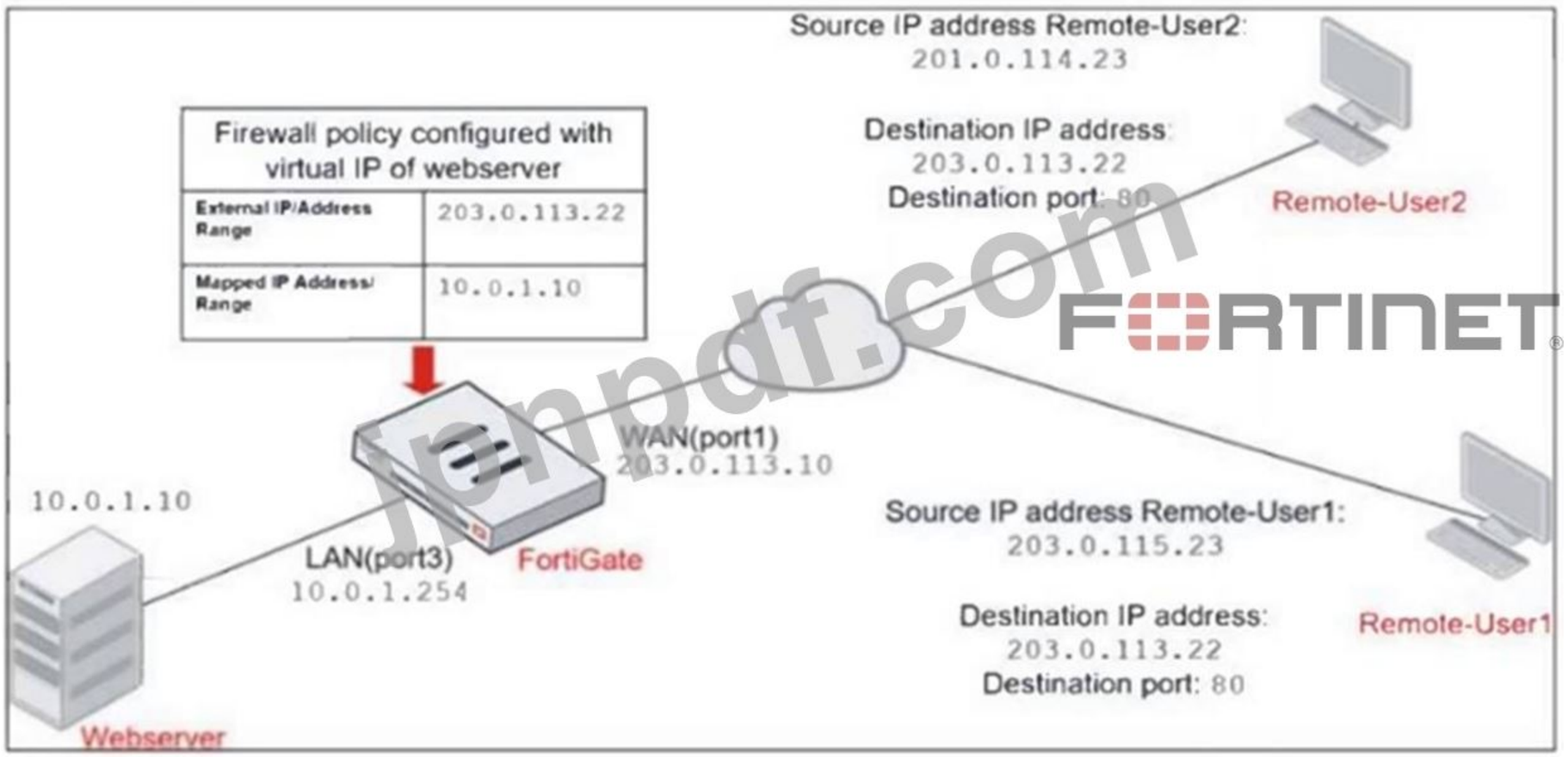
Fortinet.FCP_FGT_AD-7.4-JPN.v2025-05-17.q44

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:	44
バージョン:	v2025-05-17
アクセス数:	300
ページビュー数:	440
https://www.jpnpdf.com/Fortinet.FCP_FGT_AD-7.4-JPN.v2025-05-17.q44-mondaishu.html	

最新問題: 1
ネットワーク管理者は、FortiGate で完全な SSL 検査と Web フィルタリングを有効にしました。HTTPS Web サイトにアクセスすると、ブラウザは証明書の警告エラーを報告します。HTTP Web サイトにアクセスすると、ブラウザはエラーを報告しません。
証明書の警告エラーの原因は何ですか?
A. SSL/SSH検査プロファイルで無効なSSL証明書のオプションが許可されるように設定されています
B. ブラウザは、FortiGate が SSL 検査に使用する証明書を信頼していません
C. FortiGate が SSL 検査に使用する証明書には、必要な証明書拡張機能が含まれていません。
D. 一致するファイアウォール ポリシーがプロキシ検査モードに設定されています
Answer: B (メーッセージを残す**)**
When full SSL inspection is enabled, FortiGate intercepts HTTPS traffic, decrypts it for inspection, and re- encrypts it using its own SSL certificate before forwarding it to the browser. If the browser does not trust the SSL certificate being used by FortiGate for re-encryption, it will display certificate warning errors. To resolve this, the certificate used by FortiGate for SSL inspection must be installed and trusted in the browser's certificate store.

