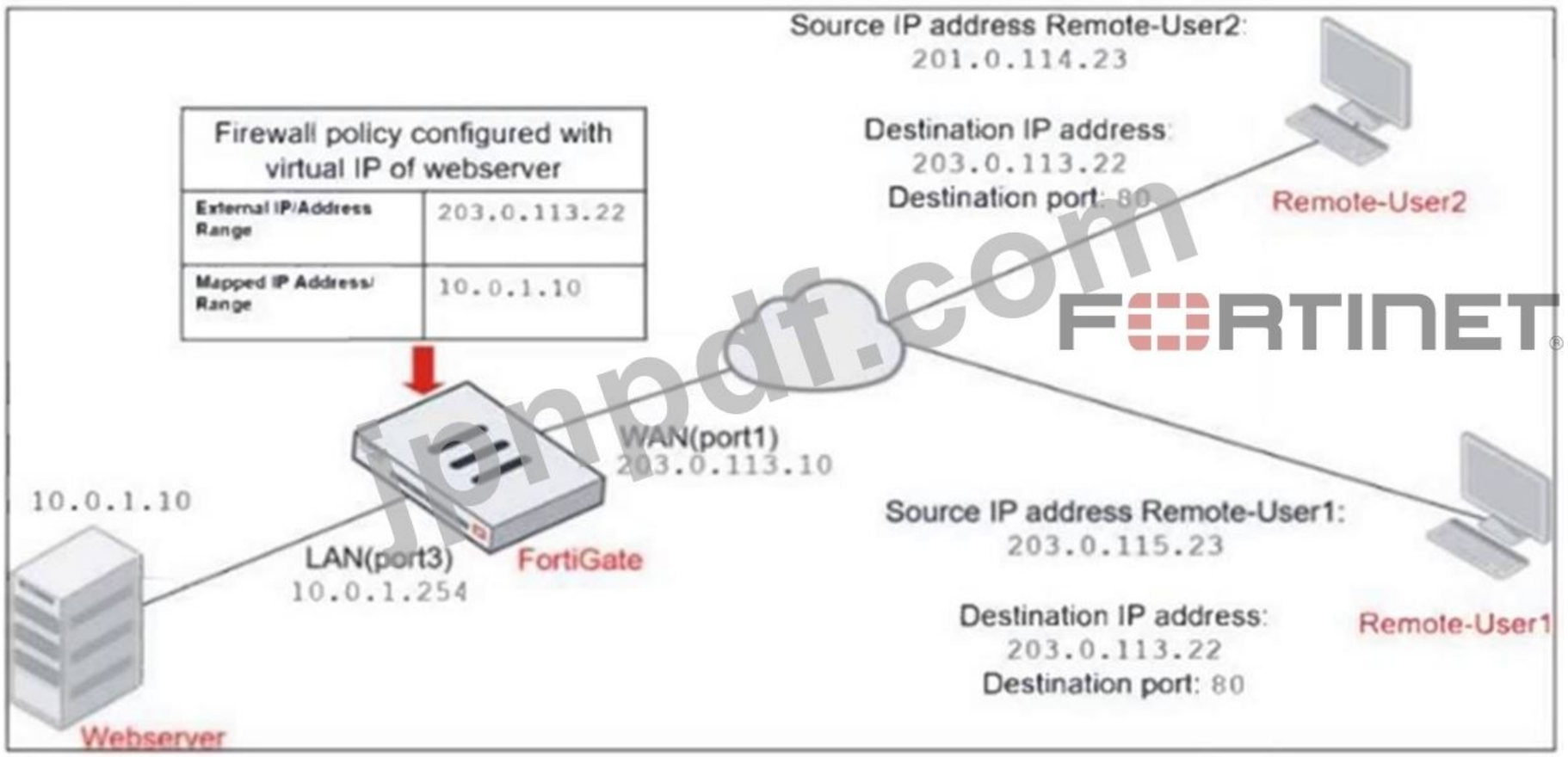
Fortinet.FCP_FGT_AD-7.4-JPN.v2025-05-19.q40

試験コード:	FCP_FGT_AD-7.4-JPN
試験名称:	FCP - FortiGate 7.4 Administrator (FCP_FGT_AD-7.4日本語版)
認定資格:	Fortinet
無料問題数:	40
バージョン:	v2025-05-19
アクセス数:	338
ページビュー数:	400
https://www.jpnpdf.com/Fortinet.FCP_FGT_AD-7.4-JPN.v2025-05-19.q40-mondaishu.html	

最新問題: **1**
展示品を参照してください。

Network diagram



展示品には、ネットワークに接続された FortiGate デバイスの図とファイアウォールの構成が示されています。
管理者は、Remote-User2 の Web サーバー アクセスを拒否するデフォルト設定の拒否ポリシーを作成しました。
このポリシーは、Remote-User1 が Web サーバーにアクセスできるようにし、Remote-User2 が Web サーバーにアクセスできないようにするように機能する必要があります。
管理者は、Remote-User2 の Web サーバー アクセスを拒否するために、ポリシーに対してどの 2 つの構成変更を行うことができますか? (2 つ選択してください。)
A. 拒否ポリシーで match-vip を有効にします。
B. 拒否ポリシーで宛先アドレスを Web サーバーとして設定します。
C. 拒否ポリシーで match-vip を無効にします。
D. Allow_access ポリシーで宛先アドレスを Deny_IP として設定します。
Answer: A,B (メーッセージを残す)
To deny access to the web server for Remote-User2 while allowing Remote-User1 to access the same web server, two configuration changes can be made:

Enable match-vip in the Deny policy:
By enabling the match-vip option in the Deny policy, the FortiGate will check for virtual IP (VIP) objects during policy matching. This setting allows the firewall policy to correctly identify and block traffic directed to a specific mapped IP address, such as the web server, when using a VIP configuration.
Set the Destination address as Webserver in the Deny policy:
Setting the Destination address to "Webserver" in the Deny policy ensures that the policy specifically targets traffic attempting to reach the web server. This configuration helps to precisely control which traffic should be blocked, focusing the Deny policy on the intended destination.
Reference:
FortiOS 7.4.1 Administration Guide: Deny matching with a policy with a virtual IP applied FortiOS 7.4.1 Administration Guide: Configuring Policies with VIPs

最新問題: 2
マルチ VDOM 環境でのセキュリティ ファブリックの展開に関する次の記述のうち正しいものはどれですか。
A. ダウンストリームデバイスは、どのVDOMからでもアップストリームデバイスに接続できます。
B. 環境内の各VDOMは、異なるセキュリティファブリックの一部になることができます。
C. デバイスが接続されたポートのない VDOM はトポロジに表示されません
D. セキュリティ評価レポートは、構成されたVDOMごとに個別に実行できます。
Answer: C (メーッセージを残す**)**
"When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

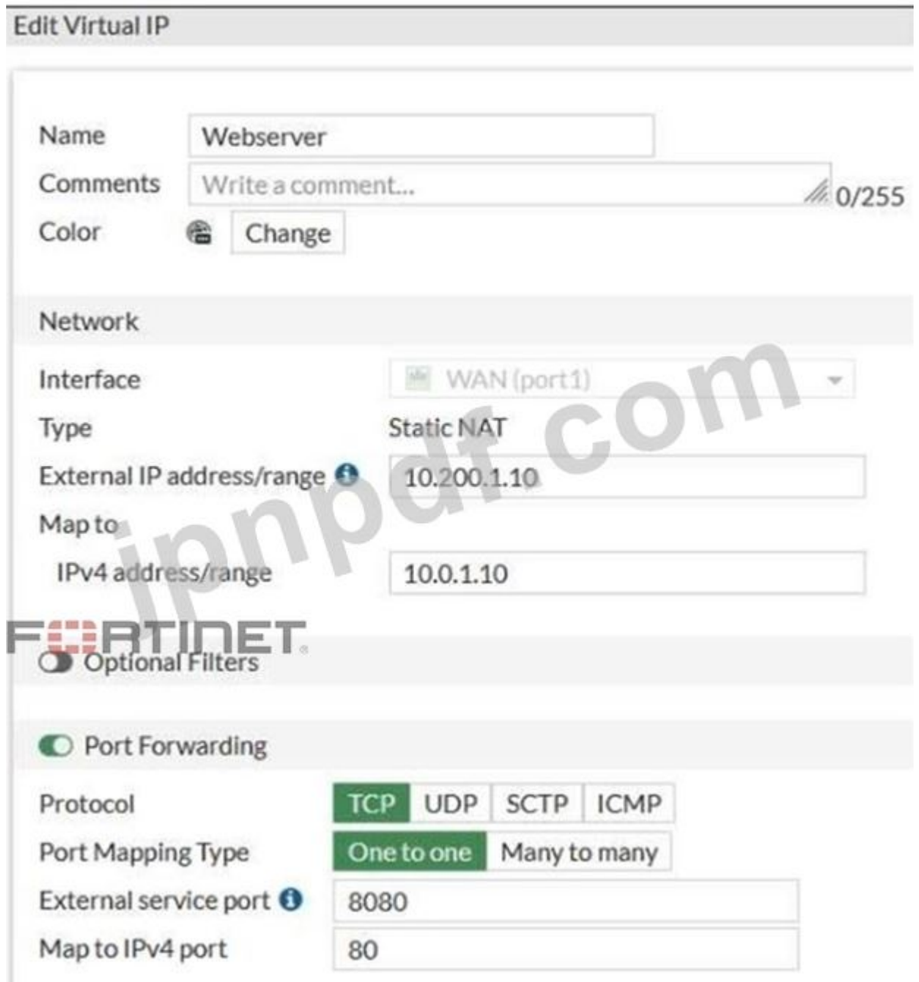
最新問題: 3
HQ FortiGate には、アグレッシブ モードで構成された複数のダイヤルアップ IPsec VPN があります。要件は、ダイヤルアップ ユーザーをそれぞれの部門の VPN トンネルに接続することです。
ユーザーをトンネルに一致させるために構成できるフェーズ 1 設定はどれですか?
A. ピアID
B. ローカルゲートウェイ
C. デッドピア検出
D. IKE モード設定
Answer: (解答を表示する**)**
When using multiple dial-up IPsec VPNs in aggressive mode, the Peer ID setting in Phase 1 can be used to distinguish between different VPN tunnels. Each dial-up user or department can be assigned a unique Peer ID, allowing the FortiGate to match the incoming VPN request to the correct tunnel based on the Peer ID value.

