適していない理由は次のとおりです。
A. エンドポイントでFortiClientを使用してインターネットアクセスを管理します。FortiClientはエンドポイントのセキュリティと管理機能を提供しますが、契約者のデバイスにインストールと設定を行う必要があります。これは、一時的な契約者や管理対象外のデバイスでは実現できない可能性があります。
B. プロキシ自動設定（PAC）ファイルを使用し、明示的なWebプロキシとしてセキュアWebゲートウェイ（SWG）サービスを提供する :このアプローチはWebトラフィックを制御できますが、ZTNA

が提供するきめ細かなアクセス制御とセキュリティポスチャ検証は提供されません。さらに、PACファイルの管理は煩雑で、ZTNAに比べて安全性が低くなる可能性があります。
D. FortiSASEでインターネットアクセスを提供するためのVPNポリシーを設定する :VPNポリシーを使用すると、ネットワークへのアクセス権が拡大するため、臨時契約社員には適していません。社内リソースへの不正アクセスのリスクが高まり、最小権限の原則にも反します。
参照：
Fortinet FCSS FortiSASE ドキュメント - ゼロトラストネットワークアクセス (ZTNA) のユースケース FortiSASE 管理ガイド - 管理対象外エンドポイントの管理

最新問題**: 42**
FortiSASE の FortiGuard フォレンジック分析機能について説明している記述はどれですか。
A. ユーザーからアプリケーションへのパフォーマンスの問題のトラブルシューティングに役立ちます。
B. 顧客がネットワークに対する潜在的なリスクを特定し、軽減するのに役立ちます。
C. エンドポイント リソースをリアルタイムで監視できます。
D. FortiSASE 環境を 24 時間 365 日監視するサービスです。
Answer: B (メーッセージを残す**)**
FortiSASEのFortiGuardフォレンジック分析機能は、お客様がネットワークへの潜在的なリスクを特定し、軽減できるよう設計されています。この機能は、FortiSASEによって検出された不審なアクティビティ、脅威、異常に関する詳細な情報を提供します。ログ、トラフィックパターン、脅威インテリジェンスを分析することで、管理者はインシデントを調査し、根本原因を理解し、ネットワークを保護するためのプロアクティブな対策を講じることができます。
他のオプションが間違っている理由は次のとおりです。
* A. ユーザーからアプリケーションへのパフォーマンスの問題のトラブルシューティングに役立ちます。パフォーマンスのトラブルシューティングは通常、フォレンジック分析ではなく、デジタル エクスペリエンス モニタリング (DEM) やアプリケーション パフォーマンス モニタリング ツールなどの機能によって処理されます。
* C. エンドポイント リソースをリアルタイムで監視できます。リアルタイムのエンドポイント監視は、FortiGuard フォレンジック分析ではなく、FortiClient や FortiEDR などのエンドポイント セキュリティ ソリューションの機能です。
* D. FortiSASE環境の24時間365日監視サービスです。フォーティネットは継続的な監視のためのマネージドサービスを提供していますが、FortiGuardフォレンジック分析は専用の監視サービスではありません。インシデント後の調査とリスク軽減に重点を置いています。
参考文献:
Fortinet FCSS FortiSASE ドキュメント - FortiGuard フォレンジック分析
FortiSASE 管理ガイド - 脅威の検出と対応

最新問題**: 43**
FortiSASE 管理者は、企業の FortiGate とエンドポイント情報を共有するために、Secure Private Access (SPA) ソリューションを構成しています。

このソリューションを実現するには、どの 3 つの構成アクションを実行すればよいですか (3 つ選択してください)。
A. FortiSASE のセキュア プライベート アクセス構成に FortiGate IP アドレスを追加します。
B. 企業のFortiGate上のFortiClient EMSクラウドコネクタを使用してFortiSASEに接続します。
C. FortiGate と FortiSASE を同じ FortiCloud アカウントに登録します。
D. FortiSASE 上の企業 FortiGate を ZTNA アクセス プロキシとして承認します。
E. 企業の FortiGate に FortiSASE ゼロ トラスト ネットワーク アクセス (ZTNA) ライセンスを適用します。
Answer: (解答を表示する**)**
参考文献:
FortiOS 7.2 管理ガイド: セキュア プライベート アクセスの構成と FortiGate との統合に関する詳細を説明します。
FortiSASE 23.2 ドキュメント: FortiSASE と企業の FortiGate 間の接続を設定および管理する方法について説明します。

最新問題**: 44**
個々のエンドポイント構成を最小限に抑えるセキュア インターネット アクセス (SIA) ユースケースはどれですか?
A. サイトベースのリモートユーザーインターネットアクセス
B. エージェントレスリモートユーザーインターネットアクセス
C. SSL VPNリモートユーザー用のSIA
D. ZTNA を使用した SIA
Answer: B (メーッセージを残す**)**
エージェントレスのリモートユーザーによるインターネットアクセスのユースケースは、個々のエンドポイント設定を最小限に抑えるように設計されています。このシナリオでは、FortiSASEはエンドポイントデバイスにエージェントをインストールすることなく、安全なインターネットアクセスを提供します。このアプローチは、各エンドポイントで複雑な設定を行う必要がないため、管理対象外のデバイスや一時的なユーザーが存在する環境に特に有効です。セキュリティポリシーはネットワークレベルで適用され、エンドポイント固有のソフトウェアに依存することなく、一貫した保護を実現します。