最新問題: 2
展示品を参照してください。

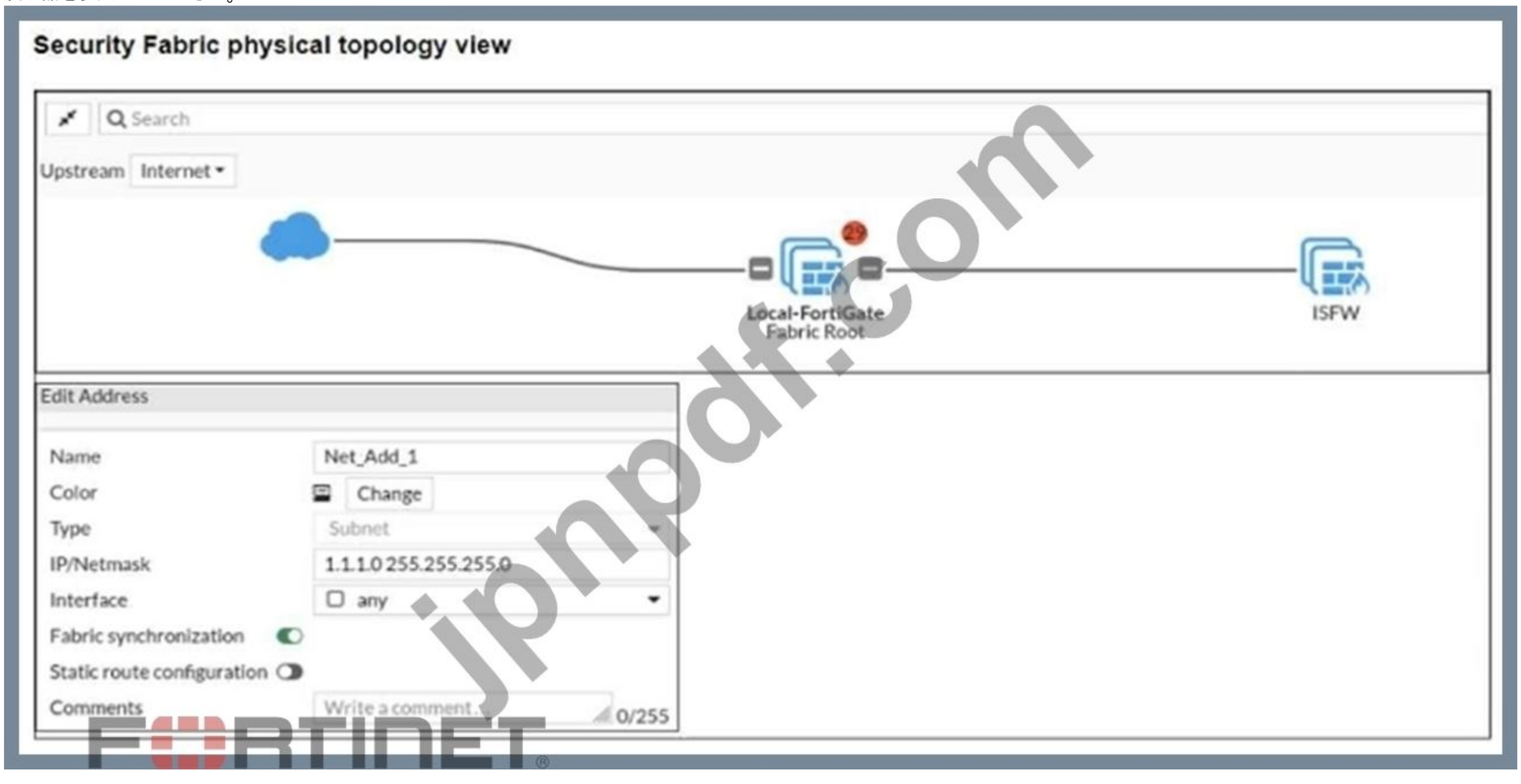
Network diagram



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.
References:
* 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: 3
展示品を参照してください。



Security Fabric configuration on Local-FortiGate

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream ''
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC Y9ynT+64RpCTpVdgSmoQHZ42mYSIzNNzLNvgzMXjyN
9hSjIJE3KYJlo3XxygldvNxPId8T5xctBUszy7tgIcHcA/qHrByXSXfPEeHC6ufkqlPJr
W6GypwDUb5O3VFgPbASFYYteQesmwoJtGe84BLqa+hUcgunLDlz/97sBp+PLt5nrA==
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
```

Security Fabric configuration on ISFW

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "10.0.1.254"
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync local
end

ISFW #
```


管理者は、セキュリティ ファブリックのルート FortiGate (Local-FortiGate) に新しいアドレス オブジェクトを作成します。同期後、このオブジェクトはダウンストリーム FortiGate (ISFW) では使用できません。
アドレス オブジェクトを同期するには、管理者は何を行う必要がありますか?
A. Local-FortiGate (ルート) の csf 設定を sec fabric-object-unification default に変更します。
B. 両方のデバイスの csf 設定を sec downscream-access enable に変更します。
C. ISFW (ダウンストリーム) の csf 設定を sec auchorizacion-requesc-cype certificace に変更します。
D. ISFW (ダウンストリーム) の csf 設定を sec configuration-sync local に変更します。
Answer: A (メーッセージを残す**)**
The current setting for the root FortiGate (Local-FortiGate) is fabric-object-unification local, which means that new address objects are not shared across the security fabric. Changing this setting to fabric-object-unification default will allow address objects to be synchronized and shared with downstream devices like the ISFW.

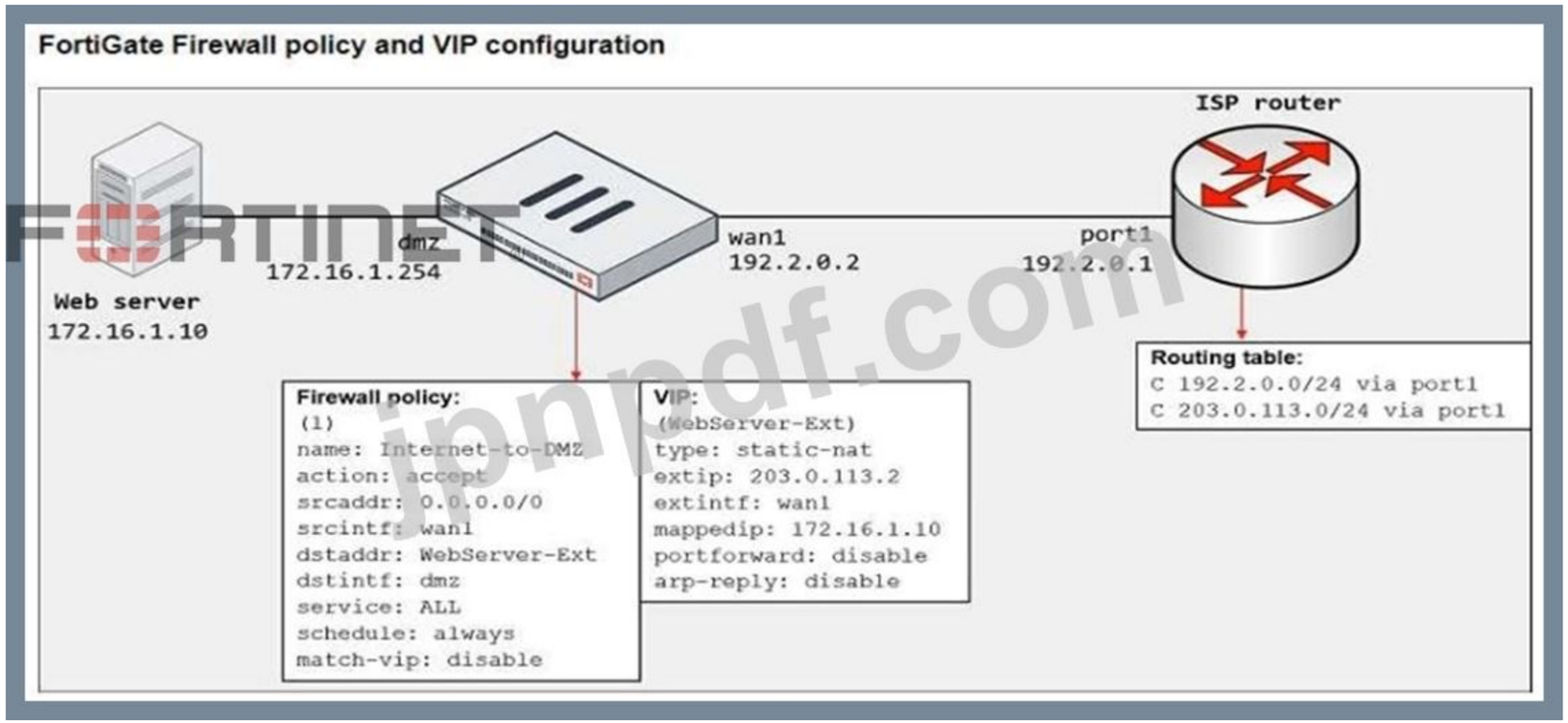
最新問題: 4
オートメーションステッチの特徴として正しい記述はどれですか?
A. セキュリティ ファブリック内のデバイスでのみ実行できます。
B. ファブリック内のダウンストリーム デバイス上でのみ作成できます。
C. 1 つ以上のトリガーを持つことができます。
D. 複数のアクションを同時に実行できます。
Answer: (解答を表示する**)**

Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.
References:
* FortiOS 7.4.1 Administration Guide: Automation Stitches

最新問題**: 5**
ネットワーク接続なしで FortiGate CLI への管理アクセスを可能にする方法はどれですか?
A. SSHコンソール
B. CLI コンソール ウィジェット
C. シリアルコンソール
D. Telnet コンソール
Answer: C (メーッセージを残す**)**
The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.
References:
* FortiOS 7.4.1 Administration Guide: Console connection

最新問題**: 6**
FortiGuard カテゴリはオーバーライドして、別のカテゴリで定義できます。example.com ホームページの Web 評価オーバーライドを作成するには、オーバーライドを特定の構文を使用して構成する必要があります。
ホームページの Web 評価オーバーライドを構成するには、どの 2 つの構文が正しいですか? (2 つ選択してください。)
A. www.example.com:443
B. www.example.com
C. www.example.com/index.hrml
D. example.com
Answer: B,D (メーッセージを残す**)**
www.example.com
This syntax targets the main domain, which is a common way to configure a web rating override for the home page of a website.
example.com
This syntax also correctly targets the main domain without specifying a subdomain (like "www"), which is valid for configuring a web rating override for the entire site, including the home page.