最新問題: 4
次世代ファイアウォール (NGFW) FortiGate でアプリケーション制御トラフィックを処理するエンジンはどれですか?
A. インターネット サービス データベース (ISDB) エンジン
B. 侵入防止システムエンジン
C. アプリケーション制御エンジン
D. ウイルス対策エンジン
Answer: B (メーッセージを残す**)**

最新問題: 5

ネットワークに接続された FortiGate デバイスの図、VIP オブジェクトの構成、およびファイアウォール ポリシーの構成を示す図を参照してください。

IP object configuration



Firewall policy configuration

Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
Internet_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT		NAT
Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	HTTPS	✓ ACCEPT		Disabled

WAN (ポート 1) インターフェイスの IP アドレスは 10.200.1.1/24 です。LAN (ポート 3) インターフェイスの IP アドレスは 10.0.1.254/24 です。
ホスト 10.200.3.1 がポート 8080 で TCP SYN パケットを 10.200.1.10 に送信する場合、FortiGate がパケットを宛先に転送する時点でのパケットの送信元アドレス、宛先アドレス、および宛先ポートはどうなるでしょうか。
A. それぞれ 10.0.1.254、10.200.1.10、8080

B. それぞれ 10.0.1.254、10.0.1.10、80
C. それぞれ 10.200.3.1、10.0.1.10、80
D. それぞれ 10.200.3.1、10.0.1.10、8080
Answer: C (メーッセージを残す)
The source address remains 10.200.3.1 because FortiGate does not modify the source address by default unless NAT is applied (which is disabled in the policy).
The destination address is translated to 10.0.1.10 by the VIP (Virtual IP) object, as this is the internal server address mapped to the external IP 10.200.1.10.
The destination port is translated from 8080 to 80 as per the port forwarding rule configured in the VIP object.

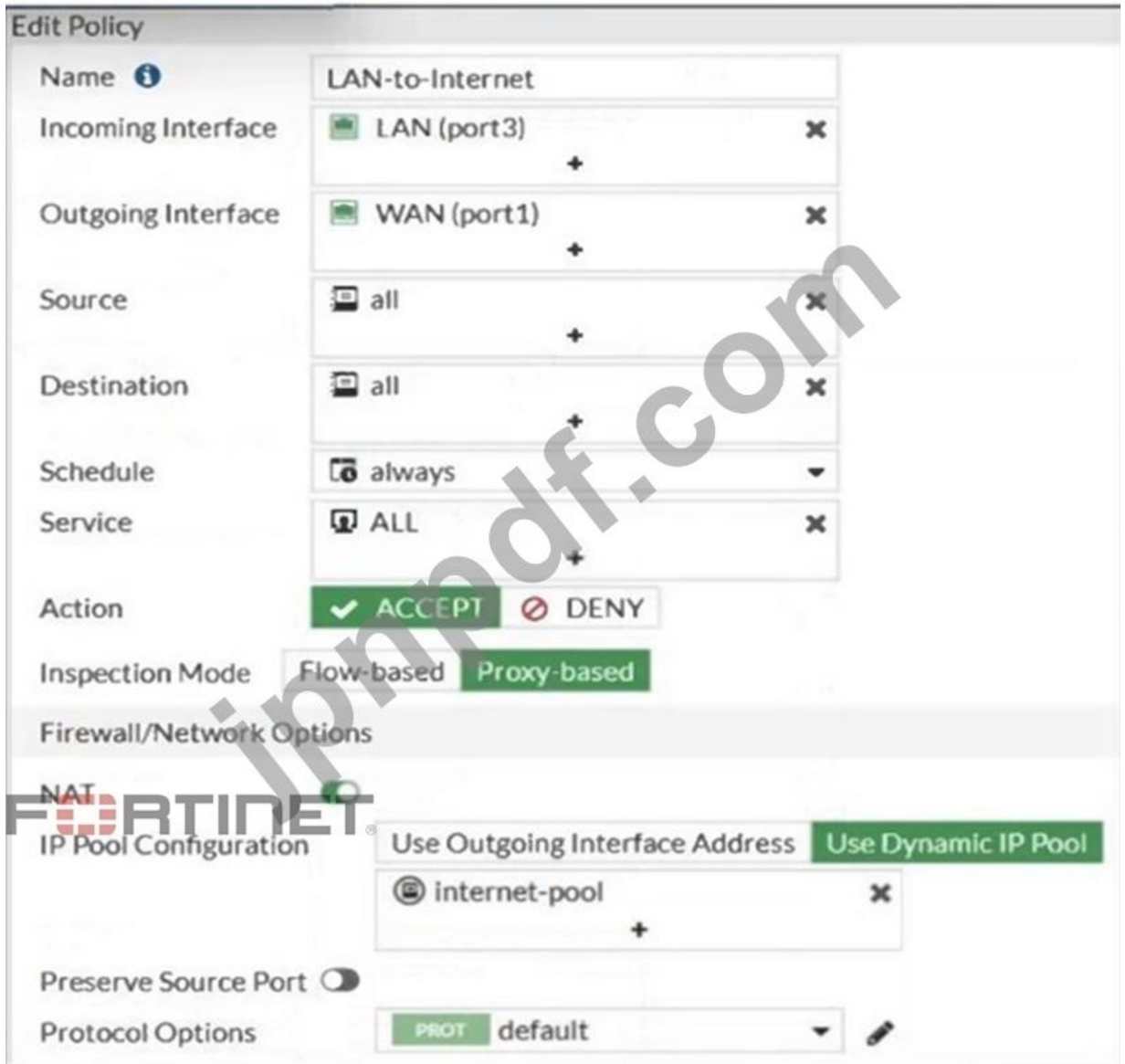
最新問題**: 6**
従業員は、遅延の大きいインターネット接続を介してオフィスに接続する必要があります。
SSL VPN ネゴシエーションの失敗を防ぐために、管理者はどの SSL VPN 設定を調整する必要がありますか?
A. SSL VPN アイドルタイムアウト
B. SSL VPN ログインタイムアウト
C. SSL VPN dtls-hello-timeout
D. SSL VPN セッション TTL
Answer: (解答を表示する)
For a high-latency internet connection, the SSL VPN setting that should be adjusted is:
C . SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.
The other options are not suitable:
A . SSL VPN idle-timeout: This setting controls the idle time allowed before a session is terminated, which is not relevant to the initial connection establishment.
B . SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.
D . SSL VPN session-ttl: This setting controls the total time-to-live for an SSL VPN session but does not directly address issues caused by high latency.
Reference
FortiOS 7.4.1 Administration Guide - SSL VPN Configuration, page 1415.

最新問題**: 7**
展示品を参照してください。

Network diagram

Dynamic IP pool

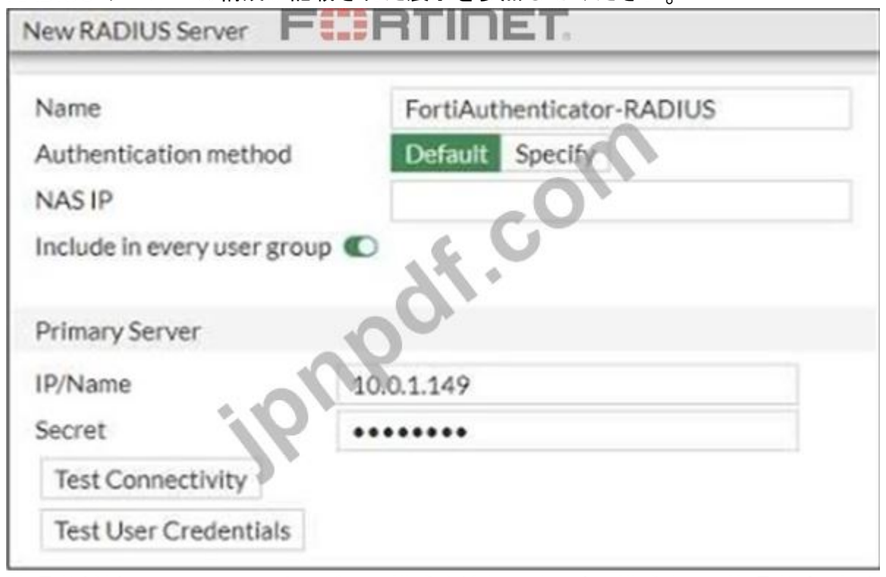
Firewall policy



図には、ネットワークに接続された FortiGate デバイスの図と、FortiGate デバイス上のファイアウォール ポリシーと IP プール構成が示されています。
2 台の PC (PC1 と PC2) が FortiGate の背後に接続されており、インターネットに正常にアクセスできます。ただし、管理者が 3 台目の PC (PC3) をネットワークに追加すると、その PC はインターネットに接続できなくなります。
展示に示されている情報に基づいて、管理者が PC3 の接続の問題を解決するために使用できる 2 つの構成オプションはどれですか? (2 つ選択してください。)
A. ファイアウォール ポリシー設定で、ソース フィールドにアドレス オブジェクトとして 10. ol 3 を追加します。
B. IP プール構成で、endig を 192.2.0.12 に設定します。

