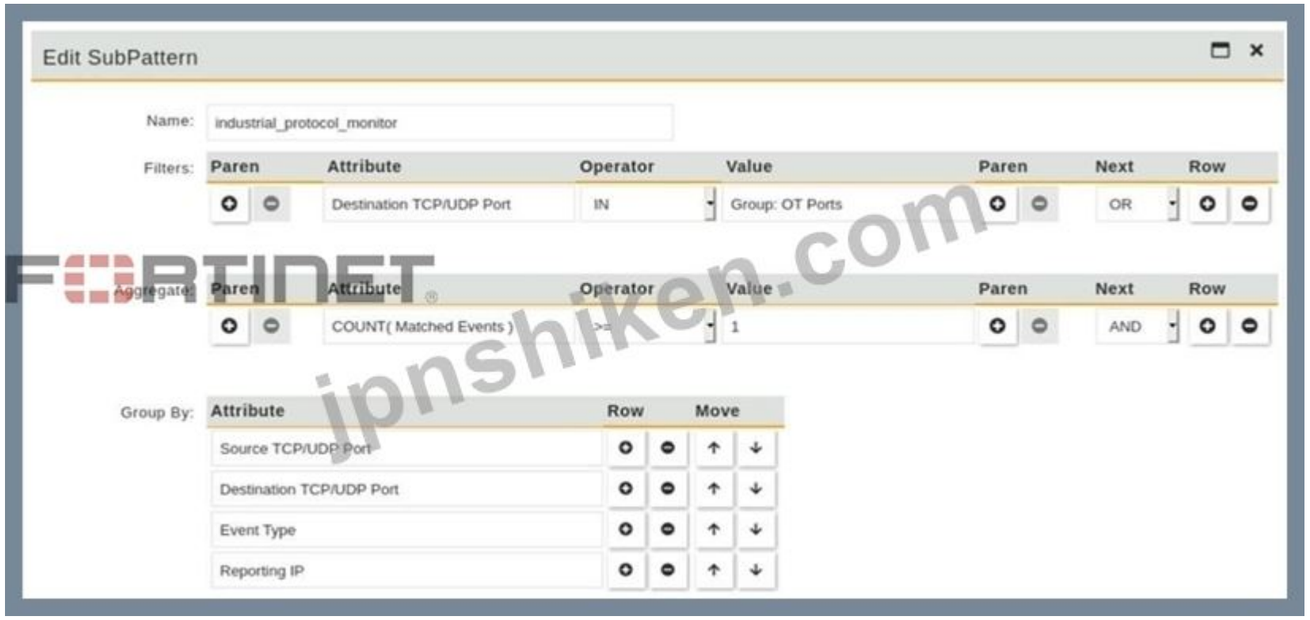
Fortinet.NSE6_OTS_AR-7.6.v2026-08-01.q91

試験コード：	NSE6_OTS_AR-7.6
試験名称：	Fortinet NSE 6 - OT Security 7.6 Architect
認証ベンダー：	Fortinet
無料問題の数：	91
バージョン：	v2026-08-01
ページの閲覧量：	104
問題集の閲覧量：	981

https://www.jpnshiken.com/shiken/Fortinet.NSE6_OTS_AR-7.6.v2026-08-01.q91.html

質問: **1**
図を参照してください。FortiSIEM 上の Modbus プロトコル トラフィックを監視するための新しい運用技術ルールが作成されています。
ネットワーク上のすべてのModbusメッセージがルールに合致するようにするには、どの操作を行うべきでしょうか？

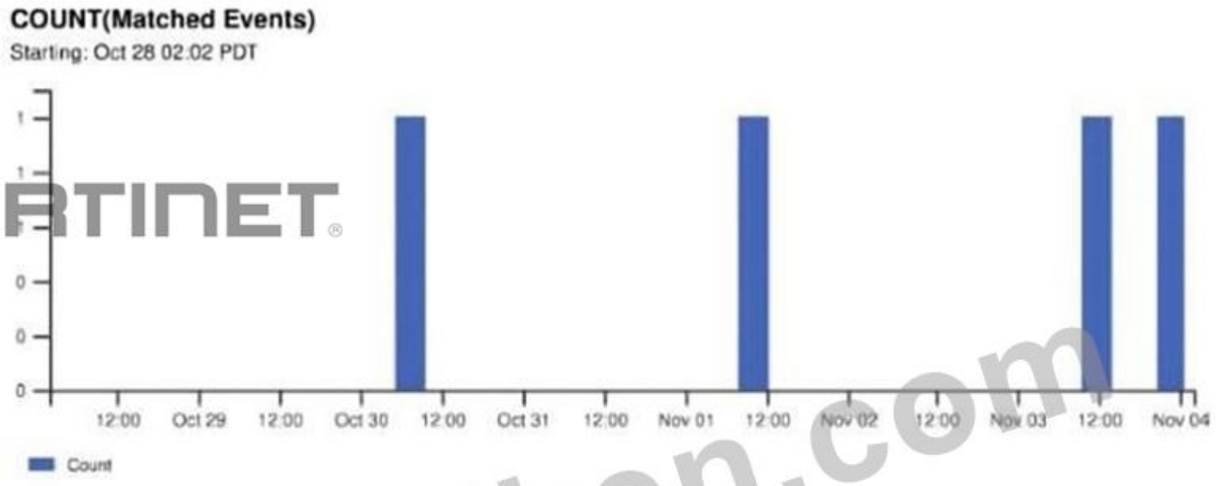


A. 集計属性の値をゼロ以上に設定します。
B. 送信元TCP/UDPポートに基づいてModbusトラフィックをフィルタリングする新しい条件を追加します。
C. このルールは有効であり、追加の変更は必要ありません。
D. フィルターセクションで設定されていない、グループ化セクションの属性を削除します。
正解: (正解を表示します)
https://community.fortinet.com/t5/FortiSIEM/Technical-Note-How-do-I-create-and-or-customize-rules-and-alerts/ta-p/196013

質問: **2**
展示資料を参照してください。

Partial FortiSIEM report

All Incidents



Results found: 4

Rank: 1 **Event Receive Time:** Nov 04 2025, 00:46:00 **Incident Title:** Info Leak exploit from 10.1.5.20 to 192.168.2.3
Event Severity Category: MEDIUM **Incident Reporting Device:** Edge-FortiGate **Incident Source:** srcIpAddr:10.1.5.20,
Incident Target: destIpAddr:192.168.2.3, **Count:** 1

Rank: 2 **Event Receive Time:** Nov 03 2025, 11:43:00
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 1

Rank: 3 **Event Receive Time:** Nov 01 2025, 12:02:45
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 1

Rank: 4 **Event Receive Time:** Oct 30 2025, 06:30:15
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 4

FORTINET
Jpnshiken.com

FortiSIEMレポートの一部を以下に示します。

報告書に記載されている情報に基づくと、正しい記述は次のうちどれですか？ 2つ選択してください。）
A. Edge-FortiGateにはセキュリティプロファイルが実装されています。
B. この報告書は7日間を対象としています。
C. 1件の事件が報告されました。
D. IPアドレス10.1.5.20のデバイスに脆弱性が存在します。
正解: **B,D (**コメントを発表する**)**
期間は10月28日から11月4日までで、7日間の報告期間に相当します。インシデントの説明によると、攻撃は10.1.5.20から発生したものであり、このデバイスが悪用された脆弱性に関連していることが示されています。

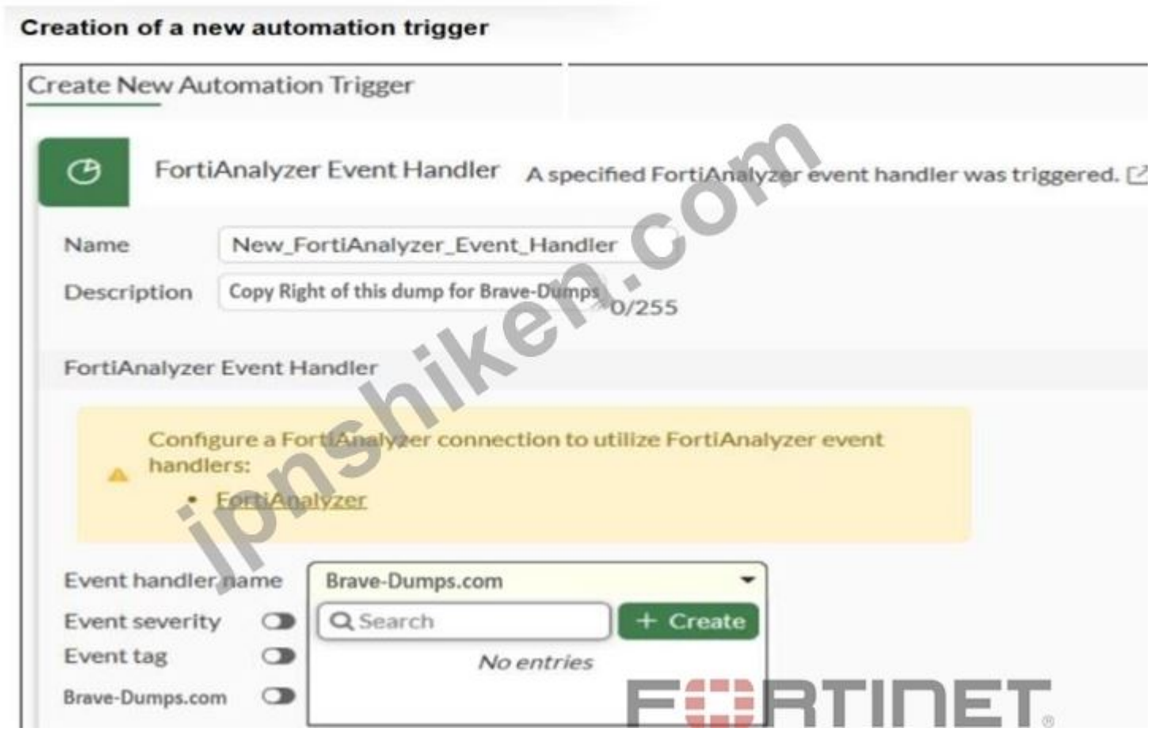
質問: **3**
FortiNACでは、不正デバイスはどのように評価されますか？
A. デバイスリストのインポートを通じて
B. デバイスプロファイリングルールを通じて
C. ローカルデバイスデータベース（CIDB）を介して
D. FortiGuardサーバーへのクエリを通じて
正解: **(**正解を表示します**)**

質問: **4**
図を参照してください。仮想パッチ適用プロファイルが示されています。

Imnshiken.com

最近SCADAシステムをアップデートしたので、SCADA仮想パッチプロファイルを適用したいと考えているのですね。
このプロフィールに関する記述のうち、正しいものはどれですか？ 2つ選択してください）
A. このプロファイルは、すべてのデバイスの重大なシグネチャをブロックします。
B. MACアドレス12:12:12:12:12のデバイスでは、低深刻度のシグネチャはブロックされません。
C. MACアドレス11:11:11:11:11のデバイスには脆弱性がないと考えられます。
D. Schneider.Electric.ClearSCADA.HTTP.Interface.XSS の脆弱性のみが残っています。
正解: **B,C** (コメントを発表する)

質問: **5**
展示資料を参照してください。



自動化トリガー作成ウィザードが表示されます。OTネットワークでいくつかのタスクを自動化したいと考えています。FortiGateデバイスで、FortiAnalyzerイベントハンドラに基づいて新しい自動化トリガーを作成します。イベントハンドラ名フィールドを設定しようとしても、FortiAnalyzerで作成したイベントハンドラが表示されません。これにはどのような理由が2つありますか？ 2つ選択してください）
A. FortiGate デバイスでファブリック設定を構成する必要があります。
B. FortiAnalyzer のイベント ハンドラーで Automation Stitch を有効にする必要があります。
C. イベントハンドラー名フィールドで ╟ 作成」をクリックする必要があります。
D. FortiGate デバイスを FortiAnalyzer に追加して認証する必要があります。
正解: **A,B** (コメントを発表する)
正解はAとBです。

選択肢Bが正解です。学習ガイドには、「ハンドラがオートメーションステッチオプションを有効にしたイベントを生成すると、FortiAnalyzerはFortiGateに通知を送信する」と記載されています。FortiAnalyzerイベントハンドラでオートメーションステッチが有効になっていない場合、そのハンドラはFortiGateのオートメーションステッチワークフローでは使用できません。また、ガイドでは、各イベントハンドラの設定に「オートメーションステッチ」と「ルール」を含めることができると説明されており、これはFortiAnalyzerからFortiGateへの自動化パスに必須の要素であることが示されています。
オプションAも正解です。学習ガイドでは、セキュリティファブリックにおける自動化フローについて、「FortiAnalyzerがログを解析し、ルートFortiGateに通知する」そして「ルートFortiGateがアクションをトリガーする」と説明しています。つまり、FortiGateはFortiAnalyzerイベントハンドラを使用する前に、セキュリティファブリック側でFortiAnalyzer接続を設定する必要があるということです。図表中のFortiAnalyzer接続の設定に関する警告も、この要件を直接指摘しています。
オプションCは、既存のイベントハンドラが見つからない理由が「Create」ではないため誤りです。「Create」は単なるインターフェース制御です。オプションDもこの項目に対する最適な回答ではありません。質問は、FortiAnalyzerトリガーによる自動化において、FortiGate上のイベントハンドラ名リストが空になっている理由についてです。このワークフローに必要な要件として、学習ガイドではFortiAnalyzerとFortiGateのファブリック接続と、FortiAnalyzerイベントハンドラでのAutomation Stitchの有効化が明記されています。

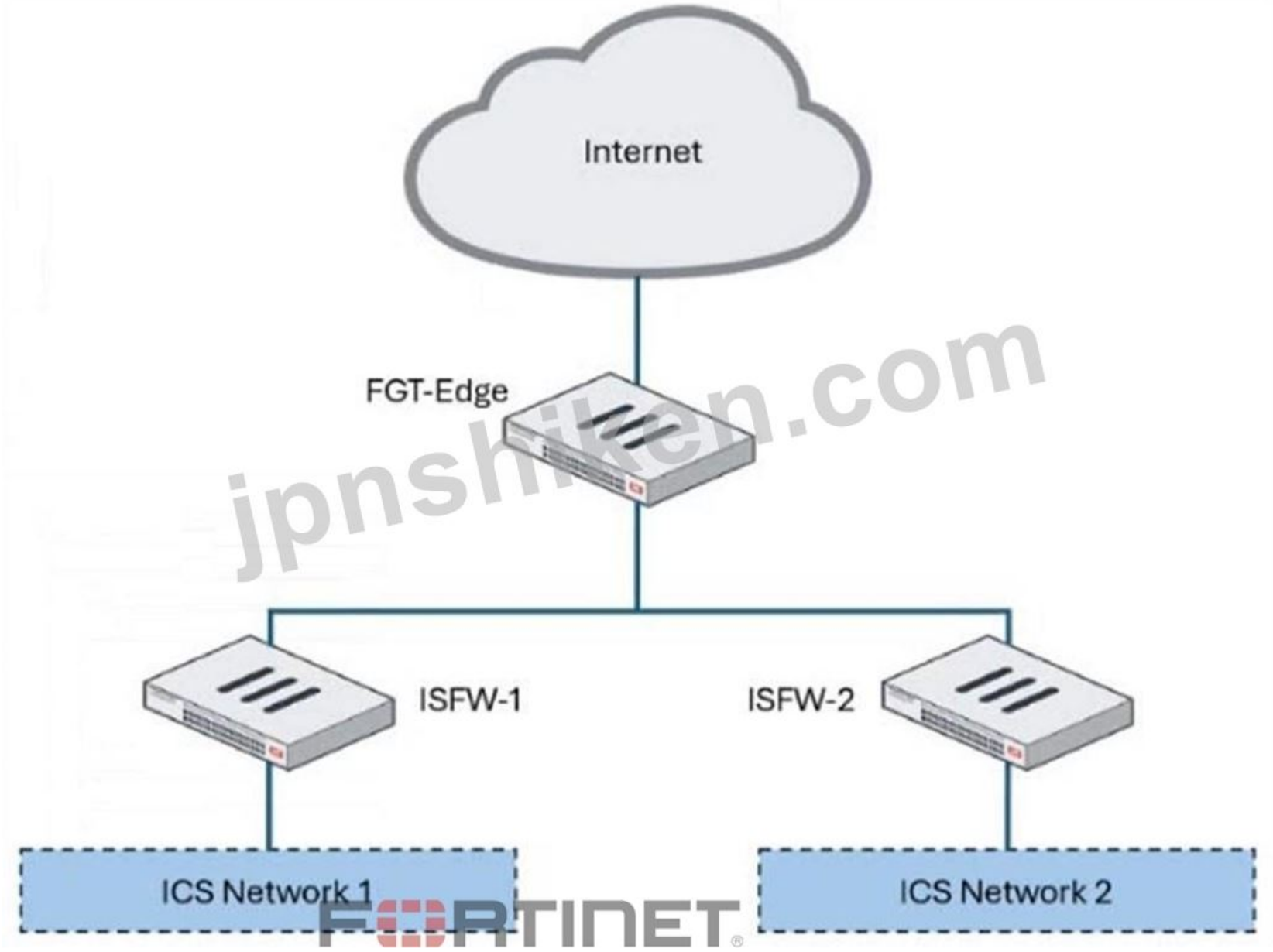
質問: **6**
展示資料を参照してください。

Event Brave-Dumps.com	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler Brave-Dumps.com	Device Name
Schneider.Electric.Modicon.	Mitigated	IPS	16	Medium	a day ago	an hour ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate
Triangle.Research.Nano-10.	Mitigated	IPS	6	Medium	19 hours ago	19 hours ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate

展示資料に示されているイベントモニターページの一部に表示されている情報に基づいて、攻撃はどのように検知されましたか？（回答は1つ選択してください）
A. ステッチで自動的に
B. 管理者による手動
C. プレイブックにより自動的に
D. イベントハンドラによって自動的に
正解: (正解を表示します)
正解はDです。イベントハンドラによって自動的に検出されます。学習ガイドには、「イベントハンドラはFortiAnalyzerでイベントを生成します」および「FortiAnalyzerはイベントハンドラを使用して、すべての受信ログをフィルタリングします。受信したログがイベントハンドラで設定された条件に一致する場合、FortiAnalyzerはイベントを生成します」と明記されています。また、「生成されたすべてのイベントはイベントモニタページで表示できます」とも記載されています。これは、イベントモニタページのエントリを示している図と直接一致します。したがって、図に示されている攻撃は、イベントハンドラによって自動的に検出されたものです。
ガイドでは、検出フローについても説明しています。「FortiAnalyzerはログを受信します」「FortiAnalyzerはログを解析します」「FortiAnalyzerは、イベントハンドラでルールが一致するとイベントを生成します」。さらに、イベントモニタービューには、イベントを生成したイベントハンドラを識別する「ハンドラ」列が含まれています。そのため、この攻撃は手動で検出されたとはみなされず、プレイブックやステッチによって主に検出されるものでもありません。
プレイブックとステッチは後続の自動化アクションに使用されますが、イベントモニターに表示されるイベントはイベントハンドラー機構によって生成されます。

質問: **7**
図を参照してください。FGT-Edgeデバイスは、リモート管理者がローカルICSネットワークにアクセスできるようにするVPNゲートウェイです。経営陣は、現場での安全衛生管理を第三者企業に委託します。この第三者企業は、外部リソースへのアウトバウンドアクセス権限を持っている必要があります。
ICSネットワークのセキュリティを維持しながら、サードパーティ企業に外部アクセスを提供するための最適なシナリオは何でしょうか？

Network topology

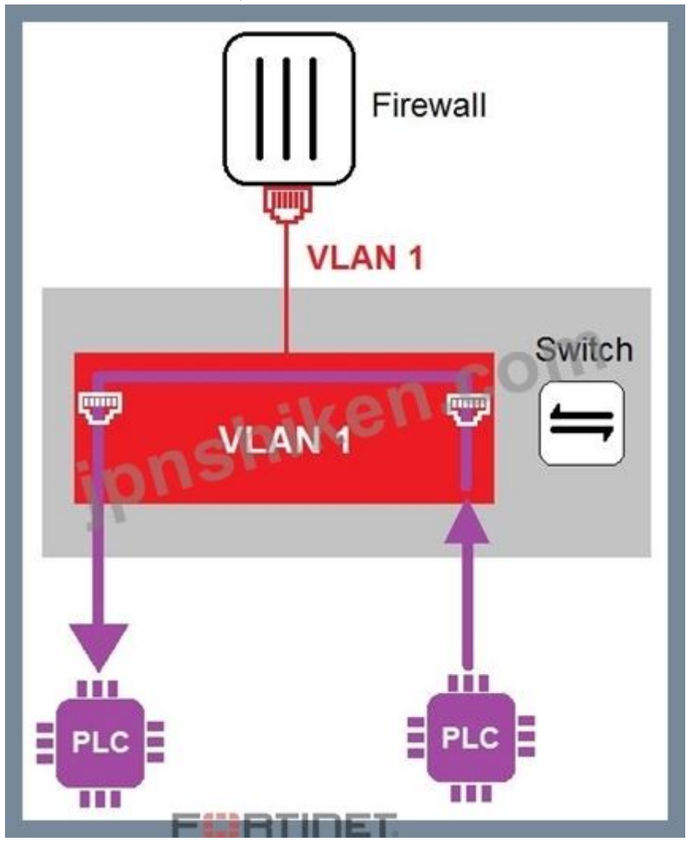


ipnshiken.com

A. サードパーティ企業の認証ユーザーを制限したアウトバウンドセキュリティポリシーを設定します。
B. 下流のFortiGateデバイスとエッジのFortiGateの間にVPNトンネルを作成し、ICSネットワークトラフィックを保護します。
C. エッジ FortiGate デバイスを複数の論理デバイスに分割し、サードパーティ企業に独立した VDOM を割り当てます。
D. インターネットへの追加のアップストリームリンクを使用して、追加のファイアウォールを実装します。
正解: **C** (コメントを発表する)

エッジ側のFortiGateをVDOMに分割することで、サードパーティ企業を独自の仮想ファイアウォール内に隔離できます。このVDOMは、他のVDOMによって保護されているICSネットワークを危険にさらしたり、外部に公開したりすることなく、インターネットへのアウトバウンドポリシーを設定できます。

質問: **8**
図を参照してください。図に示されているトポロジーでは、両方のPLCはファイアウォールを経由せずに直接通信できます。
このような状況下で、セキュリティを向上させるために何ができるでしょうか？



A. PLC同士がIEEE802.1Qプロトコルを使用して通信するように設定してください。
B. PLC間のトラフィックを保護するために、スイッチにファイアウォールポリシーを作成します。
C. VLANの機能をレイヤ2からレイヤ3に拡張するソリューションを実装します。
D. マイクロセグメンテーションを実装する。
正解: (正解を表示します)
マイクロセグメンテーションは、PLC間のトラフィックをセキュリティデバイス（ファイアウォール/ISFW）を経由させることで、無制限のレイヤ2通信を許可する代わりに、ポリシーと検査を適用できるようにします。

質問: **9**
展示資料を参照してください。

仮想パッチ適用プロファイルが表示されています。最近SCADAシステムをアップデートしたので、SCADA仮想パッチ適用プロファイルを適用したいと考えています。このプロファイルに関する記述のうち、正しいものはどれですか？ 2つ選択してください）

A. Schneider.Electric.ClearSCADA.HTTP.Interface.XSS の脆弱性のみが残っています。

B. MACアドレス12:12:12:12:12のデバイスでは、低深刻度のシグネチャはブロックされません。

C. このプロファイルは、すべてのデバイスの重大なシグネチャをブロックします。

D. MACアドレス11:11:11:11:11のデバイスには脆弱性がないとみなされます。

正解: **(**正解を表示します**)**

正解はBとDです。

オプションBが正解です。プロファイルでは中、高、重大度が選択されていますが、低の重大度は選択されていません。つまり、このプロファイルでは低重大度の仮想パッチングシグネチャは適用されません。したがって、MACアドレスが12:12:12:12:12のデバイスでは、低重大度のシグネチャはブロックされません。学習ガイドでは、仮想パッチングはデバイス固有の保護であり、 FortiGateは各デバイスに適用されるシグネチャと緩和ルールをキャッシュし」、関連するトラフィックがファイアウォールポリシーに一致したときにそれらを適用すると説明しています。

選択肢Dが正解です。仮想パッチ適用除外表にはMACアドレス11:11:11:11:11の行が表示されていますが、特定の署名は記載されていません。学習ガイドには、仮想パッチ適用プロファイルで MACアドレスまたは特定の署名を持つ特定のデバイスを除外する」ことができると記載されています。MACアドレスのみによる除外は、その特定のデバイスが仮想パッチ適用から除外されることを意味するため、実際には、このプロファイルでは適用可能な脆弱性がないものとして扱われます。

オプションCは誤りです。プロファイルはすべてのデバイスに対して重要な署名をブロックするわけではありません。除外リストを見ると、少なくとも1つのデバイスはMACアドレスによって除外でき、特定の署名も除外できることがわかります。したがって、すべてのデバイスに対して一律に適用されるわけではありません。