最新問題**: 45**
セキュア プライベート アクセス (SPA) と SD-WAN を使用する場合、スポーク間接続にはどのプロトコルが使用されますか?
応答：
A. IPSEC
B. SSL
C. ゴー
D. eBGP
Answer: (解答を表示する**)**

最新問題: **46**
デフォルト設定の FortiSASE 展開で、FortiSASE から FortiClient に自動的にプッシュされる 2 つの設定はどれですか (2 つ選択してください)。
A. SSL VPNプロファイル
B. FortiSASE CA証明書
C. リアルタイム保護
D. ZTNAタグ
Answer: A,C (メーッセージを残す**)**

最新問題: **47**
FortiSASE のセキュア インターネット アクセス (SIA) は、セキュリティ ポリシーの遵守にどのような利点をもたらしますか?
応答：
A. すべてのユーザーに対してセキュリティポリシーを一貫して適用する
B. すべてのネットワークデバイスの自動更新
C. リモートユーザーのネットワーク速度の向上
D. ユーザーセッションの集中管理
Answer: A (メーッセージを残す**)**

最新問題: **48**
FortiSASEによって生成された日次サマリーレポートを閲覧した際、管理者はレポートにデータが非常に少ないことに気付きました。このほとんど空のレポートの原因は何でしょうか？
A. デジタル エクスペリエンス モニタリングが構成されていません。
B. すべてのポリシーで、許可されたトラフィックのログがセキュリティ イベントに設定されています。
C. Webフィルタセキュリティプロファイルが監視に設定されていません
D. すべてのポリシーに適用されているセキュリティ プロファイル グループはありません。
Answer: (解答を表示する**)**
FortiSASEによって生成される日次サマリーレポートにデータが非常に少ない場合、許可されたトラフィックのログ」設定が、すべてのポリシーにおいて セキュリティイベント」のみを記録する

ように設定されていることが考えられます。この設定では、セキュリティイベントのみが記録され、通常の許可されたトラフィックは記録されないため、記録されるデータの量が制限されます。
許可されたトラフィックのログ設定:
「許可されたトラフィックをログに記録する」設定では、ログに記録されるトラフィックの種類を決定します。
「セキュリティ イベント」に設定すると、セキュリティ イベント (脅威の検出やポリシー違反など) をトリガーするトラフィックのみが記録されます。
レポートデータへの影響:
ログ設定で定期的に許可されるトラフィックを除外すると、キャプチャおよびレポートされるデータの量が大幅に削減されます。
これにより、セキュリティ関連のイベントのみが含まれるため、最小限のデータのレポートが作成されます。
参照：
FortiOS 7.2 管理ガイド: トラフィック ポリシーのログ設定の構成に関する詳細を説明します。
FortiSASE 23.2 ドキュメント: ログ記録構成がレポート生成とデータの可視性に与える影響を説明します。

最新問題**: 49**
FortiGate を FortiSASE LAN 拡張機能として設定するには、どの 3 つの構成を実行する必要がありますか? (3 つ選択してください。)
A. FortiSASE ポータルでエッジ FortiGate デバイスを承認します。
B. アクセス コントローラのアドレスとして、FortiGate GUI に FortiSASE ドメイン名を入力します。
C. FortiSASEポータルでVXLAN-over-IPsecを設定する
D. エッジFortiGateにLAN拡張VDOMを作成する
E. FortiZTP を使用して FortiGate を FortiSASE に接続します。
Answer: A,B,D (メーッセージを残す**)**

最新問題**: 50**
FortiSASE を使用してリモート ワーカーのセキュリティを確保する場合、何を優先すべきでしょうか?
（該当するものをすべて選択してください）
応答：
A. すべての通信の暗号化
B. MFA（多要素認証の実装
C. ユーザーアクティビティの継続的な監視
D. 専用ハードウェアファイアウォールの導入
Answer: A,B,C (メーッセージを残す**)**

最新問題**: 51**

X 社向けに新しいネットワークを設計していますが、新しいサイバーセキュリティ ポリシーの要件の 1 つとして、すべてのリモート ユーザーのエンドポイントを常に接続して保護する必要があることが挙げられます。この常時セキュリティ対策を容易にする FortiSASE コンポーネントはどれですか。

A. サイトベースの展開

B. シンブランチSASE拡張

C. 統合FortiClient

D. インラインCASB

Answer: C (メーッセージを残す**)**

FortiSASE の統合された FortiClient コンポーネントは、すべてのリモート ユーザー エンドポイントが常に接続され、保護されていることを保証するために必要な常時セキュリティ対策を容易にします。

統合FortiClient:

FortiClient は、FortiSASE と統合してリモート ユーザーのエンドポイントを継続的に保護する包括的なエンドポイント セキュリティ ソリューションです。

これにより、ユーザーが企業ネットワークから離れている場合でも、エンドポイントが常に FortiSASE インフラストラクチャに接続されるようになります。

常時セキュリティ:

統合された FortiClient は FortiSASE への永続的な接続を維持し、セキュリティ ポリシーを適用してエンドポイントを常に脅威から保護します。

これにより、リモート ユーザーに対する継続的な接続と保護を要求するサイバーセキュリティ ポリシーへの準拠が保証されます。

参照：

FortiOS 7.2 管理ガイド: エンドポイント セキュリティ用の FortiClient の構成と管理に関する情報を提供します。

FortiSASE 23.2 ドキュメント: FortiClient が FortiSASE と統合され、リモート エンドポイントに常時セキュリティを提供する方法について説明します。