C. PC3 のアドレスのみを送信元として一致する別のファイアウォール ポリシーを設定し、そのポリシーをリストの先頭に配置します。
D. IP プール構成で、cype をオーバーロードに設定します。
Answer: B,D (メーッセージを残す)
To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:
B . In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.
D . In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses.
The other options are not suitable:
A . In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).
C . Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.
Reference
FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.
FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

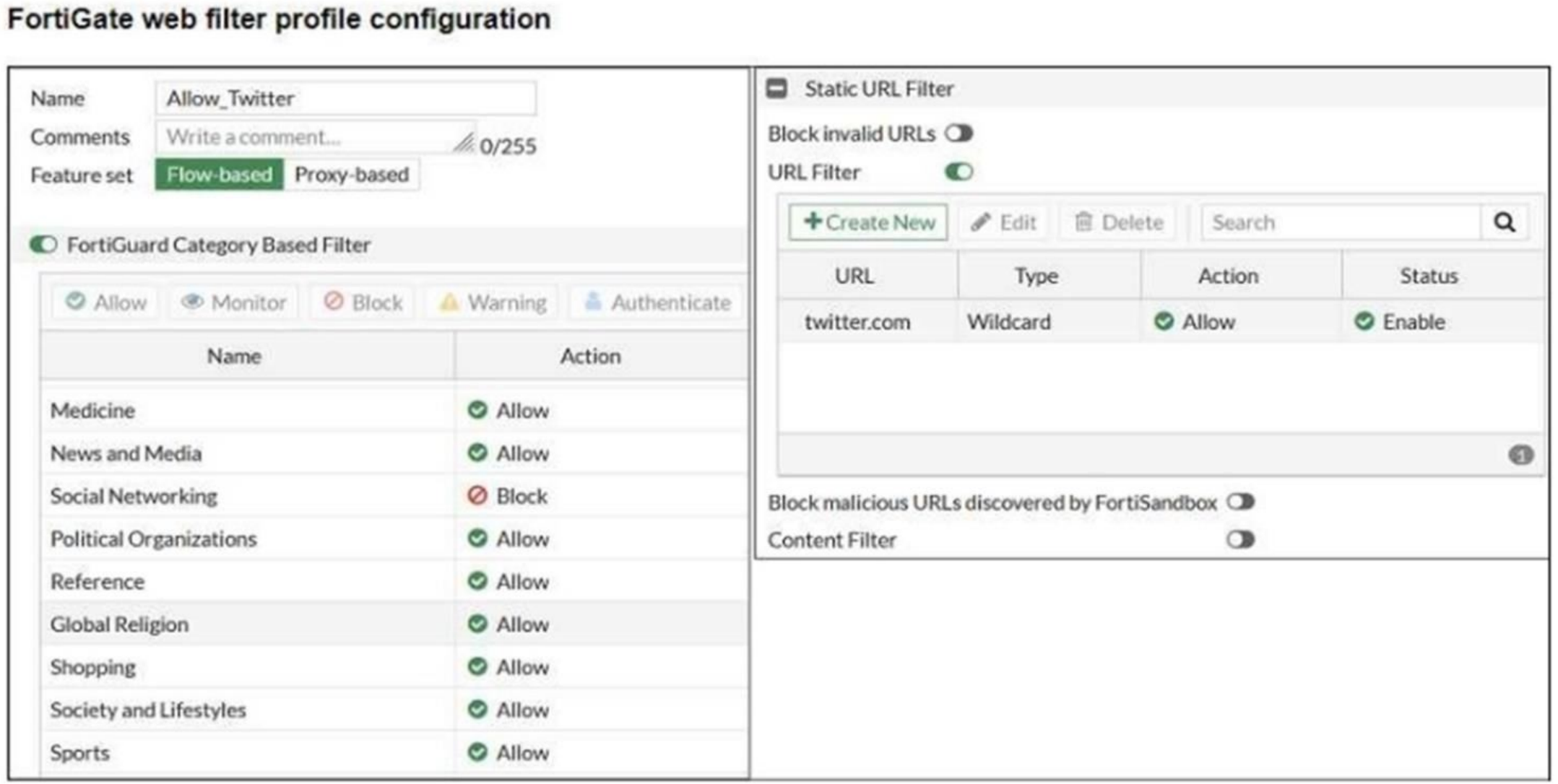
最新問題: 8
RADIUS サーバーの構成が記載された展示を参照してください。



管理者が新しい RADIUS サーバーの構成を追加しました。構成中に、管理者は すべてのユーザー グループに含める」オプションを選択しました。
RADIUS 構成で すべてのユーザー グループに含める」オプションを使用するとどのような影響がありますか?
A. このオプションは、RADIUSサーバーとそのサーバーに対して認証できるすべてのユーザーをすべてのFortiGateユーザーグループに配置します。
B. このオプションは、FortiGate上のLDAPサーバーで使用されるグループを含む、すべてのユーザーを偶数/RADIUSユーザーグループに配置します。
C. このオプションは、認証に必要なすべてのFortiGateユーザーとグループをRADIUSサーバー この場合はFortiAuthenticator)に配置します。
D. このオプションは、RADIUSサーバーと、そのサーバーに対して認証できるすべてのユーザーをすべてのRADIUSグループに配置します。

Answer: A (メーッセージを残す)
By selecting the "Include in every user group" option in the RADIUS configuration, FortiGate automatically includes this RADIUS server as an authentication source for all user groups. This means any user group configured on the FortiGate will authenticate using this RADIUS server, allowing users to authenticate against the server for any group they belong to.

最新問題: **9**
展示品を参照してください。



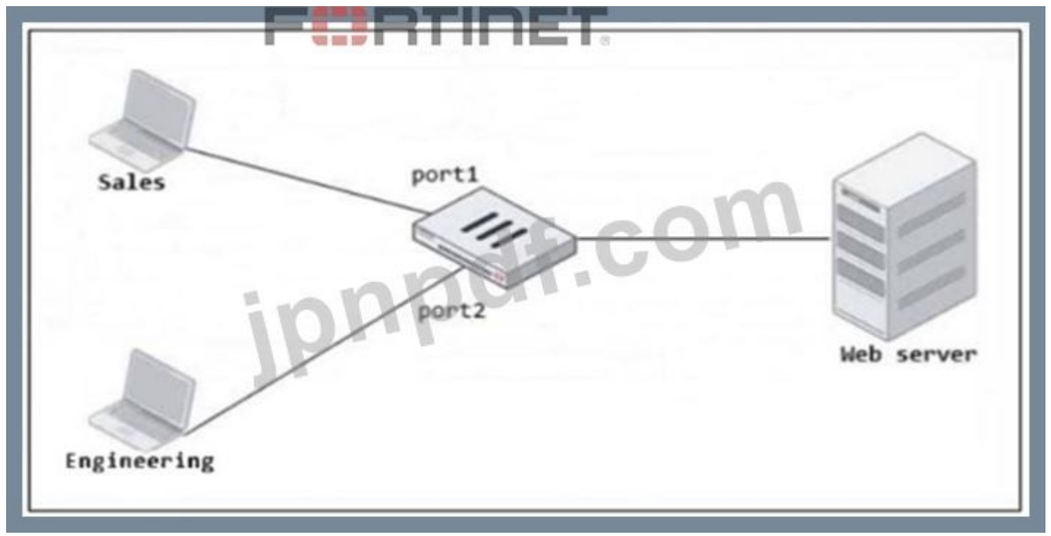
管理者は、図に示す Web フィルタリング プロファイルを設定して、Twitter を除くすべてのソーシャル ネットワーキング サイトへのアクセスをブロックしました。ただし、ユーザーが twitter.com にアクセスしようとすると、FortiGuard Web フィルタリング ブロック ページにリダイレクトされます。
展示に基づいて、管理者は Twitter を許可しながら他のすべてのソーシャル ネットワーキング サイトをブロックするためにどのような構成変更を行うことができますか?

A. 静的URLフィルターの設定で、タイプをシンプルに設定する
B. FortiGuardカテゴリベースフィルタ設定で、ソーシャルネットワーキングのアクションを警告に設定します。
C. 静的URLフィルター設定でアクションを監視に設定する
D. 静的URLフィルター設定でアクションを除外に設定する
Answer: (解答を表示する**)**
In the current configuration, although "twitter.com" is allowed in the Static URL Filter, the category "Social Networking" is set to "Block" under the FortiGuard Category Based Filter. To resolve the issue, setting the action to "Exempt" in the Static URL Filter for "twitter.com" will bypass the category-based block for this specific URL while still enforcing the block on other social networking sites.