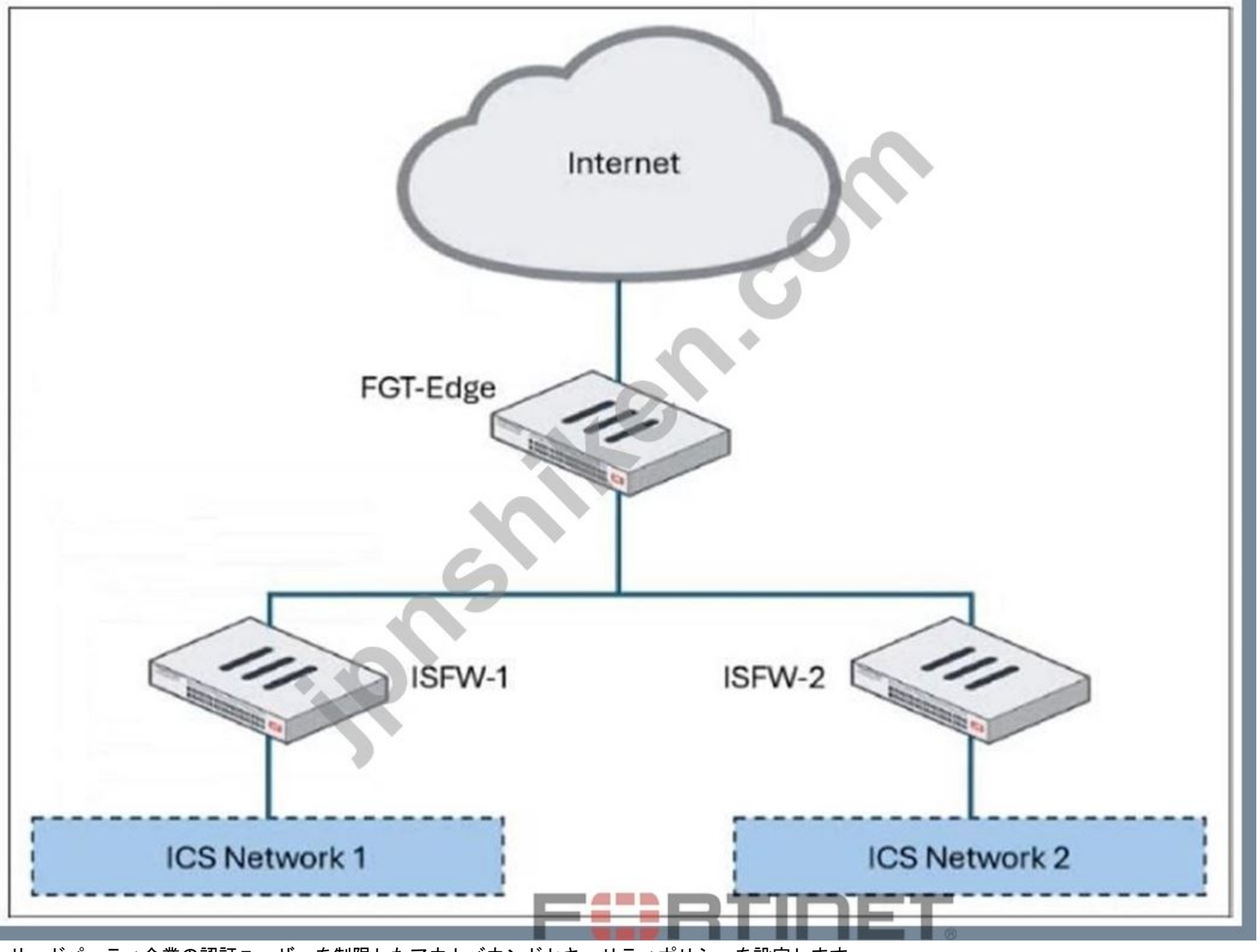
オプションAは誤りです。なぜなら、エントリ Schneider.Electric.ClearSCADA.HTTP.Interface.XSS」は、唯一残っている脆弱性としてではなく、特定の署名除外として表示されているからです。プロファイル表示は除外事項を表示しているのであって、脆弱性が1つだけ残っていることを示しているわけではありません。

質問: **10**

図を参照してください。FGT-Edgeデバイスは、リモート管理者がローカルICSネットワークにアクセスできるようにするVPNゲートウェイです。経営陣は、現場での安全衛生管理を第三者企業に委託します。この第三者企業は、外部リソースへのアウトバウンドアクセス権限を持っている必要があります。

ICSネットワークのセキュリティを維持しながら、サードパーティ企業に外部アクセスを提供するための最適なシナリオは何でしょうか？

Network topology



A. サードパーティ企業の認証ユーザーを制限したアウトバウンドセキュリティポリシーを設定します。
B. 下流のFortiGateデバイスとエッジのFortiGateの間にVPNトンネルを作成し、ICSネットワークトラフィックを保護します。
C. エッジ FortiGate デバイスを複数の論理デバイスに分割し、サードパーティ企業に独立した VDOM を割り当てます。
D. インターネットへの追加のアップストリームリンクを使用して、追加のファイアウォールを実装します。
正解: **(**正解を表示します**)**

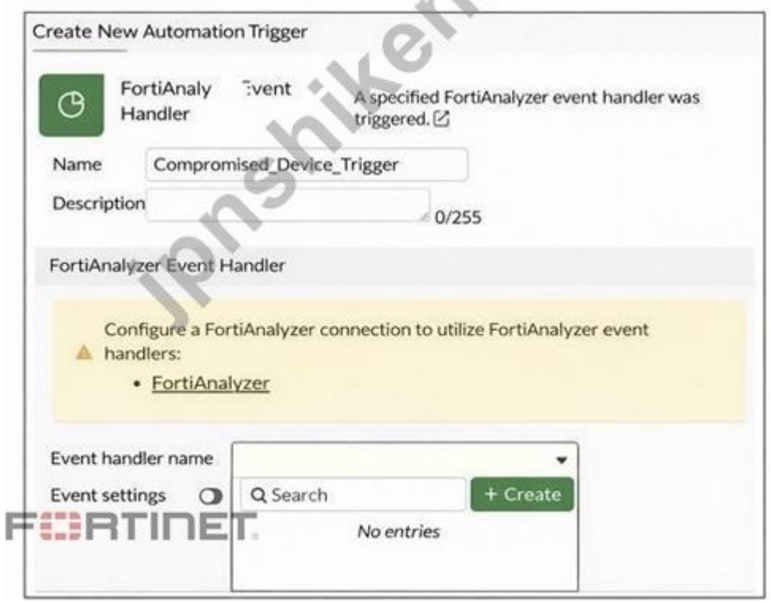
エッジ側のFortiGateをVDOMに分割することで、サードパーティ企業を独自の仮想ファイアウォール内に隔離できます。このVDOMは、他のVDOMによって保護されているICSネットワークを危険にさらしたり、外部に公開したりすることなく、インターネットへのアウトバウンドポリシーを設定できます。

質問: **11**

添付資料を参照してください。FortiAnalyzerの基本イベントハンドラーページの一部と、FortiGateデバイスでのトリガーの作成手順が示されています。

Partial Basic Event Handler page

Creation of a trigger



OTネットワークのセキュリティを強化するために、FortiAnalyzerを通じて通知された侵害されたデバイスの処理を自動化したいと考えている。

図に示すようにイベントハンドラを設定しました。FortiGateデバイスでトリガーを作成する際、「イベントハンドラ名」フィールドに「Alert_trigger」オプションが表示されません。

Alert_triggerオプションを有効にするには、どのような2つの操作を行う必要がありますか？（2つ選択してください）

A. イベントハンドラー名フィールドで「作成」をクリックする必要があります。

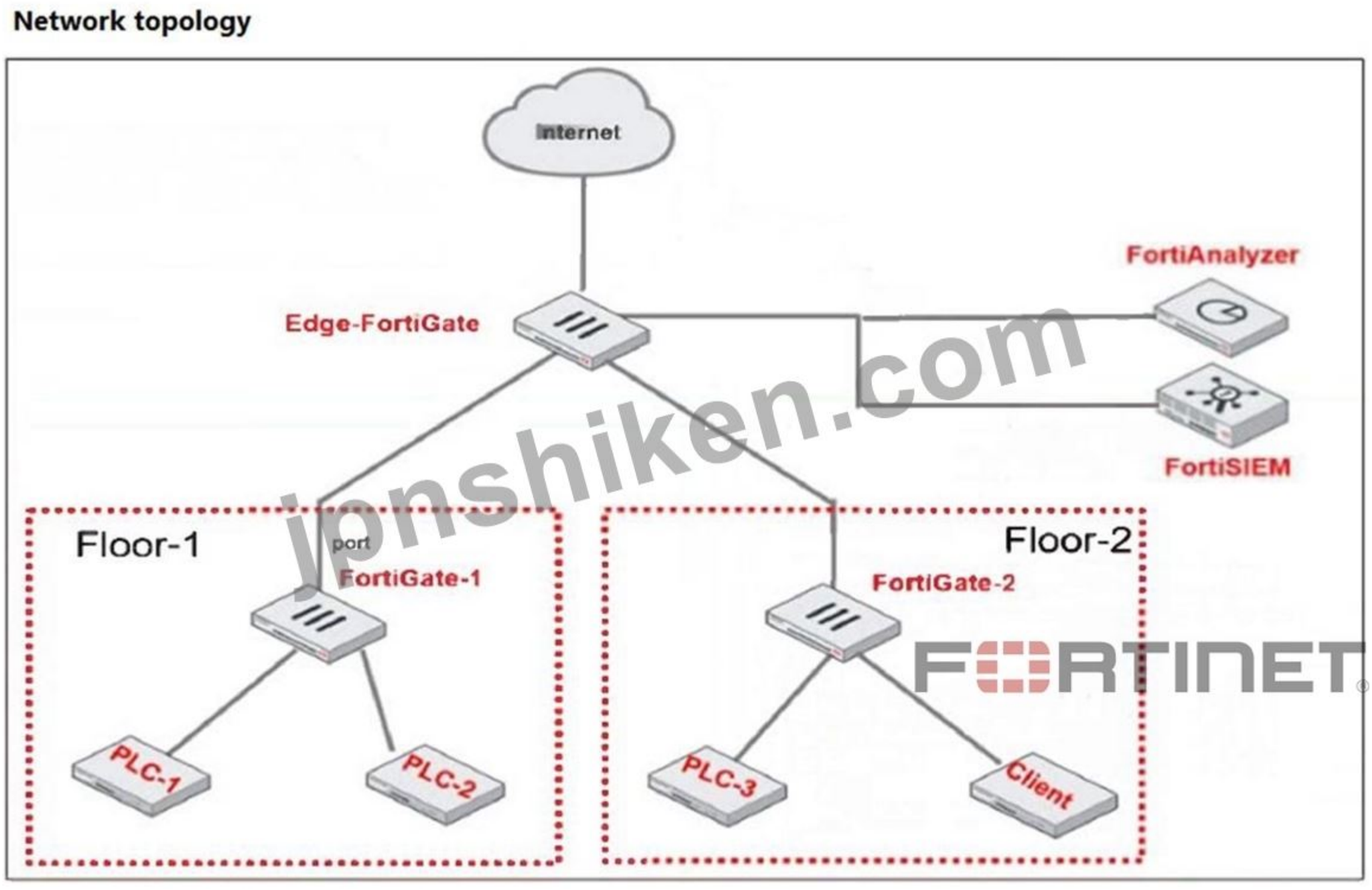
B. FortiGateデバイスでFortiAnalyzerの設定を構成する必要があります。

C. ルートFortiGateでトリガーを設定する必要があります。

D. FortiAnalyzerでFortiGateデバイスを認証する必要があります

正解: (正解を表示します)

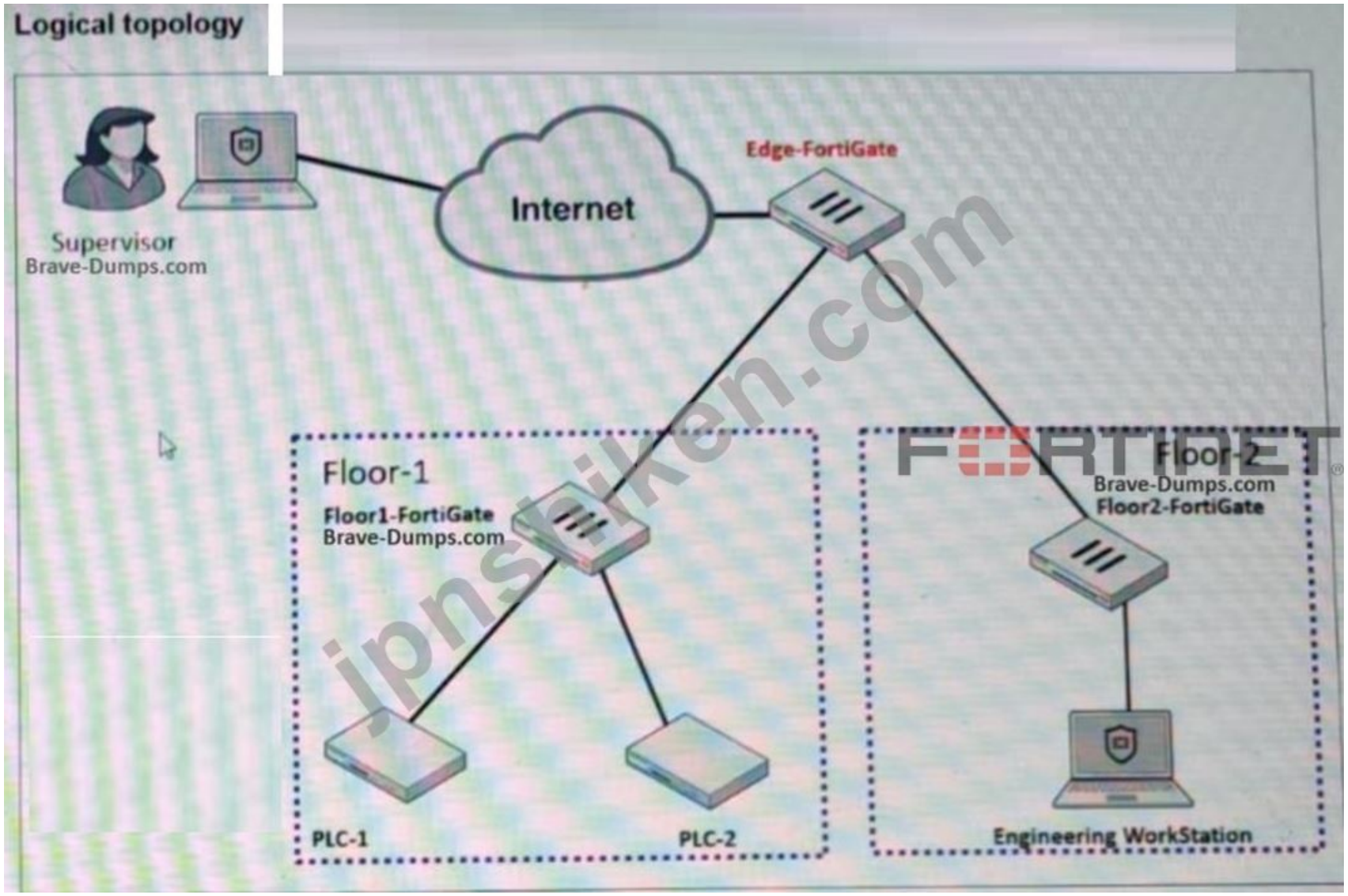
質問: **12**
図を参照してください。図中のネットワークトポロジーには、FortiGateデバイスに加え、OTネットワーク用のFortiAnalyzerおよびFortiSIEMが示されています。
OTネットワークでログ記録を設定するには、どの2つの手順を実行する必要がありますか？ 2つ選択してください。）



A. FortiSIEM を設定して、ログとアラートを FortiAnalyzer に送信するようにします。
B. FortiGate を設定して、ログを FortiAnalyzer と FortiSIEM に送信するようにします。
C. FortiAnalyzer を設定して、セキュリティ イベントを FortiSIEM に送信するようにします。
D. FortiGateとFortiAnalyzerを設定して、産業用シグネチャパターンをFortiSIEMに送信するようにします。

正解: (正解を表示します)
FortiGateは、ログを保存および相関分析するために、ログをFortiAnalyzerとFortiSIEMの両方に直接転送する必要があります。FortiAnalyzerは、関連するセキュリティイベントをFortiSIEMに転送し、OTデバイス全体にわたる集中分析を可能にします。

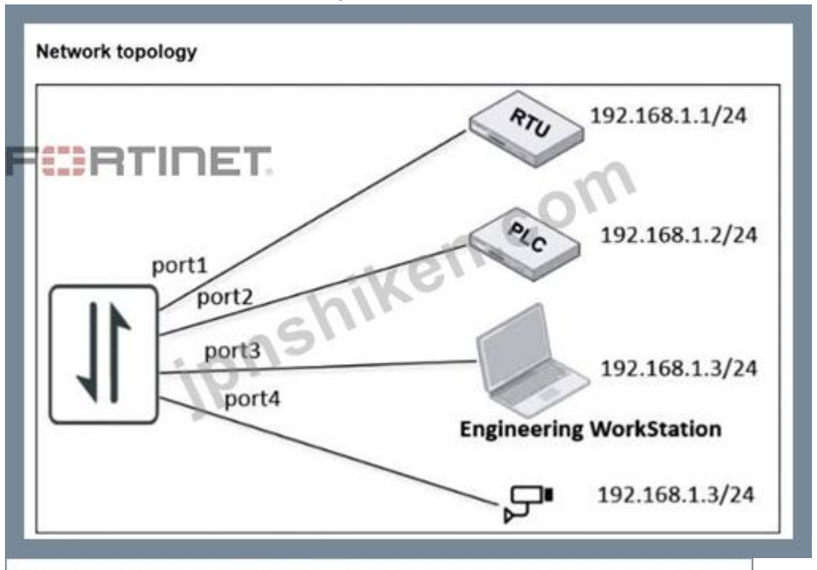
質問: **13**
展示資料を参照してください。



部分的なOTネットワークが図示されています。管理者に安全なリモートアクセスを提供したいと考えています。Edge-FortiGateで実装できる機能はどれですか？ 2つ選択してください）
A. IPsec
B. FortiToken
C. SD-WAN
D. FSSO

正解: (正解を表示します)
展示資料およびOT Security 7.6 Architectのセキュアリモートアクセスに関する標準規格に基づき、以下のとおりです。
セキュア・トンネリング（ステートメントA）この図は、VPNクラウド経由でエッジFortiGateに接続するリモートPCを示しています。Fortinetアーキテクチャでは、IPsec VPNは、リモート管理者やスーパーバイザーが外部から内部OTセグメント（レベル2/3）にアクセスするための、安全で暗号化されたトンネルを確立する主要な方法です。
多要素認証（ステートメントB）OT環境における安全なリモートアクセス（IEC 62443規格に準拠）には、強力な認証が必要です。本学習ガイドでは、VPNユーザー向けに二要素認証（2FA）を提供するFortiTokenの使用を推奨しており、認証情報が漏洩しただけでは重要なインフラストラクチャへのアクセスが不可能になることを保証します。
FSSO（ステートメントD）Fortinet Single Sign-Onは、一般的にネットワーク上に既に存在する内部ユーザーを識別し、IDベースのポリシーを適用するために使用されます。リモート接続自体を確立するための主要なメカニズムではありません。
SD-WAN（ステートメントC）SD-WANはVPNトラフィックの経路を管理できますが、認証と暗号化のコンテキストにおいて、管理者にとっての「安全なリモートアクセス」機能ではなく、WANの最適化と信頼性に関する機能です。

質問: **14**
展示資料を参照してください。



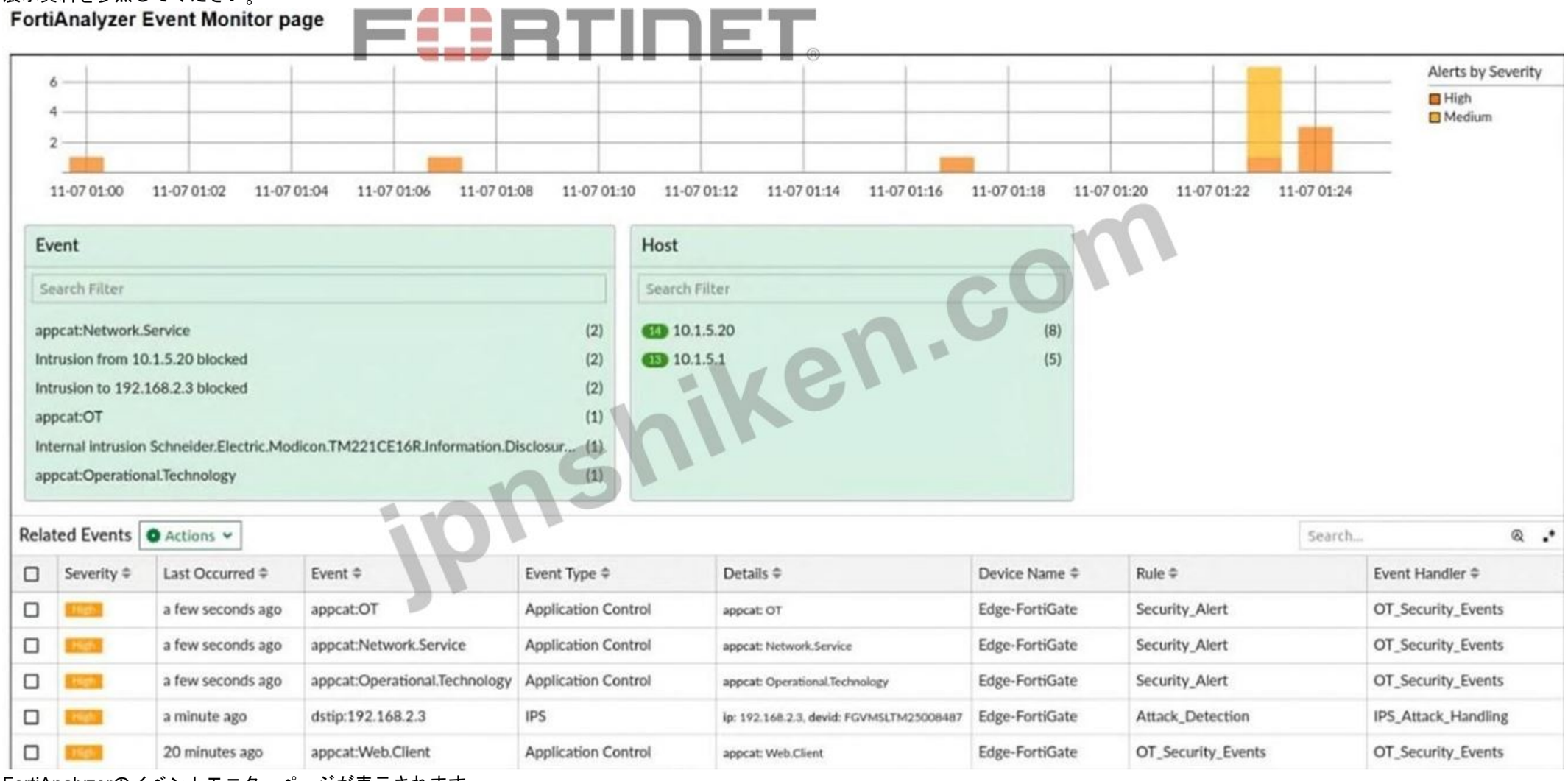
Switch-interface configuration

```
config system switch-interface
edit "Software Switch"
set vdom "root"
set member "port1" "port2" "port3" "port4"
set intra-switch-policy explicit
next
end
```

ネットワークトポロジーとソフトウェアスイッチの設定が示されています。
エンジニアリングワークステーションがPLCにアクセスできないのはなぜですか？
A. エンジニアリングワークステーションとPLCは、異なる放送領域に属しています。
B. このスイッチはレイヤ3スイッチではありません。

C. port2 と port3 のインターフェースは、同じフォワードドメイン ID を持っていません。
D. エンジニアリングワークステーションがPLCにアクセスできるようにするファイアウォールポリシーがありません。
正解: (正解を表示します)
ソフトウェアスイッチは、スイッチ内ポリシーが明示的であるように設定されているため、メンバーインターフェース間のトラフィックは自動的には許可されません。ポート3のエンジニアリングワークステーションからポート2のPLCへの通信には、アクセスを許可する明示的なファイアウォールポリシーが必要です。

質問: **15**
展示資料を参照してください。



FortiAnalyzerのイベントモニターページが表示されます。
イベントモニターページに基づいて、正しい記述は次のうちどれですか？ 2つ選択してください。）
A. 13件のイベントは、IPアドレス10.1.5.1のホストに関連しています。
B. OT_Security_Events イベントハンドラーには、複数のルールが設定されています。
C. 重大な事象が5件発生しています。

jpnshiken.com

D. IPアドレス192.168.2.3のデバイスが攻撃を受けています。
正解: **B,D** (コメントを発表する)
OT_Security_Events ハンドラに関連付けられた複数のイベントが存在するということは、イベント生成に複数のルールが使用されていることを示しています。IP を持つデバイスを参照する IPS イベント 192.168.2.3 と緩和策の表示は、このデバイスが攻撃の標的になっていることを裏付けています。

質問: **16**
展示資料を参照してください。


堅牢化されたFortiGateの背後にあるOTデバイスに脆弱性があり、ファイアウォールポリシーで仮想パッチプロファイルを適用したいと考えています。セキュリティプロファイルのセクションで仮想パッチが利用できないのはなぜですか？（回答は1つ選択してください）
A. 機能の表示設定で仮想パッチ機能を有効にする必要があります。
B. 仮想パッチ機能に対応した堅牢なFortiGateが必要です。
C. OT署名を有効にする必要があります。
D. 有効なOTセキュリティサービスライセンスが必要です。
正解: (正解を表示します)
正解はAです。機能の表示設定で仮想パッチ適用を有効にする必要があります。
学習ガイドには、「デフォルトでは、仮想パッチプロファイルはGUI上で非表示になっており、システム > 機能の表示設定から有効にする必要があります」と明記されています。これは、仮想パッチがセキュリティプロファイルの下に表示されないという図の状況と完全に一致しています。つまり、問題は機能がサポートされていないことではなく、有効にするまでGUI上で非表示になっていることなのです。
他の選択肢では、質問への回答にはなりません。仮想パッチングの署名と保護ワークフローには有効なOTセキュリティサービスライセンスが必要であり、OT署名はIPSベースのOT保護に関連していますが、それだけでは「セキュリティプロファイル」セクションにメニュー項目自体が表示されない理由が説明できません。ガイドでは、仮想パッチングプロファイルがGUIに表示されない理由として、機能の可視性設定が具体的に挙げられています。したがって、必要な操作は、「システム」> 「機能の可視性」で仮想パッチングを有効にすることです。

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu 「168問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**

展示資料を参照してください。

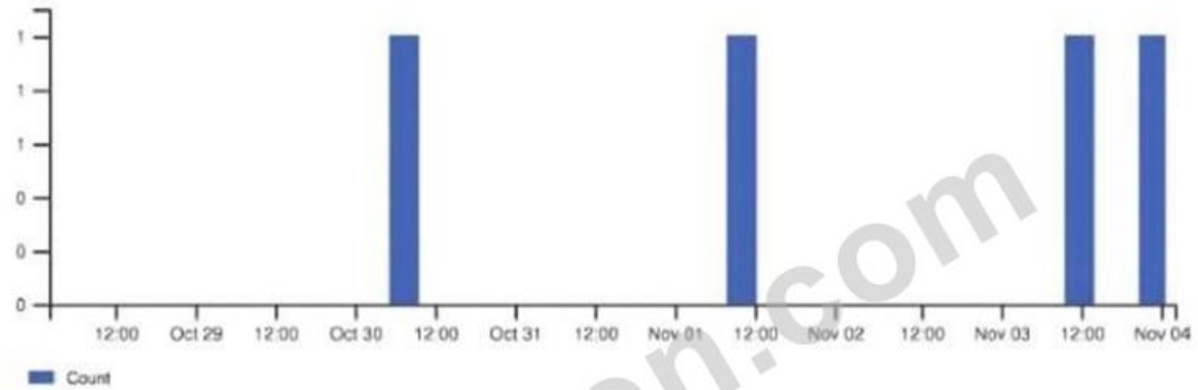
Partial FortiSIEM report

FORTINET

All Incidents

COUNT(Matched Events)