最新問題**: 7**
展示品を参照してください。



この図には、ネットワークに接続された FortiGate デバイスの図、FortiGate デバイス上のファイアウォール ポリシーと VIP 構成、および ISP ルーター上のルーティング テーブルが示されています。
管理者がインターネットから Web サーバーのパブリック アドレス (203.0.113.2) にアクセスしようとすると、接続がタイムアウトします。同時に、管理者は FortiGate でスニファーを実行して、サーバーへの着信 Web トラフィックをキャプチャしますが、出力は表示されません。
展示に示されている情報に基づいて、接続の問題を解決するために管理者はどのような構成変更を行う必要がありますか?
A. アドレス 203.0.113.2/32 のループバック インターフェイスを設定します。
B. VIP 設定で、arp-reply を有効にします。
C. ファイアウォール ポリシー設定で、match-vip を有効にします。
D. サーバー上でポート転送を有効にして、外部サービス ポートを内部サービス ポートにマップします。
Answer: B (メーッセージを残す**)**
In this scenario, the FortiGate device is using a Virtual IP (VIP) to map the public IP address (203.0.113.2) to the internal IP address of the web server (172.16.1.10). The fact that the administrator does not see any sniffer output for incoming traffic suggests that the FortiGate is not responding to ARP requests for the public IP address (203.0.113.2).
Enabling arp-reply in the VIP configuration allows the FortiGate to respond to ARP requests for the public IP, thereby allowing traffic to reach the FortiGate, which will then forward it to the web server based on the VIP mapping.

最新問題**: 8**
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.
References
* 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**: 9**
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: A,D (メーッセージを残す)
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.
References:
* FortiOS 7.4.1 Administration Guide: ECMP Configuration

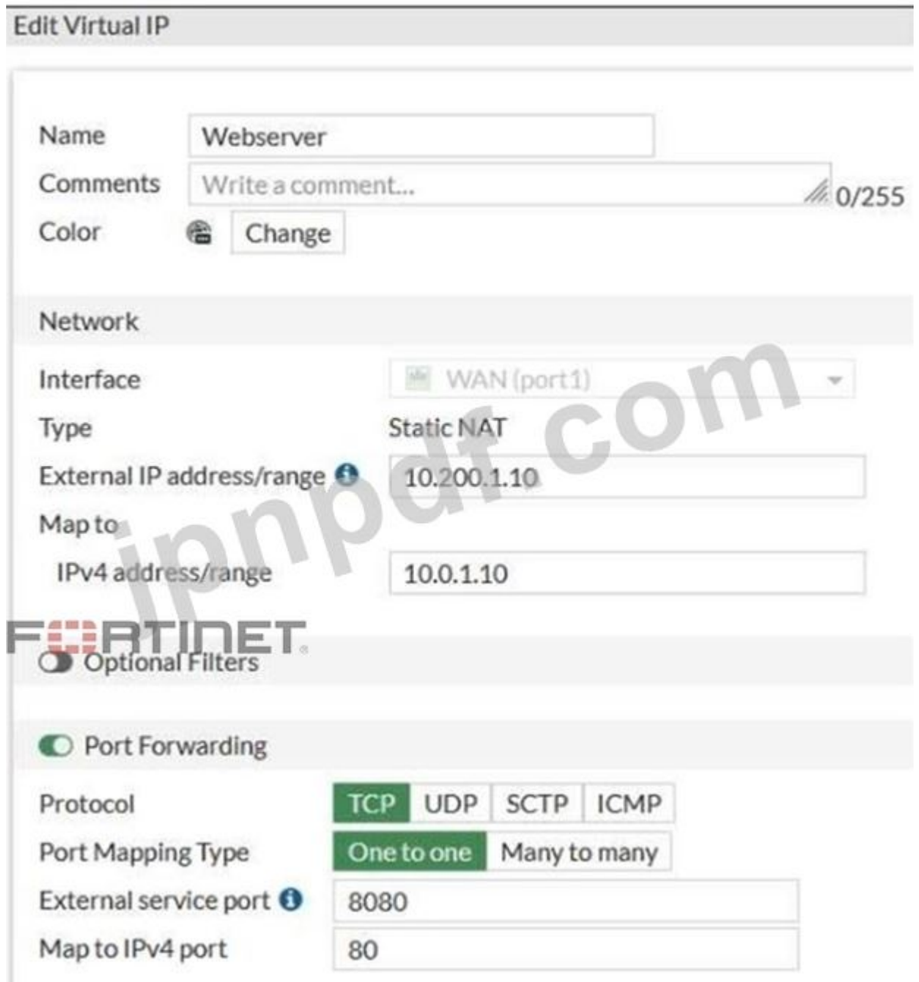
最新問題**: 10**
RPF チェックの使用方法を説明する 2 つの文はどれですか? (2 つ選択してください。)
A. RPF チェックは、新しいセッションの最初の送信パケットに対して実行されます。
B. RPF チェックは、新しいセッションの最初の応答パケットに対して実行されます。
C. RPF チェックは、新しいセッションの最初の送信パケットと応答パケットに対して実行されます。
D. RPF チェックは、FortiGate とネットワークを IP スプーフィング攻撃から保護するメカニズムです。
Answer: (解答を表示する)
The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.
References:

* FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

最新問題**: 11**

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



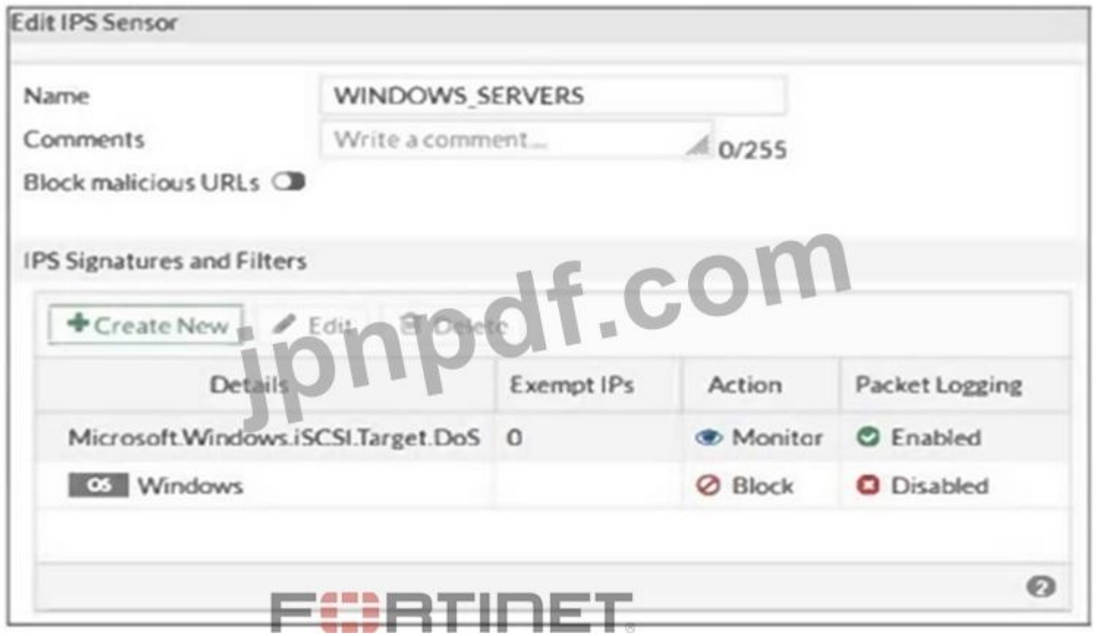
Firewall policy configuration

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.