最新問題**: 10**
FortiGate FSSO エージェントレス ポーリング モードの 2 つの機能は何ですか? (2 つ選択してください。)
A. FortiGate はコレクター エージェントにリモート LDAP サーバーを使用するように指示します。
B. FortiGate は SMB プロトコルを使用して DC からイベント ビューアー ログを読み取ります。
C. FortiGate はワークステーション チェックをサポートしていません。
D. FortiGate は AD サーバーをコレクター エージェントとして使用します。
Answer: (解答を表示する**)**
FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
In agentless polling mode, FortiGate directly connects to the Domain Controllers (DCs) using the SMB protocol to read event logs and detect user login events.
FortiGate does not support workstation check.
In agentless polling mode, FortiGate does not perform workstation checks. It relies on polling the event logs from the Domain Controllers to identify user logins.

最新問題**: 11**
管理者は、NTurbo をサポートする FortiGate モデルを管理します。
NTurbo はフローベースの検査のパフォーマンスをどのように向上させるのでしょうか?
A. NTurbo はトラフィックをコンテンツ プロセッサにオフロードします。
B. NTurbo は FortiGate デバイス上に 2 つの検査セッションを作成します。
C. NTurbo はファイル全体をバッファリングし、それをウイルス対策エンジンに送信します。
D. NTurbo は、IPS エンジンとその入力インターフェイスおよび出力インターフェイス間のトラフィックをリダイレクトするための特別なデータ パスを作成します。
Answer: D (メーッセージを残す**)**
NTurbo creates a special data path to redirect traffic from the ingress interface to IPS, and from IPS to the egress interface. NTurbo allows firewall operations to be offloaded along this path, and still allows IPS to behave as a stage in the processing pipeline, reducing the workload on the FortiGate CPU and improving overall throughput. Hardware Acceleration https://docs.fortinet.com/document/fortigate/7.0.1/hardware-acceleration/896174/nturbo-offloads-flow-based-processing

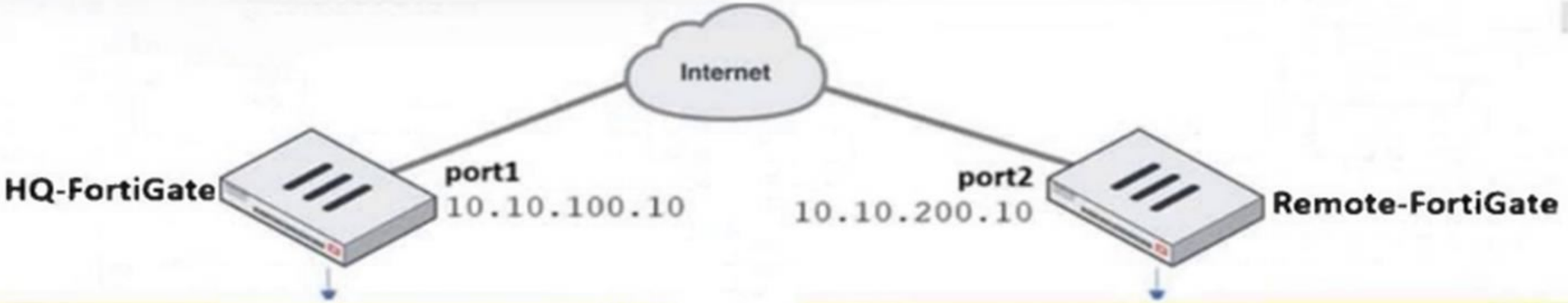
最新問題**: 12**
展示品を参照してください。



FortiGate には、営業部門とエンジニアリング部門が同じセキュリティ プロファイルを使用して同じ Web サーバーにアクセスするための 2 つの個別のファイアウォール ポリシーがあります。
2 つのポリシーを 1 つに統合するには、管理者はどのアクションを実行する必要がありますか?
A. 複数のインターフェースポリシーを有効にして、同じファイアウォールポリシーでポート1とポート2を選択します。
B. port1とport2を含むインターフェースグループを作成し、単一のファイアウォールポリシーを作成します。
C. 単一のファイアウォール ポリシーで port1 および port2 サブネットを選択します。
D. 単一のファイアウォール ポリシー内の port1 と port2 を任意のインターフェイスに置き換えます。
Answer: A (メーッセージを残す**)**
To consolidate the two separate firewall policies for Sales and Engineering departments accessing the same web server, you can create an Interface Group that includes both port1 (Sales) and port2 (Engineering). Once the Interface Group is created, you can use this group as a single incoming interface in a single firewall policy. This approach reduces the number of policies, making management more efficient.
Reference:
FortiOS 7.4.1 Administration Guide: Firewall Policy Configuration

最新問題: 13
展示品を参照してください。

IPsec tunnel configuration



Network

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.10.200.10
Interface	port1
Local Gateway	
Mode Config	
NAT Traversal	Enable / Disable / Forced
Keepalive Frequency	10
Dead Peer Detection	Disable / On Idle / On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress / Ingress
Advanced...	

Authentication

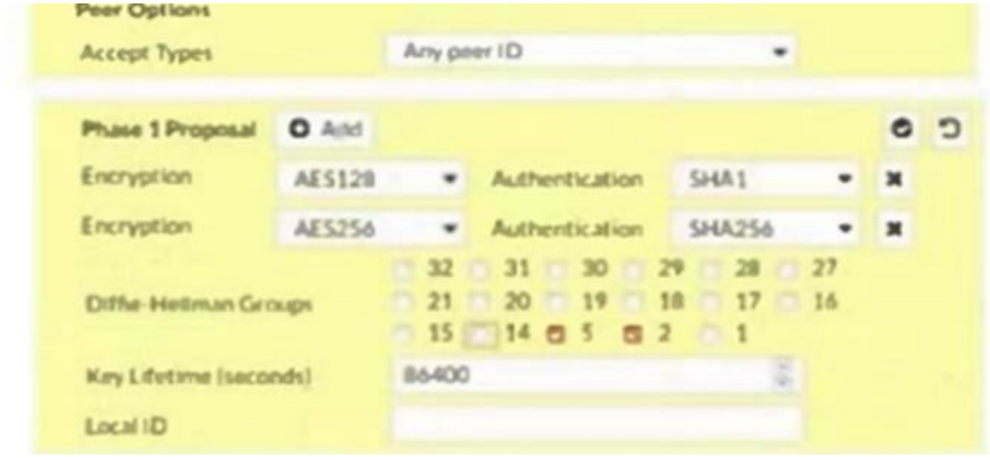
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	1 / 2
Mode	Aggressive / Main (ID protection)

Network

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.10.100.10
Interface	port1
Local Gateway	
Mode Config	
NAT Traversal	Enable / Disable / Forced
Keepalive Frequency	10
Dead Peer Detection	Disable / On Idle / On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress / Ingress
Advanced...	

Authentication

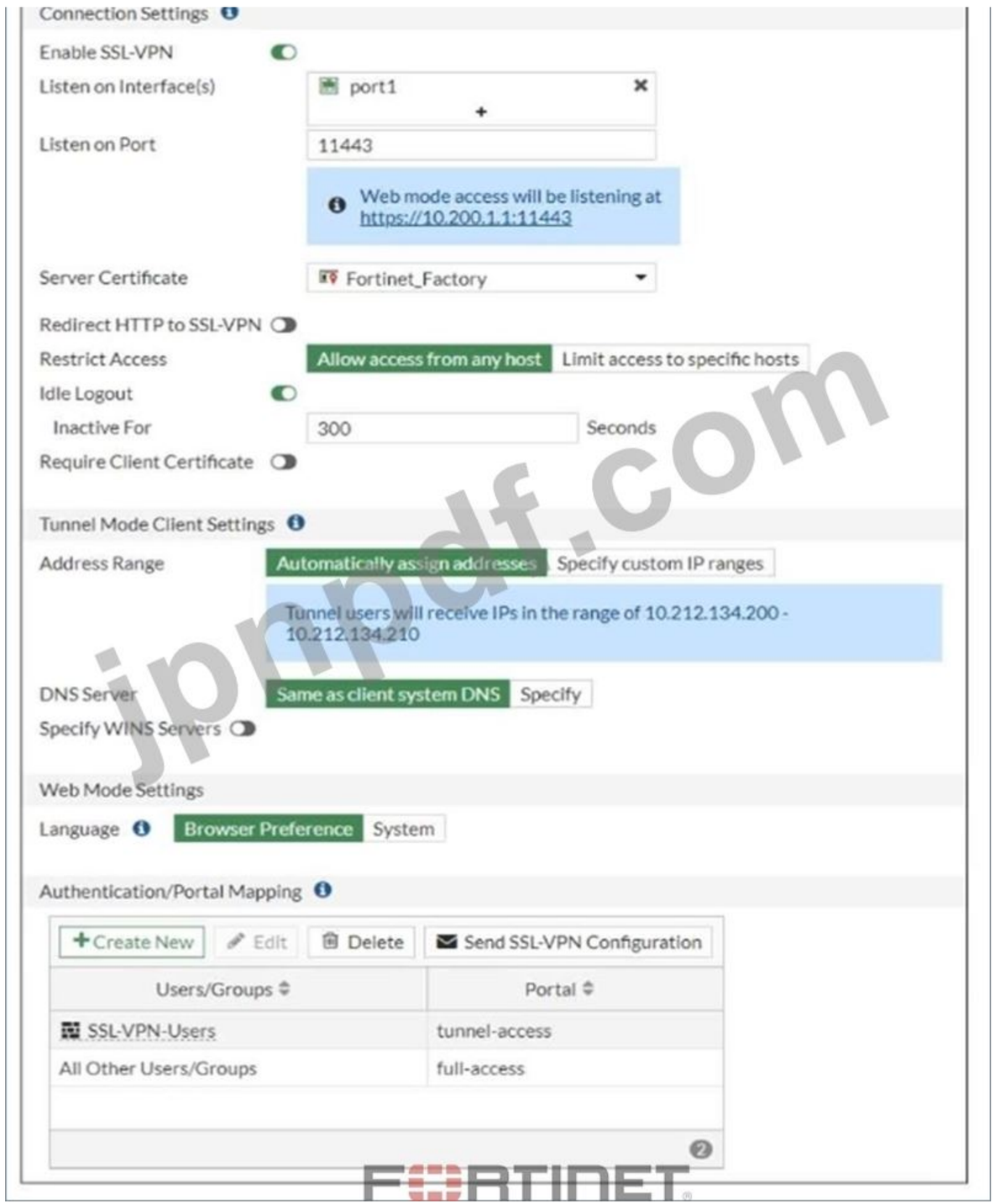
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	1 / 2