Starting: Oct 28 02:02 PDT



Results found: 4

Rank: 1 **Event Receive Time:** Nov 04 2025, 00:46:00 **Incident Title:** Info Leak exploit from 10.1.5.20 to 192.168.2.3
Event Severity Category: MEDIUM **Incident Reporting Device:** Edge-FortiGate **Incident Source:** srcIpAddr:10.1.5.20,
Incident Target: destIpAddr:192.168.2.3, **Count:** 1

Rank: 2 **Event Receive Time:** Nov 03 2025, 11:43:00
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 1

Rank: 3 **Event Receive Time:** Nov 01 2025, 12:02:45
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 1

Rank: 4 **Event Receive Time:** Oct 30 2025, 06:30:15
Incident Title: FortiSIEM HA elected a new replication leader FortiSIEM 10.1.3.180 **Event Severity Category:** MEDIUM
Incident Reporting Device: FortiSIEM **Incident Source:** [None] **Incident Target:** hostName:FortiSIEM, hostIpAddr:10.1.3.180,
Count: 4

FortiSIEMレポートの一部を以下に示します。

報告書に記載されている情報に基づくと、正しい記述は次のうちどれですか？ 2つ選択してください。）

A. Edge-FortiGateにはセキュリティプロファイルが実装されています。
B. この報告書は7日間を対象としています。
C. 1件の事件が報告されました。
D. IPアドレス10.1.5.20のデバイスに脆弱性が存在します。
正解: **(**正解を表示します**)**
期間は10月28日から11月4日までで、7日間の報告期間に相当します。インシデントの説明によると、攻撃は10.1.5.20から発生したものであり、このデバイスが悪用された脆弱性に関連していることが示されています。

質問: **18**
ネットワークに接続されたインフラ機器のレイヤ2ポーリングをトリガーするものは何ですか？
A. 一致するプロファイリングルール
B. リンクアップまたはリンクダウンのトラップ
C. 一致するセキュリティポリシー
D. レイヤー3ポーリングの失敗
正解: **B (**コメントを発表する**)**

質問: **19**
展示資料を参照してください。

プレイブックモニターページの一部と、それに対応するプレイブックの設定が表示されます。
モニターページとプレイブックの設定に基づいて、Run_Reportタスクをトリガーした原因は何ですか？
（いずれか1つを選択してください）
A. IPS_Attack_Handling イベント
B. IPSインシデントの作成
C. イベントトリガーログ

D. IPS_Attack_Incidentログ
正解: **A (**コメントを発表する**)**
FortiAnalyzerプレイブックエンジンから提供されたデータに基づくと、以下のようになります。
* プレイブックのトリガー条件：部分的なプレイブック構成図は、基本ハンドラー名が IPS_Attack_Handling と等しいという条件に基づいてプレイブックがトリガーされるように設定されていることを示しています。
* イベントとログ :FortiAnalyzerでは、[基本ハンドラー名]フィールドはイベントレコードのプロパティであり、イベントを生成した特定のイベントハンドラーを示します。この条件で構成されたプレイブックは、生のログではなく、イベントによってトリガーされます。
* プレイブック実行フロー：部分プレイブックモニタービューには、実行シーケンスが表示されます。
* Event_Trigger (Starter) : これはプレイブックのエントリポイントであり、構成で定義された条件に一致します。
* IPS_Attack_Incident : トリガー発生後に最初に実行されるタスク。
* Run_Report :スターターによって開始された自動化ワークフローの一部として実行される、対象となるタスク。
* 結論 :プレイブックの 「Starter」はIPS_Attack_Handlingハンドラー名で定義されているため、そのハンドラーによって生成されたイベントは、Run_Reportタスクを含むプレイブック全体の実行のルートトリガーとなります。
したがって、IPS_Attack_Handling イベントによって (プレイブックの一部として) Run_Report タスクがトリガーされました。

質問: **20**
展示資料を参照してください。

Partial Incident Analysis page

インシデント分析ページの一部が表示されています。360度セキュリティレビューOTレポートは、どのようにインシデントに添付されましたか？（回答は1つ選択してください）

A. ステッチで自動的に

B. イベントハンドラによって自動的に

C. プレイブックにより自動的に

D. 管理者による手動

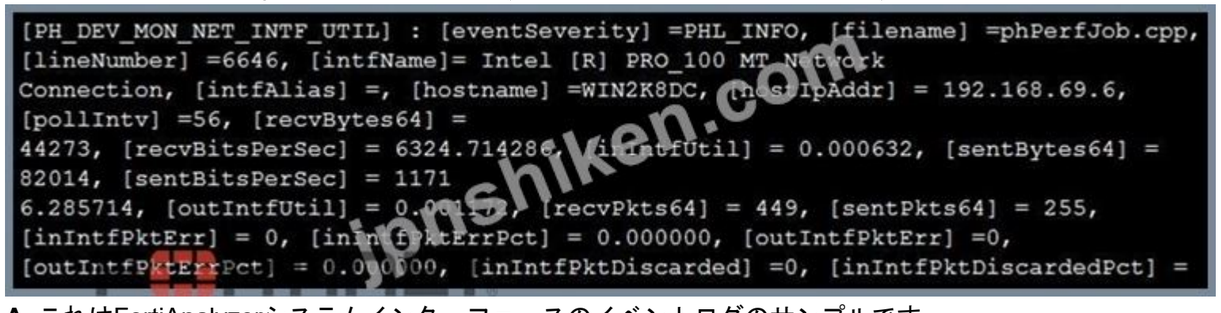
正解: (正解を表示します)

学習ガイドによると、プレイブックはレポートの実行やインシデントの作成 ·更新といったタスクを自動化するために使用される。また、プレイブックがトリガーされると、設定されたタスクが順次実行されるとも説明されている。

ipnshiken.com

さらに、イベントが検出され、インシデントが作成され、レポートが実行され、詳細情報がインシデントに添付されるという、プレイブックのサンプルシーケンスも示されています。これはまさに、インシデント分析ビューに表示されるワークフローと同じです。
それに対し、学習ガイドでは、イベントハンドラはログが設定されたルールに一致した場合にイベントを生成すると述べている。イベントハンドラは検出のためのものであり、インシデントにレポートを添付するためのものではない。

質問: **21**
図を参照してください。出力の分析結果から、出力に関する以下の記述のうち、正しいものはどれですか？



A. これはFortiAnalyzerシステムインターフェースのイベントログのサンプルです。
B. これはSNMP温度制御イベントログのサンプルです。
C. これはPAMイベントタイプのサンプルです。
D. これはFortiGateインターフェースの統計情報のサンプルです。
正解: **(**正解を表示します**)**
ph_dev_monはPAMイベントです。ホスト名はFortigateではなくWIN2K8DC（Windowsサーバー）です。

質問: **22**
FortiNACによる不正デバイスの処理に関して、正しい記述はどれですか？
A. FortiNAC は、一致したデバイスを再検証できません。
B. FortiNACは不正デバイスのマッチングルールを記憶します。
C. FortiNAC は、以前にプロファイルされた不正デバイスのマッチングルールを無効にします。
D. FortiNAC は、1 つのデバイス プロファイリング ルールのみで不正デバイスを照合します。
正解: **(**正解を表示します**)**
FortiNACは、不正デバイスをプロファイリングルールに照合すると、その照合ルールを記憶します。
FortiNACは、デバイスが接続するたび、またはユーザーが定義した間隔で、そのルールに基づいてデバイスを再検証します。
デバイスが再検証ルールに適合しなくなった場合、FortiNACは安全対策として自動的にデバイスを無効にすることができます。
FortiNACは、以前にプロファイルされた不正デバイスのマッチングルールを無効にしたり、不正デバイスを単一のプロファイリングルールのみに一致させたりすることはありません。プロファイリングルールは複数設定できますが、デバイスは最初に一致したルールに関連付けられます。

質問: **23**
以下の機能のうち、ほとんどの産業用プロトコルに欠けているものはどれですか？（2つ選択してください。）
A. リアルタイムデータ交換
B. 決定論的タイミング
C. TLS暗号化

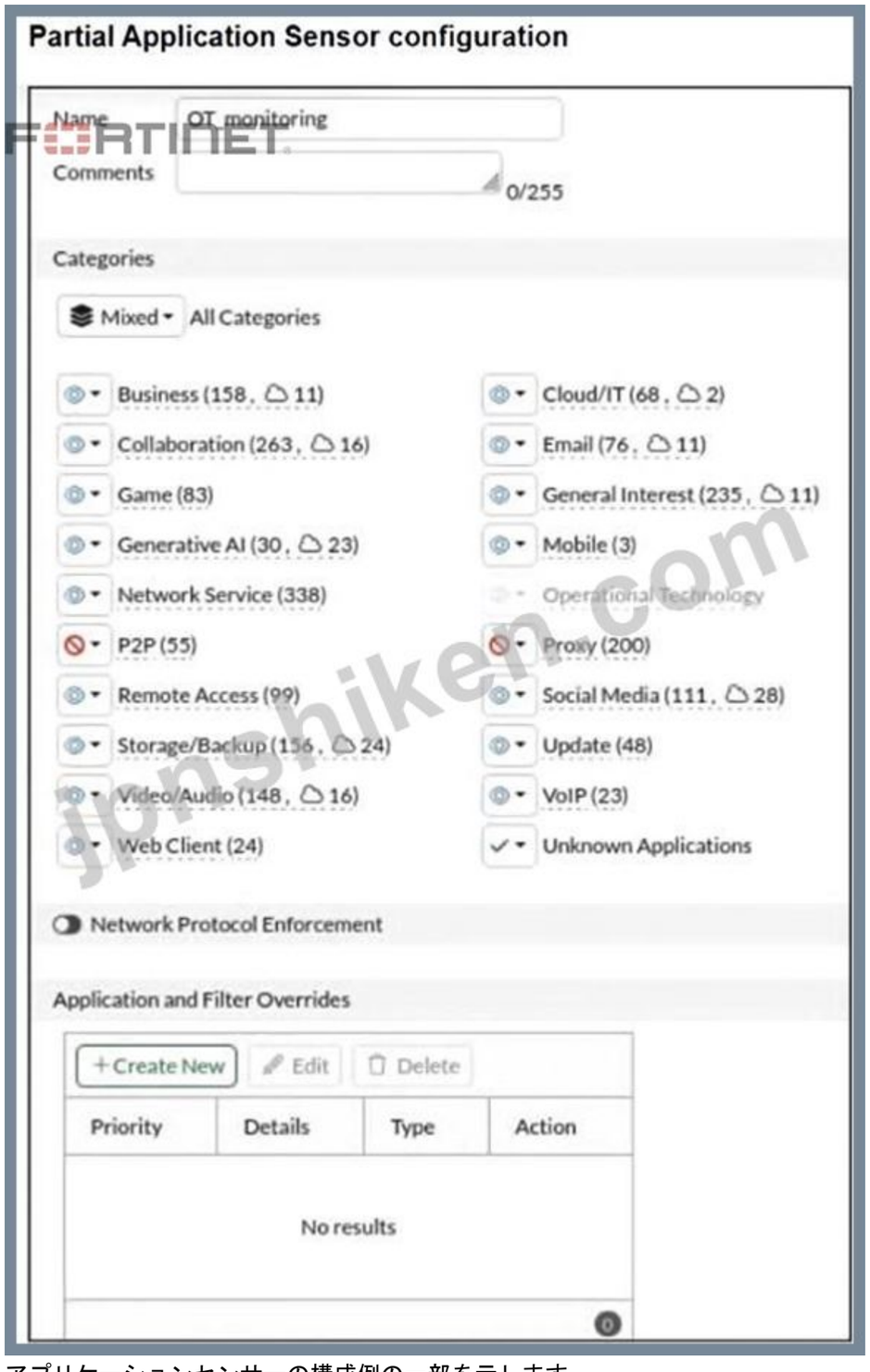
D. 認証
正解: **C,D** (コメントを発表する)
ほとんどの従来のOT/産業用プロトコルは、セキュリティではなく速度と決定性を重視して構築されているため、通常はTLS暗号化および認証メカニズムが組み込まれていません。

質問: **24**
OT（運用技術）管理者は、FortiGateデバイスに産業用署名データベースを用いたセキュリティを実装することで、ネットワークを保護する必要があります。
FortiGateの産業用署名データベースに関する記述として正しいのはどれですか？
A. 管理者はカスタム署名を使用して独自のデータベースを作成する必要があります。
B. 管理者は FortiGate CLI を介してこれを有効にできます。
C. デフォルトでは、産業用データベースが有効になっています。
D. 管理者は産業用署名データベースを購入し、それをFortiGateにインポートする必要があります。
正解: (正解を表示します)

質問: **25**
管理者がFortiGateデバイス上でソフトウェアスイッチを設定しています。ファイアウォールポリシーを使用して、ソフトウェアスイッチ上のメンバーインターフェイス間のトラフィックを制御するために、管理者はFortiGate上でどのような設定を行う必要がありますか？
A. 管理者は、ソフトウェアスイッチ用に別の転送ドメインを設定する必要があります。
B. 管理者は、ソフトウェアスイッチに異なる VLAN インターフェイスを追加する必要があります。
C. 管理者は、スイッチ内ポリシーを明示的に設定する必要があります。
D. 管理者は、ソフトウェアスイッチに少なくとも1つの無線インターフェースと1つのVLANインターフェースを設定する必要があります。
正解: (正解を表示します)

質問: **26**
OTネットワークにおいて、リモートアクセスと内部可用性をどのように実現できますか？
A. 冗長性対策として、バックエンドのバックアップネットワークを構築する。
B. 各ISPリンク上のトラフィックを管理するためにSD-WANを導入する。
C. OTデバイスにアクセスするための追加の内部ファイアウォールを追加します。
D. 不正アクセスを防止するために、アクセス ポリシーをさらに作成します。
正解: (正解を表示します)
SD-WANは、複数のISPリンクを信頼性高く効率的に管理し、高い可用性と最適化されたトラフィックルーティングを実現します。
これは、継続的な可用性が不可欠なOTネットワークにとって重要な冗長性とパフォーマンスの向上を提供します。
SD-WANは、トラフィックを動的にルーティングし、セッションの永続性を維持し、リモート環境と社内OT環境間の安全な接続を提供することができます。

質問: **27**
展示資料を参照してください。

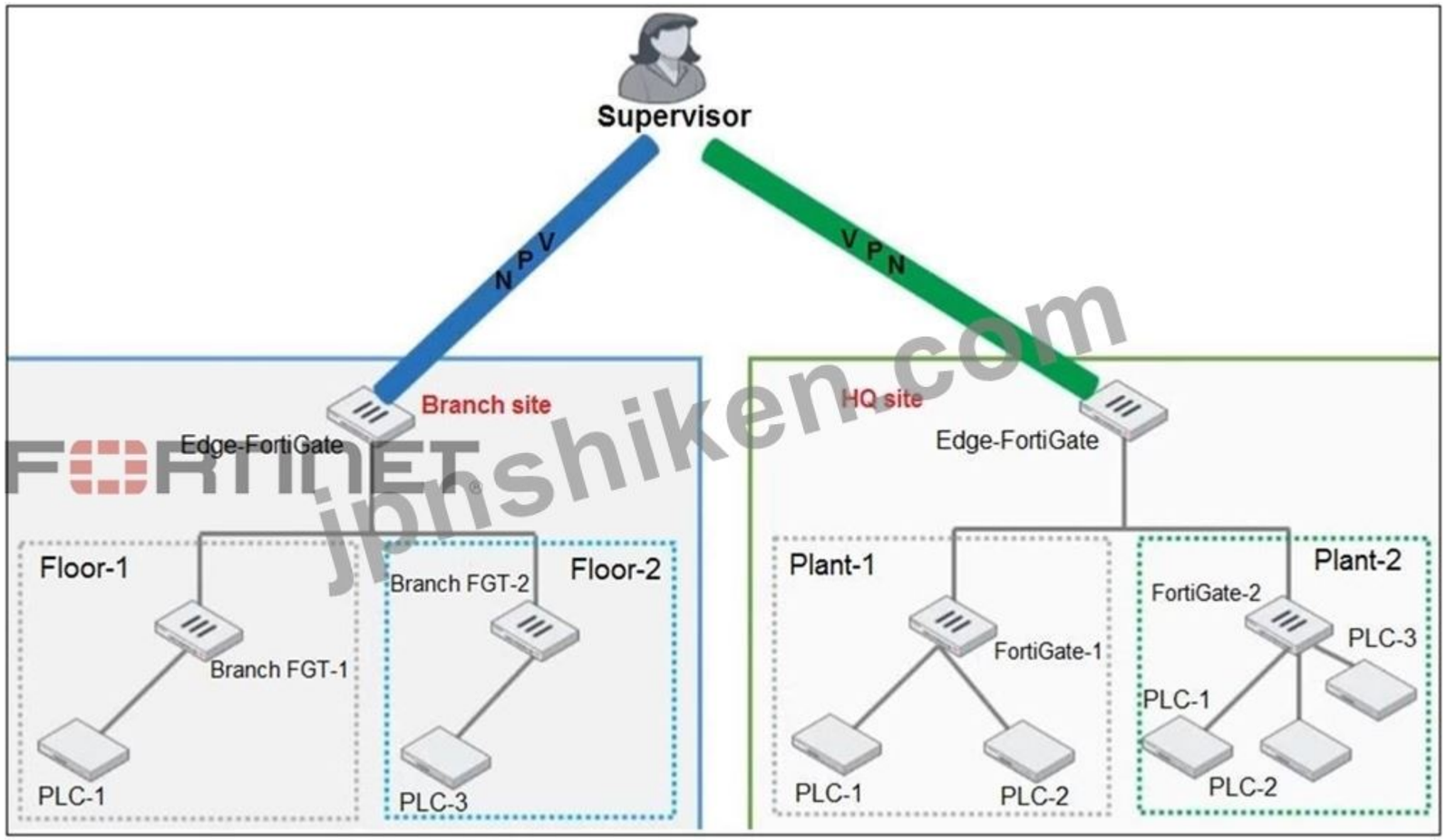


アプリケーションセンサーの構成例の一部を示します。

ネットワーク内のOTプロトコルを監視したいと考え、ファイアウォールポリシーにOT_monitoringプロファイルを適用しました。OTトラフィックを生成した後、アプリケーション制御セクションにOT関連のログが表示されません。
どの行動をとらなければなりませんか？
A. アプリケーションとフィルタのオーバーライドのセクションでOTプロトコルを定義する必要があります。
B. OT署名を有効にする必要があります。
C. ネットワークプロトコルの強制を有効にする必要があります。
D. 「すべてのカテゴリ」フィールドを「監視」に設定する必要があります。
正解: **(**正解を表示します**)**
アプリケーションコントロールは、監視またはブロックするように明示的に設定されたアプリケーションに対してのみログを生成します。
カテゴリが監視対象に設定されていないため、OTトラフィックはログに記録されません。すべてのカテゴリを監視対象に設定することで、OTプロトコルのアクティビティがログに記録され、アプリケーションコントロールで確認できるようになります。

質問: **28**
運用技術（OT）ネットワークにSD-WANを導入する主な目的は何ですか？
A. 標準リンクを低コストの接続に交換する
B. OTアプリケーションのネットワークパフォーマンスを向上させる
C. セキュリティリスクと脅威攻撃を軽減する
D. 中央集権型のネットワークセキュリティポリシーを削除します。
正解: **(**正解を表示します**)**
運用技術（OT）ネットワークにSD-WANを導入する主な目的は、OTアプリケーションのパフォーマンスと信頼性を向上させることです。SD-WANは、アプリケーション要件、ネットワーク状況、およびビジネス上の優先順位に基づいてトラフィックルーティングを最適化し、重要なOTアプリケーションの低遅延と高可用性を確保します。これは、アプリケーションのパフォーマンスが運用効率と安全性に直接影響を与えるOT環境において不可欠です。

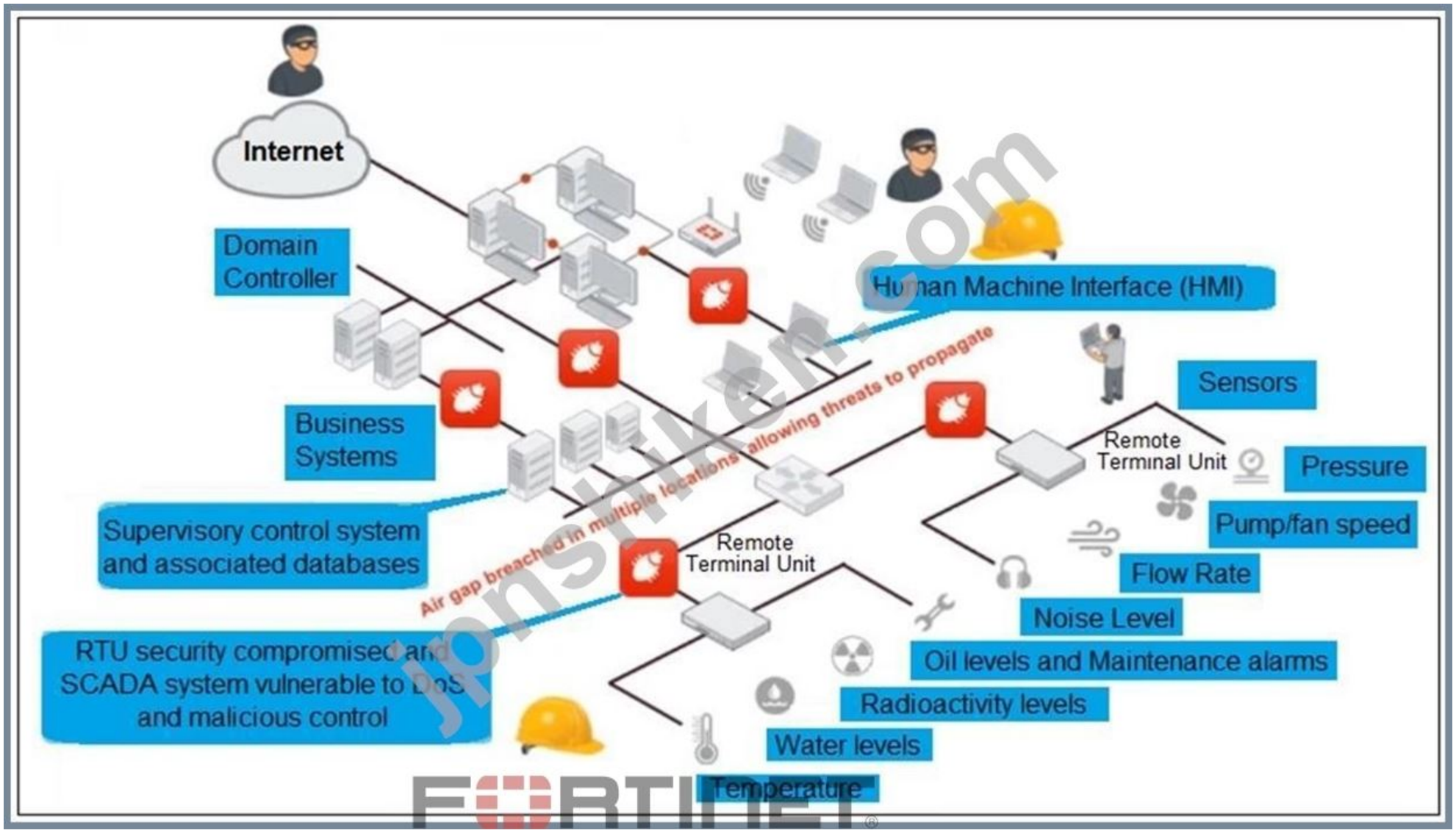
質問: **29**
図を参照してください。侵害発生現場と本社拠点の管理者向けに、同じFortiTokenソフトを使用してVPNユーザーアクセスを設定する必要があります。各拠点にはFortiGate VPNゲートウェイが設置されています。
この目標を達成するためには、何をすべきでしょうか？



FORTINET
jpnshiken.com

A. ユーザー自己登録サーバーを使用する必要があります。
B. サードパーティ製のRADIUS OTPサーバーを使用する必要があります。
C. FortiAuthenticatorを使用する必要があります。
D. 複数のFortiGateに同じFortiTokenを登録する必要があります。
正解: **C** (コメントを発表する)

質問: **30**
展示資料を参照してください。そこには、保護されていない手術室環境が示されています。



管理者はOTネットワークに適切な保護対策を講じる必要があります。管理者はOTネットワークを保護するために、どのような3つの手順を踏むべきでしょうか？ 3つ選択してください。）

A. インターネットとOTネットワークの間にエッジFortiGateを1アームスニファとして配置します。

B. 各ICSネットワーク内にFortiGateデバイスを導入します。

C. 産業用プロトコルセンサーを使用してファイアウォールポリシーを設定する

D. セグメンテーションを使用する

E. Webフィルタを使用してファイアウォールポリシーを設定し、さまざまなICSネットワークを保護します。

正解: **B,C,D (**コメントを発表する**)**

質問: **31**

展示資料を参照してください。

アプリケーションセンサープロファイルの一部が表示されています。このプロファイルをファイアウォールポリシーに適用する場合、正しい記述は次のうちどれですか？ (2つ選択してください)

A. OT署名が有効になっています。

B. すべてのOTプロトコルは監視されています。

C. Modbus書き込みコマンドはブロックされています。

D. Modbusの保持レジスタ読み取りコマンドごとにログが提供されます。

正解: (正解を表示します)

正解はAとCです。学習ガイドには、「アプリケーション制御シグネチャを使用してOTプロトコルを検出できる」こと、およびアプリケーション制御によって「きめ細かなメッセージタイプの識別」が可能になることが説明されています。図では、運用技術アプリケーションカテゴリがアプリケーションセンサープロファイルに含まれているため、このプロファイルではOTアプリケーションシグネチャが有効になっています。

オプションCも正解です。オーバーライドテーブルには、Modbus_Read.Holding.Registers = Allow、Modbus = Block と表示されているからです。学習ガイドには、特定のModbusコマンドを許可し、他のすべてのコマンドをブロックするために、きめ細かなアプリケーション制御シグネチャを使用できると記載されており、また、アプリケーション制御はメッセージレベルで読み取りコマンドと書き込みコマンドを個別に識別できることも示されています。したがって、このプロファイルではModbus書き込みコマンドはブロックされます。

オプションBは、プロファイルが単にすべてのOTプロトコルを監視しているのではなく、Modbusのブロックアクションが含まれているため、誤りです。オプションDは、学習ガイドではOTプロトコルの可視性をモニターのステータスに具体的にリンクしているのに対し、展示ではModbus_Read.Holding.Registersが「モニター」ではなく「許可」に設定されているため、誤りです。