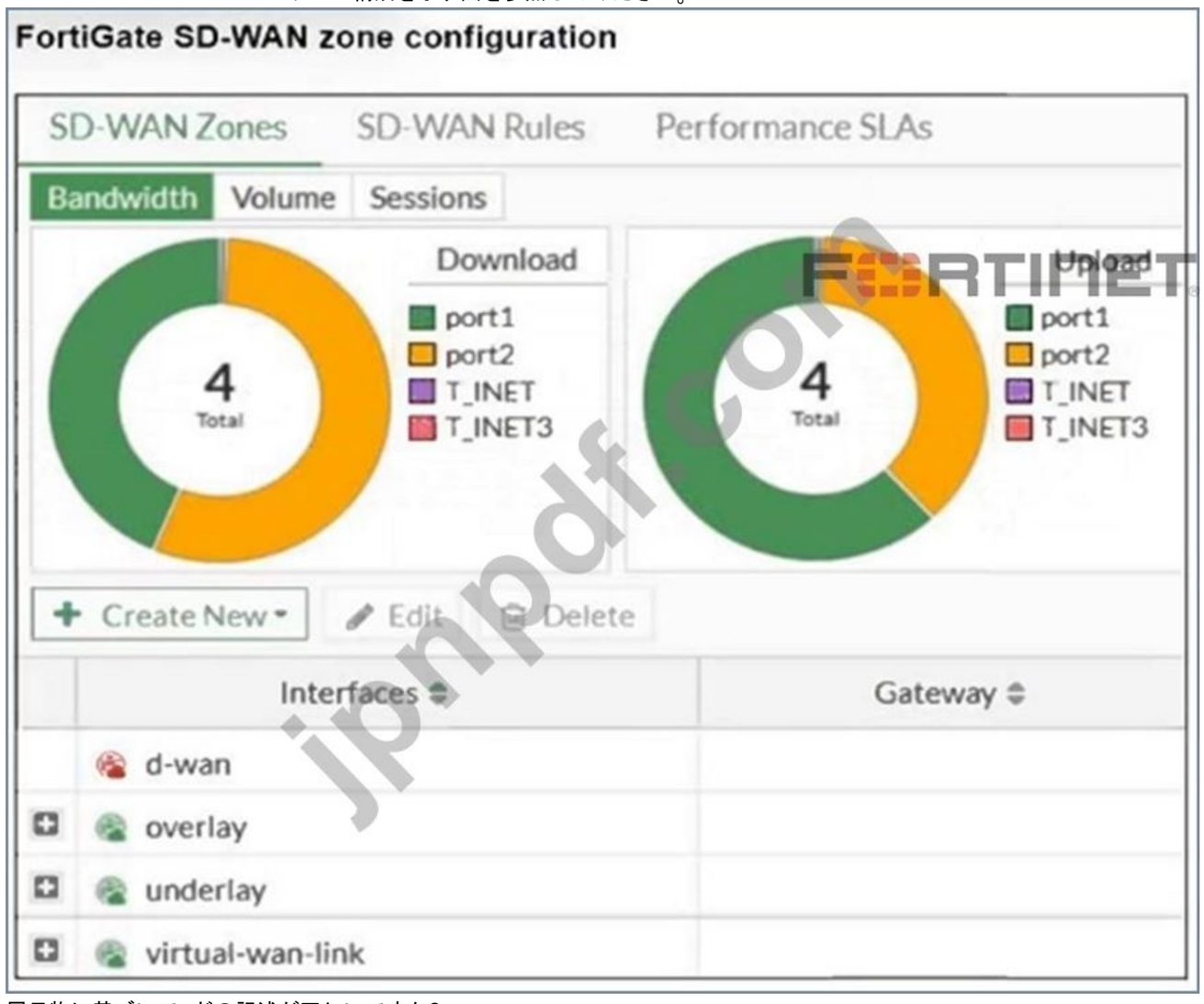
最新問題**: 12**
IPS センサーの構成を示す展示を参照してください。



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、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。
B. 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。
C. 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。
D. 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。
Answer: A,C (メーッセージを残す)
The IPS sensor configuration shows that:
* The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.
* The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.
Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.
References:
* FortiOS 7.4.1 Administration Guide: IPS Configuration

最新問題: **13**

FortiGate GUI 上の SD-WAN ゾーン構成を示す図を参照してください。



展示物に基づいて、どの記述が正しいですか?

A. アンダーレイゾーンにはポート1と

B. d-wan ゾーンにメンバーが含まれていません。

C. d-wan ゾーンは削除できません。

D. 仮想 WAN リンク ゾーンにメンバーが含まれていません。

Answer: B (メーッセージを残す**)**

The "d-wan" zone in FortiGate SD-WAN configuration is the default SD-WAN zone created when SD-WAN is enabled. This zone contains all the interfaces assigned to SD-WAN and is essential for the functionality of the SD-WAN feature. The "d-wan" zone cannot be deleted because it is required for SD-WAN operations.
Option A is incorrect because the underlay zone does not contain port1. Options B and D are incorrect because they incorrectly describe the configuration of zones.
References:
* FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

最新問題**: 14**
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**: 15**
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: (解答を表示する**)**
In a multi-VDOM environment, each VDOM can be treated as an independent virtual firewall, and each VDOM can belong to a separate Security Fabric. This allows administrators to configure and manage separate Security Fabrics for different VDOMs, providing flexibility in managing security policies and fabric connections across virtual domains.

最新問題**: 16**
SSL 検査で CA 証明書として使用できるようにするには、証明書に必要な 2 つの属性はどれですか? (2 つ選択してください。)
A. 発行者はパブリック CA である必要があります
B. CA拡張はTRUEに設定する必要があります
C. 認証局キー識別子はSSLタイプである必要があります
D. keyUsage拡張は次のように設定する必要があります
Answer: (解答を表示する**)**
The CA extension must be set to TRUE
This indicates that the certificate can be used to issue other certificates, a requirement for it to function as a CA.
The keyUsage extension must be set to keyCertSign
This specifies that the certificate can be used to sign other certificates, which is essential for a CA certificate.

最新問題: **17**
展示品を参照してください。

図に示されている侵入防止システム (IPS) 診断コマンドを調べます。
オプション 5 を IPS 診断コマンドで使用し、結果として CPU 使用率が減少した場合、正しい結論は何ですか?
A. IPS エンジンがすべてのトラフィックをブロックしています。
B. IPS エンジンは大量のトラフィックを検査しています。
C. IPS エンジンは侵入攻撃を防ぐことができません。
D. IPS エンジンは通常の状態で動作を続けます。
Answer: (解答を表示する**)**
Option 5 in the IPS diagnostic command toggles the bypass status. If this option is used and results in a decrease in CPU usage, it means the IPS engine is no longer processing traffic, effectively blocking or bypassing the traffic. In this case, IPS is not inspecting the traffic anymore, leading to a decrease in CPU usage, which indicates that the traffic might be blocked instead of inspected.