ネットワーク管理者は、2 つの FortiGate デバイス間の IPsec トンネルのトラブルシューティングを行っています。管理者は、フェーズ 1 が起動に失敗したと判断しました。また、管理者は両方の FortiGate デバイスで事前共有キーを再入力し、それらが一致することを確認しました。
フェーズ 1 の構成と図に示されている図に基づいて、管理者がフェーズ 1 を起動するために実行できる 2 つの構成変更はどれですか (2 つ選択してください)。
A. HQ-FortiGate で、Diffie-Helman グループ 2 を無効にします。
B. リモートFortiGateで、ポート2をインターフェースとして設定します。
C. 両方の FortiGate デバイスで、Dead Peer Detection を On Demand に設定します。
D. HQ-FortiGate で、IKE モードをメイン (ID 保護) に設定します。
Answer: (解答を表示する**)**
Based on the phase 1 configuration and the diagram shown in the exhibit, the administrator can make the following two configuration changes to bring phase 1 up:
B . On Remote-FortiGate, set port2 as Interface: The diagram indicates that port2 is currently not selected under 'Interface' for Remote-FortiGate. Aligning this setting with HQ-FortiGate, which has port1 set as Interface, might resolve inconsistencies.
D . On HQ-FortiGate, set IKE mode to Main (ID protection): The current setting on HQ-FortiGate is Aggressive for IKE mode, while Remote-FortiGate is set to Main mode. Matching these settings may help in establishing phase 1 of the IPsec tunnel.

最新問題**: 14**
FortiGate が節約モードに入るときに正しい記述はどれですか? (2 つ選択してください。)
A. FortiGate は設定変更を拒否します
B. FortiGate はシステム全体の動作を停止し、利用可能なリソースを回復するには再起動が必要です。
C. FortiGate は、隔離などの重要なセキュリティ アクションを引き続き実行します。
D. IPSのフェールオープングローバル設定が有効になっている場合、FortiGateはIPS検査なしでパケットを送信し続けます。
Answer: (解答を表示する**)**

最新問題**: 15**
展示品を参照してください。


Connection Settings
Enable SSL-VPN
Listen on Interface(s)
port1
Listen on Port
11443
Web mode access will be listening at https://10.200.1.1:11443
Server Certificate
Fortinet_Factory
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Web Mode Settings
Language
Browser Preference
System
Authentication/Portal Mapping
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Portal
SSL-VPN-Users
tunnel-access
All Other Users/Groups
full-access

VPN connection status

ユーザーが SSL VPN に接続しようとすると、接続が失敗します。
SSL VPN に正常に接続するには、ユーザーは何をする必要がありますか?
A. SSL VPN ポータルをトンネルに変更します。
B. アイドル タイムアウトを変更します。
C. サーバーの IP アドレスを変更します。
D. クライアントの SSL VPN ポートを変更します。
Answer: D (メーッセージを残す**)**
The SSL VPN is configured to listen on port 11443 on the FortiGate device, as shown in the SSL VPN settings in the exhibit. However, the user is attempting to connect to the server using port 1443, as displayed in the VPN connection status. The mismatch between the ports is causing the connection failure. To resolve this, the user should change the client configuration to use port 11443 to match the FortiGate SSL VPN configuration.

最新問題**: 16**
Facebook のファイアウォール ポリシーとセキュリティ プロファイルを示す展示を参照してください。

Firewall policy

Security profile

Categories

Mixed · All Categories

- Business (179, 6)
- Cloud/IT (31)
- Collaboration (293, 6)
- Email (87, 12)
- Game (124)
- General Interest (241, 9)
- Mobile (3)
- Network Service (332)
- P2P (85)
- Proxy (106)
- Remote Access (91)
- Social Media (150, 31)
- Storage/Backup (296, 16)
- Update (48)
- Video/Audio (206, 13)
- VoIP (31)
- Web Client (18)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	Facebook Facebook_Like.Button Facebook_Video.Play	Application	Allow

ユーザーには Facebook ウェブ アプリケーションへのアクセス権が与えられます。Facebook でホストされているビデオ コンテンツを再生することはできますが、ビデオやその他の種類の投稿に反応を残すことはできません。問題を解決するには、構成のどの部分を変更する必要がありますか?
A. セキュリティポリシーのURLカテゴリにFacebookを追加する
B. セキュリティポリシーに追加するために必要な追加のアプリケーション署名を取得します
C. SSL検査をディープコンテンツ検査にする
D. WebブラウザでHTTPからHTTPSへのリダイレクトを無効にする
Answer: (解答を表示する)

最新問題: **17**
展示品を参照してください。

Application sensor configuration

Edit Application Sensor

Categories

All Categories

Business (179, 6)	Cloud.IT (31)
Collaboration (293, 6)	Email (87, 12)
Game (124)	General.Interest (241, 9)
Mobile (3)	Network.Service (332)
P2P (85)	Proxy (106)
Remote.Access (91)	Social.Media (150, 31)
Storage.Backup (296, 16)	Update (48)
Video/Audio (206, 13)	VoIP (31)
Web.Client (18)	Unknown Applications

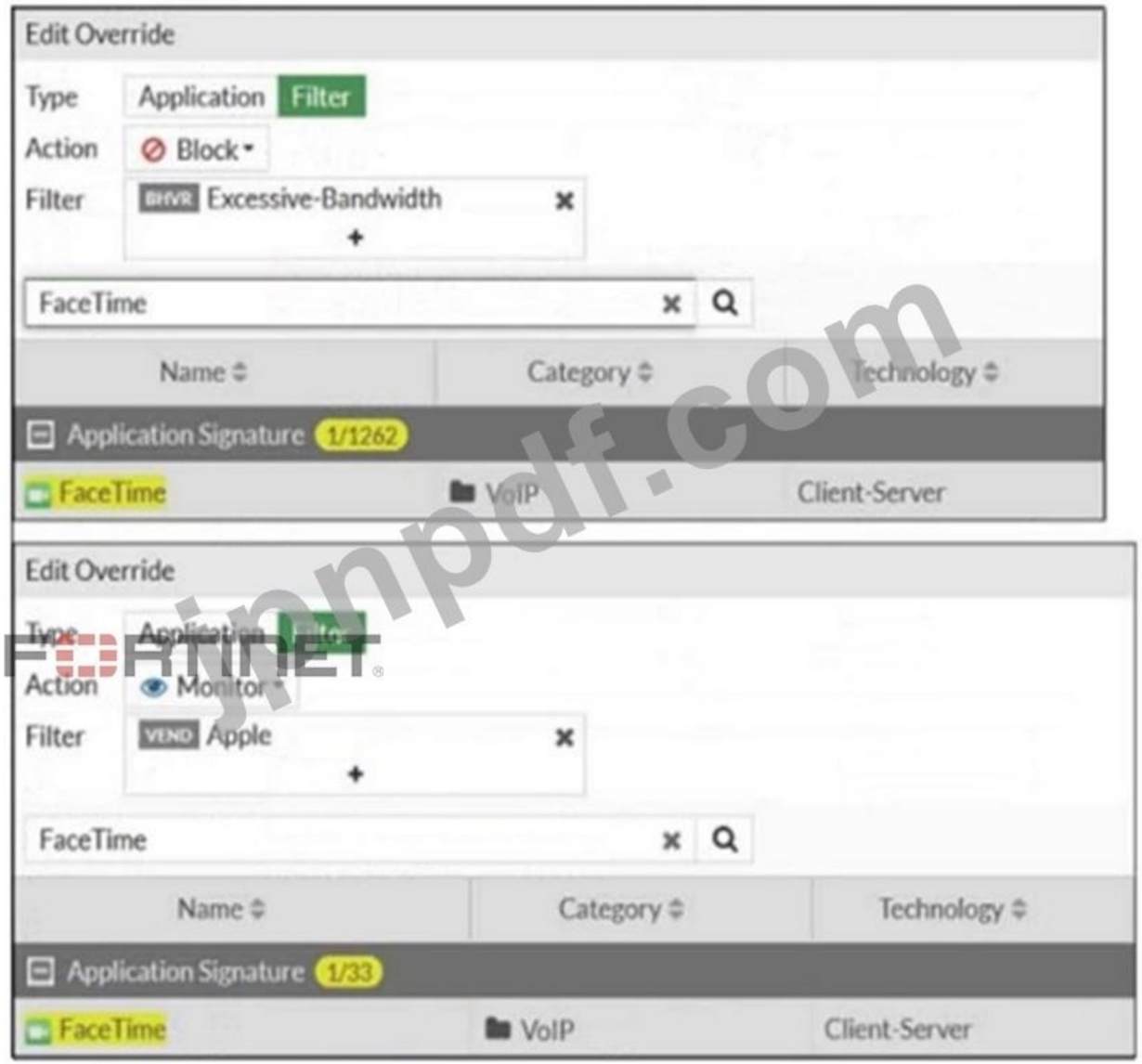
Network Protocol Enforcement

Application and Filter Overrides

Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Apple	Filter	Monitor

Application and Filter override configuration



展示には、アプリケーション センサーの構成と、過剰帯域幅および Apple フィルターの詳細が表示されます。
設定に基づいて、発信または着信の通話が少ない場合、Apple FaceTime はどうなるでしょうか?