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu　**168**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
無線ネットワーク統合において、FortiNACは接続先のMACアドレス情報をどのように取得するのですか？
A. 半径
B. リンクトラップ
C. エンドステーションのトラフィック監視
D. MAC通知トラップ
正解: **A** (コメントを発表する)
FortiNACは、複数の方法を用いてネットワークに接続するエンドポイントを学習しますが、無線ネットワーク統合における主要な方法の一つがRADIUS通信です。
デバイスが接続を試みると、RADIUSリクエストによってMACアドレス情報がFortiNACに提供されます。
FortiNACはSNMPトラップ（リンクトラップまたはMAC通知トラップ）やトラフィック監視も利用できますが、無線MACアドレス取得の主要な標準方式はRADIUSです。

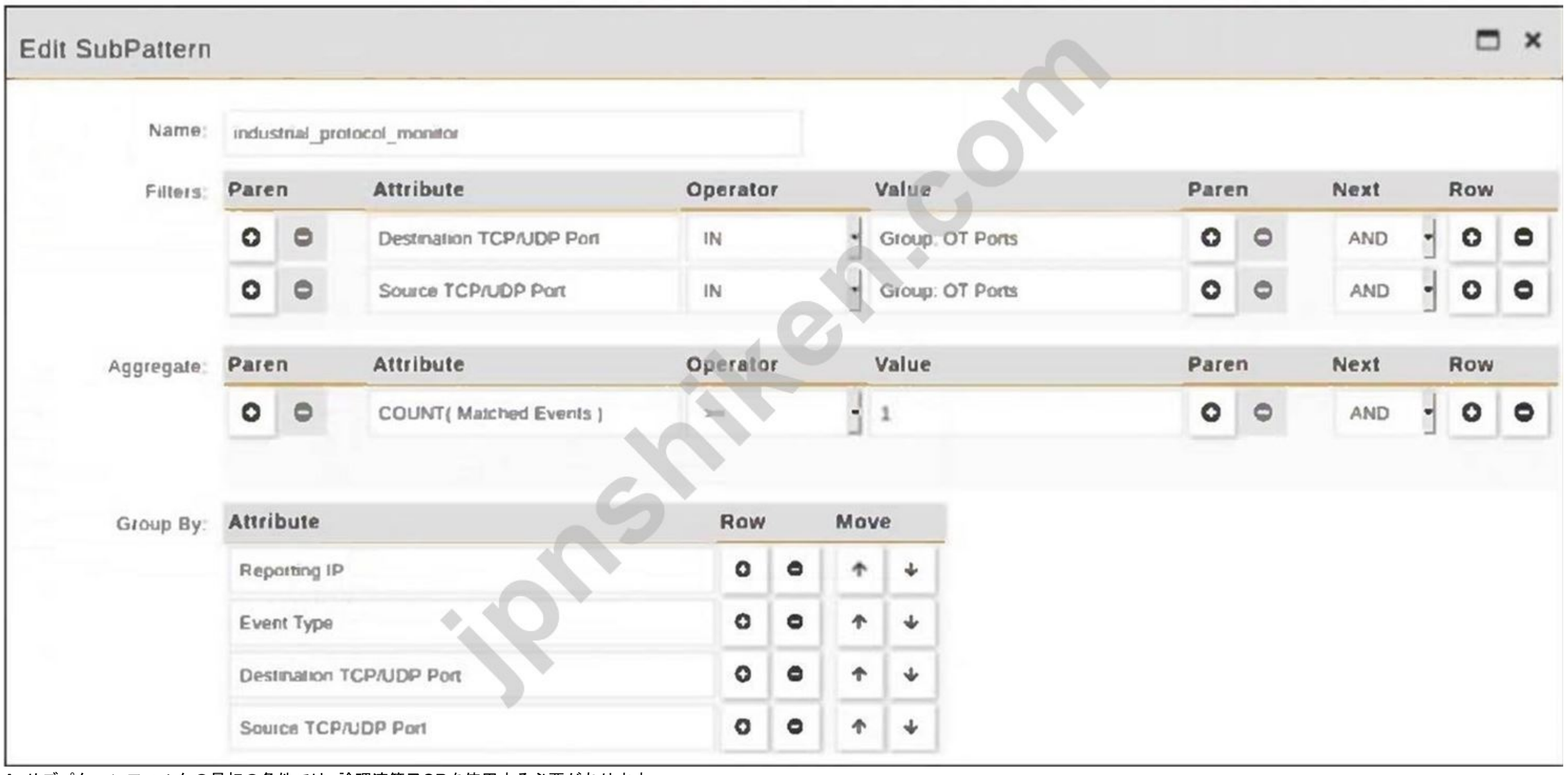
質問: **33**
展示資料を参照してください。

アプリケーションセンサープロファイルの一部が表示されています。このプロファイルをファイアウォールポリシーに適用する場合、正しい記述は次のうちどれですか？ 2つ選択してください）

A. OT署名が有効になっています。
B. すべてのOTプロトコルは監視されています。
C. Modbus書き込みコマンドはブロックされています。
D. Modbusの保持レジスタ読み取りコマンドごとにログが提供されます。
正解: **(**正解を表示します**)**
正解はAとCです。学習ガイドには、「アプリケーション制御シグネチャを使用してOTプロトコルを検出できる」こと、およびアプリケーション制御によって きめ細かなメッセージタイプの識別」が可能になることが説明されています。図では、運用技術アプリケーションカテゴリがアプリケーションセンサープロファイルに含まれているため、このプロファイルではOTアプリケーションシグネチャが有効になっています。
オプションCも正解です。オーバーライドテーブルには、Modbus_Read.Holding.Registers = Allow、Modbus = Blockと表示されています。学習ガイドには、特定のModbusコマンドを許可し、他のすべてのコマンドをブロックするために、きめ細かなアプリケーション制御シグネチャを使用できると記載されており、また、アプリケーション制御はメッセージレベルで読み取りコマンドと書き込みコマンドを個別に識別できることも示されています。したがって、このプロファイルではModbus書き込みコマンドはブロックされます。
オプションBは、プロファイルが単にすべてのOTプロトコルを監視しているのではなく、Modbusに対するブロックアクションが含まれているため、誤りです。オプションDは、学習ガイドではOTプロトコルの可視性をモニターのステータスに具体的に関連付けているのに対し、図表ではModbus_Read.Holding.Registersがモニターではなく許可に設定されているため、誤りです。

質問**: 34**
図を参照してください。FortiSIEM上でModbusプロトコルを監視するための運用技術ルールが作成され、正常に有効化されています。しかし、FortiSIEMがModbusトラフィックとアプリケーションログを正しく受信しているにもかかわらず、ルールはインシデントをトリガーしません。
ルール設定に関する問題点を正しく説明しているのは、次のうちどれですか？

A new OT rule



A. サブパターンフィルタの最初の条件では、論理演算子ORを使用する必要があります。

B. 「グループ化」セクションの属性は、「フィルター」セクションの属性と一致している必要があります。

C. 集計属性のCOUNT式はフィルターと互換性がありません。

D. サブパターンに Modbus プロトコルに一致するフィルターがありません。

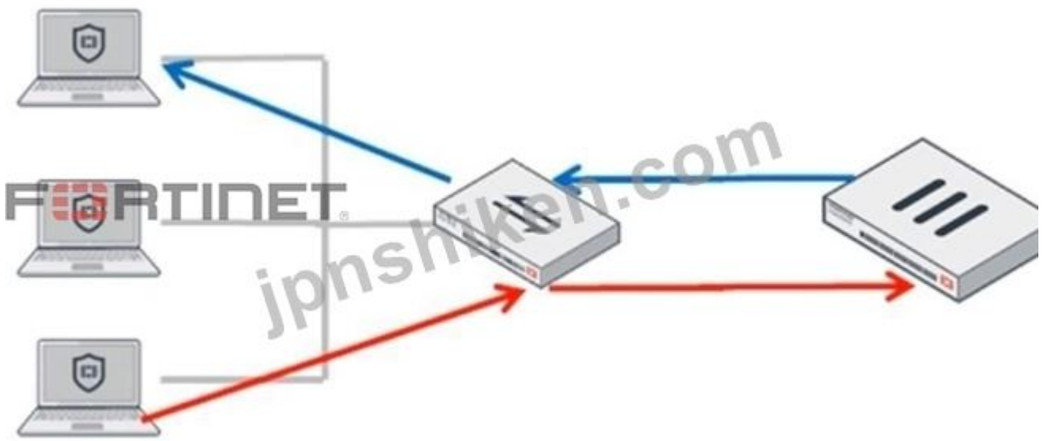
正解: **(**正解を表示します**)**

このサブパターンはTCP/UDPポート（「OTポート」グループ）のみをフィルタリングし、Modbusは指定しません。

プロトコル または特定のModbusポート）フィルタがない場合、FortiSIEMはModbusイベントを照合しないため、インシデントはトリガーされません。

jpnshiken.com

質問: **35**
図を参照してください。FortiGateデバイスをルーターオンアスティックとして機能させるには、OTネットワークアーキテクトはFortiGate上でVLAN間ルーティングを実現するためにどのような設定を行う必要がありますか？

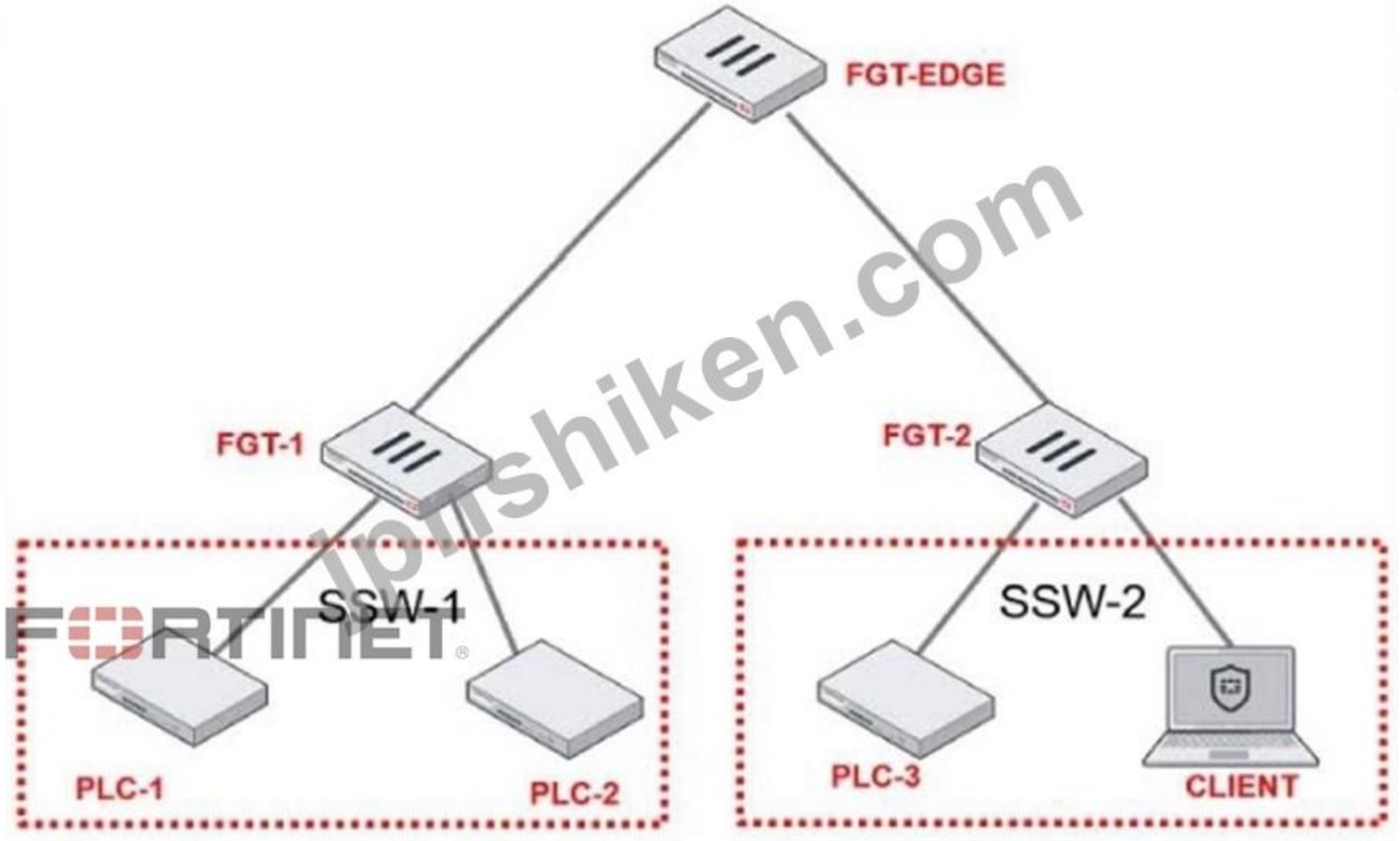


jpnshiken.com

A. ネットワーク上の各インターフェースに固有のフォワードドメインを設定します。
B. FortiGateを透過モードで動作するように設定します。
C. FortiGate にソフトウェア スイッチを設定して、VLAN 間トラフィックを処理します。
D. FortiGateインターフェースをスイッチと802.1qトランクとして動作するように設定します。
正解: (正解を表示します)
ルーターオンアスティック構成では、FortiGate上の単一の物理インターフェースで、802.1q VLANタギングを使用して複数のVLANのトラフィックを伝送する必要があります。
スイッチに接続されているFortiGateのインターフェースは、タグ付きVLANトラフィックを処理するためにトランクポートとして設定する必要があります。
次に、FortiGate上に各VLANごとにサブインターフェースが作成され、VLAN間でトラフィックをルーティングする。
この構成により、単一の物理リンク上で効率的なVLAN間ルーティングが可能になります。図に示すように、複数のVLANからのトラフィックがスイッチに集約され、トランクポートを介して伝送されます。

質問: **36**
図を参照してください。PLC-3とCLIENTは、PLC-1とPLC-2にトラフィックを送信できます。FGT-2には、PLC-3とCLIENTの両方を接続するソフトウェアスイッチ（SW-2）が1つだけあります。PLC-3とCLIENTは、レイヤ2レベルで相互にトラフィックを送信できます。
運用技術（OT）管理者は、PLC-3とクライアント間のレイヤー2レベルの通信を防止するために、どのような対策を講じる必要がありますか？

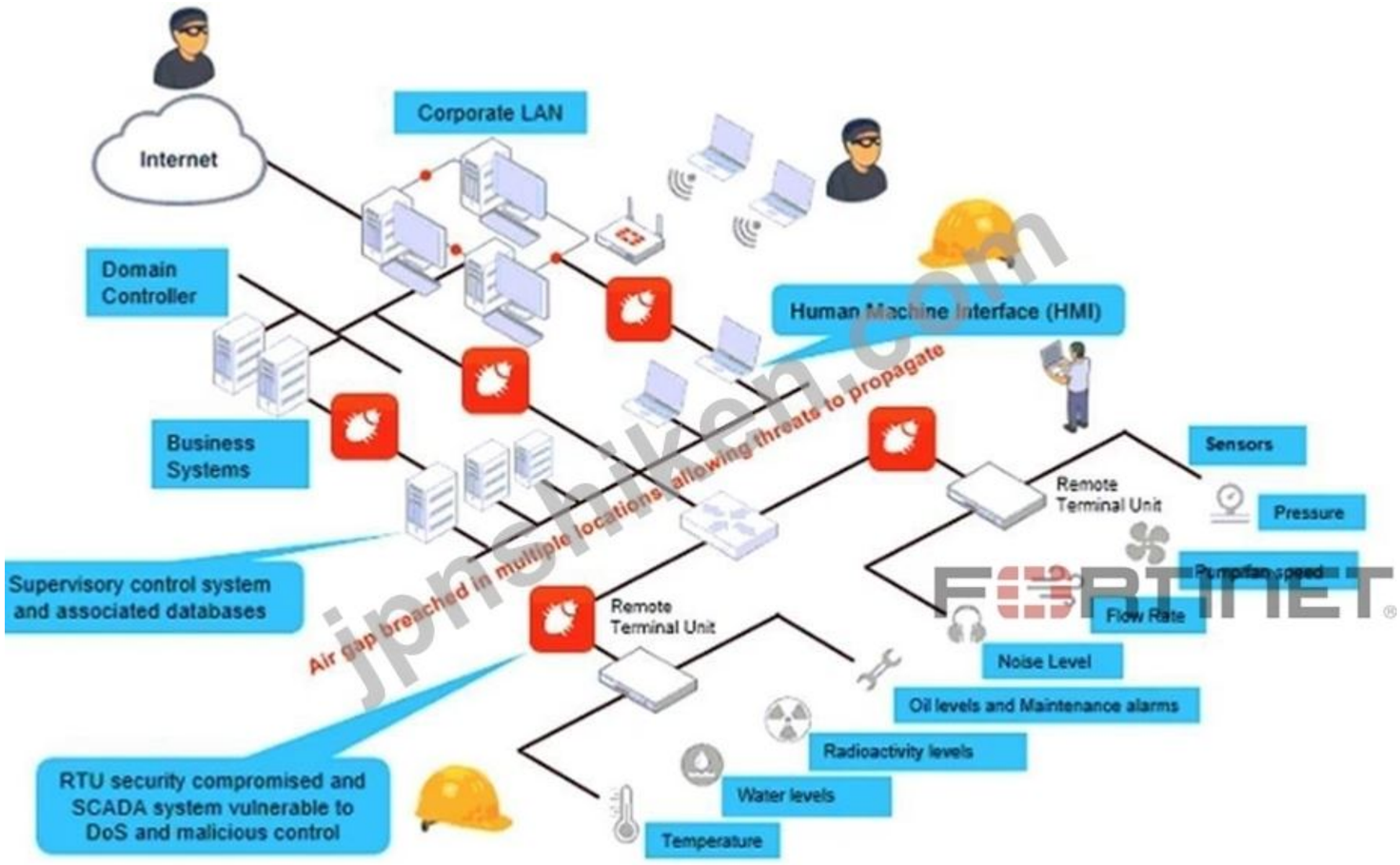
Network topology



1pushiken.com

A. ソフトウェアスイッチの各インターフェースに固有のフォワードドメインを設定します。
B. 各デバイス用にVLANを作成し、現在のFGT-2ソフトウェアスイッチメンバーを置き換えます。
C. FGT-2 上でファイアウォール ポリシーを要求する明示的なスイッチ内ポリシーを有効にします。
D. FGT-2 にポリシー ルートを実装して、デバイス間のトラフィックを制御します。
正解: **(**正解を表示します**)**
ソフトウェアスイッチを明示的なスイッチ内ポリシーに設定することで、メンバーポート間のトラフィックはレイヤ2でブリッジされるのではなく、FortiGateのポリシーを経由するようになります。これにより、PLC-3とクライアントがレイヤ2で直接通信することが防止されます。

質問: **37**
図を参照してください。図は保護されていないOT環境を示しています。管理者はOTネットワークに適切な保護対策を実装する必要があります。
OTネットワークを保護するために、管理者はどのような3つの手順を踏むべきでしょうか？ 3つ選択してください。）



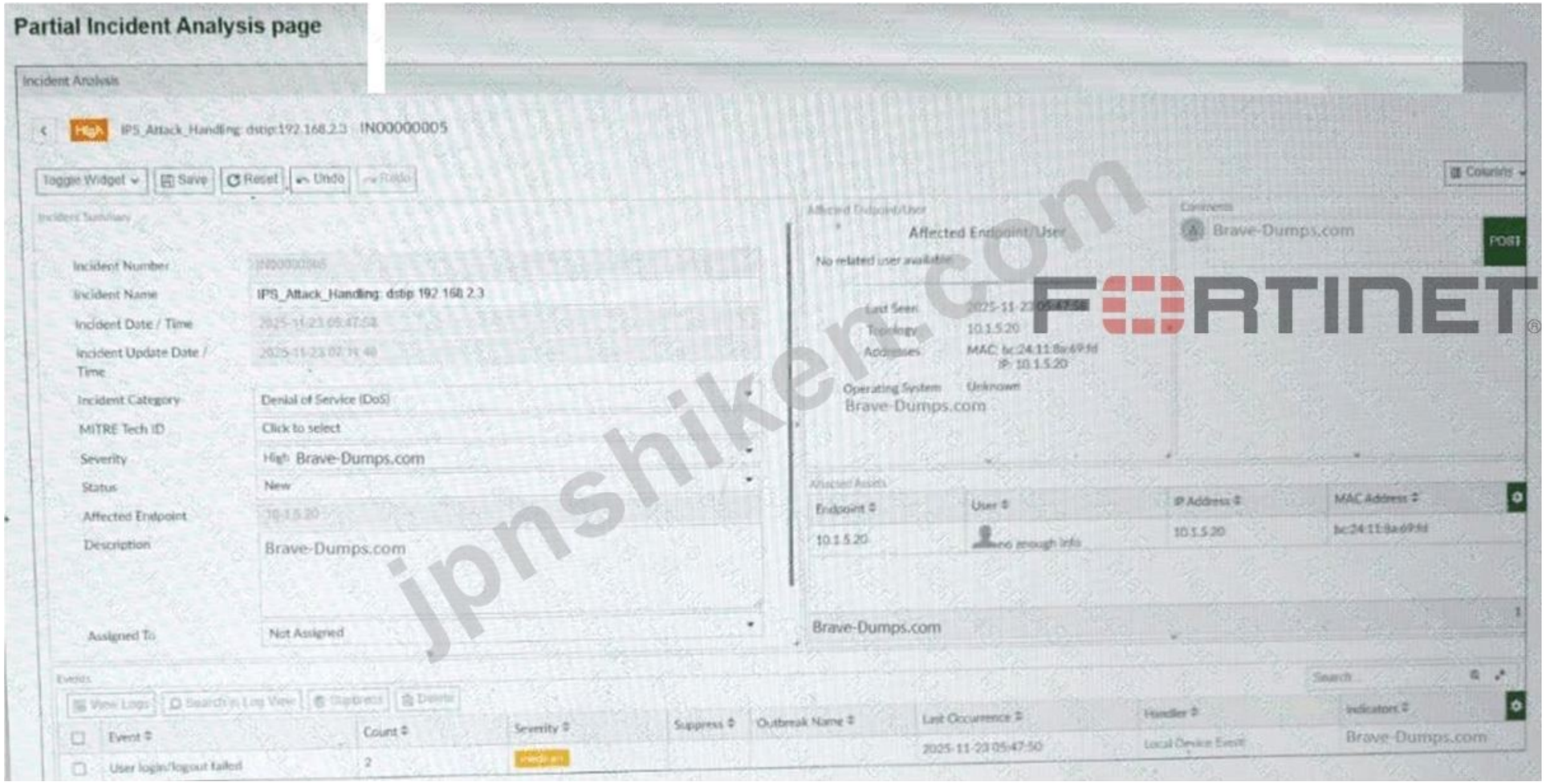
A. セグメンテーションを使用します。
B. Webフィルタリングを使用してファイアウォールポリシーを設定し、さまざまなICSネットワークを保護します。
C. 各ICSネットワーク内にFortiGateデバイスを導入します。
D. 産業用プロトコルセンサーを使用してファイアウォールポリシーを設定します。
E. インターネットとOTネットワークの間にエッジFortiGateを1アームスニファとして配置します。
正解: **(**正解を表示します**)**
ネットワークセグメンテーションの活用：OT環境において、ネットワークセグメンテーションは、異なるICS（産業制御システム）ネットワークを分離し、機密性の高いシステムを保護するために不可欠です。これにより、脅威の拡散を抑制し、セグメント間のアクセス制御が可能になります。
各ICSネットワーク内にFortiGateデバイスを導入する：各ICSネットワーク内にFortiGateデバイスを導入することで、不正アクセスや脅威を検知・防止するための局所的なセキュリティ対策が確実に実施されます。
産業用プロトコルセンサーを使用してファイアウォールポリシーを構成する：産業用プロトコルセンサーを使用してポリシーを構成すると、OT固有のトラフィック（Modbus、DNP3など）の監視と保護に役立ちます。
これにより、FortiGateはOTプロトコルを標的とした悪意のある活動を検知し、対応することが可能になります。

質問: **38**
パデュー大学のモデルでは、産業用IoT（IIoT）のような物理的資産はどのレベルに位置づけられるのでしょうか？

jpnshiken.com

（いずれか1つを選択してください）
A. レベル5のみ
B. レベル1のみ
C. レベル4以上
D. レベル3.5以下
正解: **(**正解を表示します**)**
OT Security 7.6 Architect 学習ガイドのパーデューモデルに関する記述によると、次のようになります。
* 資産の所在場所：学習ガイドには、「すべての重要な物理的資産は工場の現場に配置され、IIoTセンサーが装備されている」と記載されている。
* レベル分類：「プラントフロア」は、レベル0、1、2で構成される「制御エリアゾーン」としてさらに定義されます。
* 階層:「オペレーション & コントロール」ゾーンはレベル 3 およびレベル 3.5 として識別されます。
* 直接回答：「はじめに」レッスンの知識確認において、「パデューモデルでは、IIoTはどのレベルに位置付けられますか？」という具体的な質問に対して、検証済みの回答「レベル3.5未満」が提供されています。
。

質問: **39**
展示資料を参照してください。



jpnshiken.com
FORTINET

Log details related to the event

FORTINET
Brave-Dumps.com
jpnshiken.com

インシデント分析ページの一部と、イベントに関連するログの詳細が表示されます。OTネットワークで攻撃が発生したことが報告されました。該当するインシデントを分析します。インシデント分析ページとログの詳細に表示されている情報に基づいて、正しい記述は次のうちどれですか？ (2つ選択してください)