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: (解答を表示する)
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**
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: A (メーッセージを残す)
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**: 20**
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: (解答を表示する**)**
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.

最新問題**: 21**
展示品を参照してください。

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. 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。
B. 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。
C. 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。
D. 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。
Answer: C (メーッセージを残す**)**
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.
References:
* FortiOS 7.4.1 Administration Guide: Firewall Policy Views

最新問題: **22**
FortiGuard 接続のデバッグ出力を示す展示を参照してください。

FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale        : english

Service       : Web-filter
Status        : Enable
License       : Contract

Service       : Antispam
Status        : Disable

Service       : Virus Outbreak Prevention
Status        : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Thu Jun  9 11:26:56 2022) -=-

IP              Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
173.243.141.16      -8   18     DI   0                    4          0           0  Thu Jun  9 11:26:24 2022
12.34.97.18         20   30          1                    1          0           0  Thu Jun  9 11:26:24 2022
210.7.96.18        160  305          9                    0          0           0  Thu Jun  9 11:26:24 2022
```

出力に基づいて、管理者は FortiGuard 接続についてどの 2 つの事実を知っていますか? (2 つ選択してください。)

A. 契約情報を取得するために 1 つのサーバーに接続されました。

B. 連続してパケットを失ったサーバーが少なくとも 1 台あります。

C. ローカル FortiManaqer は、FortiGate が通信するサーバーの 1 つです。

D. FortiGate はデフォルトの FortiGuard 通信設定を使用しています。

Answer: A,D (メーッセージを残す)

The debug output indicates that FortiGate connected to one server (173.243.141.16) to retrieve contract information as it shows four FortiGuard requests without any packet loss, which confirms the connection to the server. Additionally, the default FortiGuard communication settings are being used, as indicated by the use of the HTTPS protocol on port 443, which is the default setting for FortiGuard connections.

References:

* FortiOS 7.4.1 Administration Guide: FortiGuard Connection Settings

最新問題**: 23**
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。

Security profile

Name: Facebook Access

Comments: 0/255

FORTINET

Categories

Mixed - All Categories

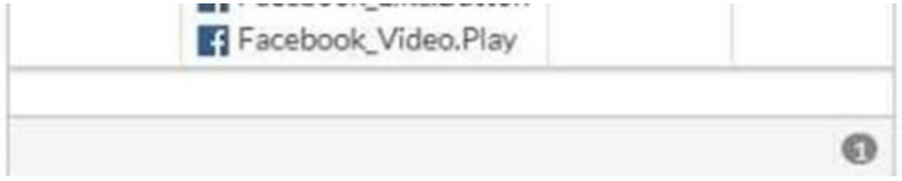
Business (179, 6)	Cloud/IT (31)
Collaboration (293, 6)	Email (87, 12)
Game (124)	General Interest (241, 9)
Mobile (3)	Network Service (332)
P2P (85)	Proxy (106)
Remote Access (91)	Social Media (150, 31)
Storage/Backup (296, 16)	Update (48)
Video/Audio (206, 13)	VoIP (31)
Web Client (18)	Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	Facebook Facebook_Like.Button	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. SSL検査をディープコンテンツ検査にする
B. セキュリティポリシーのURLカテゴリにFacebookを追加する
C. WebブラウザでHTTPからHTTPSへのリダイレクトを無効にする
D. 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
Answer: (解答を表示する**)**
In the security profile, there are application overrides for specific Facebook-related features, such as
"Facebook" and "Facebook_Video.Play." However, the absence of specific signatures for actions like
"Facebook_Like.Button" might be preventing reactions. You need to ensure that the necessary application signatures for all desired Facebook features, including reactions (like buttons), are included in the security policy.
Therefore, retrieving or adding those signatures would resolve the issue.

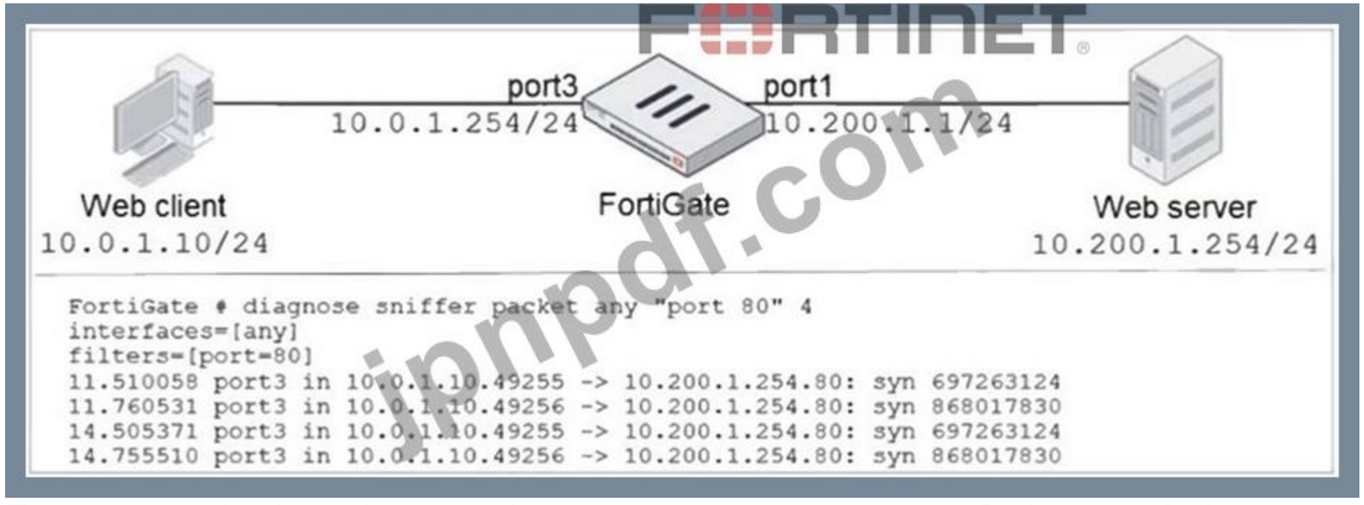
最新問題**: 24**
管理者が次の設定を構成しました:

この構成の 2 つの結果は何ですか? (2 つ選択してください。)
A. 拒否されたユーザーは 30 分間ブロックされます。
B. 拒否されたトラフィックのセッションが作成されます。
C. 拒否されたトラフィックによって生成されるログの数が削減されます。
D. すべてのインターフェースでのデバイス検出が 30 分間強制されます。
Answer: B,C (メーッセージを残す**)**
A session for denied traffic is created.
The command set ses-denied-traffic enable ensures that sessions for denied traffic are logged, meaning a session will be created for traffic that is denied by security policies.
The number of logs generated by denied traffic is reduced.
The set block-session-timer 30 command sets a timer to prevent excessive logging of denied traffic within a short period, which helps reduce the number of logs generated by repeated denied traffic sessions. This timer blocks sessions for a specified period (30 seconds in this case) to avoid overwhelming the log system with repetitive entries.