A. ビデオ/オーディオ カテゴリの構成に基づいて、Apple FaceTime が許可されます。

B. Apple フィルター設定に基づいて、Apple FaceTime が許可されます。

C. Apple FaceTime は、アプリケーションとフィルターの上書きの Apple フィルターが許可に設定されている場合にのみ許可されます。

D. 過剰帯域幅フィルターの設定に基づいて、Apple FaceTime がブロックされます。
Answer: D (メーッセージを残す**)**
Based on the application sensor configuration and the filter details:
D . Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration: The "Excessive-Bandwidth" filter is set to block, which includes "FaceTime" under its application signature. As a result, FaceTime will be blocked regardless of the "Apple" filter configuration because the "Excessive-Bandwidth" filter takes precedence due to its block action setting.
The other options are not correct:
A . Apple FaceTime will be allowed, based on the Video/Audio category configuration: The Video/Audio category is not relevant because FaceTime is specifically included in the Excessive-Bandwidth filter, which blocks it.
B . Apple FaceTime will be allowed, based on the Apple filter configuration: Although the Apple filter is set to monitor, the block action of the Excessive-Bandwidth filter will override this.
C . Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow: The allow setting for the Apple filter is irrelevant in this context, as the block action in the Excessive-Bandwidth filter will prevail.
Reference
FortiOS 7.4.1 Administration Guide - Application Control and Filtering, page 978.
FortiOS 7.4.1 Administration Guide - Application Sensor Configuration, page 982.

最新問題**: 18**
ネットワーク管理者はウイルス対策を有効にし、ファイアウォール ポリシーで SSL 検査プロファイルを選択しました。
HTTP 経由で EICAR テスト ファイルをダウンロードすると、FortiGate はウイルスを検出し、ファイルをブロックします。HTTPS 経由で同じファイルをダウンロードすると、FortiGate はウイルスを検出せず、ファイルをブロックしないため、ダウンロードが許可されます。
管理者は、トラフィックが設定されたファイアウォール ポリシーと一致していることを確認します。
FortiGate によるウイルス検出が失敗する 2 つの理由は何ですか? (2 つ選択してください。)
A. 選択されたSSL検査プロファイルでは証明書検査が有効になっています
B. ブラウザはFortiGateの自己署名CA証明書を信頼していません
C. EICAR テスト ファイルがプロトコル オプションのオーバーサイズ制限を超えています
D. ウェブサイトはSSL検査の対象外です
Answer: A,D (メーッセージを残す**)**
The selected SSL inspection profile has certificate inspection enabled
If the SSL inspection profile is set to certificate inspection instead of full SSL inspection, FortiGate will only inspect the certificate of the HTTPS connection but will not decrypt and inspect the actual traffic content, leading to a failure in virus detection.
The website is exempted from SSL inspection
If the website hosting the EICAR test file is exempt from SSL inspection, FortiGate will not decrypt the traffic, meaning it cannot inspect the file content for viruses, resulting in the file being downloaded without detection.

最新問題**: 19**
FortiGate HA 構成の同期に関して正しい記述はどれですか? (2 つ選択してください。)
A. デバイスのチェックサムが相互に比較され、構成が同じであることを確認します。
B. 増分構成同期は、プライマリ FortiGate デバイスで行われた変更からのみ実行できます。
C. HAクラスタ内の任意のFortiGateデバイスで行われた変更から増分構成同期が発生する可能性があります。
D. 一部の構成項目が他の HA メンバーに同期されていないため、デバイスのチェックサムは互いに異なります。
Answer: A,C (メーッセージを残す**)**
"After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link"

最新問題: **20**
SD-WAN ゾーンに関する次の 3 つの記述のうち正しいものはどれですか? (3 つ選択してください。)
A. SD-WANゾーンには物理インターフェースと論理インターフェースを含めることができます
B. 静的ルート定義でSD-WANゾーンを使用できます
C. FortiGateデバイスごとに最大3つのSD-WANゾーンを定義できます。
D. SD-WANゾーンには少なくとも2つのメンバーが含まれている必要があります
E. SD-WANゾーンはメンバーの論理的なグループです
Answer: A,B,E (メーッセージを残す**)**
An SD-WAN zone can contain physical and logical interfaces
SD-WAN zones can include both physical and logical interfaces, allowing flexible configuration for different network types.
You can use an SD-WAN zone in static route definitions
SD-WAN zones can be referenced in static routes, enabling dynamic path selection based on SD-WAN rules.
An SD-WAN zone is a logical grouping of members
An SD-WAN zone is a logical grouping of interfaces (members), used to simplify the management and application of SD-WAN rules.

最新問題: **21**
展示品を参照してください。

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

このファイアウォール ポリシー リストに関する次の記述のうち正しいものはどれですか。
A. ファイアウォール ポリシーは ID シーケンス ビューで一覧表示されます。
B. LAN から WAN。WAN から LAN。および暗黙的は、シーケンス グループ化ビュー リストです。
C. 暗黙的グループには、複数の拒否ファイアウォール ポリシーを含めることができます。
Answer: B (メーッセージを残す**)**
D. ファイアウォール ポリシーは、入力および出力インターフェイスのペアリング ビューによって一覧表示されます。

最新問題: **22**
フローベースのウイルス対策プロファイルを説明する 3 つの文はどれですか? (3 つ選択してください。)
A. ウイルスが検出されると、最後のパケットがクライアントに配信されます。
B. FortiGate はファイル全体をバッファリングしますが、同時にクライアントに送信します。
C. フローベースの検査はプロキシベースの検査に比べてパフォーマンスが最適化されます
D. IPS エンジンはプロセスをスタンドアロンとして処理します。
E. フローベースの検査では、プロキシベースの検査で利用可能なスキャンモードのハイブリッドを使用します。
Answer: (解答を表示する**)**

最新問題: **23**
SD-WAN における 3 つの主要なルーティング原則は何ですか? (3 つ選択してください。)
A. デフォルト。宛先への有効なルートがない場合、SD-WANメンバーはスキップされます。
B. デフォルト。宛先へのルートが1つしか利用できない場合は、SD-WANルールはスキップされます。
C. デフォルト。宛先への最適なルートがSD-WANメンバーでない場合は、SD-WANルールはスキップされます。
D. SD-WAN ルールは他の種類のルートよりも優先されます
E. 通常のポリシールートは SD-WAN ルールよりも優先されます
Answer: A,C,E (メーッセージを残す**)**
SD-WAN rules are matched only if the best route to the destination points to SD-WAN SD-WAN member is selected only if it has a route to the destination
https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-sd-branch-architecture-for-mssps/768108/sd-wan-routing-logic SDWAN rules are 'policy routes', but regular policy routes have precedence over SD-WAN rules.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explaining-the-SD-WAN-rule-matching-process/ta-p/284325

最新問題: **24**
問題が物理層でもリンク層でもない場合、レイヤー 3 の問題をトラブルシューティングするために使用できる 3 つの CLI コマンドはどれですか? (3 つ選択してください。)
A. トレースルートを実行する
B. システム ARP を取得する
C. pingを実行する
D. スニファーパケットを診断する
E. システムトップを診断する
Answer: A,C,D (メーッセージを残す**)**

最新問題: **25**
SSL 証明書検査が有効になっている場合、FortiGate は SSL サーバーのホスト名を識別するためにどの 3 つの情報を使用しますか? (3 つ選択してください。)
A. HTTP ヘッダーのホスト フィールド。
B. クライアントの Hello メッセージ内のサーバー名表示 (SNI) 拡張。
C. サーバー証明書のサブジェクト別名 (SAN) フィールド。
D. サーバー証明書のサブジェクト フィールド。
E. サーバー証明書のシリアル番号。
Answer: B,C,D (メーッセージを残す**)**
When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:
Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows

FortiGate to identify the server's hostname during the SSL handshake.
Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server's identity during SSL certificate inspection.
The other options are not used in SSL certificate inspection for hostname identification:
Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.
Reference
FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.
FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

最新問題: 26
展示品を参照してください。

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

SD-WAN は、どの SD-WAN ルールにも一致しないトラフィックを分散するためにどのアルゴリズムを使用しますか?
A. 送信元 IP から宛先 IP へのすべてのトラフィックは同じインターフェースに送信されます。
B. トラフィックは、遅延が最も低いリンクに送信されます。
C. トラフィックは、各インターフェースを通過するセッションの数に基づいて分散されます。
D. 送信元IPからのすべてのトラフィックは同じインターフェースに送信されます
Answer: A (メーッセージを残す**)**
For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface. This ensures that a consistent path is used for traffic between the same source and destination IP addresses. Options B, C, and D do not apply because the default algorithm does not prioritize by latency, session count, or source IP alone.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Load Balancing Algorithms

最新問題: **27**

展示品を参照してください。

FortiGate routing database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```


このデータベース テーブルのルーティング エントリについて正しい記述はどれですか。(2 つ選択してください。)

A. ルーティング データベース テーブル内のすべてのエントリが FortiGate ルーティング テーブルにインストールされます。

B. ポート2インターフェースは非アクティブとしてマークされています。

C. 両方のデフォルト ルートの管理距離が異なります。

D. ポート2のデフォルトルートはスタンバイルートとしてマークされています。

Answer: (解答を表示する**)**

The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:

The default route through port2 has an administrative distance of 20.