A. この攻撃はModbusプロトコルを使用します。

B. 攻撃は軽減されました。

C. この攻撃はIEC 104プロトコルを使用します。

D. 事象の深刻度は高い。

E. ターゲットデバイスのIPアドレスは10.1.5.20です。

正解: **(正解を表示します)**

展示資料およびOT Security 7.6 Architectカリキュラムに記載されている技術データに基づくと、以下のようになります。

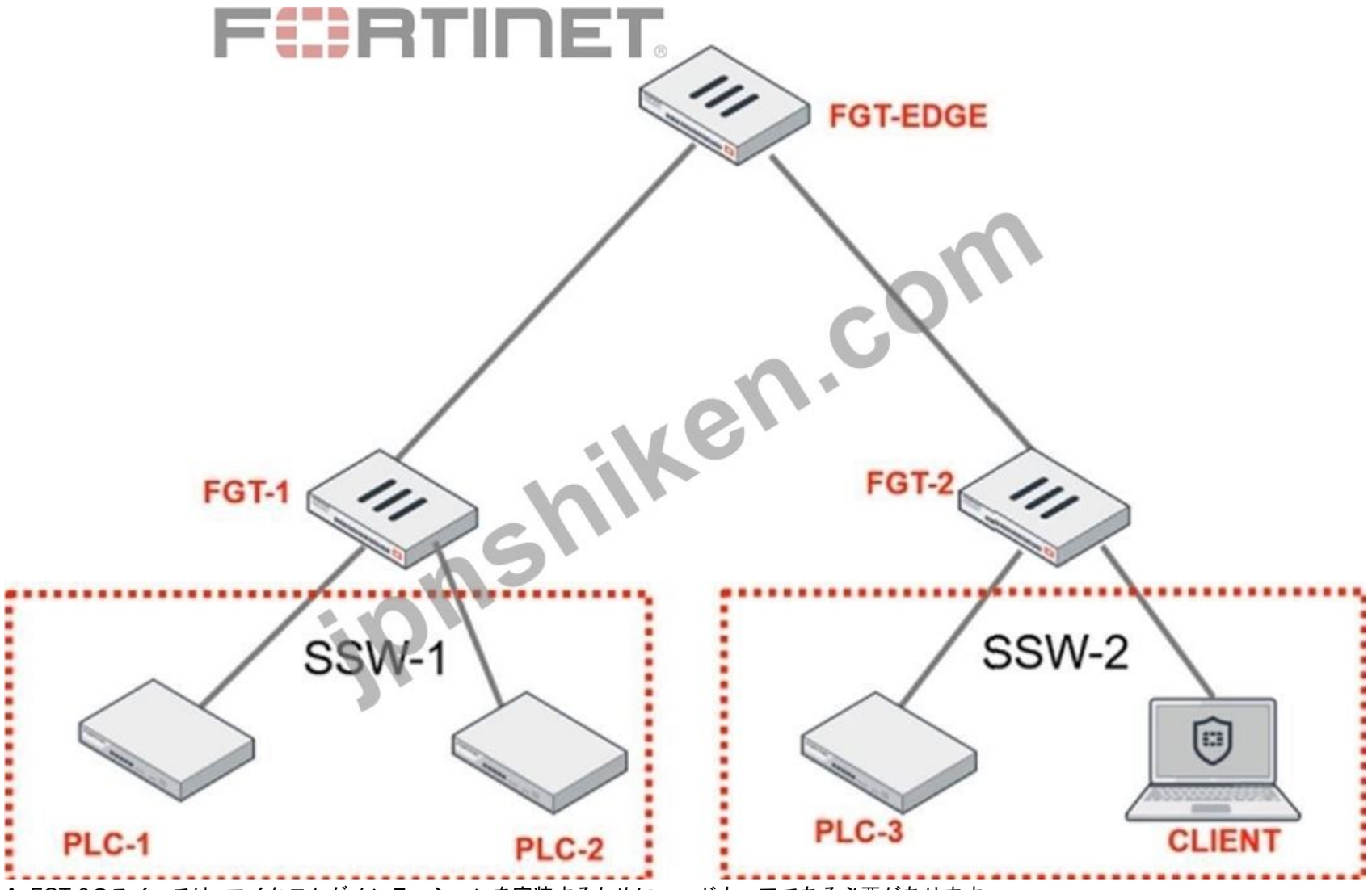
* 産業用プロトコルの識別（ステートメントA）：ログの詳細表示には、攻撃で使用された宛先ポートが502であることが明確に示されています。学習ガイドの産業用プロトコル保護のセクションによると、Modbus TCPプロトコルで使用される標準ポートは502です。さらに、攻撃名には「Triangle.Research.Nano-10.PLC」が識別されていますが、これは通信にModbusを一般的に使用する産業用コントローラです。

* 攻撃軽減（ステートメントB）：ログの詳細には、FortiGate（Edge-FortiGate）によって実行されたアクションがドロップされたと記載されています。サイバーセキュリティおよびFortinetファブリックの運用において、IPSシグネチャに関連付けられたパケットをドロップするということは、トラフィックがターゲットに到達するのをブロックし、それによって攻撃を軽減したことを意味します。

* ターゲット IP アドレス (ステートメント E) : ログの詳細には、宛先 IP が 192.168.2.3 と明示的に記載されています。
インシデント分析ページにも、インシデントのタイトルとしてdstip:192.168.2.3と記載されています。 影響を受けたエンドポイント」は10.1.5.20と表示されていますが、ログに示されているように 送信」攻撃方向では、これはおそらく内部の送信元/攻撃者のIPアドレスを指しており、ターゲットは宛先IPアドレス（192.168.2.3）です。したがって、ステートメントEは誤りです。
* プロトコルの競合 （ステートメントC） IEC 104プロトコルは通常ポート2404を使用します。ログにはポート502が指定されているため、ステートメントCは誤りです。
* 重大度の区別 （ステートメント D） インシデントの重大度は 高」とマークされていますが、質問ではイベントの重大度について具体的に尋ねています。インシデント分析ページの下部にある 「イベント」テーブルには、重大度が中程度の 「ユーザーのログイン/ログアウト失敗」イベントが表示されています。管理コンソールでは、個々のイベントの重大度と集約されたインシデントの重大度が区別されており、ステートメント A と B はポートとアクションに基づいて技術的に明確であるため、A と B が正しいアーキテクチャ上の選択肢です。

質問: **40**
運用技術（OT）ネットワークアナリストは、ネットワークを悪用する脅威を調査するために、さまざまなレベルのレポートを実行します。アナリストは、すべてのルーター、スイッチ、ファイアウォールに対してこれらのレポートを実行できます。
アナリストは、イメージファームウェアファイルを悪用する脅威を特定するために、FortiSIEMのどのレポート方法を使用できますか？
A. CMDBレポート
B. 脅威ハンティングレポート
C. コンプライアンスレポート
D. OT/IoTレポート
正解: (正解を表示します)
脅威ハンティングレポートを使用すると、アナリストはルーター、スイッチ、ファイアウォール全体にわたるイベントや指標（異常なファームウェアイメージへのアクセスや使用など）を照会し、ファームウェアファイルを標的としたエクスプロイトを明らかにすることができます。

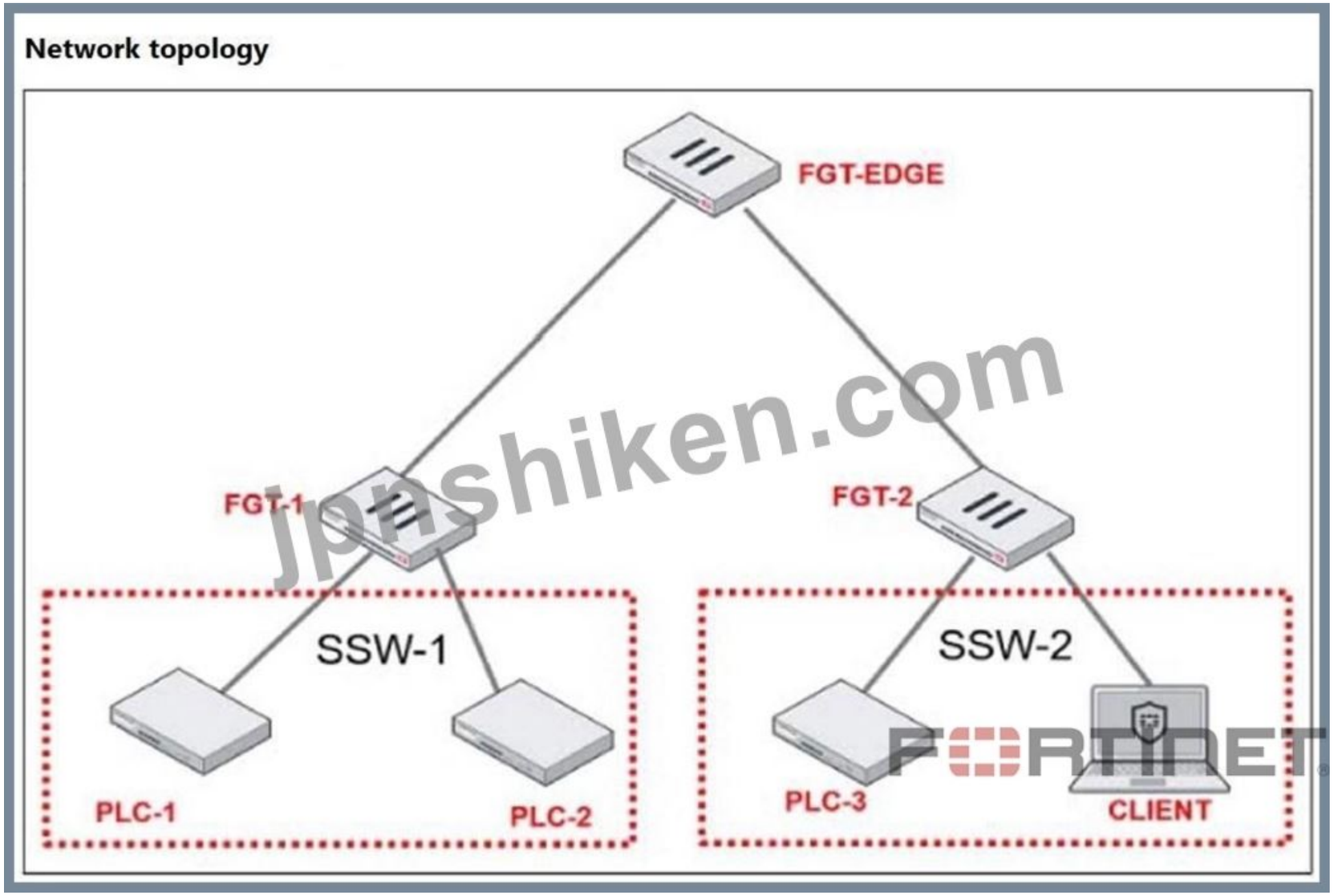
質問: **41**
図を参照してください。PLC-3とCLIENTは、PLC-1とPLC-2にトラフィックを送信できます。FGT-2には、PLC-3とCLIENTを接続するソフトウェアスイッチ（SW-1）が1つだけあります。PLC-3とCLIENTは相互にトラフィックを送信できません。
PCL-1とPLC-2間の通信に関する記述のうち、正しいものはどれですか？ （2つ選択してください。）



A. FGT-2のスイッチは、マイクロセグメンテーションを実装するためにハードウェアである必要があります。
B. FGT-2のマイクロセグメンテーションにより、デバイス間の直接通信が防止されます。
C. OTネットワークでは、トラフィックはFGT-EDGEによって検査されなければなりません。
D. FGT-2はファイアウォールポリシーを通じてVLAN内トラフィックを制御します。
正解: **B,D** (コメントを発表する)
マイクロセグメンテーションは、FGT-2のソフトウェアスイッチに接続されたPLC-3とCLIENTなど、同じVLANまたはスイッチレベルにあるデバイス間の直接的なトラフィックフローを防止します。
FGT-2は、インターフェースにファイアウォールポリシーを適用することで、OTネットワーク内のVLAN内（東西方向）トラフィックを制御し、この制御を強制します。
FGT-2のスイッチはハードウェアである必要はなく、ソフトウェアスイッチでもマイクロセグメンテーションを強制できる。
FGT-EDGEによるトラフィック検査は可能ですが、VLAN内トラフィックのセグメンテーションと制御はFGT-2の責任となります。

質問: **42**

図を参照してください。PLC-3とCLIENTは、PLC-1とPLC-2にトラフィックを送信できます。FGT-2には、PLC-3とCLIENTの両方を接続するソフトウェアスイッチ（SW-2）が1つだけあります。PLC-3とCLIENTは、レイヤ2レベルで相互にトラフィックを送信できます。
運用技術（OT）管理者は、PLC-3とクライアント間のレイヤー2レベルの通信を防止するために、どのような対策を講じる必要がありますか？



jpnshiken.com

A. ソフトウェアスイッチの各インターフェースに固有のフォワードドメインを設定します。
B. 各デバイス用にVLANを作成し、現在のFGT-2ソフトウェアスイッチメンバーを置き換えます。
C. FGT-2 上でファイアウォール ポリシーを要求する明示的なスイッチ内ポリシーを有効にします。
D. FGT-2 にポリシー ルートを実装して、デバイス間のトラフィックを制御します。
正解: **(**正解を表示します**)**
ソフトウェアスイッチを明示的なスイッチ内ポリシーに設定することで、メンバーポート間のトラフィックはレイヤ2でブリッジされるのではなく、FortiGateのポリシーを経由するようになります。これにより、PLC-3とクライアントがレイヤ2で直接通信することが防止されます。

質問: **43**
図を参照してください。堅牢化されたFortiGateの背後にあるOTデバイスには脆弱性があり、ファイアウォールポリシーに仮想パッチプロファイルを適用する必要があります。

セキュリティプロファイルのセクションで仮想パッチが利用できないのはなぜですか？（回答は1つ選択してください）
A. OT署名を有効にする必要があります。
B. 機能の表示設定セクションで仮想パッチ適用を有効にする必要があります。
C. 有効なOTセキュリティサービスライセンスが必要です。
D. 仮想パッチ機能に対応した堅牢なFortiGateが必要です。
正解: (正解を表示します)

質問: **44**
図を参照してください。Run_reportタスクが表示されています。

FortiAnalyzerで新しく作成されたレポートの生成を自動化したい。

PlaybookでRun_reportタスクを設定しても、レポートが[レポート]フィールドに表示されないのはなぜですか？ （2つ選択してください）
A. まずレポートで自動キャッシュを有効にする必要があります。
B. まずイベントハンドラを設定する必要があります。
C. まずコネクタを設定する必要があります。
D. まず「プレイブックスターター」を選択し、次に新しく作成したレポートを選択する必要があります。
E. まず、レポートで拡張ログフィルタリングを有効にする必要があります。
正解: **(**正解を表示します**)**

質問: **45**
OTネットワーク管理者がアクティブ認証の実装を試みている。
管理者はこの目的を達成するために、どの2つの方法を用いるべきでしょうか？ （2つ選択してください。）
A. FortiAuthenticatorでの二要素認証
B. FortiNACにおけるロールベース認証
C. FortiGateにおけるFSSO認証
D. FortiGateでのローカル認証
正解: **(**正解を表示します**)**
FortiGateにおけるローカル認証とFortiAuthenticatorによる二要素認証は、いずれもユーザーが認証情報（およびワンタイムパスワード）を積極的に提示する必要があり、これがアクティブ認証の本質です。

質問: **46**
大規模なOTネットワークのアクセス制御をパッシブ認証を使用して強化したい場合、FortiGateでどのような設定を行う必要がありますか？（回答は1つ選択してください）
A. Fortinetシングルサインオン（FSSO）
B. ローカルユーザー
C. 二段階認証
D. FortiAuthenticatorデバイスをリモートサーバーとして使用する
正解: **A (**コメントを発表する**)**
正解は A. Fortinet Single-Sign On (FSSO) です。学習ガイドの「アクティブ認証とパッシブ認証」の項には、パッシブ認証の場合、「ユーザーは FortiGate からログインプロンプトを受け取らない」と記載されています。
「認証情報は自動的に決定されます」とあり、具体的には「FSSO、RSSO、NTLMが使用できます」と説明されています。そして、シングルサインオン方式ではパッシブ認証が行われること、そしてFortinet SSO（FSSO）がそれらの方式の1つであることを明示的に示しています。
ガイドにはさらに、「パッシブ認証にはFSSOを実装できます。FSSOを使用すると、別のシステムを通じてネットワーク上で既に認証済みのユーザーを透過的に識別できます。ネットワーク上の任意のシステムに最初にログインした後、ユーザーは認証情報の入力を求められることなく、許可されたリソースにアクセスできます。」と記載されています。これはまさに質問の内容、つまりパッシブ認証を使用して大規模なOTネットワークのアクセス制御を改善する方法について尋ねているものです。
他のオプションはパッシブ認証には該当しません。ローカルユーザーはローカル認証の一部であり、2要素認証はセキュリティ要素を追加しますが、アクティブ認証を使用します。また、リモートサーバーとしてのFortiAuthenticatorは中規模から大規模ネットワーク向けの集中認証をサポートしますが、それ自体はここで問われている特定のパッシブ認証方法ではありません。学習ガイドには、パッシブ認証のためのFortiGate構成はFSSOであると明記されています。

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu **168**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**

図を参照してください。アプリケーションセンサーのプロファイルの一部を示しています。

このプロファイルをファイアウォールポリシーに適用する場合、正しい記述は次のうちどれですか？ 2つ選択してください）

A. Modbus書き込みコマンドはブロックされます。

B. OT署名が有効になっています。

C. すべてのOTプロトコルが監視されています。

D. Modbusの保持レジスタ読み取りコマンドごとにログが提供されます。

正解: **A,D (**コメントを発表する**)**

質問: **48**

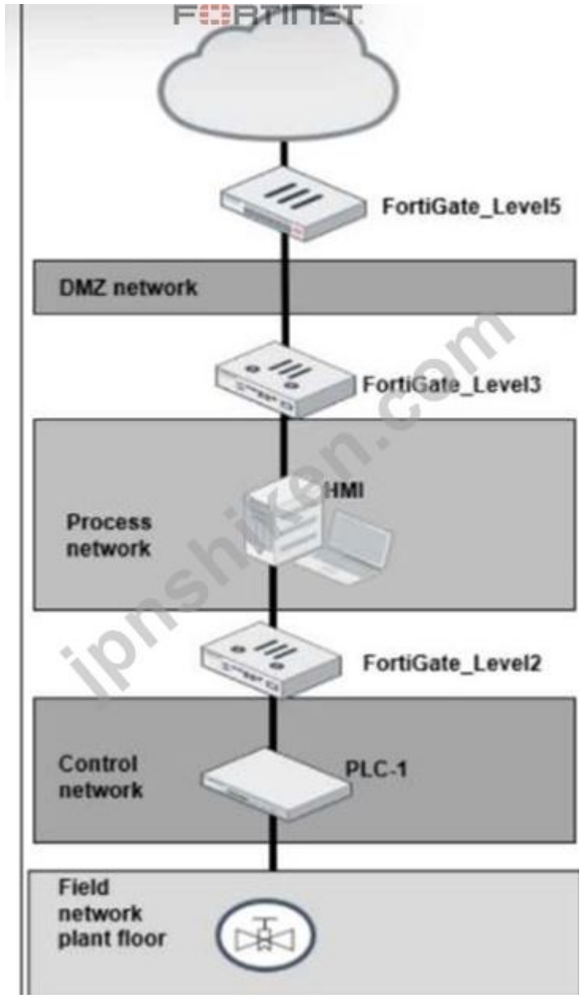
OTネットワークのセキュリティを強化するために、FortiAnalyzerによって通知された侵害されたデバイスの処理をFortiGate上で自動化したいと考えています。どのような設定が必要ですか？

A. FortiAnalyzerでAutomation Stitchパラメータが有効になっているイベントハンドラ
B. FortiAnalyzer 上の LOCAL_HOST コネクタを使用した自動化
C. FortiGateのセキュリティファブリック設定
D. FortiGate上のFortiOSイベントログトリガー
正解: (正解を表示します)
FortiAnalyzerとFortiGate間の自動化は、Automation Stitchが有効になっているFortiAnalyzerに設定されたイベントハンドラに依存しており、これにより、侵害されたデバイスなどの特定のイベントが検出された際に、FortiAnalyzerがFortiGate上で自動アクションをトリガーできるようになります。

質問: **49**
展示資料を参照してください。

FortiGateデバイスの論理トポロジーページが表示されています。貴社のOT企業はネットワークの可視性を高めたいと考えています。そこで、セキュリティファブリックを使用してデバイス検出を実装することにしました。図に基づいて、正しい記述はどれですか？（2つ選択してください）
A. 他の識別されたデバイスでデバイス検出が有効になっています。
B. 他の識別されたデバイスは、ルートFortiGateで認証されている必要があります。
C. 他の識別されたデバイスは、FortiAnalyzer で認証されている必要があります。
D. ポート3でデバイス検出が有効になっています。
正解: (正解を表示します)
正解はAです。他の識別されたデバイスでデバイス検出が有効になっています。
学習ガイドでは、デバイス識別は 「セキュリティファブリックのトポロジービューにとって便利な機能」であり、 FortiGateはネットワーク内のほとんどのサードパーティ製デバイスを検出し、セキュリティファブリックのトポロジービューに追加する」と説明されています。また、インターフェースセクションでデバイス検出を有効にできること、そしてこの検出によってFortiGateは観測されたトラフィックに基づいてデバイスを識別できることも記載されています。
展示資料では、ツールチップに 「1台のデバイスが認証を必要としています」と 「1台の他の識別済みデバイス」が区別されています。つまり、認証されていないデバイスは別のFortiGate/Fabricメンバーの問題であり、他の識別済みデバイスはデバイス検出が機能しているためトポロジーに表示される、検出されたサードパーティ製デバイスにすぎません。したがって、正しい解釈は、その識別済みデバイスに対してデバイス検出が有効になっているということです。オプションBは、展示資料に他の識別済みデバイスが認証を必要としているとは記載されていないため誤りです。オプションCは学習ガイドでサポートされておらず、オプションDは、展示資料にポート3で検出が有効になっていることを裏付ける証拠がないため、具体的すぎます。

質問: **50**
OT管理者はOTネットワークのセキュリティを確保するために多数のデバイスを導入しました。しかし、SOCチームからはアラートが多すぎること、そしてその多くが誤検知であるとの報告を受けています。OT管理者は、反復作業をなくし、効率性を向上させ、時間とリソースを節約できるソリューションを求めています。
管理者は、これらの問題に対処し、SOCチームが行っている手作業の大部分を自動化するために、どの製品を導入すべきでしょうか？
A. FortiSandboxとFortiSIEM
B. FortiSIEMとFortiManager
C. FortiSOARとFortiSIEM
D. syslogサーバーとFortiSIEM
正解: (正解を表示します)

質問: **51**
展示資料を参照してください。


簡略化されたOTネットワークが図示されています。このOTネットワークの保護を最適化したい場合、どの2つの制御策を実装する必要がありますか？ 2つ選択してください）
A. FortiGate_Level3 のオフライン IDS。

B. FortiGate_Level5 の IPS。
C. FortiGate_Level2 での仮想パッチ適用。
D. FortiGate_Level5 の OT 署名。
正解: (正解を表示します)
正解はB. FortiGate_Level5のIPSとC. FortiGate_Level2の仮想パッチ適用です。
学習ガイドでは、「第一の防御線はネットワークのIT側を保護することである」と説明し、FortiGateはICS環境を保護し、ITからOTへの脅威の伝播を阻止するために配置する必要があると述べています。また、「今日の脅威環境では、IPSがより広範囲の脅威をブロックし、OTセキュリティを向上させる必要がある」ため、IPSはOTセキュリティを向上させると述べており、IPSモードでは脆弱なデバイスが保護されます。このことから、DMZと外部接続に近い上位境界にあるFortiGate_Level5は、主要な保護制御としてIPSを実装するのに最適な場所であると言えます。
学習ガイドのパデューモデルセクションでは、「レベル2は、レベル1にあるPLC、RTU、およびIEDを制御するプロセスとプログラムで構成される」こと、そして「これらのサーバーをファイアウォールセグメンテーションでセグメント化、あるいはマイクロセグメント化し、アプリケーション制御や仮想パッチ適用を含むポリシーを適用する必要がある」と記載されています。さらに、仮想パッチ適用セクションでは、「仮想パッチ適用は、まだ更新されていないOTデバイスを脆弱性の悪用から保護する」とあり、脆弱なデバイスに関連するトラフィックがファイアウォールポリシーに到達した際に適用されます。FortiGate_Level2はプロセスネットワークと制御ネットワークの間に位置しているため、PLC側の資産を保護するための仮想パッチ適用の適切な適用ポイントとなります。
オプションAは最適な回答とは言えません。オフラインIDSは攻撃を検出してログに記録するだけであり、ガイドにはオフラインIDSモードでは「FortiGateを通過するトラフィックがない」と記載されていますが、IPSは実際に脅威をブロックできます。オプションDも最適な回答とは言えません。OTシグネチャはIPSフレームワーク内で有効になっていますが、この設計で明示的に説明されているより強力な制御方法は、IPSを上位境界に配置し、仮想パッチを脆弱なOTデバイスにより近い場所に展開することです。

質問: **52**
OT産業制御システム（ICS）における機器識別に使用できるFortinet製品を3つ選択してください。
A. FortiSIEM
B. FortiManager
C. FortiAnalyzer
D. FortiGate
E. FortiNAC
正解: (正解を表示します)
FortiNACは、アクティブスキャンやパッシブスキャンなど、さまざまな方法を用いて、OTネットワーク内のデバイスの識別情報、プロファイル、分類を継続的に収集します。
FortiGateは、デバイスの識別と分類に役立つセッションデータとフローデータを提供することで貢献します。
FortiSIEMは、FortiGateやFortiNACなど様々なソースからセキュリティデータと運用データを集約し、包括的な可視性と識別機能を提供します。

質問: **53**
VLANをサポートしていない産業用プロトコルはどれですか？（1つ選択してください）
A. 【展示物ではっきりと確認できない】
B. 産業用プロトコルによるイーサネット
C. EtherCAT
D. TCP経由のModbus
正解: (正解を表示します)
正解はC. EtherCATです。
学習ガイドには、「Ethernet/IPやModbus/TCPなどの産業用イーサネットプロトコルでは、VLANを使用して物理LANを複数の論理LANに分割できる」と記載されています。これは、Ethernet/IPとModbus/TCPがOT環境においてVLANベースのセグメンテーションをサポートしていることを直接的に裏付けています。

対照的に、このガイドでは EtherCATはレイヤ3から6をスキップしてリアルタイム通信を実現する」と説明し、 オープンソフトウェアによる改良型イーサネット」のアプローチであると述べている。EtherCATは、通常のVLANベースのセグメンテーションに使用される標準的なEthernet/IPモデルとは異なる動作をするため、Ethernet/IPやModbus/TCPのようにVLANをサポートしないプロトコルとしてここで挙げられている。
したがって、学習ガイドの比較に基づくと、正解はEtherCATです。

質問: **54**
パデュー大学のモデルでは、産業用IoT（IIoT）のような物理的資産はどのレベルに位置づけられるのでしょうか？
A. レベル5のみ
B. レベル1のみ
C. レベル4以上
D. レベル3.5以下
正解: (正解を表示します)
パデュー大学のモデルでは、レベル1は基本的な制御と物理プロセスを表しており、センサー、アクチュエーター、およびIIoTデバイスが物理環境と直接相互作用する。