最新問題**: 25**
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,D (メーッセージを残す)
By default, SD-WAN members are skipped if they do not have a valid route to the destination SD-WAN ensures that only members with valid routes to the destination are considered during routing decisions.
By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member If the best route is not an SD-WAN member, SD-WAN rules are bypassed and standard routing takes over.
SD-WAN rules have precedence over any other type of routes
SD-WAN rules are evaluated first, meaning they take precedence over other routing mechanisms, such as static routes or policy-based routes.

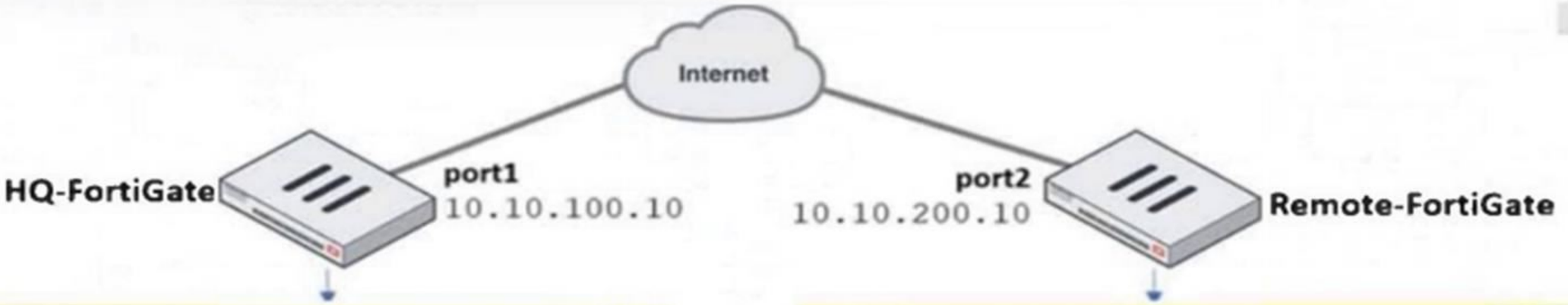
最新問題**: 26**
展示品を参照してください。



図に示すネットワークでは、Web クライアントは HTTP Web サーバーに接続できません。管理者は FortiGate 組み込みスニファーを実行し、図に示す出力を取得します。
問題をトラブルシューティングするために、管理者は次に何をすべきでしょうか?
A. デバッグフローを実行します。
B. part1 に接続された外部スニファーを使用してトラフィックをキャプチャします。
C. 今回はフィルター「host 10.o.1.10」を使用して、FortiGate で別のスニファーを実行します。
D. Web サーバー上でスニファーを実行します。
Answer: A (メーッセージを残す)
The sniffer output shows that packets from the web client are reaching the FortiGate and being forwarded to the web server, but there is no indication that the web server is responding. To troubleshoot this issue, executing a debug flow will help analyze the traffic path and pinpoint where the problem might be occurring, such as a possible issue in firewall policy or route settings that is causing the server not to respond correctly.
References:
* FortiOS 7.4.1 Administration Guide: Troubleshooting network connectivity

最新問題**: 27**
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

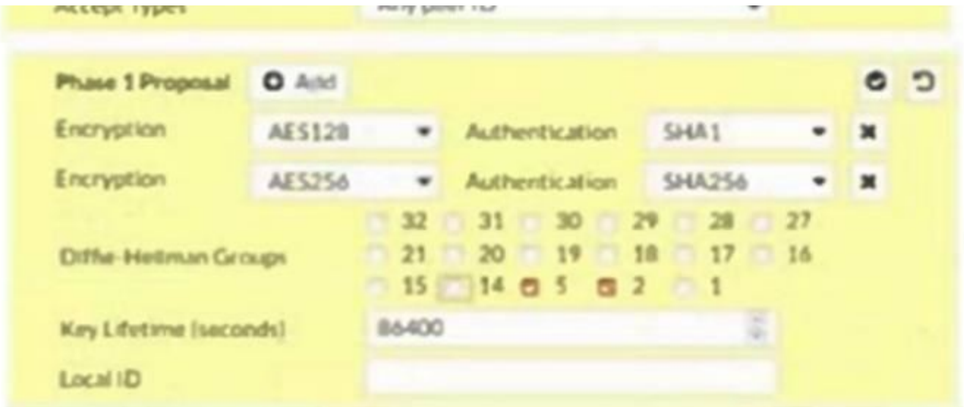
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	1 / 2
Mode	Aggressive / Main (ID protection)
Peer Options	
Accept Types	Any peer ID

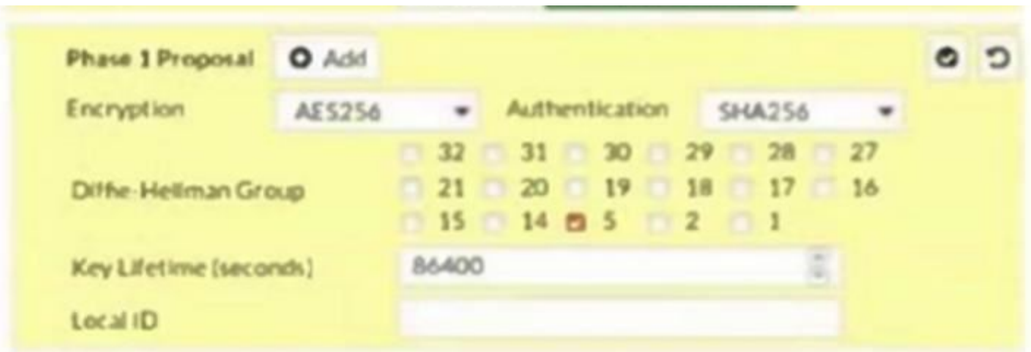
Network

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
Mode	Aggressive / Main (ID protection)





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: C,D (メーッセージを残す)
To bring Phase 1 up, the following changes can be made:
* A. On HQ-FortiGate, disable Diffie-Helman group 2: This is incorrect because Diffie-Hellman group 2 is already selected on both devices. Disabling it would not help.
* B. On Remote-FortiGate, set port2 as Interface: This is incorrect as both sides should be consistent in their interface settings for the IPsec tunnel, and the interface is correctly set to port1 on both FortiGates in the IPsec configuration.
* C. On both FortiGate devices, set Dead Peer Detection to On Demand: This is a valid option.
Setting Dead Peer Detection (DPD) to "On Demand" helps maintain the IPsec connection by checking if the peer is still available, which can help in some cases where the connection fails due to timeouts.
* D. On HQ-FortiGate, set IKE mode to Main (ID protection): This is also a valid option because the Remote-FortiGate is already set to Main mode (ID protection). Ensuring that both ends use the same mode is crucial for successful phase 1 negotiation.
Thus, the correct answers are:C. On both FortiGate devices, set Dead Peer Detection to On Demand.D.
On HQ-FortiGate, set IKE mode to Main (ID protection).

最新問題**: 28**
管理者は FortiGate で厳密な RPF チェックを設定しました。
厳密な RPF チェックはどのように機能しますか?
A. 厳密な RPF は、着信インターフェイスを使用して送信元への最適なルートをチェックします。
B. 厳密な RPF では、すべてのアクティブなルートを使用してパケットを送信元に戻すことができます。
C. 厳密な RPF は、着信インターフェイスを使用して送信元に戻るアクティブなルートが少なくとも 1 つ存在するかどうかのみをチェックします。
D. 新しいセッションの最初の送信パケットと応答パケットに対して厳密な RPF チェックが実行されます。
Answer: A (メーッセージを残す)
Strict RPF (Reverse Path Forwarding) check ensures that the packet is received on the same interface that the FortiGate device would use to send traffic back to the source. It verifies that the best route to the source of the packet is through the same interface it arrived on, enhancing security by preventing IP spoofing. If the check fails, the packet is dropped.

最新問題**: 29**
HA オーバーライド設定が無効になっている場合のプライマリ FortiGate 選択プロセスは何ですか?
A. 接続されている監視対象ポート > 優先度 > システム稼働時間 > FortiGate のシリアル番号
B. 接続されている監視対象ポート > システム稼働時間 > 優先度 > FortiGate のシリアル番号
C. 接続されている監視ポート > 優先度 > HA 稼働時間 > FortiGate のシリアル番号
D. 接続されている監視ポート > HA 稼働時間 > 優先度 > FortiGate シリアル番号
Answer: (解答を表示する**)**
When the HA override setting is disabled, FortiGate uses the primary election process based on the following criteria:
* Connected monitored ports: The unit with the most monitored ports up is preferred.
* Priority: The unit with the highest priority is preferred.
* System uptime: The unit with the longest uptime is preferred.