The default route through port1 has an administrative distance of 10.

Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.

Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.

Reference:

FortiOS 7.4.1 Administration Guide: Default route configuration

FortiOS 7.4.1 Administration Guide: Routing table explanation

最新問題: **28**

FortiGate のシステム パフォーマンス出力と高メモリ使用量しきい値のデフォルト構成を示す展示を参照してください。

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```


システムパフォーマンス出力に基づいて、考えられる 2 つの結果は何でしょうか? (2 つ選択してください。)

A. FortiGate は、検査のためにすべてのファイルを FortiSandbox に送信し始めます。

B. FortiGate は節約モードに入りました。

C. 管理者は設定を変更できません。

D. 管理者はコンソール ポート経由でのみ FortiGate にアクセスできます。

Answer: B,D (メーッセージを残す)

Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the

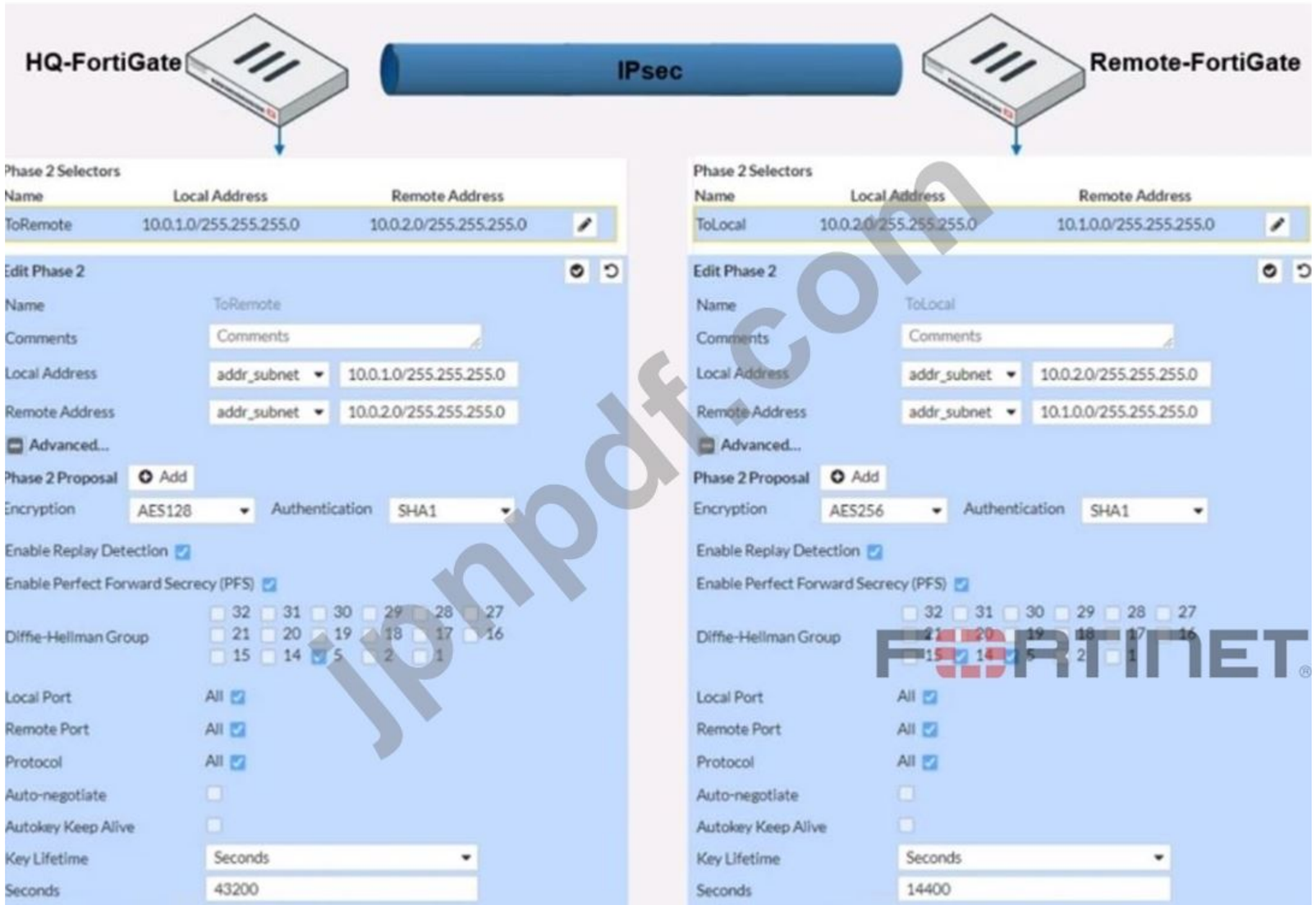
FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:
B . FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.
D . Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.
The other options are not correct:
A . FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
C . Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.
Reference
FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

最新問題**: 29**
2 つの FortiGate デバイス間で SSL VPN を機能させるために必要な 2 つの設定はどれですか? (2 つ選択してください。)
A. クライアント FortiGate では、SSL VPN に接続するために SSL VPN トンネル インターフェイス タイプが必要です。
B. サーバー FortiGate では、クライアント FortiGate 証明書を検証するために CA 証明書が必要です。
C. クライアント FortiGate には、サーバー FortiGate 上の CA によって署名されたクライアント証明書が必要です。
D. クライアント FortiGate では、リモート サブネットへのルートを手動で追加する必要があります。
Answer: A,B (メーッセージを残す**)**
If fortigate is used as an SSL VPN client, it needs a ssl virtual tunnel interface to connect to the SSL VPN server. This is the client virtual interface that the vpn server will assign the temporary IP address to during the lifetime of an ssl connection. The SSL VPN server also needs a correct CA certificate to authenticate/trust client's certificate.

最新問題**: 30**
管理者は、デッド トンネルを検出するために、IPsec VPN でデッド ピア検出 (DPD) を設定したいと考えています。要件は、送信トラフィックがあり、ピアからの応答がない場合にのみ、FortiGate が DPD プローブを送信することです。
FortiGate のどの DPD モードがこの要件を満たしていますか?
A. オンデマンド
B. アイドル時
C. 無効
D. 有効
Answer: (解答を表示する**)**
The On Demand mode for Dead Peer Detection (DPD) on FortiGate sends DPD probes only when there is outbound traffic and no response from the peer. This mode is used to detect if the peer is still available without continuously sending DPD probes, reducing unnecessary traffic.

最新問題**: 31**
展示品を参照してください。

Ipsec tunnel configuration



ネットワーク管理者は、2 つの FortiGate デバイス間の IPsec トンネルのトラブルシューティングを行っています。管理者は、フェーズ 1 のステータスはアップであることを確認しましたが、フェーズ 2 はアップしません。
図に示されているフェーズ 2 の構成に基づいて、どの 2 つの構成変更によってフェーズ 2 が起動しますか (2 つ選択してください)。

A. HQ-FortiGate で、暗号化を AES256 に設定します。

B. HQ-FortiGate で、Diffie-Hellman グループ 2 を有効にします。

C. リモート FortiGate で、リモート アドレスを 10.0.1.0/255.255.255.0 に設定します。

D. リモート FortiGate で、秒数を 43200 に設定します。

Answer: A,C (メーッセージを残す)

最新問題: 32
NGFW プロファイルベース モードの 2 つの機能は何ですか? (2 つ選択してください。)
A. NGFW プロファイル ベース モードは、個々の VDOM ではなく、グローバルにのみ適用できます。
B. NGFWプロファイルベースモードでは、中央ソースNATポリシーの使用が必須です。
C. NGFW プロファイルベース モード ポリシーは、フロー検査とプロキシ検査の両方をサポートします。
D. NGFW プロファイル ベース モードでは、ファイアウォール ポリシーでアプリケーションと Web フィルタリング プロファイルを適用することをサポートします。
Answer: C,D (メーッセージを残す)
NGFW (Next Generation Firewall) profile-based mode in FortiGate allows policies to use both flow-based and proxy-based inspection modes, providing flexibility depending on security and performance requirements. Additionally, profile-based mode supports applying applications and web filtering profiles directly in a firewall policy, allowing granular control over the traffic.
Reference:
FortiOS 7.4.1 Administration Guide: NGFW Mode Configuration

最新問題: 33
展示品を参照してください。

FortiGate はファイアウォール認証用に構成されています。外部 Web サイトにアクセスしようとすると、ログイン プロンプトは表示されません。
この状況の最も可能性の高い理由は何でしょうか?
A. ファイアウォール ポリシーにはサービス DNS が必要です。
B. ユーザーが間違ったユーザー名を使用しています。
C. リモート ユーザー グループは宛先に追加されません。
D. このユーザーに一致するユーザー アカウントが存在しません。
Answer: A (メーッセージを残す)
Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.
Reference:
FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

最新問題: 34
IPS センサーの構成を示す展示を参照してください。

トラフィックがこの IPS センサーと一致した場合、センサーが実行すると予想される 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. センサーは、Microsoft.Windows.iSCSI.Target.DoS シグネチャに一致する攻撃を許可します。

B. センサーは、一致したすべてのトラフィックのパケット ログを収集します。

C. センサーは Windows サーバーを狙ったすべての攻撃をブロックします。

D. センサーはこれらのシグネチャに一致するすべての接続をリセットします。

Answer: A,C (メーッセージを残す**)**

最新問題**: 35**

展示品を参照してください。

NOC チームからのこの特定の要求に応えるために、管理者は何を構成する必要がありますか?