質問: **55**
OTネットワークアーキテクトは、産業用リモートネットワーク内の燃料ポンプを保護するためのソリューションを導入する必要があります。すべての燃料ポンプは、温度変動がないか企業ネットワークから厳密に監視されなければなりません。
OTネットワークアーキテクトは、どのようにしてこの目標を達成できるのでしょうか？
A. リモートネットワーク上に燃料サーバーを設定し、企業ネットワーク上に単一パターンの温度セキュリティルールを持つFortiSIEMをデプロイします。
B. リモートネットワーク上に燃料サーバーを設定し、企業ネットワーク上に単一パターンの温度パフォーマンスルールを持つFortiSIEMをデプロイします。
C. 社内ネットワーク上に燃料サーバーを設定し、リモートネットワーク上に単一パターンの温度パフォーマンスルールを持つFortiSIEMをデプロイします。
D. 企業ネットワーク上で、燃料サーバーとFortiSIEMの両方に単一パターンの温度パフォーマンスルールを設定します。
正解: (正解を表示します)
遠隔OTネットワークに設置された燃料サーバーがポンプの温度データをローカルで収集し、企業側のFortiSIEMが単一パターンのパフォーマンスルールを用いてそれを分析することで、温度変動を検出します。これにより、ポンプを直接監視することなく一元的な可視性を確保し、運用指標（温度の監視に適したルールタイプを使用できます。

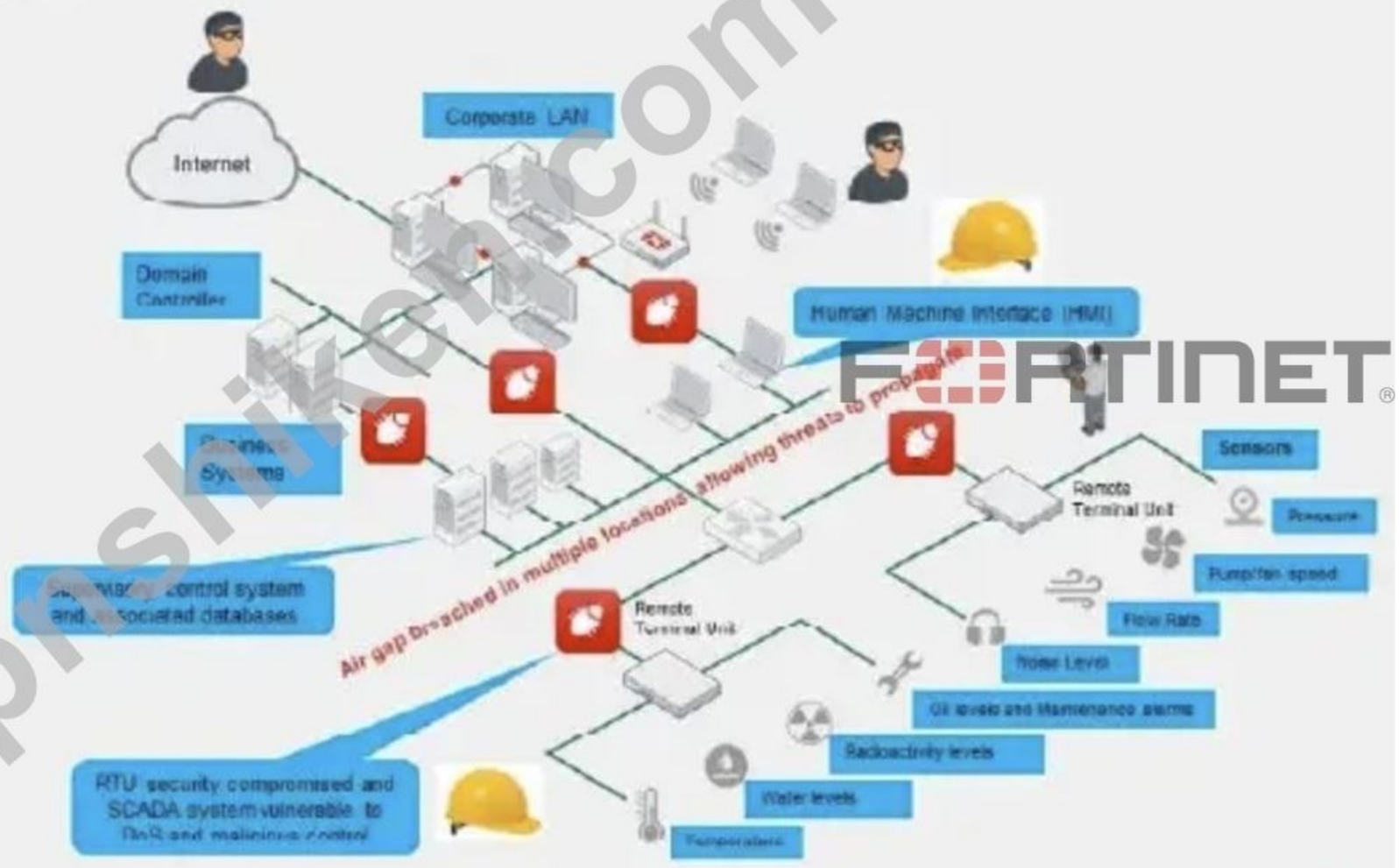
質問: **56**
ある組織が、運用技術（OT）ネットワークにエントリーレベルのFortiGateデバイスを導入しました。管理者は、誤検知を一切発生させることなく、ネットワークの特定部分におけるすべてのネットワーク侵入を検知・ブロックするシンプルなソリューションを求めています。
管理者はこの目標を達成するために、どの解決策を用いるべきでしょうか？
A. ローカルインファイアウォールポリシーを設定します。
B. すべての海外からの着信トラフィックをブロックします。
C. 侵入防御システム（IPS）を有効にし、通常のシグネチャデータベースを使用します。
D. IPSグローバル設定で産業用署名データベースを有効にします。
正解: (正解を表示します)
IPS産業用シグネチャデータベースを有効にすることで、OT/ICSプロトコルと既知の攻撃パターンに検出対象を絞り込み、エントリーレベルのFortiGateでも誤検知を最小限に抑えつつ正確なブロックを実現します。

質問: **57**

一般的なOT環境で見られる、よくある侵害箇所を3つ挙げてください。3つ選択してください。）
A. グローバルハット
B. ヘルメット
C. VLANの脆弱性を悪用する
D. 黒い帽子
E. RTUの悪用
正解: **(**正解を表示します**)**

Understand Breach Points for the OT Environment

- Breach points are everywhere
  - Outside threat—Black Hat
  - Inside threat—Hard Hat
  - Air gap breached
  - RTU or HMI exploits
  - DoS attack of protocols
  - Droppers USB



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

質問: **58**

FortiNACでは、不正デバイスはどのように評価されますか？

A. デバイスプロファイリングルールを通じて

B. FortiGuardサーバーへのクエリを通じて

C. デバイスリストのインポートを通じて
D. ローカルデバイスデータベース（CIDB）を介して
正解: (正解を表示します)
FortiNACは、MACアドレス、トラフィックパターン、動作などの観測されたネットワーク属性を分析するデバイスプロファイリングルールを使用して不正デバイスを評価し、未知のデバイスや不正なデバイスを分類および識別します。

質問: **59**
OT管理者はFortiSIEMを使用してインシデント通知ポリシーを定義し、通知ポリシーをシステムに設定したいと考えています。インシデントが発生した場合、管理者はFortiSIEMからIPアドレスをブロックしたり、Active Directory内のユーザーを無効化したりできるようにしたいと考えています。このタスクを実行するために、管理者はどの手順を実行する必要がありますか？
A. FortiSIEM 上で通知ポリシーを使用してファブリックコネクタを設定し、FortiGate に接続します。
B. FortiSIEM 上で通知ポリシーを作成し、スクリプト/修復を定義します。
C. FortiManagerでスクリプト/修復を定義し、FortiSIEMで通知ルールを有効にします。
D. Active Directory に緩和スクリプトをデプロイし、FortiSIEM に通知ポリシーを作成します。
正解: (正解を表示します)
https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript

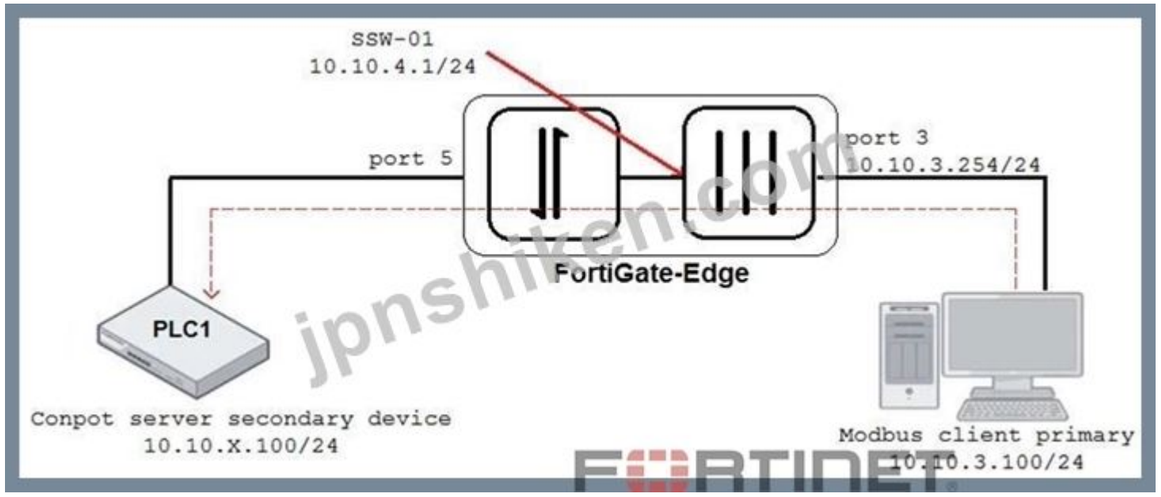
質問: **60**
展示資料を参照してください。

Event Brave-Dumps.com	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler Brave-Dumps.com	Device Name
Schneider.Electric.Modicon.	Mitigated	IPS	16	Medium	a day ago	an hour ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate
Triangle.Research.Nano-10.	Mitigated	IPS	6	Medium	19 hours ago	19 hours ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate

展示資料に示されているイベントモニターページの一部に表示されている情報に基づいて、攻撃はどのように検知されましたか？（回答は1つ選択してください）
A. ステッチで自動的に
B. 管理者による手動
C. プレイブックにより自動的に
D. イベントハンドラによって自動的に
正解: (正解を表示します)
正解はDです。イベントハンドラによって自動的に検出されます。学習ガイドには、「イベントハンドラはFortiAnalyzer上でイベントを生成します」および「FortiAnalyzerはイベントハンドラを使用して、受信するすべてのログをフィルタリングします。受信したログがイベントハンドラで設定された条件に一致する場合、FortiAnalyzerはイベントを生成します」と明記されています。また、「生成されたすべてのイベントはイベントモニタページで確認できます」とも記載されています。これは、イベントモニタページにエントリが表示されている図と直接一致します。したがって、図に示されている攻撃は、イベントハンドラによって自動的に検出されたものです。
ガイドでは、検出フローについても説明しています。「FortiAnalyzer はログを受信します」、「FortiAnalyzer はログを解析します」、「FortiAnalyzer は、イベントハンドラでルールが一致するとイベントを生成します」。さらに、イベントモニタビューには、イベントを生成したイベントハンドラを識別する「ハンドラ」列が含まれています。そのため、この攻撃は手動で検出されたとはみなされず、プレイブックやステッチによって主に検出されたわけでもありません。プレイブックとステッチは後続の自動化アクションに使用されますが、イベントモニタに表示されるイベントはイベントハンドラメカニズムによって生成されます。

質問: **61**
図を参照してください。OTアーキテクトは、シミュレーションサーバーConpotを使用してModbus TCPを実装し、OTネットワーク内のModbusトラフィックを識別および制御しています。FortiGate-Edgeデバイスは、ソフトウェアスイッチインターフェイスssw-01で構成されています。

図に示されたトポロジーに基づいて、クライアントとサーバー間のトラフィックのシミュレーションが成功したことに関する記述のうち、正しいものはどれですか？ 2つ選択してください。）



A. FortiGate-Edge デバイスは NAT モードである必要があります。
B. FortiGate デバイスはオフライン IDS モードです。
C. ポート5はソフトウェアスイッチのメンバーではありません。
D. FortiGateファイアウォールポリシーでポート3からssw-01へのNATが無効になっています。
正解: (正解を表示します)

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu 168問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
図を参照してください。OTネットワークでFortiSIEMを操作しています。図に示されている情報はどのように表示され、FortiGateデバイスのセキュリティステータスは何を示していますか？

Maint	Device	Type	Organization	Avail Status	Perf Status	Security Status
●	FG240D3913800441	Fortinet FortiOS	Super	●	●	⊗
●	SJ-QA-F-Lnx-CHK	Checkpoint FireWall	Super	●	●	⚠
●	FAPS321C-default	Fortinet FortiAP	Super		●	●

A. PCIログダッシュボードに、FortiGateデバイスに関する1つ以上の重大度の高いセキュリティインシデントが表示されています。
B. ビジネスサービスダッシュボードに、FortiGateデバイスに関する重大度の高いセキュリティインシデントが1件以上表示されています。

C. サマリーダッシュボードに、FortiGateデバイスに関する重大度の高いセキュリティインシデントが1件以上表示されています。
D. ウィジェットダッシュボードに、FortiGateデバイスに関する重大度の高いインシデントが1つ以上あります。
正解: **(**正解を表示します**)**

質問: **63**
既知の脆弱性から保護するために、更新されていないOTデバイスを保護するため、ファイアウォールポリシーに仮想パッチを適用します。OTデバイスに仮想パッチが適用されていることを確認するには、何をチェックする必要がありますか？
（いずれか1つを選択してください）
A. OTビューページ
B. CLIコマンドget virtual-patch profileの出力
C. 資産識別リストページ
D. CLIコマンド get rule otvp status の出力
正解: **(**正解を表示します**)**

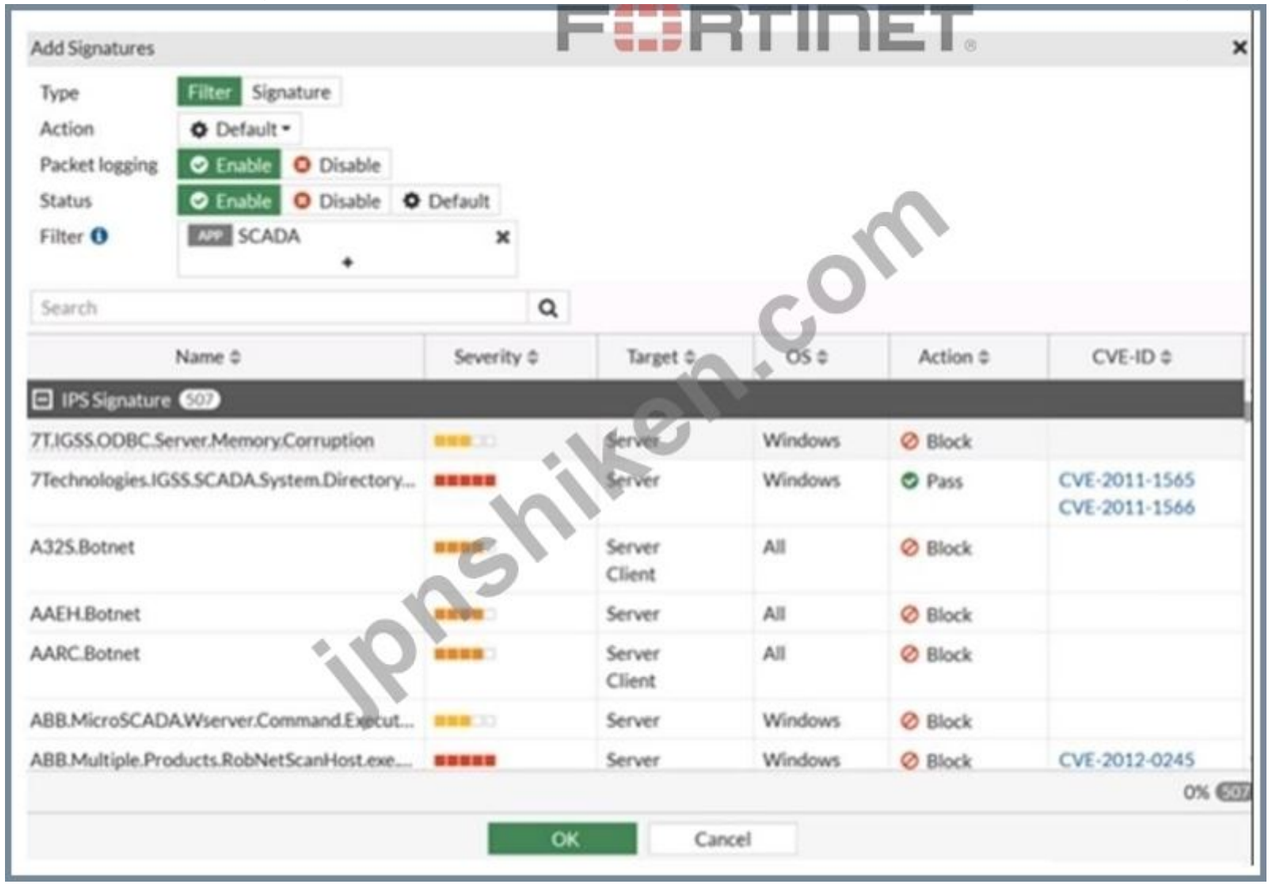
質問: **64**
OTネットワーク管理者として、FortiSIEMに送信されるデータと同じ種類のデータを主に利用するレポートを作成する必要があります。これらのレポートは、事前にロードされた分析検索に基づいています。FortiSIEMで実行中のレポートを将来的に活用するために、実行できる操作を2つ選択してください。
A. 追加の分析検索を処理するためのカスタムレポートを作成します。
B. プリロードされた分析検索を外部のsyslogサーバーにエクスポートする
C. 分析検索を保存し、レポート定義に変換します。
D. 新しいログを受信したときにこれらのレポートの実行を自動化する
正解: **A,C (**コメントを発表する**)**
追加の分析検索を処理するためのカスタムレポートを作成する：FortiSIEMでは、特定の要件に合わせてカスタマイズしたレポートを作成できます。これは、プリロードされた分析検索ではレポート作成のニーズを完全に満たせない場合や、追加のデータ処理が必要な場合に役立ちます。
分析検索を保存してレポート定義に変換する：FortiSIEMでは、分析検索を保存して再利用可能なレポート定義に変換できます。これらのレポート定義を使用することで、今後同じ基準に基づいて一貫性のあるレポートを生成できます。

質問: **65**
大規模なOTネットワークのアクセス制御をパッシブ認証を使用して強化したい場合、FortiGateでどのような設定を行う必要がありますか？
A. Fortinetシングルサインオン（FSSO）
B. ローカルユーザー
C. 二段階認証
D. FortiAuthenticatorデバイスをリモートサーバーとして使用する
正解: **(**正解を表示します**)**
FortiGateにおけるパッシブ認証は、Fortinet Single Sign-On（FSSO）を使用して実現されます。FSSOは、ユーザーが再度ログインする必要なく、認証ソースからユーザーID情報を透過的に収集します。

質問: **66**
OTアーキテクトは、パデューモデル（プロセス制御）のレベル1にあるOTネットワークにレイヤ2スイッチを導入しました。このレイヤ2スイッチの目的は、PLC1とPLC2間のトラフィックを2つのVLANでセグメント化することです。
PLC1とPLC2間のすべてのトラフィックは、まずレイヤ2スイッチを経由し、次にレイヤ2監視制御ネットワーク内のFortiGateデバイスを経由する必要があります。

PLC1とPLC2間の通信に関する記述として正しいのはどれですか？
A. 通信を行うには、PLC1 と PLC2 が同じ VLAN に属している必要があります。
B. レイヤ2スイッチは、FortiGateデバイスにトラフィックを送信する前にVLANタグを書き換えます。
C. レイヤ2スイッチは、イーサネットリンクを介してFortiGateデバイスにトラフィックをルーティングします。
D. PLC間の通信には、FortiGateを「トラフィック型ルーター」として構成する必要があります。
正解: **D** (コメントを発表する)
レイヤ2スイッチ上でPLC1とPLC2が別々のVLANに属している場合、VLAN間のトラフィックはルーティングする必要があります。
FortiGateは、単一の物理リンク上のVLANサブインターフェース（「トラフィック型ルーター」）を使用することで、ルーティングとポリシー制御を実現し、PLC1↔PLC2間のすべてのトラフィックを通過させます。

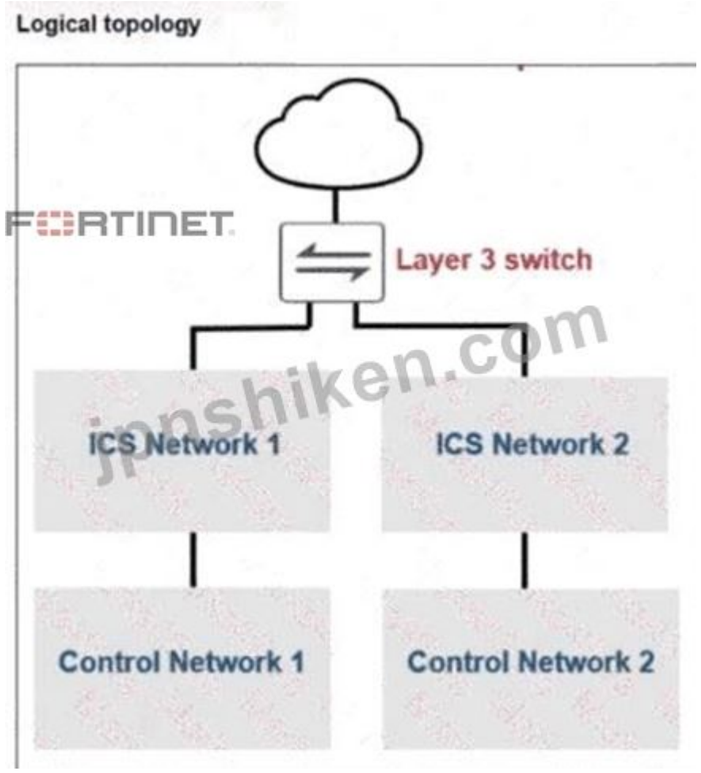
質問: **67**
図を参照してください。IPSプロファイルはFortiGate上のすべてのセキュリティポリシーに追加されます。OTネットワークの場合、IPSプロファイルの次の記述のうち、正しいものはどれですか？



A. FortiGateにはIPS産業用シグネチャデータベースが有効になっていません。
B. リストされているIPSシグネチャはSCADAアプリケーションに分類されます。
C. すべてのIPSシグネチャは上書きされ、シグネチャパターンに一致するトラフィックをブロックする必要があります。
D. IPSプロファイルは、SCADA機器から発信されるトラフィックのみを検査します。
正解: (正解を表示します)

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/533327/ips-signatures-for-the-operational-technology-security-service

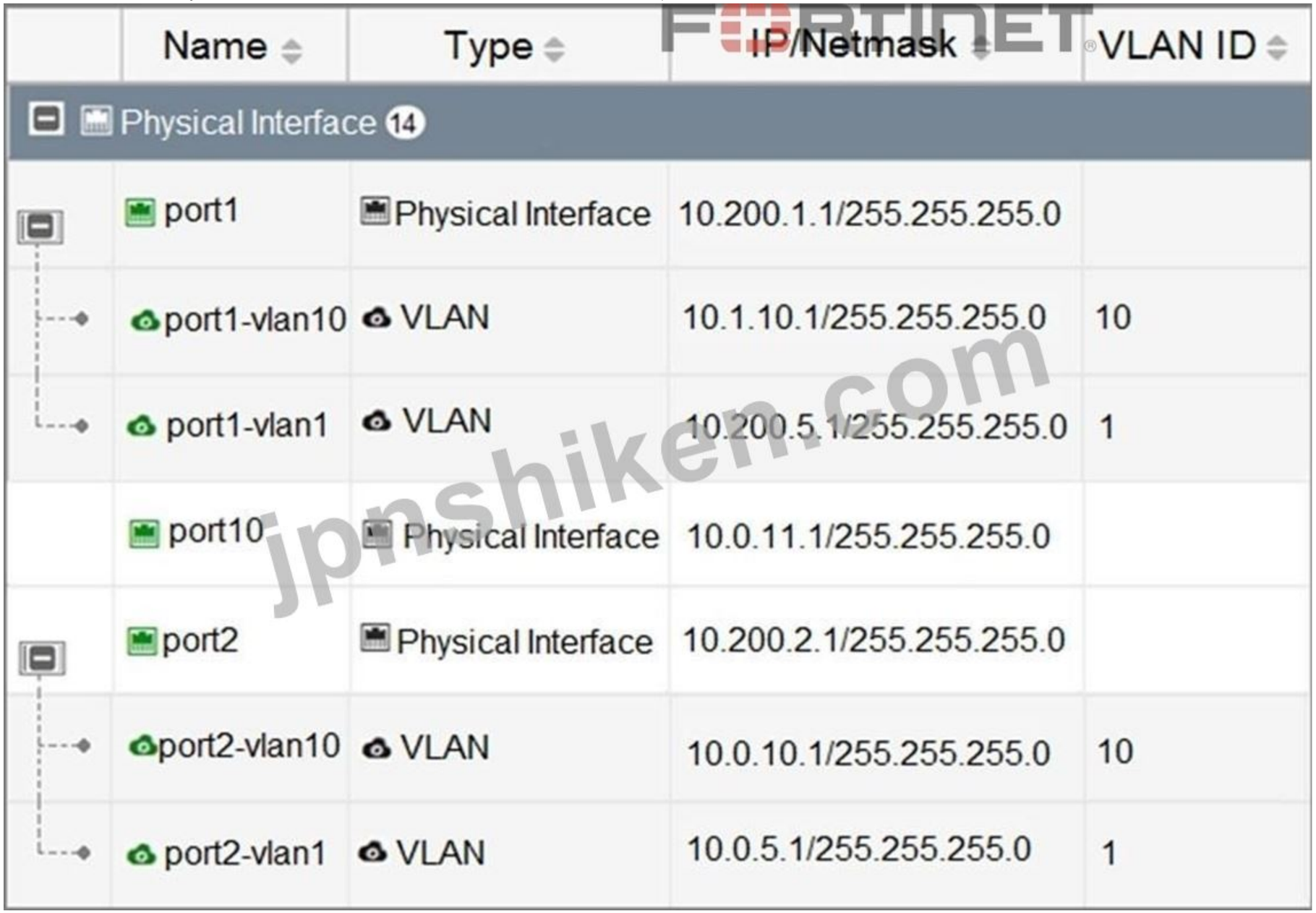
質問: **68**
図を参照してください。部分的なOTネットワークが示されています。このOTネットワークのセキュリティを向上させ、ネットワーク1とネットワーク2の間で内部セグメンテーションを実装する必要があります。どのようにセグメンテーションを実現できますか？
（いずれか1つを選択してください）