* FortiGate serial number: Used as the final criterion to break any remaining ties.
References:
* FortiOS 7.4.1 Administration Guide: HA election process

最新問題**: 30**
FortiGate HA メンバー間で同期される情報はどれですか? (2 つ選択してください。)
A. OSPF隣接関係
B. IPsec セキュリティ アソシエーション
C. BGPピアリング
D. DHCPリース
Answer: (解答を表示する**)**
IPsec security associations
IPsec security associations (SAs) are synchronized between HA members to ensure seamless failover and continuity of VPN tunnels.
DHCP leases
DHCP lease information is synchronized between HA members to maintain consistent IP address assignments and prevent disruptions when failover occurs.

最新問題**: 31**
展示品を参照してください。

この図は、企業の Web フィルター プロファイルの FortiGuard カテゴリ ベース フィルター セクションを示しています。
管理者は、フリーウェアおよびソフトウェアのダウンロード カテゴリに属する download.com へのアクセスをブロックする必要があります。管理者は、同じカテゴリの他の Web サイトも許可する必要があります。
要件を満たす 2 つの解決策は何ですか? (2 つ選択してください。)
A. アクション Deny と、宛先アドレスとして *.download,com の FQDN アドレス オブジェクトを指定した別のファイアウォール ポリシーを構成します。
B. フリーウェアとソフトウェアのダウンロード カテゴリのアクションを警告に設定する
C. ダウンロード、com の Web オーバーライド評価を構成し、サブカテゴリとして悪意のある Web サイトを選択します。
D. タイプとアクションをそれぞれワイルドカードとブロックに設定して、download、com の静的 URL フィルター エントリを構成します。
Answer: (解答を表示する**)**
To block access specifically to download.com while allowing other sites in the "Freeware and Software Downloads" category, you can create a separate firewall policy with a deny action specifically for the FQDN *.download.com. This approach allows blocking this particular site without affecting the other sites in the same category. Alternatively, configuring a static URL filter entry with the type set to Wildcard and action set to Block will also achieve the desired effect by directly blocking the specific URL without impacting other sites in the category.
References:

* FortiOS 7.4.1 Administration Guide: URL filter configuration

最新問題**: 32**
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. 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。
B. 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
C. 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。
D. 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。
E. 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。
Answer: B,C,E (メーッセージを残す**)**
Flow-based inspection optimizes performance compared to proxy-based inspection.
Flow-based inspection scans traffic in real-time as it passes through, resulting in better performance compared to proxy-based inspection, which buffers traffic.
FortiGate buffers the whole file but transmits to the client at the same time.
In flow-based inspection, the file is scanned while it is being transmitted, improving speed and reducing latency.
The IPS engine handles the process as a standalone.
In flow-based antivirus inspection, the IPS engine is used to inspect traffic, making it more efficient and integrated within the broader security mechanisms.

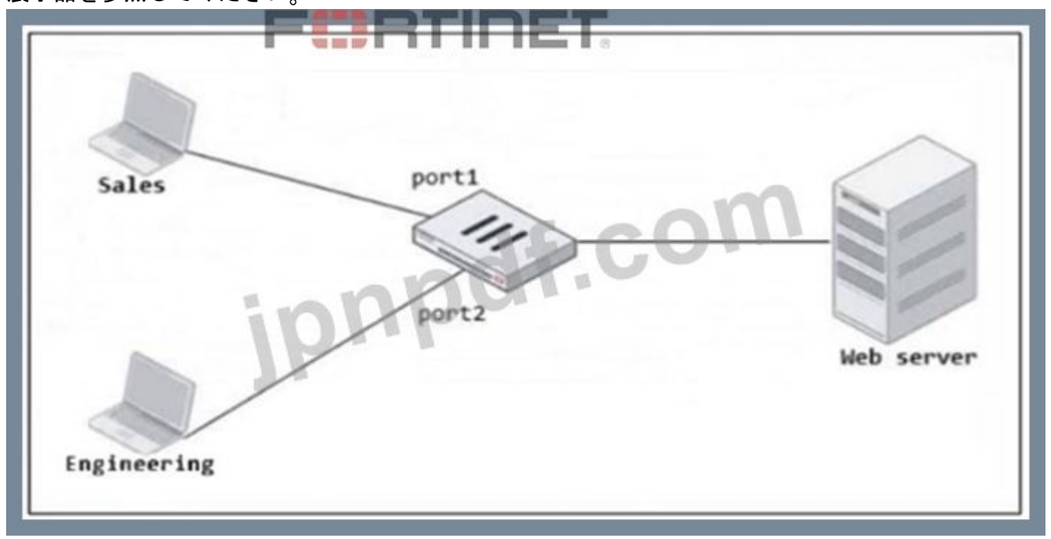
最新問題**: 33**
FortiGate は FortiAnalyzer および FortiManager と統合されています。
ファイアウォール ポリシーを作成すると、機能性を向上させ、FortiAnalyzer または FortiManager へのログの記録をサポートするために、どの属性がポリシーに追加されますか?
A. ログID
B. ポリシーID
C. (シーケンスID
D. ユニバーサルユニーク識別子
Answer: D (メーッセージを残す**)**
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

最新問題**: 34**
展示品を参照してください。

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	ACCEPT	NAT	Standard	WEB Category_Monitor SSL certificate-inspection

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: (解答を表示する**)**
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.
References:
* FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

最新問題: 35
展示品を参照してください。

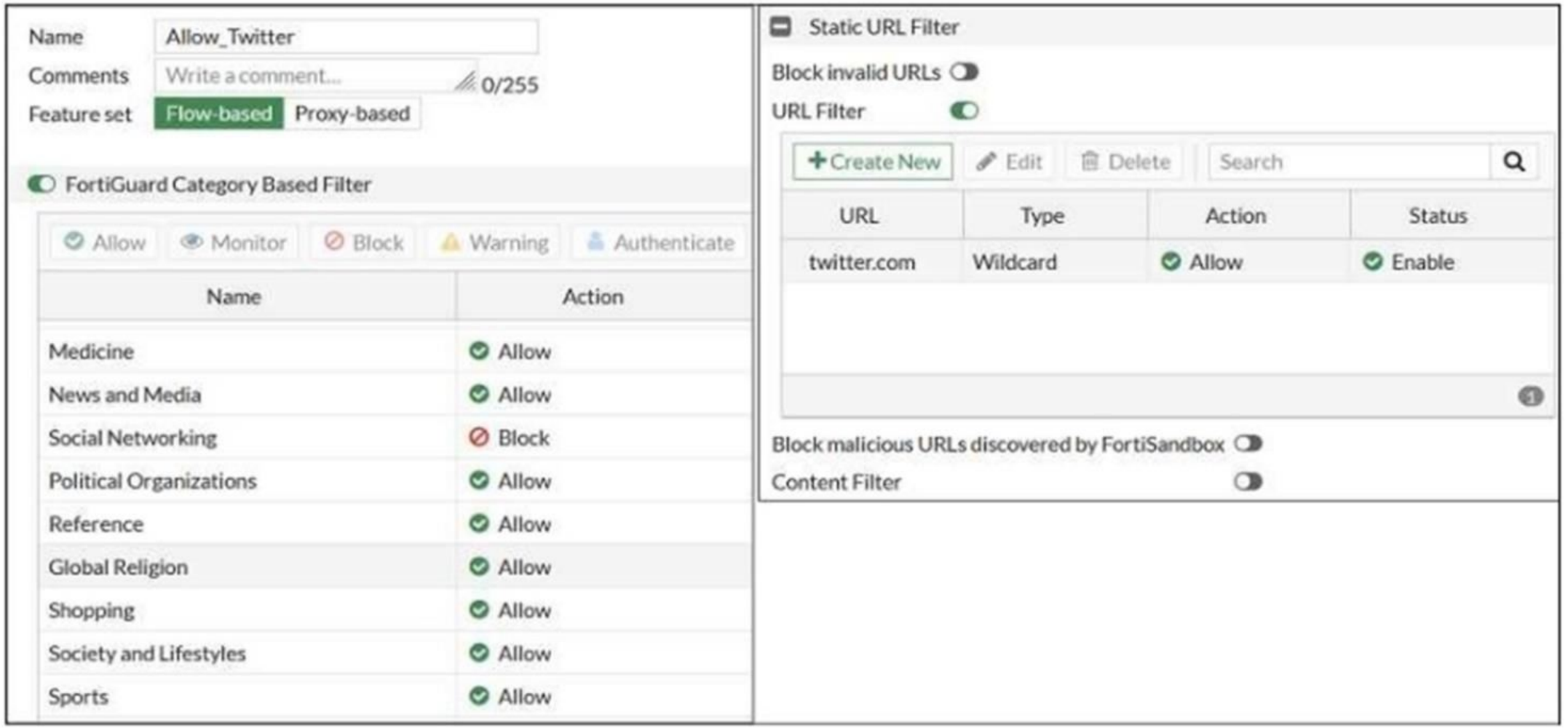


FortiGate には、営業部門とエンジニアリング部門が同じセキュリティ プロファイルを使用して同じ Web サーバーにアクセスするための 2 つの個別のファイアウォール ポリシーがあります。
2 つのポリシーを 1 つに統合するには、管理者はどのアクションを実行する必要がありますか?

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: (解答を表示する**)**
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.
References:
* FortiOS 7.4.1 Administration Guide: Firewall Policy Configuration

最新問題**: 36**
展示品を参照してください。

FortiGate web filter profile configuration



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

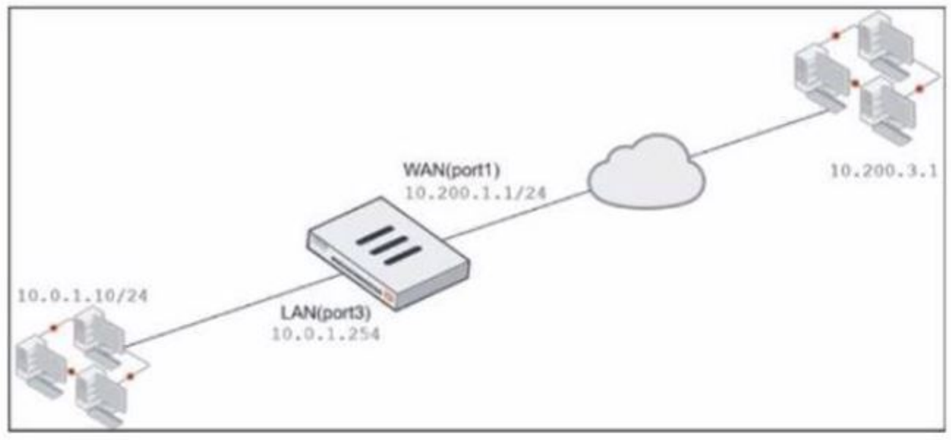
Answer: D (メーッセージを残す**)**

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: **37**
管理者は、エージェントレス ポーリング モードのコレクターとして機能するように FortiGate を設定しました。
AD ユーザー グループ情報を取得するために、管理者は FortiGate デバイスに何を追加する必要がありますか?
A. LDAP サーバー
B. RADIUS サーバー
C. DHCPサーバー
D. Windows サーバー
Answer: A (メーッセージを残す**)**
To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

最新問題: **38**
展示品を参照してください。

Network diagram



VIP object configuration

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
```