NOC チームは、NOC_Access 管理者プロファイルを使用して FortiGate GUI に接続します。非アクティブなときに GUI セッションが早期に切断されないように要求します。

A. 管理者プロファイルで タイムアウトしない」パラメータを有効にする

B. config system accprofile super_admin の admintimeout 値を増やします。

C. config system globalのadmintimeout値を増やす

D. NOC_Access管理プロファイルのOverride Idle Timeoutパラメータのオフライン値を増やす

Answer: D (メーッセージを残す)
"You can override the idle timeout setting per administartor profile using the Override Idle Timeout setting. You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. Then Override Idel Timeout setting allows the admintimeout value, under the config system accprofile, to be overridden per access profile."

最新問題**: 36**
FortiGate の等コスト マルチパス (ECMP) 構成に関する次の 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。)
A. SD-WAN が有効になっている場合は、パラメータ load-balance-mode を使用して負荷分散アルゴリズムを制御します。
B. SD-WAN が無効になっている場合は、パラメータ v4-ecmp-mode をボリュームベースに設定できます。
C. SD-WANが有効になっている場合、距離と優先度の値が等しくないルートをECMPの一部として設定できます。
D. SD-WAN が無効になっている場合は、構成システム設定で負荷分散アルゴリズムを構成します。
Answer: (解答を表示する)
When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.
Reference:
FortiOS 7.4.1 Administration Guide: ECMP Configuration

最新問題**: 37**
展示品を参照してください。

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool
LAN (port3) → WAN (port1)							
2	Internet_Access	all	all	always	ALL	✓ ACCEPT	
WAN (port1) → LAN (port3)							
3	Allow_access	all	Webserver	always	HTTP HTTPS	✓ ACCEPT	

Sniffer CLI output

```
Local-FortiGate # diagnose sniffer packet any 'icmp' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
4.487597 port3 in 10.0.1.10 -> 10.200.3.1: icmp: echo request
4.487679 port1 out 10.200.1.1 -> 10.200.3.1: icmp: echo reques
4.489203 port1 in 10.200.3.1 -> 10.200.1.1: icmp: echo reply
```

```
FortiGate # diagnose sniffer packet any 'icmp' 4
Original Sniffing Mode
aces=[any]
s=[icmp]
97 port3 in 10.0.1.10 -> 10.200.3.1: icmp: echo request
79 port1 out 10.200.1.1 -> 10.200.3.1: icmp: echo request
03 port1 in 10.200.3.1 -> 10.200.1.1: icmp: echo reply
51 port3 out 10.200.3.1 -> 10.0.1.10: icmp: echo reply
```


展には、ネットワークに接続された FortiGate デバイスの図、VIP 構成、ファイアウォール ポリシー、および FortiGate デバイス上のスニファー CLI 出力が示されています。
WAN (ポート 1) インターフェイスの IP アドレスは 10.200.1.1 /24 です。
LAN (ポート3) インターフェースの IP アドレスは 10.0.1.254/24 です。
Web サーバー ホスト (10.0.1.10) は、リモート サーバー (10.200.3.1) に ping を実行するときに、VIP 外部 IP アドレスを送信元 NAT (SNAT) として使用する必要があります。
この目標を達成するために有効な 2 つのステートメントはどれですか? (2 つ選択してください。)
A. Allow_access ファイアウォール ポリシーで NAT を有効にします。
B. Web サーバーの Internet_Access の前に新しいファイアウォール ポリシーを作成し、IP プールを適用します。
C. Internet_Access ファイアウォール ポリシーで NAT を無効にします。
D. VIP オブジェクトでのポート転送を無効にします。
Answer: A,D (メーッセージを残す)
Enable NAT on the Allow_access firewall policy (A):

The Allow_access firewall policy must have NAT enabled to allow the webserver to use its VIP external IP address (10.200.1.10) as the source NAT when initiating traffic, such as pings, to the remote server.
Disable port forwarding on the VIP object (D):
Port forwarding is designed for specific port mapping, typically for services like HTTP or HTTPS. To use the VIP external IP as a source NAT, port forwarding should be disabled. Disabling port forwarding ensures that the full VIP IP address is used without being tied to specific ports.
Why other options are not correct:
B . Create a new firewall policy before Internet_Access for the webserver and apply the IP pool:
This is unnecessary as the VIP object itself is used for SNAT in this case, and an additional firewall policy is not required.
C . Disable NAT on the Internet_Access firewall policy:
Disabling NAT on this policy would prevent the NAT functionality needed for the webserver to use the VIP external IP address as the source IP.
Thus, enabling NAT on the Allow_access policy and disabling port forwarding on the VIP configuration are the valid steps to achieve the goal.

最新問題**: 38**
FortiGate は NAT モードで動作しており、それぞれ LAN ネットワークと DMZ ネットワークに接続された 2 つの物理インターフェースを備えています。
FortiGate 上の接続された物理インターフェースの要件について正しい記述はどれですか? (2 つ選択してください。)
A. 両方のインターフェースにインターフェースロールが割り当てられている必要があります
B. 両方のインターフェースはルーティングテーブル上に直接接続されたルートを持っている必要があります
C. 両方のインターフェースでDHCPが有効になっている必要があります
D. 両方のインターフェースにIPアドレスを割り当てる必要があります
Answer: (解答を表示する**)**
Both interfaces must have directly connected routes on the routing table In NAT mode, each interface must have a corresponding entry in the routing table, typically as a directly connected route, to route traffic between them effectively.
Both interfaces must have IP addresses assigned
In NAT mode, each interface must have an IP address to participate in routing and NAT operations. The IP addresses allow the FortiGate to forward traffic between different network segments.

最新問題**: 39**
コレクター エージェントの高度なモードの 2 つの機能は何ですか? (2 つ選択してください。)
A. 高度なモードでは、FortiGate を LDAP クライアントとして設定し、FortiGate でグループ フィルターを設定できます。
B. 詳細モードでは、ネストされたグループまたは継承されたグループがサポートされます。
C. 詳細モードでは、セキュリティ プロファイルは個々のユーザーではなく、ユーザー グループにのみ適用できます。
D. 詳細モードでは、Windows 規則 -NetBios: Domain\Username が使用されます。
Answer: (解答を表示する**)**
Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

最新問題**: 40**
展示品を参照してください。

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	Accept (8.08 kB / 27...	1 (DIA)	port2		
YouTube	Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	Accept (3.33 kB / 10...	1 (DIA)	port1		
YouTube	Accept (44.63 kB / 3....	1 (DIA)	port2		
CNN	Accept (UTM Allowed)	1 (DIA)	port1		
CNN	Accept (UTM Allowed)	1 (DIA)	port2		
CNN	Accept (UTM Allowed)	1 (DIA)	port2		

管理者は SD-WAN ルールを設定し、FortiGate トラフィック ログ ページに SD-WAN 固有の列 $D-WAN 品質と SD-WAN ルール名）を表示するように設定しました。
FortiGate はポリシー ID 1 に従ってトラフィックを許可します。これは SD-WAN トラフィックを許可するポリシーです。
これらの設定にもかかわらず、トラフィック ログには、これらのトラフィック フローを制御するために使用される SD-WAN ルールの名前は表示されません。
理由は何でしょうか?

A. FortiGate は暗黙の SD-WAN ルールに従ってトラフィックを負荷分散しました。
B. ファイアウォール ポリシーにアプリケーション制御プロファイルが適用されていません。
C. SD-WAN ルールの宛先はアプリケーションごとに設定されていますが、機能の可視性は有効になっていません。
D. SD-WAN ルール名はすぐには表示されません。管理者はページを更新する必要があります。

Answer: A (メーッセージを残す**)**

If the SD-WAN traffic logs do not show the specific SD-WAN rule name, it likely means that FortiGate is using the default or implicit SD-WAN rule to balance traffic. The implicit rule comes into effect when no explicit SD-WAN rule is matched, and as a result, the SD-WAN rule name is not displayed in the logs. The default behavior is to load balance the traffic across available interfaces based on SD-WAN strategy.