A. ユニバーサルZTNAを設定できます。
B. 1 つのトラフィック VDOM を設定できます。
C. 明示的なソフトウェアスイッチを設定できます。
D. 各ネットワークごとに転送ドメインIDを設定できます。
正解: (正解を表示します)
正解はDです。各ネットワークにフォワードドメインIDを設定できます。学習ガイドでは、FortiGateの透過モードでは「VLAN IDが異なるインターフェースであっても、すべてのインターフェースが同じブロードキャストドメインに属する」と説明し、set forward-domain <domain_ID>コマンドを使用して「複数のブロードキャストドメインに分割する」必要があると述べています。さらに、「同じドメインIDを持つインターフェースは同じブロードキャストドメインに属する」こと、そして「あるインターフェースに到着したトラフィックは、同じフォワードドメインIDを持つインターフェースにのみブロードキャストされる」ことが定義されています。これはまさに、内部ネットワークを分離し、セグメンテーションを向上させるために使用される仕組みです。
他のオプションはこの要件を満たしていません。ユニバーサルZTNAは、アプリケーションへのユーザーアクセスを制御するものであり、2つの内部OTネットワークをセグメント化するものではありません。明示的なソフトウェアスイッチは、同じソフトウェアスイッチブロードキャストドメイン内のスイッチ内またはVLAN内のトラフィックを制御するためのものであり、2つのルーティングされた内部ネットワークを分離するよりもマイクロセグメンテーションに適しています。1つのトラフィックVDOMだけではセグメンテーションは作成されません。VDOMによるセグメンテーションには、1つではなく複数のVDOMが必要です。したがって、このシナリオでネットワーク1とネットワーク2をセグメント化する最良の選択肢は、個別のフォワードドメインIDを割り当てることです。

質問: **69**

図を参照してください。図に示されているインターフェースに関する記述のうち、正しいものはどれですか？



A. port1-vlan10とport2-vlan10は同じブロードキャストドメインに属しています

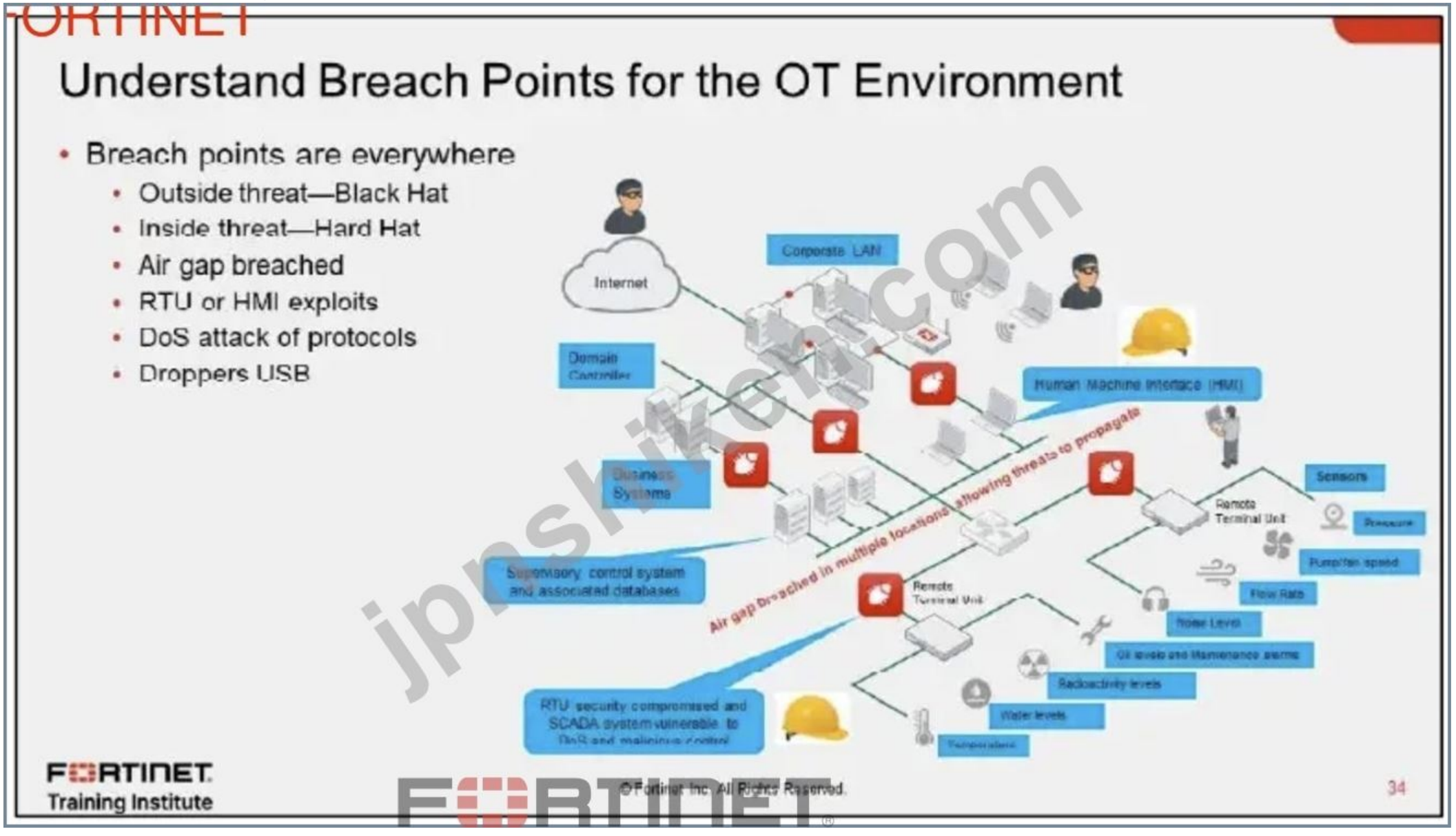
B. port1、port1-vlan10、およびport1-vlan1は異なるブロードキャストドメインに属しています

C. port1-vlan1 の VLAN ID を VLAN ID 10 に変更できます。

D. port2、port2-vlan10、およびport2-vlan1はソフトウェアスイッチインターフェースの一部です。

正解: **(**正解を表示します**)**

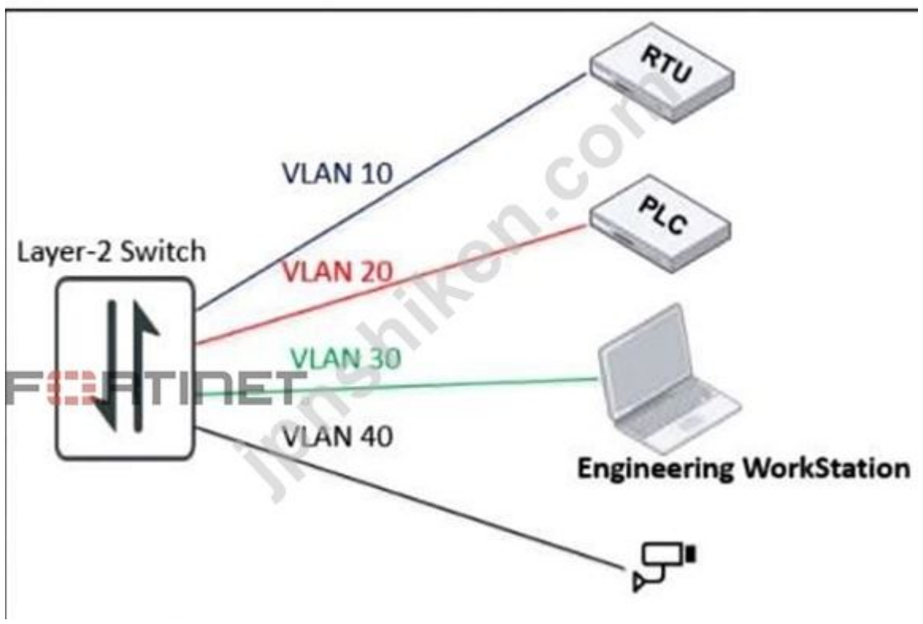
質問: **70**
一般的なOT環境で見られる、よくある侵害箇所を3つ挙げてください。3つ選択してください。）
A. グローバルハット
B. ヘルメット
C. VLANの脆弱性を悪用する
D. 黒い帽子
E. RTUの悪用
正解: **B,D,E** (コメントを発表する)



質問: **71**
OT管理者はOTネットワークのセキュリティを確保するために多数のデバイスを導入しました。しかし、SOCチームからはアラートが多すぎること、そしてその多くが誤検知であるとの報告を受けています。OT管理者は、反復作業をなくし、効率性を向上させ、時間とリソースを節約できるソリューションを求めています。
管理者は、これらの問題に対処し、SOCチームが行っている手作業の大部分を自動化するために、どの製品を導入すべきでしょうか？
A. FortiSIEMとFortiManager
B. FortiSandboxとFortiSIEM
C. FortiSOARとFortiSIEM
D. syslogサーバーとFortiSIEM
正解: (正解を表示します)
OT管理者は、FortiSOARとFortiSIEM（オプションC）を導入して、手動タスクを自動化し、誤検知を減らし、SOCの効率を向上させる必要があります。FortiSIEMはログを統合して分析し、包括的なセキュリティ可視性を実現する一方、FortiSOARはプレイブックを使用してアラートに対応するための自動化とオーケストレーションを提供し、ワークフローを効果的に合理化してSOCのリソースを解放します。

質問: **72**
FortiGateデバイスがOTネットワークセキュリティファブリックのエッジゲートウェイとして新たに導入されました。下流側のFortiGateデバイスも、制御エリアゾーンを保護するためのセキュリティファブリックリーフとして新たに導入されました。
追加の必須ネットワーク機器がない状態で、このOTネットワーク上でマイクロセグメンテーションを実装するには、OTネットワークアーキテクトはVLAN内トラフィックを制御するためにどのような構成を適用する必要がありますか？
A. エッジ側のFortiGateデバイスで透過モードを有効にします。
B. 制御領域ゾーンに接続されているすべてのインターフェースでセキュリティプロファイルを有効にします。
C. ダウンストリームとエッジのFortiGateデバイス間でVPNトンネルを設定します。
D. 各下流のFortiGateデバイスにソフトウェアスイッチを作成します。
正解: (正解を表示します)
ソフトウェアスイッチは、レイヤ2で複数のインターフェースをグループ化します。
しかし、マイクロセグメンテーションの場合、通常はサブネット/デバイスグループごとにインターフェースを分離し、FortiGate上でインターフェース間のポリシーを適用します。
これにより、FortiGateは追加のネットワークハードウェアなしで、VLAN内（またはサブネット内）のトラフィックを制御できます。

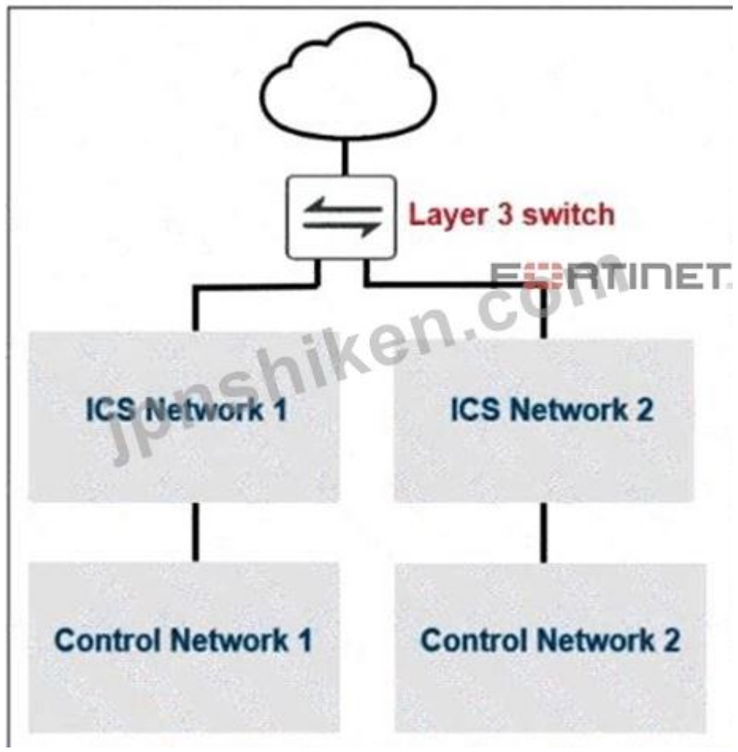
質問: **73**
展示資料を参照してください。



OTネットワークの一部を示す。
FortiGateデバイスにVLANを設定してOTネットワークをセグメント化しました。管理者はエンジニアリングワークステーションからPLCに接続しようとしています。
エンジニアリングワークステーションからPLCへのアクセスを許可するにはどうすればよいですか？
A. スイッチ内ポリシーを明示的に設定する必要があります。
B. スイッチ内ポリシーを暗黙的に設定する必要があります。
C. 転送ドメインIDを設定する必要があります。
D. レイヤー3スイッチを設定する必要があります。
正解: **A** (コメントを発表する)
FortiGateスイッチでVLANを設定し、VLAN間の通信を制御する場合は、スイッチ内ポリシーを明示的に設定して、VLAN間トラフィックがファイアウォールポリシーによって処理されるようにする必要があります。これにより、エンジニアリングワークステーションVLANが制御された方法でPLC VLANにアクセスできるようになります。

質問: **74**
展示資料を参照してください。

Logical topology



jpnshiken.com

部分的なOTネットワークが図示されています。このOTネットワークのセキュリティを向上させ、ネットワーク1とネットワーク2の間で内部セグメンテーションを実装する必要があります。セグメンテーションを実現するにはどうすればよいでしょうか？（回答を1つ選択してください）

A. ユニバーサルZTNAを設定できます。

B. 1 つのトラフィック VDOM を設定できます。

C. 明示的なソフトウェアスイッチを設定できます。

D. 各ネットワークごとに転送ドメインIDを設定できます。

正解: **D** (コメントを発表する)

正解はDです。各ネットワークごとに転送ドメインIDを設定できます。

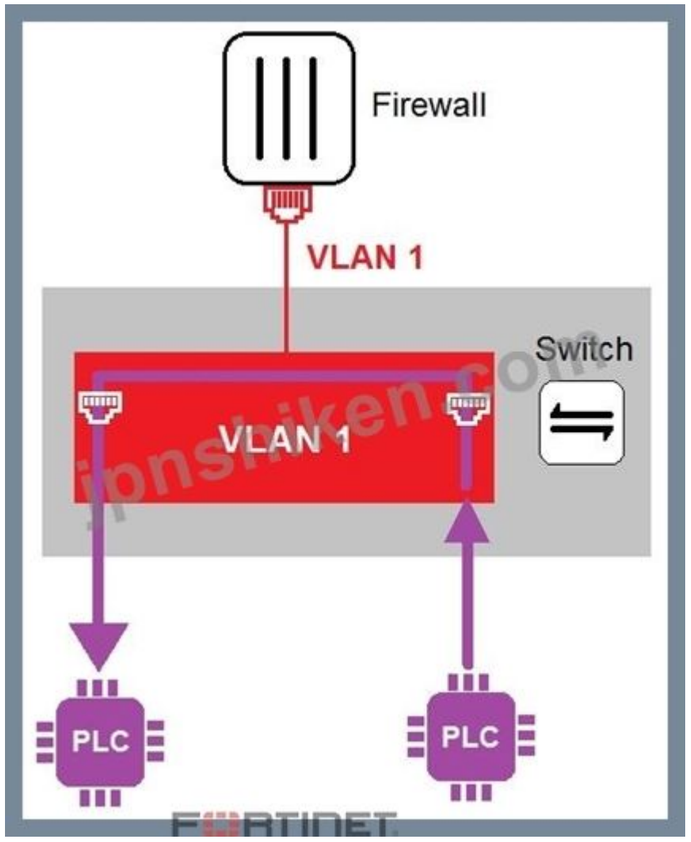
学習ガイドでは、FortiGate の透過モードでは、異なる VLAN ID を持つインターフェイスであっても、すべてのインターフェイスが同じブロードキャスト ドメインに属すると説明し、set forward-domain < domain_ID > を設定することで 複数のブロードキャスト ドメインに分割できる」と述べています。また、 同じドメイン ID を持つインターフェイスは同じブロードキャスト ドメインに属する」とも述べており、複数のフォワード ドメインでは、

あるインターフェースに到着したトラフィックは、同じフォワードドメインIDを持つインターフェースにのみブロードキャストされる。」これが、内部ネットワークを分離し、ネットワークセグメント間のトラフィックを制限するために使用されるメカニズムです。

他のオプションはこの要件を満たしていません。ユニバーサルZTNAはアプリケーションアクセス制御用であり、2つのOTネットワーク間のセグメンテーション用ではありません。1つのトラフィックVDOMだけではセグメンテーションは作成されません。そのような分離を実現するには、複数のVDOMが必要です。明示的なソフトウェアスイッチは、同じソフトウェアスイッチドメイン内のスイッチ内トラフィックを制御するものであり、ネットワーク1とネットワーク2のような別々のネットワーク間のセグメンテーションを制御するものではありません。したがって、質問で求められている内部セグメンテーションを正しく実装するには、各ネットワークに異なるフォワードドメインIDを割り当てる必要があります。

質問: **75**

図を参照してください。図に示されているトポロジーでは、両方のPLCはファイアウォールを経由せずに直接通信できます。
このような状況下で、セキュリティを向上させるために何ができるでしょうか？



A. PLC同士がIEEE802.1Qプロトコルを使用して通信するように設定してください。
B. PLC間のトラフィックを保護するために、スイッチにファイアウォールポリシーを作成します。
C. VLANの機能をレイヤ2からレイヤ3に拡張するソリューションを実装します。
D. マイクロセグメンテーションを実装する。
正解: **(**正解を表示します**)**
マイクロセグメンテーションは、PLC間のトラフィックをセキュリティデバイス（ファイアウォール/ISFW）を経由させることで、無制限のレイヤ2通信を許可する代わりに、ポリシーと検査を適用できるようにします。

質問: **76**
展示資料を参照してください。

Partial Incident Analysis page

jpnshiken.com

インシデント分析ページの一部が表示されています。
この事件はどのようにして発生したのか？

A. プレイブックにより自動的に
B. イベントハンドラによって自動的に
C. 管理者による手動
D. ステッチで自動的に

正解: (正解を表示します)

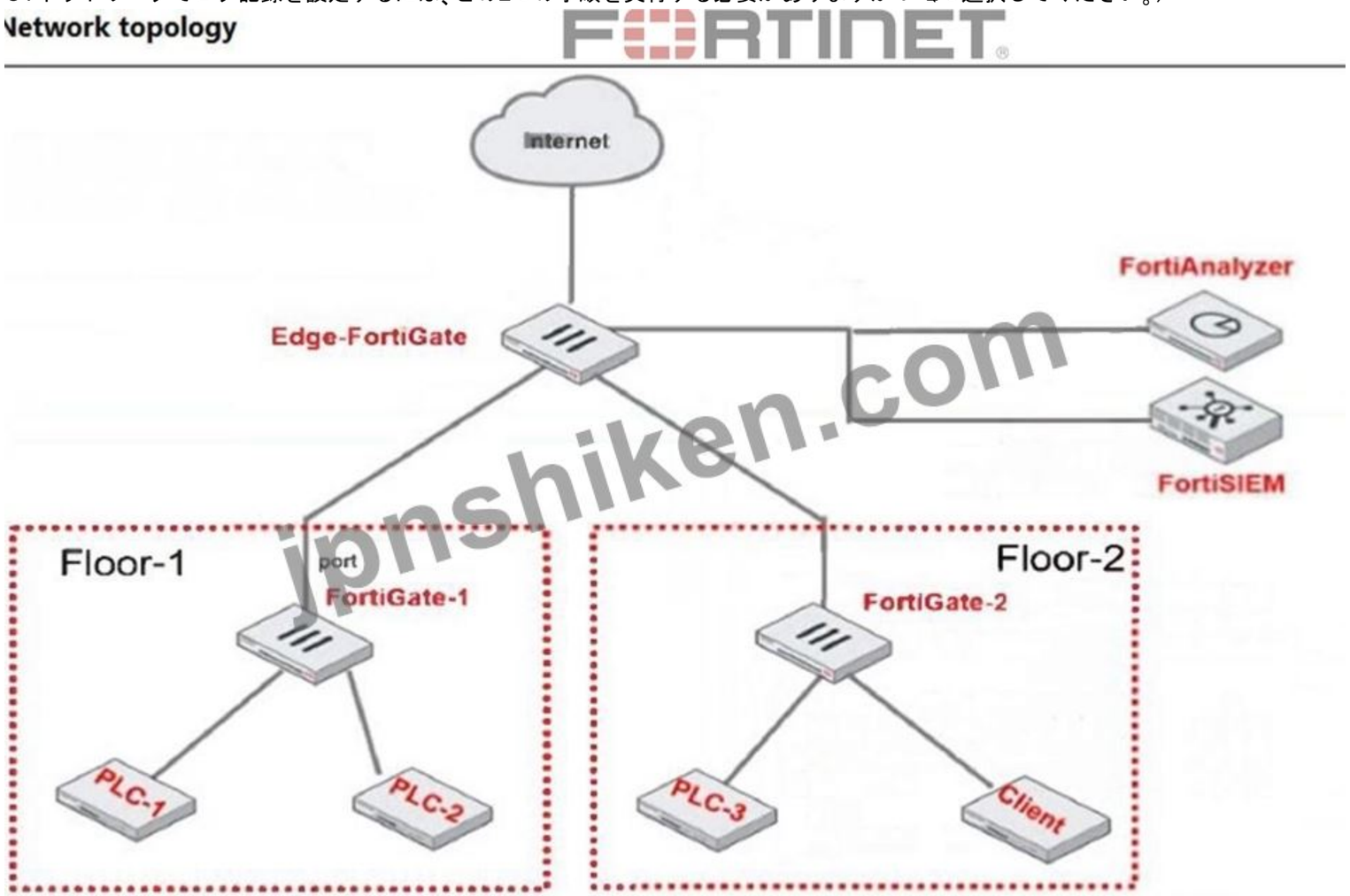
タイムラインには、インシデントに関連付けられたイベントと、それに続く自動アクションが表示されており、これは、イベントを関連付けてインシデントを自動的に作成するイベントハンドラによってインシデントが生成されたことを示しています。

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu **168**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**

図を参照してください。図中のネットワークトポロジーには、FortiGateデバイスに加え、OTネットワーク用のFortiAnalyzerおよびFortiSIEMが示されています。

OTネットワークでログ記録を設定するには、どの2つの手順を実行する必要がありますか？ 2つ選択してください。）



A. FortiSIEM を設定して、ログとアラートを FortiAnalyzer に送信するようにします。

B. FortiGate を設定して、ログを FortiAnalyzer と FortiSIEM に送信するようにします。

C. FortiAnalyzer を設定して、セキュリティ イベントを FortiSIEM に送信するようにします。

D. FortiGateとFortiAnalyzerを設定して、産業用シグネチャパターンをFortiSIEMに送信するようにします。

正解: **(**正解を表示します**)**

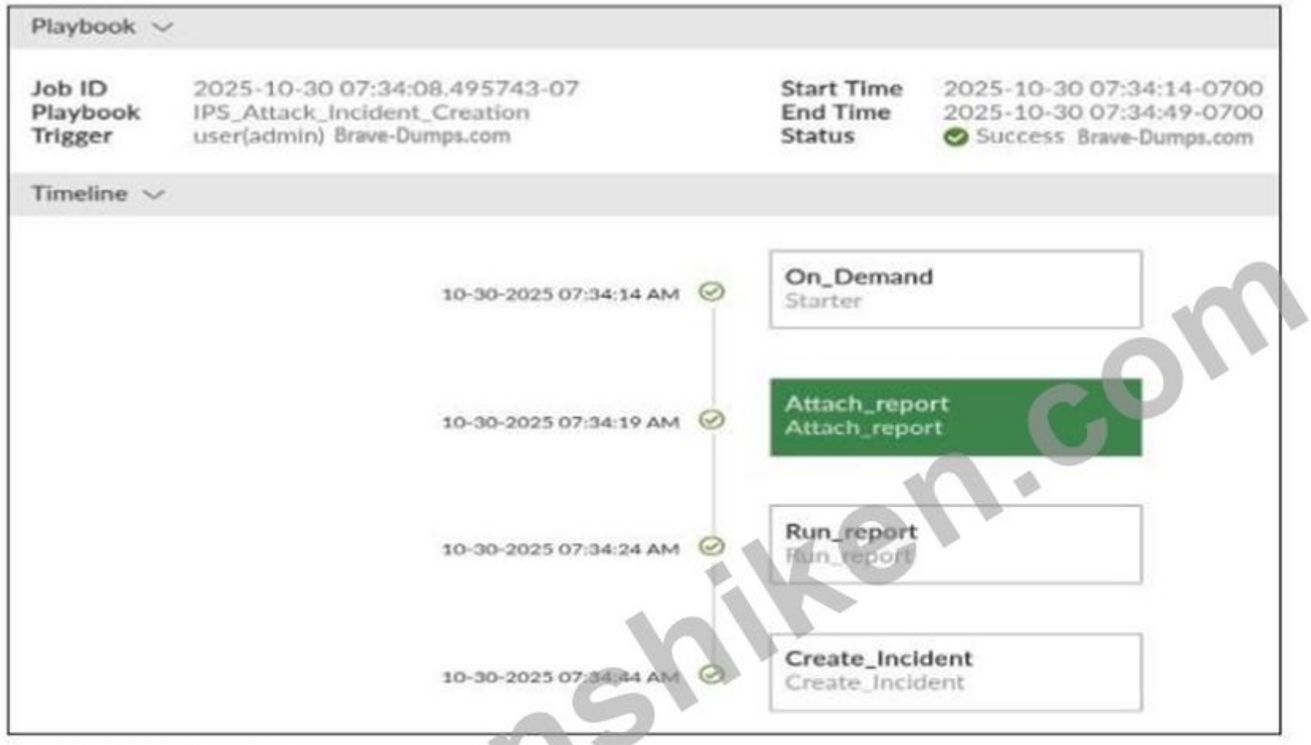
FortiGateは、ログを保存および相関分析するために、ログをFortiAnalyzerとFortiSIEMの両方に直接転送する必要があります。FortiAnalyzerは、関連するセキュリティイベントをFortiSIEMに転送し、OTデバイス全体にわたる集中分析を可能にします。

質問: **78**
ネットワークアクセス制御ポリシーを使用して、何を割り当てることができますか？
A. レイヤー3のポーリング間隔
B. FortiNACデバイスのポーリング方法
C. 論理ネットワーク
D. プロファイリングルール
正解: **(**正解を表示します**)**
FortiNACにおけるネットワークアクセス制御ポリシーは、ユーザー/ホストプロファイルとネットワークアクセス構成で構成されます。
ネットワークアクセス構成は、ユーザーやデバイスがネットワークに接続する際にどのように扱われるかを定義します。
これには、VLANなどの特定の論理ネットワークへの割り当てや、アクセス制御リスト（ACL）の適用などが含まれます。
論理ネットワークは、ポリシー条件に基づいてデバイスのアクセスをセグメント化および制御することを可能にする。

質問: **79**
OTネットワークアーキテクトは、複数の異なるネットワークにデバイスをプロビジョニングするために、単一のネットワークアクセスポリシーで制御領域ゾーンを保護する必要があります。これはどのデバイスで実現できますか？
A. FortiSwitch
B. FortiEDR
C. FortiGate
D. FortiNAC
正解: **C (**コメントを発表する**)**

質問: **80**
展示資料を参照してください。

Playbook Monitor



Incident Analysis

Playbook Monitorダッシュボードと、対応するインシデント分析の結果が表示されます。このプレイブックは、作成されたインシデントにレポートを自動的に添付することを目的として作成されました。正しい記述は次のうちどれですか？ 2つ選択してください）

A. レポートが作成され、事件に添付されるまでお待ちください。

B. Create_Incidentタスクのみが実行されました。

C. プレイブック内のタスクの順序を変更する必要があります。

D. プレイブックが手動で起動されました。

正解: **(**正解を表示します**)**

正解はCとDです。

選択肢Dが正解です。Playbook Monitorには、スターターがOn_Demand、トリガーがuser(admin)と明確に表示されているからです。学習ガイドには「ON_DEMAND：管理者が手動で起動するとプレイブックが実行されます」と記載されており、手動で実行するには、プレイブックを選択して「実行」をクリックするとも書かれています。これは展示内容と完全に一致するため、プレイブックは手動で起動されたことがわかります。
オプションCも正解です。学習ガイドでは、「タスクは順番に実行される」こと、そして「必要に応じて、あるタスクの出力を後続のタスクで使用できる」ことが説明されています。また、インシデントを作成してから詳細を添付するなど、ワークフローロジックが重要になる例も示されています。図では、Attach_report、Run_report、Create_Incidentの順でタスクが実行されていますが、インシデント分析ではレポートが添付されていません。レポートが正しく添付されるには、レポートが存在し、インシデントが既に利用可能になっている必要があるため、タスクの順序が間違っており、並べ替える必要があります。
オプションBは、モニターにCreate_Incidentだけでなく複数のタスクが正常に完了したことが示されているため、誤りです。オプションAも、展示資料で示されている主な問題は単なる待ち時間ではなく、ワークフローの順序が間違っているため、最適な回答ではありません。プレイブックは正常に完了しているにもかかわらず、レポートが添付されていないことから、単なる遅延ではなく、タスクシーケンスの設計上の問題があることがわかります。

質問: **81**
IEC 104プロトコルに関する以下の記述のうち、正しいものはどれですか？
A. IEC 104は、電気工学アプリケーションにおける遠隔制御SCADAに使用されます。
B. IEC 104 は、古い SCADA システムでは IEC 101 に準拠しています。
C. IEC 104はOTデバイスとサービス間のデータ伝送を保護します。
D. IEC 104はTCP/IP以外の規格を使用します。
正解: **A** (コメントを発表する)
IEC 104は、電気工学分野、特に遠隔制御における監視制御およびデータ収集（SCADA）の分野で広く使用されているプロトコルです。電力系統における制御ステーションと変電所間の通信を円滑化するように設計されています。

質問: **82**
展示資料を参照してください。

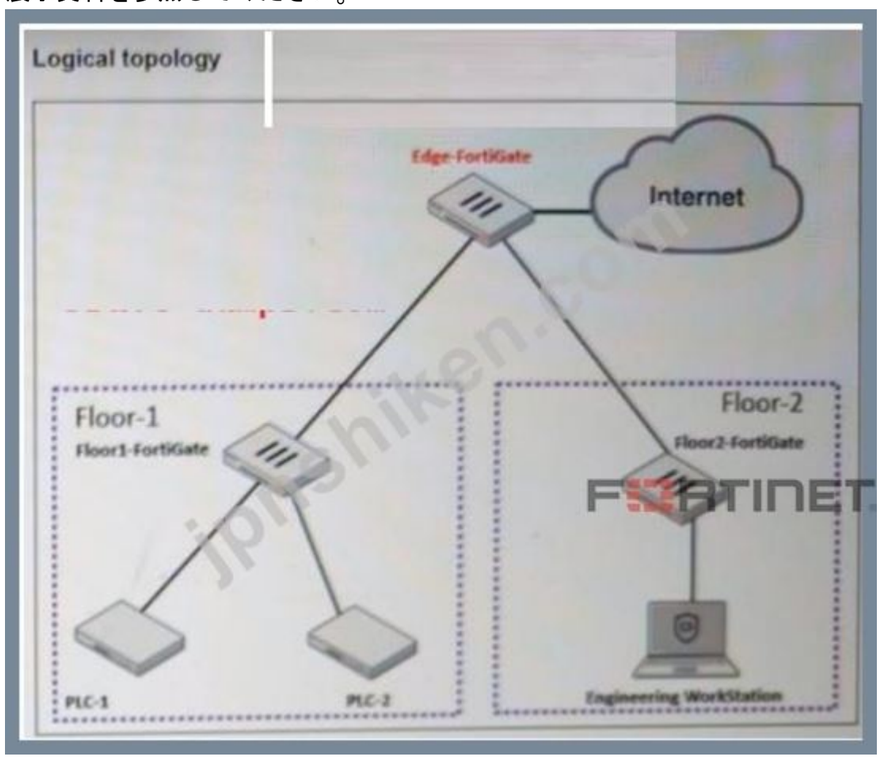
Jpnshiken.com

ファイアウォールポリシーページが表示されます。
OTネットワークのセキュリティを強化するため、図に示すようにファイアウォールポリシーにスーパーバイザープロファイルを設定しました。しかし、スーパーバイザーからPLC-1へのpingができないという報告を受けています。
理由は2つあります。それは何ですか？（2つ選択してください。）

A. 管理者は、HTTPSやTelnetなどのプロトコルを使用して最初に認証を行う必要があります。
B. リモートサーバーにスーパーバイザープロファイルが設定されていません。
C. ファイアウォールポリシーID 8が有効になっていません。
D. CLI パラメータ auth-on-demand が always に設定されています。
正解: (正解を表示します)
IDベースのポリシーを使用する場合、ICMPなどのトラフィックが許可される前に、ユーザーはHTTPSやTelnetなどのサポートされている方法で認証を行う必要があります。さらに、auth-on-demandが常に設定されている場合は、トラフィックが許可される前に認証が必要となるため、ユーザーが認証されるまでpingは実行されません。

質問: **83**
NozomiとFortiNACを統合するメリットを2つ挙げてください。2つ選択してください。）
A. 接続ポイントの詳細を強化
B. VLANの直接割り当て
C. マルチアダプタホスト向けアダプタ統合
D. 宿主の輸入と分類
正解: (正解を表示します)
Nozomiに登録されているデバイスは、自動的にインポート、登録、または分類できます。インポートされたデバイスは、Nozomi製品から取得した情報に基づいてプロファイリングされます。
複数のネットワークアダプタを搭載したデバイスは、FortiNAC内で単一のデバイスとして統合されます。

質問: **84**
展示資料を参照してください。

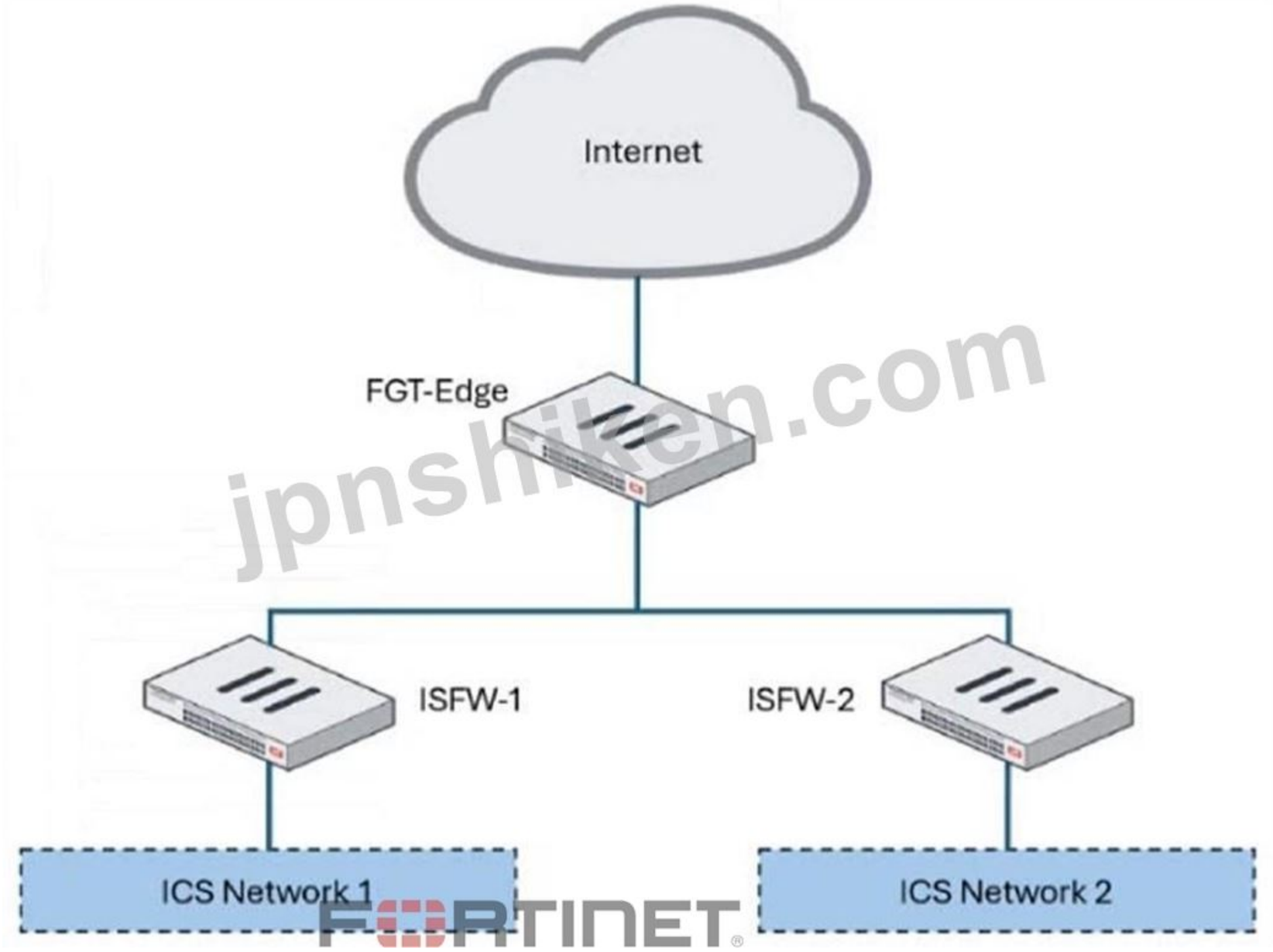


部分的なOTネットワークが図示されています。リンクで多くの切断が発生しており、このネットワークの可用性を改善したいと考えています。どのような対策を実行できますか？（回答は1つ選択してください）
A. HAクラスタを実装できます。
B. 1階のFortiGateと2階のFortiGateでSD-WANを実装できます。
C. 並列冗長プロトコルを実装できます。
D. Edge-FortiGateでVDOMを実装できます。
正解: **(**正解を表示します**)**
正解はCです。並列冗長プロトコルを実装できます。学習ガイドでは、メディア冗長性とは、ネットワークの一部が故障した場合に使用できるバックアップパスを作成することであると説明されており、特に「並列冗長プロトコル（PRP）はスター型トポロジーに使用できる」と明記されています。説明されている問題はリンクの切断が多いことなので、問題はリンクの可用性であり、これはファイアウォールの仮想化やポリシー分離の問題ではなく、メディア冗長性の問題です。PRPは、リンクが故障した場合に復旧時間の短いバックアップ通信パスを提供するように設計されています。
他のオプションもこのシナリオには適していません。HAクラスタは、ネットワークノードの冗長性を実現するソリューションとしてガイドに記載されており、プライマリデバイスが故障した場合にバックアップファイアウォールまたはスイッチが引き継ぎます。SD-WANは、このトポロジーに示されているローカルフロアリンクではなく、複数のWANリンクを介したリモートサイトアクセスに推奨されています。VDOMは論理的なセグメンテーションを提供しますが、リンクの冗長性やリンク可用性の向上には役立ちません。質問は特にリンクの切断が繰り返されることに関するものであるため、最善の対策はPRPを実装することです。

質問: **85**
あるOT（運用技術）顧客は、ネットワーク内で複数のFortiGateデバイスを使用し、ハードウェアFortiTokenによる二要素認証を実装しています。管理者は、異なるFortiGateデバイスの背後にある重要なサーバーにログインする際に使用する複数のFortiTokenを携帯しています。
OTネットワークアーキテクトとして、ユーザーごとに1つのトークンを割り当てつつ、複数のFortiGateデバイスで二要素認証を使用するには、どのようなアプローチを取るべきでしょうか？
A. Edge-FortiGate デバイスにすべての FortiToken をプロビジョニングし、他の FortiGate デバイス上でリモート認証サーバーとして構成します。
B. FortiManagerを実装し、OTネットワーク内のすべてのFortiGateデバイスを管理してFortiTokensデータベースを共有します。
C. 各ユーザー用にプロビジョニングされた FortiToken を使用して FortiAuthenticator を実装し、OT ネットワーク内のすべての FortiGate デバイスで FortiAuthenticator をリモート認証サーバーとして構成します。
D. FSSOベースの二要素認証を設定します。
正解: **(**正解を表示します**)**

質問: **86**
図を参照してください。FGT-Edgeデバイスは、リモート管理者がローカルICSネットワークにアクセスできるようにするVPNゲートウェイです。経営陣は、現場での安全衛生管理を第三者企業に委託します。この第三者企業は、外部リソースへのアウトバウンドアクセス権限を持っている必要があります。
ICSネットワークのセキュリティを維持しながら、サードパーティ企業に外部アクセスを提供するための最適なシナリオは何でしょうか？

Network topology



ipnshiken.com

A. サードパーティ企業の認証ユーザーを制限したアウトバウンドセキュリティポリシーを設定します。
B. 下流のFortiGateデバイスとエッジのFortiGateの間にVPNトンネルを作成し、ICSネットワークトラフィックを保護します。
C. エッジ FortiGate デバイスを複数の論理デバイスに分割し、サードパーティ企業に独立した VDOM を割り当てます。
D. インターネットへの追加のアップストリームリンクを使用して、追加のファイアウォールを実装します。
正解: **(**正解を表示します**)**

エッジ側のFortiGateをVDOMに分割することで、サードパーティ企業を独自の仮想ファイアウォール内に隔離できます。このVDOMは、他のVDOMによって保護されているICSネットワークを危険にさらしたり、外部に公開したりすることなく、インターネットへのアウトバウンドポリシーを設定できます。

質問: **87**
図を参照してください。FortiGate-2デバイスの 「アネットワークセキュリティコネクタ」ページが表示されています。

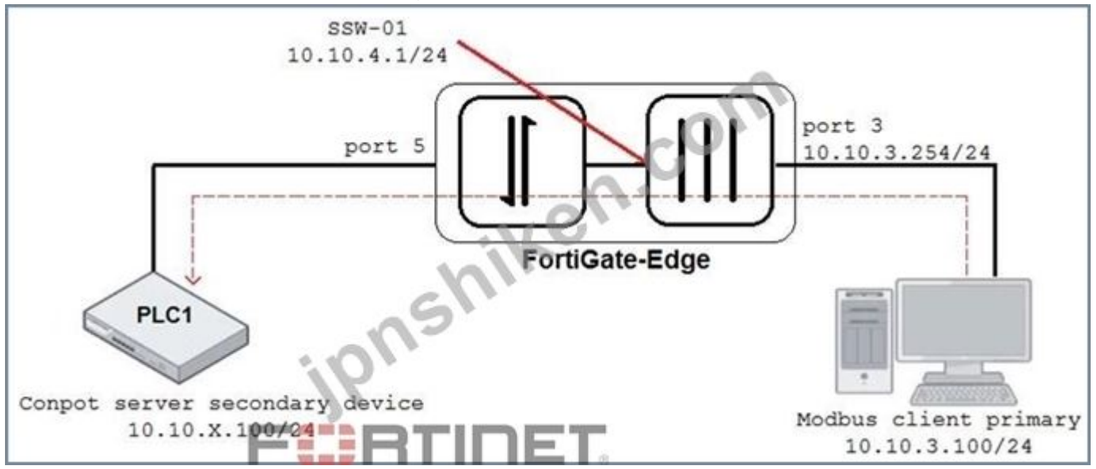
正しい記述はどれですか？ (いずれか1つを選択してください)
A. FortiGate-2でFortiAnalyzerの設定を構成する必要があります。
B. FortiGate-2 はルート FortiGate で認証されていません。
C. FortiGate-2はファブリックルートとして機能します。
D. FortiGate-2インターフェースでセキュリティファブリック接続を有効にする必要があります。
正解: **(**正解を表示します**)**

質問: **88**
OTネットワーク保護計画の最初のステップとして、FortiGateデバイスがサポートするOTプロトコルを特定する必要があります。このFortiGateデバイスで実装する必要がある設定はどれですか？ (2つ選択してください)
A. すべてのインターフェースでデバイス検出を有効にする必要があります。
B. OT を監視するアプリケーション制御セキュリティ プロファイルを実装する必要があります。
C. OT署名を有効にする必要があります。
D. OTを監視する侵入防止セキュリティプロファイルを実装する必要があります。
正解: **B,C (**コメントを発表する**)**

jpnshiken.com

正解はBとCです。学習ガイドには、「アプリケーション制御シグネチャを使用してOTプロトコルを検出できます」および「アプリケーション制御は、Modbus、IEC 104などのアプリケーションで使用されるプロトコルや、テレコントロールメッセージの内容を検出します」と記載されています。また、ファイアウォールポリシーでModbusアプリケーション制御プロファイルを有効にすることで、「モニターステータスでOTプロトコルを表示できる」ことも示されています。これは、アプリケーション制御がFortiGateでOTプロトコルを識別および監視するために使用される機能であるため、Bを直接的に裏付けています。
ガイドでは、IPS の項目で「デフォルトでは、OT シグネチャは CLI で config ips global と set exclude-signatures none を使用して有効にするまで、GUI のシグネチャ リストから除外されます」と説明しています。有効にすると、FortiGate はこれらの OT シグネチャを使用して OT 対応の検査と保護を実行できます。これにより、2 番目の必須設定である C がサポートされます。A はプロトコル識別ではなくデバイス検出に関連しており、D は OT プロトコルを識別するという最初のステップの目標ではなく、エクスプロイトと脆弱性の検出に重点を置いています。

質問: **89**
図を参照してください。OTアーキテクトは、シミュレーションサーバーConpotを使用してModbus TCPを実装し、OTネットワーク内のModbusトラフィックを識別および制御しています。FortiGate-Edgeデバイスは、ソフトウェアスイッチインターフェイスssw-01で構成されています。
図に示されたトポロジーに基づいて、クライアントとサーバー間のトラフィックのシミュレーションが成功したことに関する記述のうち、正しいものはどれですか？ 2つ選択してください。）



A. FortiGateファイアウォールポリシーでポート3からssw-01へのNATが無効になっています。
B. ポート5はソフトウェアスイッチのメンバーではありません。
C. FortiGate デバイスはオフライン IDS モードです。
D. FortiGate-Edge デバイスは NAT モードである必要があります。
正解: **A,D (**コメントを発表する**)**

質問: **90**
展示資料を参照してください。

Run_reportタスクが表示されています。FortiAnalyzerで新しく作成されたレポートの生成を自動化したいと考えています。PlaybookでRun_reportタスクを設定しても、レポートが[レポート]フィールドに表示されないのはなぜですか？ 2つ選択してください）

A. まずコネクタを設定する必要があります。

B. まず、レポートで拡張ログフィルタリングを有効にする必要があります。

C. まずレポートで自動キャッシュを有効にする必要があります。

D. まずイベントハンドラを設定する必要があります。

E. まず「Playbook Starter」を選択し、次に新しく作成したレポートを選択する必要があります。

正解: **(**正解を表示します**)**

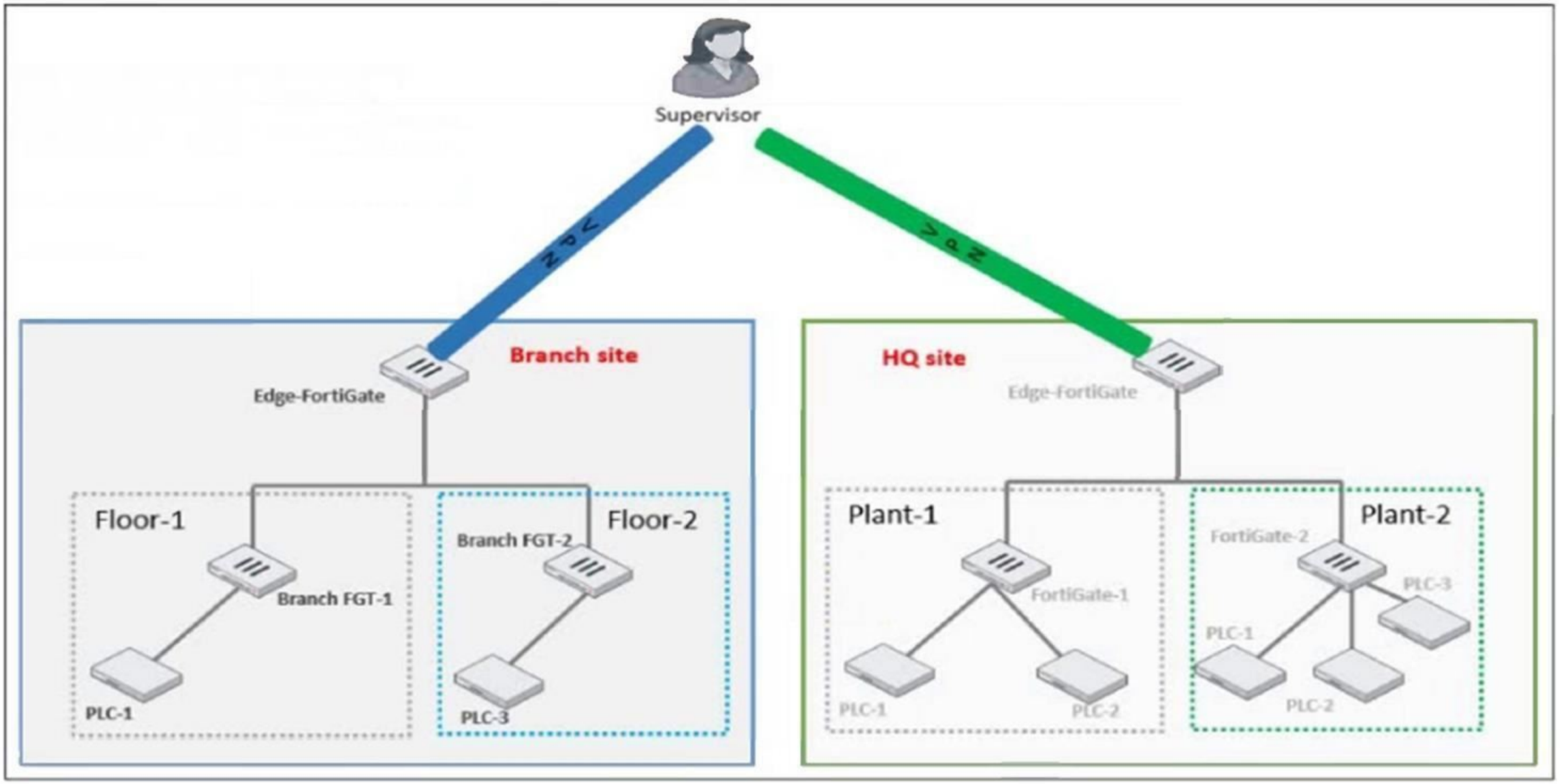
セキュリティファブリック内のFortiAnalyzerのアーキテクチャと自動化機能に基づき、以下の点が挙げられます。

* 自動化ステッチとレポート：Security Fabric環境において、FortiAnalyzerは自動化ステッチとプレイブックを作成する上で重要な要素となります。プレイブックタスク（図に示すRun_reportタスクなど）内でレポートを選択できるようにするには、レポート構成における特定の技術的前提条件を満たす必要があります。
* 自動キャッシュ要件（回答C）：レポートを自動生成に使用するには、手動による介入なしにエンジンで処理できる「準備完了」の状態である必要があります。プレイブックによってトリガーされたときにレポートが動的かつ効率的に生成されるようにするには、レポート設定で自動キャッシュを有効にする必要があります。
* 拡張ログフィルタリング（回答B）：プレイブックは、トリガーから特定の変数（特定のデバイスIPや時間範囲など）をレポートに渡すことがよくあります。レポートがこれらの動的なパラメータを受け入れ、プレイブックインターフェイスで「自動化互換」レポートとして表示されるようにするには、拡張ログフィルタリングを有効にする必要があります。
* ワークフローの制約: レポート自体でこれらの 2 つの設定が有効になっていない場合、Playbook エンジンはレポートの正常な生成またはパラメータの挿入を保証できないため、Run_report タスクで使用可能な選択リストから除外されます。

質問: **91**

図を参照してください。支店と本社サイトの管理者向けに、同じソフトFortiTokenを使用してVPNユーザーアクセスを設定する必要があります。各サイトにはFortiGate VPNゲートウェイが設置されています。この目標を達成するためには、何をすべきでしょうか？

Network topology



A. ユーザーを自己登録サーバーポータルに誘導します。
B. 各FortiGateにFortiTokenをインポートします。
C. FortiAuthenticatorをデプロイします。
D. RADIUS OTPサーバーを使用します。
正解: (正解を表示します)
単一のソフトFortiTokenを複数のFortiGate VPNゲートウェイで検証できるのは、トークン認証が集中管理されている場合のみです。FortiAuthenticatorは集中管理型のOTP/RADIUSサービスを提供するため、両方のFortiGateはスーパーバイザーに対して同じトークンレコードを照会します。

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu **168**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

有効的な**NSE6_OTS_AR-7.6**問題集はJPNTest.com提供され、**NSE6_OTS_AR-7.6**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE6_OTS_AR-7.6**試験問題集を提供します。JPNTest.com NSE6_OTS_AR-7.6試験問題集はもう更新されました。ここで**NSE6_OTS_AR-7.6**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE6_OTS_AR-7.6-mondaishu **168**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」