展示には、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**: 39**
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. porc2 上のデフォルト ルートはスタンバイ ルートとしてマークされます。
Answer: C,D (メーッセージを残す)
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.
References:
* FortiOS 7.4.1 Administration Guide: Default route configuration
* FortiOS 7.4.1 Administration Guide: Routing table explanation

最新問題**: 40**
FortiGate ファイアウォール ポリシーはアクティブ認証で構成されていますが、ユーザーは Web サイトにアクセスするときに認証できません。
ユーザーが認証できない場合でも、FortiGate はどのプロトコルを許可する必要がありますか?
A. LDAP
B. ICMP
C. DNS
D. DHCP
Answer: C (メーッセージを残す)

最新問題**: 41**
ファイアウォール ポリシーとウイルス対策プロファイルの構成を示す展示を参照してください。

感染したファイルを初めてダウンロードするときに、ユーザーがブロック置換メッセージを受信できないのはなぜですか?

A. フローベースの検査モードを使用する場合は、侵入防止セキュリティ プロファイルを有効にする必要があります。

B. 検査のためにファイルを FortiSandbox に送信するオプションが有効になっています。

C. ファイアウォール ポリシーは、ファイルに対して完全なコンテンツ検査を実行します。

D. フローベースの検査が使用され、最後のパケットがユーザーにリセットされます。

Answer: D (メーッセージを残す**)**

In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

最新問題**: 42**

Web アプリケーションを検査するためのアプリケーション制御の使用に関して正しい記述はどれですか?

A. アプリケーション制御は子アプリケーションと親アプリケーションを識別し、それぞれに対して異なるアクションを実行できます。

B. アプリケーション制御シグネチャは、Fortinet Antivirusエンジンに含まれています

C. アプリケーション制御では、ブロックされたWebアプリケーションの代替メッセージは表示されません。
D. アプリケーション制御では、Web アプリケーションの識別に SSL 検査は必要ありません。
Answer: (解答を表示する**)**
FortiGate's application control can differentiate between parent and child applications and allows administrators to configure distinct actions for each. For example, it can identify Facebook (parent application) and specific functions within it (child applications) like Facebook video or chat, enabling more granular control over application traffic.

最新問題**: 43**
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. 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。
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. 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。
Answer: (解答を表示する**)**
In a multi-VDOM environment, each VDOM can be treated as an independent virtual firewall, and each VDOM can belong to a separate Security Fabric. This allows administrators to configure and manage separate Security Fabrics for different VDOMs, providing flexibility in managing security policies and fabric connections across virtual domains.

最新問題**: 44**
ネットワーク管理者は、完全な SSL 検査用に定義され、プライベート CA 証明書が設定された SSL/SSH 検査プロファイルを構成しました。トラフィックを許可するファイアウォール ポリシーは、SSL 検査にこのプロファイルを使用し、Web フィルタリングを実行します。HTTPS Web サイトにアクセスすると、ブラウザーは証明書の警告エラーを報告します。
証明書の警告エラーの理由は何ですか?
A. SSL 検査プロファイルで SSL 暗号準拠オプションが有効になっていません。SSL 検査プロファイルがプライベート CA 証明書で定義されている場合は、この設定が必要です。
B. FortiGate が SSL 検査に使用する証明書には、必要な証明書拡張機能が含まれていません。
C. ブラウザは、使用中の証明書が信頼できる CA によって署名されたものとして認識しません。
D. 完全な SSL 検査では、ブラウザ レベルで証明書の警告エラーを回避することはできません。
Answer: C (メーッセージを残す**)**
The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.
References:
* FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration