PaloAltoNetworks.PSE-Strata-Pro-24.v2026-03-26.q39

試験コード:	PSE-Strata-Pro-24
試験名称:	Palo Alto Networks Systems Engineer Professional - Hardware Firewall
認定資格:	Palo Alto Networks
無料問題数:	39
バージョン:	v2026-03-26
アクセス数:	122
ページビュー数:	390
https://www.jpnpdf.com/PaloAltoNetworks.PSE-Strata-Pro-24.v2026-03-26.q39-mondaishu.html	

最新問題: **1**
20,000を超えるグループを擁する大規模なActive Directory（AD）を運用する企業では、ディレクトリ内のグループメンバーシップに基づいてユーザーロールを設定しています。セキュリティポリシーでは最大1,000個のグループを使用できます。この企業は運用担当者が限られているため、ファイアウォールとグループの同期管理にかかる管理オーバーヘッドを削減したいと考えています。
会社の AD を Palo Alto Networks ファイアウォールと同期するための推奨アーキテクチャは何ですか?
A. ユーザー ロールにマップされる LDAP 属性のカスタム フィルターを使用して、グループ マッピング プロファイルを構成します。
B. フィルターなしでグループ マッピング プロファイルを構成し、すべてのグループを同期します。
C. 包含グループ リストを使用してグループ マッピング プロファイルを構成します。
D. Cloud Identity Engine (CIE) とエージェントを展開した後、AD と同期するように NGFW を構成します。
Answer: (解答を表示する**)**
20,000を超えるグループを持つ大規模なActive Directory（AD）を同期する場合、すべてのグループを同期すると、特にセキュリティポリシーに必要なグループの一部（例1:,000グループ）のみの場合、大きなオーバーヘッドが発生する可能性があります。最も効率的な方法は、不要な同期を最小限に抑え、管理オーバーヘッドを削減するために、グループマッピングプロファイルにグループリストを含めるように設定することです。
* 「グループマッピングプロファイルにグループリストを含める」必要があるのはなぜですか（正解）。グループマッピングプロファイルにグループリストを含めると、必要な1,000

グループのみがファイアウォールと同期されます。このアプローチには以下の利点があります。
* 同期されるグループの数を制限することで、ファイアウォールのユーザー ID プロセスの負荷を軽減します。
* セキュリティ ポリシーに関連する特定のグループに焦点を当てることで管理を簡素化します。
* 非効率的でリソースを大量に消費するディレクトリ全体 (20,000 グループ) の同期を回避します。
* 「フィルターなしのグループマッピングプロファイルを設定し、すべてのグループを同期する」(オプションB)という方法はなぜ採用しないのでしょうか？20,000グループすべてを同期すると、管理とリソースのオーバーヘッドが不必要に増加します。このアプローチは、管理負担の軽減という要件に反します。
* 「ユーザーロールにマッピングされているLDAP属性用のカスタムフィルターを含むグループマッピングプロファイルを設定する」(オプションA)はなぜダメなのでしょうか？LDAP属性のフィルタリングは確かに便利ですが、このアプローチはグループリストを含める方法に比べて実装と管理が複雑です。同期を特定のグループのサブセットに限定するという問題に直接対処するものではありません。
* 「Cloud Identity Engine (CIE) とエージェントを導入した後、NGFW を AD と同期するように構成する」(オプション D)はなぜ推奨されないのでしょうか？Cloud Identity Engine (CIE) はユーザーとグループのマッピングのための最新のソリューションですが、このシナリオでは必要ありません。対象リストを含む従来のグループマッピングプロファイルで十分であり、実装も簡単です。CIE は通常、複雑なハイブリッド環境やクラウド環境で使用されます。
参考: Palo Alto Networks グループ マッピングのドキュメントでは、ポリシーの適用に AD グループのサブセットのみが必要なシナリオでは、含めるグループ リストを使用することを推奨しています。

最新問題**: 2**
Palo Alto Networks NGFWで物理データセンターサーバーを保護している企業では、NGFWがサーバーに大量のリクエストと更新を送信しているため、Active Directory (AD)サーバーのパフォーマンスに問題が発生しています。ADサーバーに過負荷をかけずに、NGFWでユーザーを効率的に識別するにはどうすればよいでしょうか？
A. AD 認証ログからユーザーの IP アドレスとユーザーのマッピングを学習するように Cloud Identity Engine を構成します。
B. NGFW を GlobalProtect ゲートウェイとして構成し、すべてのユーザーに GlobalProtect Windows SSO を実行させてユーザー情報を収集させます。
C. データ再配布を設定して、ハブ NGFW から他のスポーク NGFW に IP アドレスとユーザーのマッピングを再配布します。

D. NGFW を GlobalProtect ゲートウェイとして構成し、すべてのユーザーに GlobalProtect エージェントを実行させてユーザー情報を収集させます。

Answer: A (メーッセージを残す)

Palo Alto Networks NGFWからActive Directoryサーバーへのトラフィック量の増加によってパフォーマンスの問題が発生する場合、NGFWがユーザーとIPアドレスのマッピング情報を収集する方法を最適化することが重要です。Palo Alto Networksは、ユーザーID情報を収集する複数の方法を提供しており、Cloud Identity Engineは、効率的かつ正確なマッピングを維持しながら、ADサーバーの負荷を軽減するソリューションを提供します。

* オプションA（正解）Cloud Identity Engine を使用すると、NGFW は Active Directory の認証ログやその他の ID ソースから、ユーザーと IP アドレスのマッピング情報を直接収集できるため、AD サーバーに過大なトラフィックを発生させることはありません。この機能を活用することで、NGFW は認証関連タスクをオフロードし、AD サーバーに過負荷をかけることなく効率的にユーザーを識別できます。このソリューションはスケーラブルで、AD サーバーへの頻繁なユーザー ID クエリによって発生するオーバーヘッドを最小限に抑えます。

* オプションB :GlobalProtect Windows SSOを使用してユーザー情報を収集すると、複雑さが増す可能性があり、この問題に対する最も効率的な解決策とは言えません。すべてのユーザーにGlobalProtectエージェントをインストールする必要があり、すべての環境で実行可能とは限らず、運用上の課題が生じる可能性があります。

* オプションC :データ再配分では、ユーザーとIPアドレスのマッピングを1つのNGFW（ハブ）から他のNGFW（スポーク）に再配分します。これによりADサーバーに送信されるクエリ数は削減されますが、ハブが既にADサーバーからマッピングを収集していることが前提となるため、ADサーバーのパフォーマンス問題は依然として残ります。

* オプションD :GlobalProtectエージェントを使用してユーザー情報を収集する方法は、GlobalProtectが既に導入されている環境では有効な手段ですが、今回の問題に対する最も効率的かつ直接的な解決策ではありません。また、エージェントの導入、構成、管理に依存関係が生じます。

ユーザー ID マッピング用の Cloud Identity Engine を実装する方法:

* Palo Alto Networks コンソールから Cloud Identity Engine を有効にします。
* Cloud Identity Engine を AD サーバーと統合して、認証ログを直接取得できるようにします。
* AD サーバーに直接クエリを実行するのではなく、ユーザー ID マッピングに Cloud Identity Engine を使用するように NGFW を構成します。
* パフォーマンスを監視して、AD サーバーが過負荷になっていないこと、およびマッピングが効率的に取得されていることを確認します。

参考文献:

Cloud Identity Engine の概要: https://docs.paloaltonetworks.com/cloud-identity ユーザー ID のベスト プラクティス: https://docs.paloaltonetworks.com

最新問題: 3
Advanced DNS Security が検出して防止できる DNS 攻撃の例はどれですか?
A. 高エントロピーDNSドメイン
B. ポリモーフィックDNS
C. CNAMEクローキング
D. DNSドメインのリブランディング
Answer: (解答を表示する)
Palo Alto NetworksファイアウォールのAdvanced DNS Securityは、幅広いDNSベースの攻撃を識別・防御するように設計されています。リストされているオプションの中で、「高エントロピーDNSドメイン」は、Advanced DNS Securityが検出・ブロックできるDNS攻撃の具体的な例です。
* なぜ「高エントロピーDNSドメイン」なのか（正解A）？高エントロピーDNSドメインは、マルウェアやボットが検出を回避するためにランダムに生成されたドメイン名（例：gfh34ksdu.com）を利用する攻撃でよく使用されます。これは、ドメイン生成アルゴリズム（DGA）ベースの攻撃の特徴です。
高度なDNSセキュリティ機能を備えたPalo Alto Networksファイアウォールは、機械学習を用いてDNSクエリのエントロピー（ランダム性）を分析することで、このようなドメインを検出します。エントロピー値が高い場合、動的に生成されたドメイン、または悪意のあるドメインである可能性が高いことを示します。
*「ポリモーフィックDNS」（オプションB）ではないのはなぜですか？ポリモーフィックDNSは、検出を回避するためにDNSレコードを動的に変更する手法を指しますが、Palo Alto Networksのドキュメントでは、Advanced DNS Securityによって軽減される攻撃の種類として明確には示されていません。ファイアウォールは、DGAドメインや異常なDNSトラフィックパターンの検出など、DNSクエリの挙動に重点を置いています。
*「CNAMEクローキング」（オプションC）はなぜダメなのでしょうか？CNAMEクローキングとは、CNAMEレコードを利用してDNSクエリを悪意のあるドメインや隠蔽されたドメインにリダイレクトすることです。Palo Altoのファイアウォールは悪意のあるDNSリダイレクトを検出してブロックできますが、Advanced DNS Securityは主にDGAドメイン、トンネリング、高エントロピークエリといったDNS不正利用のパターンを特定することに重点を置いています。
*「DNSドメインのリブランディング」（オプションD）はなぜダメなのか？DNSドメインのリブランディングとは、悪意のある活動に関連付けられたドメイン名を変更し、検出を回避することです。これは通常、持続的な活動を行うために用いられる戦術ですが、Advanced DNS Securityが特に対処しているDNS攻撃の種類ではありません。
高度なDNSセキュリティは、高エントロピードメイン、DNSトンネリング、プロトコル違反といった疑わしいDNSパターンを動的かつリアルタイムで特定することに重点を置いています。高エントロピーDNSドメインはDGAなどの攻撃メカニズムと直接結びついているため、これが正解です。

最新問題: 4
システムエンジニア（SE）が、顧客ベースへのエッジ接続にPAN-OSを採用するマネージドセキュリティサービスプロバイダー（MSSP）のチームに加わりました。MSSPは、すべての顧客とのルーティングを効率的に処理する方法、特にBGPピアリングの処理方法について懸念を抱いています。なぜなら、MSSPは各顧客に適用し、維持・更新する標準的なルールと設定を作成しているからです。このソリューションでは、顧客ごとに論理的に分離されたBGPピアリング設定が必要です。Palo Alto Networksが案件を獲得する可能性を高めるために、SEは何をすべきでしょうか？
A. MSSP と協力して、PAN-OS アドバンスド ルーティング エンジンで論理ルーターを有効にし、論理ルーター間でルーティング プロファイルを共有できるように計画します。
B. MSSP と協力して、ルーティング フィルター、マップ、および関連アクションの標準セットを含む API 呼び出しを作成します。その後、MSSP は新しい顧客を獲得するたびに API を呼び出すことができます。
C. 既存の仮想ルータでは論理的に分離された BGP ピアリング設定が可能だが、すべてのルータにわたって標準基準を処理する方法はないことを MSSP に確認します。
D. 顧客データが混在しないように環境を分離するためのよりよい方法として、MSSP と協力して vsys の使用を確立します。
Answer: A (メーッセージを残す)
MSSPの要件である論理的に分離されたBGPピアリング設定に対応しながら、標準的なルーティングルールとアップデートを効率的に管理するために、Palo Alto NetworksはPAN-OS 11.0で導入されたAdvanced Routing Engineを提供しています。Advanced Routing Engineは、このシナリオで極めて重要な論理ルーターのサポートを含むルーティング機能を強化します。
Aが正しい理由
* 論理ルーターにより、MSSP は顧客ごとに分離された BGP ピアリング構成を作成できます。
* 高度なルーティング エンジンにより、MSSP は標準ルーティング プロファイル (フィルタ、ポリシー、マップなど) を論理ルータ間で共有できるようになり、ルーティング構成の展開と保守が簡素化されます。
* このアプローチでは、各論理ルータが共有ルーティング ルールを活用しながら顧客の固有のニーズに対応できるため、スケーラビリティが確保されます。
他の選択肢が間違っている理由
* B: APIを使用してデプロイメントを自動化することは有益ですが、論理的に分離されたBGPピアリング設定の必要性は解消されません。論理ルーターはネイティブにこの分離機能を提供します。
* C:PAN-OS の仮想ルータは BGP ピアリング設定を分離できますが、複数のルータ間での標準ルーティング ルールとプロファイルの効率的な共有はサポートされていません。

* D: 仮想システム（vsys）は、ルーティング設定ではなく、管理ドメインを分離するために使用されます。vsysは、複数の顧客にわたるBGPピアリング設定の管理には適切なソリューションではありません。
重要なポイント:
* 論理ルーターを備えた PAN-OS アドバンスド ルーティング エンジンにより、MSSP の BGP ピアリング管理が簡素化されます。
* 論理ルーターは、共有構成プロファイルを有効にしながら、顧客環境に必要な分離を提供します。
参考文献:
* Palo Alto Networks PAN-OS 11.0 高度なルーティングドキュメント

最新問題: **5**
復号化を有効にしたファイアウォール展開のサイズ設定に関するベスト プラクティスを正しく説明している 2 つの文はどれですか (2 つ選択してください)。
A. SSL 復号化トラフィックの量はネットワークによって異なります。
B. 平均トランザクション サイズが大きいと、復号化に多くの処理能力が消費されます。
C. Diffie-Hellman Ephemeral (DHE) や Elliptic-Curve Diffie-Hellman Exchange (ECDHE) などの Perfect Forward Secrecy (PFS) 一時キー交換アルゴリズムは、Rivest-Shamir-Adleman (RSA) アルゴリズムよりも多くの処理リソースを消費します。
D. Rivest-Shamir-Adleman (RSA) 証明書認証方法 (RSA キー交換アルゴリズムではありません) は、楕円曲線デジタル署名アルゴリズム (ECDSA) よりも多くのリソースを消費しますが、ECDSA の方が安全です。
Answer: A,C (メーッセージを残す**)**
SSL/TLS復号化を有効にしたファイアウォールの導入を計画する際には、暗号化されたトラフィックの復号化と検査によって発生する追加の処理オーバーヘッドを考慮することが重要です。各ステートメントの詳細は次のとおりです。
* 「SSL復号トラフィックの量はネットワークごとに異なる」のはなぜですか（正解A）？SSL復号トラフィックの量は、組織固有のネットワーク環境、ユーザーの行動、アプリケーションによって異なります。例えば、Webトラフィック、クラウドアプリケーション、暗号化されたVoIPトラフィックが多いネットワークでは、SSL/TLS復号処理の要件がより高くなります。この変動性のため、各導入環境を適切に評価し、それに応じて規模を調整する必要があります。
* 「Diffie-Hellman Ephemeral (DHE) や Elliptic-Curve Diffie-Hellman Exchange (ECDHE) などの Perfect Forward Secrecy (PFS) 一時鍵交換アルゴリズムは、Rivest-Shamir-Adleman (RSA) アルゴリズムよりも多くの処理リソースを消費する」のはなぜですか (正解 C)？
DHE や ECDHE などの PFS アルゴリズムは、接続ごとに固有のセッション鍵を生成するため、セキュリティは向上しますが、RSA 鍵交換に比べて大幅に多くの処理能力を必要とします。復号化が有効になっている場合、ファイアウォールは暗号化されたセッションご

とにこれらの計算コストの高い操作を処理する必要があり、パフォーマンスとサイジング要件に影響を与えます。
* 「平均トランザクションサイズが大きいほど、復号化に必要な処理能力が増加する」(オプションB)ではなぜダメなのでしょうか？トランザクションサイズが大きいと追加のリソースを消費する可能性がありますが、SSL/TLSの復号化はトランザクションサイズよりも、セッション数と使用される暗号化アルゴリズムの複雑さに大きく依存します。したがって、これはベストプラクティスの主要な考慮事項ではありません。
* 「Rivest-Shamir-Adleman (RSA) 証明書認証方式は楕円曲線デジタル署名アルゴリズム(ECDSA)よりも多くのリソースを消費しますが、ECDSAの方が安全です」(オプションD)としないのはなぜですか？この記述は証明書認証方式について述べているものであり、SSL/TLSの復号化パフォーマンスについて述べているものではありません。ECDSAはRSAよりも効率的で安全ですが、復号化を有効にしたファイアウォール導入におけるサイジングの検討とは直接関係がありません。
参考: Palo Alto Networks SSL 復号化のベスト プラクティスでは、SSL トラフィックの変動や ECDHE などの暗号化アルゴリズムの影響など、復号化を使用した展開のサイズ設定に関する考慮事項について概説しています。

最新問題: **6**
システムエンジニア (SE)が、顧客ベースへのエッジ接続にPAN-OSを採用するマネージドセキュリティサービスプロバイダー (MSSP)のチームに加わりました。MSSPは、すべての顧客とのルーティングを効率的に処理する方法、特にBGPピアリングの処理方法について懸念を抱いています。なぜなら、MSSPは各顧客に適用し、維持・更新する標準的なルールと設定を作成しているからです。このソリューションでは、顧客ごとに論理的に分離されたBGPピアリング設定が必要です。Palo Alto Networksが案件を獲得する可能性を高めるために、SEは何をすべきでしょうか？
A. MSSP と協力して、PAN-OS アドバンスド ルーティング エンジンで論理ルーターを有効にし、論理ルーター間でルーティング プロファイルを共有できるように計画します。
B. MSSP と協力して、ルーティング フィルター、マップ、および関連アクションの標準セットを含む API 呼び出しを作成します。その後、MSSP は新しい顧客を獲得するたびに API を呼び出すことができます。
C. 既存の仮想ルータでは論理的に分離された BGP ピアリング設定が可能だが、すべてのルータにわたって標準基準を処理する方法はないことを MSSP に確認します。
D. 顧客データが混在しないように環境を分離するためのよりよい方法として、MSSP と協力して vsys の使用を確立します。
Answer: (解答を表示する**)**
MSSPの要件である論理的に分離されたBGPピアリング設定に対応しながら、標準的なルーティングルールとアップデートを効率的に管理するために、Palo Alto NetworksはPAN-OS 11.0で導入されたAdvanced Routing Engineを提供しています。Advanced

Routing Engineは、このシナリオで極めて重要な論理ルーターのサポートを含むルーティング機能を強化します。
Aが正しい理由
* 論理ルーターにより、MSSP は顧客ごとに分離された BGP ピアリング構成を作成できます。
* 高度なルーティング エンジンにより、MSSP は標準ルーティング プロファイル (フィルタ、ポリシー、マップなど) を論理ルータ間で共有できるようになり、ルーティング構成の展開と保守が簡素化されます。
* このアプローチでは、各論理ルータが共有ルーティング ルールを活用しながら顧客の固有のニーズに対応できるため、スケーラビリティが確保されます。
他の選択肢が間違っている理由
* B: APIを使用してデプロイメントを自動化することは有益ですが、論理的に分離されたBGPピアリング設定の必要性は解消されません。論理ルーターはネイティブにこの分離機能を提供します。
* C: PAN-OS の仮想ルータは BGP ピアリング設定を分離できますが、複数のルータ間での標準ルーティング ルールとプロファイルの効率的な共有はサポートされていません。
* D: 仮想システム (vsys) は、ルーティング構成ではなく、管理ドメインを分離するために使用されます。
Vsys は、複数の顧客にわたる BGP ピアリング設定を管理するための適切なソリューションではありません。
重要なポイント:
* 論理ルーターを備えた PAN-OS アドバンスド ルーティング エンジンにより、MSSP の BGP ピアリング管理が簡素化されます。
* 論理ルーターは、共有構成プロファイルを有効にしながら、顧客環境に必要な分離を提供します。
参考文献:
Palo Alto Networks PAN-OS 11.0 高度なルーティングドキュメント

最新問題**: 7**
ある顧客が、Advanced WildFire が誤ってファイルを悪意のあるファイルとして分類したと主張し、別のベンダーがそのファイルは無害であると主張しているため、証拠を求めています。
システム エンジニアはどのようにして、Advanced WildFire が正確であることを顧客に保証できるでしょうか?
A. 顧客に提供する情報については、脅威ログを確認してください。
B. ログ内の WildFire 分析レポートを使用して、ファイルが実行されたときに実行された悪意のあるアクションを顧客に示します。
C. 顧客の TAG チケットを開き、サポート エンジニアが適切なアクションを決定できるようにします。

D. 顧客は Advanced WildFire が正しいと認識するため、何もしないでください。
Answer: B (メーッセージを残す**)**
Advanced WildFireは、Palo Alto Networksが提供するクラウドベースのマルウェア分析 -防御ソリューションです。サンドボックス環境でファイルを実行し、その挙動を観察することで、ファイルが悪意のあるファイルかどうかを判定します。ファイルの分類に関するお客様の懸念に対処するため、システムエンジニアはファイルの挙動を示す証拠を提供する必要があります。各オプションの分析結果は以下の通りです。
* オプションA: 顧客に提供する情報について脅威ログを確認する
* 脅威ログは、悪意のあるファイルに関するイベントと判定の概要を提供できますが、顧客を納得させるために必要な詳細な動作分析は含まれていません。
* ログを確認することは予備的なステップとしては役立ちますが、顧客が必要とするレベルの証明は提供されません。
* このオプションだけでは不十分です。
* オプションB: ログ内のWildFire分析レポートを使用して、ファイルが起動されたときに実行された悪意のあるアクションを顧客に示します。
* WildFire は、ネットワーク アクティビティ、ファイルの変更、プロセス実行、侵害の兆候 (IoC) など、サンドボックス内でのデトネーション中のファイルの動作に関する詳細を含む分析レポートを生成します。
* このレポートは、ファイルが悪意のあるファイルとしてフラグ付けされた理由を示す具体的な証拠を提供します。これは、WildFire の判断が観察された悪意のある動作に基づいていることをお客様に保証する最も正確な方法です。
* これが最善の選択肢です。
* オプションC: 顧客のためにTAGチケットを開き、サポートエンジニアが適切なアクションを決定できるようにします。
* サポート チケットを開くことは、さらなる分析や異議申し立てを行うための有効なアクションですが、顧客に現在の WildFire の判定を直接的に保証する方法ではありません。
* このオプションは、即時証明を求める顧客の要求に直接対応するものではありません。
* このオプションは理想的ではありません。
* オプションD: 顧客はAdvanced WildFireが正しいと認識するので何もしない
* このアプローチは顧客の懸念を無視しており、WildFire の決定を裏付ける証拠を何も提供していません。
* このオプションは不適切です。
参考文献:
* Palo Alto Networks の WildFire に関するドキュメント
* 山火事分析レポート

最新問題**: 8**
ある企業には複数の事業部があり、それぞれが異なるドメイン名を持つ独自のユーザーディレクトリとIDプロバイダー（IdP）を管理しています。同社のネットワークセキュリティ

チームは、各事業部のIdPに対してユーザーを認証するために、全事業部で共通のGlobalProtectリモートアクセスサービスを導入したいと考えています。
どの構成により、ネットワーク セキュリティ チームが GlobalProtect ユーザーを複数の SAML IdP に対して認証できるようになりますか?
A. 各SAML IdPに対して複数の認証プロファイルを持つGlobalProtect
B. GlobalProtect ポータルおよびゲートウェイで使用するための複数認証モードの Cloud Identity Engine 認証プロファイル
C. 異なる認証方法を使用する複数の認証プロファイルを持つ認証シーケンス
D. 各ビジネス ユニットに複数の Cloud Identity Engine テナント
Answer: A (メーッセージを残す**)**
複数のSAMLアイデンティティプロバイダ（IdP）からユーザーを認証するようにGlobalProtectを設定するには、IdPごとに1つずつ、複数の認証プロファイルを作成するのが正しい方法です。各オプションの分析は以下のとおりです。
* オプションA: 各SAML IdPに複数の認証プロファイルを備えたGlobalProtect
* GlobalProtect では、それぞれ特定の IdP に対応する複数の SAML 認証プロファイルを設定できます。
* これらのプロファイルはGlobalProtectポータルまたはゲートウェイに関連付けられています。ユーザーが認証を試みると、ドメインやその他の属性に基づいて適切なIdPに誘導されます。
* これは、複数の IdP からのユーザーの認証を有効にするための正しい方法です。
* オプション B: GlobalProtect ポータルおよびゲートウェイで使用するための複数認証モードの Cloud Identity Engine 認証プロファイル
* Cloud Identity Engine (CIE) は複数のディレクトリの ID を同期できますが、共有 GlobalProtect セットアップの複数の SAML IdP を直接サポートしません。
* このオプションは適用されません。
* オプションC: 異なる認証方法を使用する複数の認証プロファイルを持つ認証シーケンス
* 認証シーケンスを使用すると、同じユーザーに対して複数の認証方法 (LDAP、RADIUS、SAML など) を順番に試すことができますが、複数の SAML IdP を処理するようには設計されていません。
* このオプションはシナリオには適していません。
* オプション D: 各ビジネス ユニットに複数の Cloud Identity Engine テナント
* 各ビジネス ユニットに複数の CIE テナントを展開すると、不要な複雑さが追加されますが、複数の SAML IdP に対してユーザーを認証するように GlobalProtect を構成する必要はありません。
* このオプションは適切ではありません。

最新問題**: 9**
Strata Cloud Manager (SCM) または Panorama を使用すると、顧客はどの 3 つのソリューションを監視および管理できますか?
（3選択してください。）

A. プリズマアクセス
B. プリズマクラウド
C. コルテックス XSIAM
D. NGFW
E. プリズム SD-WAN
Answer: A,D,E (メーッセージを残す)
* Prisma Access (回答 A):
* Strata Cloud Manager (SCM) と Panorama は、リモート ユーザーとブランチ オフィス向けの Palo Alto Networks のクラウド配信セキュリティ プラットフォームである Prisma Access の集中的な可視性と管理を提供します。
* NGFW（回答D） :
* SCM と Panorama はどちらも、オンプレミス、ハイブリッド、またはマルチクラウド環境に導入された Palo Alto Networks 次世代ファイアウォール (NGFW) を管理および監視するために使用されます。
* Prisma SD-WAN (回答 E):
* SCM と Panorama は Prisma SD-WAN と統合してブランチの接続性とセキュリティを管理し、SD-WAN 環境でのシームレスな運用を保証します。
* なぜBではないのか:
* Prisma Cloud は、クラウド ネイティブ セキュリティ向けに設計された独自のプラットフォームであり、Strata Cloud Manager または Panorama を通じて直接管理されるものではありません。
* なぜCではないのか:
* Cortex XSIAM (Extended Security Intelligence and Automation Management) は Cortex プラットフォームの一部であり、SCM または Panorama によって管理されません。
Palo Alto Networks ドキュメントからの参照:
* Strata Cloud Managerの概要
* パノラマの機能と利点

最新問題**: 10**
ある企業は、可視性の向上と、アプリケーションとデータへの最小限の権限アクセスを実現するIDベースの制御を実現するために、IDの導入を計画しています。この企業ではオンプレミスのActive Directory（AD）を導入しておらず、デバイスの接続と管理はEntra IDとJamfの組み合わせによって行われています。
サポートされている ID ソースのうち、この環境に適したものはどれですか (2 つ選択してください)。
A. キャプティブポータル
B. WMIクライアントプローブ用に構成されたユーザーIDエージェント
C. 内部ゲートウェイ展開を備えた GlobalProtect
D. Cloud Identity Engine が Entra ID と同期されました
Answer: C,D (メーッセージを残す)

このシナリオでは、企業はオンプレミスのActive Directoryを使用せず、Entra IDとJamfを使用してデバイスを管理します。これは、クラウドネイティブかつ最新の管理環境を意味します。以下は各オプションの評価です。
* オプションA: キャプティブポータル
* キャプティブポータルは、管理対象外デバイスやゲストユーザーに対してIDマッピングが必要な環境で一般的に使用されます。ユーザーがWebインターフェースを通じて認証を行うためのメカニズムを提供します。
* ただし、今回のケースでは、企業はEntra IDとJamfを使用してデバイスを管理しており、ID情報は既に他の手段で一元管理できる可能性があります。キャプティブポータルは理想的なソリューションではありません。
* このオプションは適切ではありません。
* オプション B: WMI クライアント プローブ用に構成されたユーザー ID エージェント
* WMI (Windows Management Instrumentation) クライアントプロービングは、Windows 環境において IP アドレスとユーザー名をマッピングするために使用されるメカニズムです。このアプローチはオンプレミスの Active Directory 展開に特有のものであり、Windows エンドポイントとの直接通信が必要です。
※当社ではオンプレミスADを導入しておらず、Entra IDとJamfを使用しているため、この方法は適用できません。
* このオプションは適切ではありません。
* オプションC: 内部ゲートウェイを導入したGlobalProtect
* GlobalProtectは、Palo Alto NetworksのVPNソリューションであり、安全なリモートアクセスを実現します。また、内部ゲートウェイと連携して導入することで、IDベースのマッピングもサポートします。
* この場合、内部ゲートウェイを備えた GlobalProtect は、ゲートウェイを介して接続する管理対象デバイスに基づいて、ユーザーとデバイスの可視性を提供するメカニズムとして機能します。
* このオプションは適切です。
* オプションD: Cloud Identity EngineをEntra IDと同期
* Cloud Identity Engine は、Entra ID (旧 Azure AD) などの ID プロバイダーからの ID 情報を同期するためのクラウドベースのアプローチを提供します。
* Entra ID と Jamf を使用したクラウド ネイティブ環境では、Cloud Identity Engine がシームレスに統合され、アプリケーションとデータの ID 可視性を提供するため、最適です。
* このオプションは適切です。
参考文献:
* Cloud Identity Engine に関する Palo Alto Networks のドキュメント
* Palo Alto Knowledge Base の GlobalProtect の構成と使用例

最新問題: 11

Palo Alto Networks AIOps for NGFW の機能と購入オプションを明確に説明している 2 つの文はどれですか (2 つ選択してください)。
A. 商用エディションとエンタープライズ エディションの 2 つのライセンス レベルで提供されます。
B. 無料バージョンとプレミアム バージョンの 2 つのライセンス レベルで提供されます。
C. テレメトリ データを使用して問題を予測、予防、または特定し、機械学習 (ML) を使用してプロセスを調整および強化します。
D. 問題を予測、防止、または特定するためにログ データを Advanced WildFire に転送し、機械学習 (ML) を使用してプロセスを改善し、適応します。
Answer: B,C (メーッセージを残す)
Palo Alto Networks AIOps for NGFW は、テレメトリ データと機械学習 (ML) を活用して、プロアクティブな運用分析情報、ベスト プラクティスの推奨事項、問題の防止を提供するクラウド配信サービスです。
* なぜ 無料版とプレミアム版の 2 つのライセンス層で提供される」のですか (正解 B)。AIOps for NGFW は次の 2 つの層で利用できます。
* 無料レベル: 追加費用なしで、基本的な運用上の洞察とベスト プラクティスを提供します。
* プレミアム レベル: AI を活用した予測、問題の予防、強化された ML ベースの推奨事項などの高度な機能を提供します。
* テレメトリデータを用いて問題を予測、予防、または特定し、機械学習（ML）を用いてプロセスを調整・強化する」（正解C）理由は何ですか？AIOpsは、NGFWからのテレメトリデータを用いて運用傾向を分析し、潜在的な問題を予測し、問題が発生する前に解決策を提案します。MLは、実世界のデータから学習することでこれらの洞察を継続的に洗練させ、時間の経過とともに精度と有効性を高めます。
* 商用エディションとエンタープライズ エディションの 2 つのライセンス レベルで提供されます」(オプション A) ではダメですか? これは誤りです。AIOps のライセンス モデルは、「商用」エディションと「エンタープライズ」エディションではなく、「無料」および「プレミアム」レベルに基づいているためです。
* 問題を予測、防止、または特定するためにログデータをAdvanced WildFireに転送し、機械学習（ML）を使用してプロセスを改善し、適応させる」（オプションD）ではダメなのでしょうか？AIOpsはAdvanced WildFireに依存しません。代わりに、NGFWから直接テレメトリデータを取得し、運用およびセキュリティ分析を実行します。

最新問題**: 12**
顧客の RFP に応答しているときに、システム エンジニア (SE) が「PANW ファイアウォールは、ゼロ トラスト原則の一環としてトランザクションのマッピングをどのように可能にするのか」という質問を受けました。SE がこの質問に答えるために使用できる 2 つの説明はどれですか。(2 つ選択してください。)

A. ゼロ トラストをイデオロギーとして強調し、ゼロ トラストの原則にどのように準拠するかは顧客が決定することを強調します。
B. 悪意のないトラフィックを検証するための復号化とセキュリティ保護の重要性を強化します。
C. すべてのトラフィック フローを可視化できるように、NGFW をネットワークに配置する方法を説明します。
D. ユーザー、アプリケーション、およびデータ オブジェクトを使用して、Palo Alto Networks NGFW セキュリティ ポリシーがどのように構築されるかについて説明します。
Answer: (解答を表示する**)**
この設問は、Palo Alto Networks (PANW) Strataハードウェアファイアウォールがゼロトラスト原則の一環としてトランザクションのマッピングをどのように実現するかを問うもので、システムエンジニア (SE) は顧客向けRFPへの回答として2つの説明文を提供する必要があります。ゼロトラストとは、デフォルトで信頼を前提としないセキュリティモデルであり、ネットワークの内外を問わず、すべてのトランザクション、ユーザー、デバイスの継続的な検証が必要です。Strataポートフォリオの一部であるPalo Alto Networks次世代ファイアウォール (NGFW) は、高度な可視性、復号化、ポリシー適用機能を通じてこれをサポートします。以下は、Palo Alto Networksの公式ドキュメントに基づき、選択肢BとDが正しい説明文である理由を詳しく説明したものです。
ステップ1: PAN-OSにおけるゼロトラストとトランザクションマッピングを理解する
NIST SP 800-207などのフレームワークで定義されているゼロトラスト原則は、ユーザーID、アプリケーション、データなどのコンテキストに基づいて、すべてのトランザクション（ネットワークフロー、アプリケーションリクエストなど）を識別および検証することに重点を置いています。Palo Alto NetworksのNGFWにおいて、「トランザクションのマッピング」とは、ネットワークトラフィックをきめ細かく識別、分類、制御する機能を指し、ゼロトラストに準拠した検証と適用を可能にします。
PAN-OS オペレーティング システムは、次の方法でこれを実現します。
* App-ID: ポートやプロトコルに関係なくアプリケーションを識別します。
* ユーザー ID: IP アドレスをユーザー ID にマッピングします。
* コンテンツ ID: 可視性を確保するための復号化を含め、コンテンツを検査して保護します。
* セキュリティ ポリシー: これらのマッピングに基づいてルールを適用します。

最新問題**: 13**
Palo Alto Networks NGFW のデフォルト構成に当てはまる記述はどれですか?
A. セキュリティ プロファイルはデフォルトですべてのポリシーに適用され、ファイアウォールを通過するデータの暗黙的な信頼が排除されます。
B. ゾーン内トラフィックのデフォルトのポリシー アクションは拒否であり、セキュリティ ゾーン内の暗黙的な信頼が排除されます。

C. デフォルトのポリシーアクションでは、明示的に拒否されない限り、すべてのトラフィックが許可されます。
D. ゾーン間トラフィックのデフォルトのポリシー アクションは拒否であり、セキュリティゾーン間の暗黙的な信頼が排除されます。
Answer: (解答を表示する**)**
Palo Alto Networks NGFWのデフォルト設定には、明示的なルールが定義されていない場合のトラフィックの処理方法を決定するデフォルトのセキュリティルールセットが含まれています。各オプションの説明は以下のとおりです。
* オプションA: セキュリティプロファイルはデフォルトですべてのポリシーに適用され、ファイアウォールを通過するデータの暗黙的な信頼を排除します。
* セキュリティプロファイル（ウイルス対策、スパイウェア対策、URLフィルタリングなど）は、デフォルトではどのポリシーにも適用されません。管理者がセキュリティルールに明示的に適用する必要があります。
* この記述は誤りです。
* オプションB: ゾーン内トラフィックのデフォルトのポリシーアクションは拒否であり、セキュリティゾーン内の暗黙の信頼を排除します。
* デフォルトでは、同一ゾーン内のトラフィック（ゾーン内トラフィック）は許可されます。例えば、「信頼」ゾーン内のデバイス間のトラフィックは、管理者が明示的に拒否しない限り許可されます。
* この記述は誤りです。
* オプションC: デフォルトのポリシーアクションは、明示的に拒否されない限り、すべてのトラフィックを許可します。
* Palo Alto Networks ファイアウォールには、「すべて許可」のデフォルトルールはありません。代わりに、ゾーン間トラフィックに対してはデフォルトで「すべて拒否」ルールが、ゾーン内トラフィックに対しては暗黙的に「許可」ルールが設定されます。
* この記述は誤りです。
* オプションD: ゾーン間トラフィックのデフォルトのポリシーアクションは拒否であり、セキュリティゾーン間の暗黙の信頼を排除します。
* デフォルトでは、異なるゾーン間のトラフィック（ゾーン間トラフィック）は拒否されます。これはゼロトラストの原則に準拠しており、ゾーン間のトラフィックが暗黙的に許可されないようにします。
管理者は、ゾーン間トラフィックを許可するための明示的なルールを定義する必要があります。
* この記述は正しいです。
参考文献:
* セキュリティポリシーのデフォルトに関する Palo Alto Networks のドキュメント
* デフォルトのセキュリティルールに関するナレッジベースの記事

最新問題**: 14**

高度な DNS セキュリティに加えて、インライン機械学習 (ML) を活用している 3 つのクラウド配信セキュリティ サービス (CDSS) サブスクリプションはどれですか (3 つ選択してください)。
A. 高度なURLフィルタリング
B. 高度な脅威防止
C. 高度な山火事
D. エンタープライズ DLP
E. IoTセキュリティ
Answer: A,B,D (メーッセージを残す)

最新問題: **15**
Advanced DNS Security が検出して防止できる DNS 攻撃の例はどれですか?
A. 高エントロピーDNSドメイン
B. ポリモーフィックDNS
C. CNAMEクローキング
D. DNSドメインのリブランディング
Answer: A (メーッセージを残す)
Palo Alto NetworksファイアウォールのAdvanced DNS Securityは、幅広いDNSベースの攻撃を識別・防御するように設計されています。リストされているオプションの中で、「高エントロピーDNSドメイン」は、Advanced DNS Securityが検出・ブロックできるDNS攻撃の具体的な例です。
* なぜ「高エントロピーDNSドメイン」なのか（正解A）？高エントロピーDNSドメインは、マルウェアやボットが検出を回避するためにランダムに生成されたドメイン名（例：gfh34ksdu.com）を利用する攻撃でよく使用されます。これは、ドメイン生成アルゴリズム（DGA）ベースの攻撃の特徴です。
高度なDNSセキュリティ機能を備えたPalo Alto Networksファイアウォールは、機械学習を用いてDNSクエリのエントロピー（ランダム性）を分析することで、このようなドメインを検出します。エントロピー値が高い場合、動的に生成されたドメイン、または悪意のあるドメインである可能性が高いことを示します。
* 「ポリモーフィックDNS」（オプションB）ではないのはなぜですか？ポリモーフィックDNSは、検出を回避するためにDNSレコードを動的に変更する手法を指しますが、Palo Alto Networksのドキュメントでは、Advanced DNS Securityによって軽減される攻撃の種類として明確には示されていません。ファイアウォールは、DGAドメインや異常なDNSトラフィックパターンの検出など、DNSクエリの挙動に重点を置いています。
* 「CNAMEクローキング」（オプションC）はなぜダメなのでしょうか？CNAMEクローキングとは、CNAMEレコードを利用してDNSクエリを悪意のあるドメインや隠蔽されたドメインにリダイレクトすることです。Palo Altoのファイアウォールは悪意のあるDNSリダイレクトを検出してブロックできますが、Advanced DNS Securityは主にDGAドメイン、トン

ネリング、高エントロピークエリといったDNS不正利用のパターンを特定することに重点を置いています。
* 「DNSドメインのリブランディング」オプションD）はなぜダメなのか？DNSドメインのリブランディングとは、悪意のある活動に関連付けられたドメイン名を変更し、検出を回避することです。これは通常、持続的な活動を行うために用いられる戦術ですが、Advanced DNS Securityが特に対処しているDNS攻撃の種類ではありません。
高度なDNSセキュリティは、高エントロピードメイン、DNSトンネリング、プロトコル違反といった疑わしいDNSパターンを動的かつリアルタイムで特定することに重点を置いています。高エントロピーDNSドメインはDGAなどの攻撃メカニズムと直接結びついているため、これが正解です。
参考: Palo Alto Networks の Advanced DNS Security ドキュメントによると、高エントロピー ドメインの検出はサービスの中核機能であり、機械学習と動作分析を活用して、このような悪意のあるアクティビティを識別してブロックします。

最新問題: **16**
ある顧客が 10 の新しい支社を取得しましたが、各支社のユーザー数は 50 人未満で、既存のファイアウォールはありませんでした。
システムエンジニアは、各ブランチオフィスに高度な脅威防御機能を備えたPAシリーズNGFWを推奨したいと考えています。インターネットトラフィックのセキュリティ保護において、最もコスト効率の高いNGFWシリーズはどれでしょうか？
A. PA-200
B. PA-400
C. PA-500
D. PA-600
Answer: (解答を表示する**)**
PA-400シリーズは、小規模ブランチオフィスに最適な、最もコスト効率の高いパロアルトネットワークスのNGFWです。選択肢を分析してみましょう。
PA-400シリーズ（推奨オプション）
* PA-400 シリーズ (PA-410、PA-415 など) は、ユーザー数が 50 人未満の小規模から中規模のブランチ オフィス向けに特別に設計されています。
* 上位モデルに比べて低価格で、高度な脅威防止を含む必要なセキュリティ機能をすべて提供します。
* PAN-OS およびクラウド配信セキュリティ サービス (CDSS) をサポートしているため、ブランチ オフィスでのインターネット トラフィックのセキュリティ保護に適しています。
他の選択肢が間違っている理由
* PA-200 :PA-200は旧モデルであり、現在は販売されていません。現代のブランチオフィスのセキュリティに必要な性能と機能を備えていません。
* PA-500:PA-500 も旧モデルであり、PA-400 シリーズほどコスト効率は良くありません。
* PA-600:PA-600シリーズは存在しません。

重要なポイント:
* ユーザー数が 50 人未満のブランチ オフィスの場合、PA-400 シリーズはコストとパフォーマンスの最適なバランスを提供します。
参考文献:
* Palo Alto Networks PA-400 シリーズ データシート

最新問題: **17**
見込み顧客は Palo Alto Networks NGFW に興味があり、社内ネットワークを独自の BGP 環境に分離する機能を評価したいと考えています。
このニーズに対応する NGFW の能力を説明している記述はどれですか。
A. PAN-OS がサポートしていないため、対処できません。
B. 複数の eBGP 自律システムを作成することで対処できます。
C. BGP 連合で対処できます。
D. BGP が機能するには内部で完全にメッシュ化されている必要があるため、対処できません。
Answer: (解答を表示する**)**
ステップ1: 要件とコンテキストを理解する
* 顧客のニーズ: 内部ネットワークを固有の BGP 環境に分離し、単一の組織内に複数の分離されたルーティング ドメインまたは半分離されたルーティング ドメインを提案します。
* BGPの基礎:
* BGP は、自律システム (AS) 間でルーティング情報を交換するために使用されるルーティング プロトコルです。
* eBGP: 異なる AS 間で使用される外部 BGP。
* iBGP: 単一の AS 内で使用される内部 BGP。コンフェデレーションやルート リフレクタなどの技術によって軽減されない限り、通常は完全なメッシュのピアが必要です。
* Palo Alto NGFW: PAN-OS 内の仮想ルータ (VR) で BGP をサポートし、Strata ハードウェア ファイアウォール (PA シリーズなど) の高度なルーティング機能を有効にします。
* 参考資料: PAN-OS は動的ルーティングとネットワーク セグメンテーションのために BGP をサポートしています」(docs.
paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp)。
ステップ2: 各オプションを評価する

オプションA: PAN-OSがサポートしていないため対処できません
* 分析：
* PAN-OS は、eBGP、iBGP、コンフェデレーション、ルート リフレクタを含む BGP を完全にサポートしており、「ネットワーク > 仮想ルーター > BGP」で設定できます。
* 複数の仮想ルータや BGP などの機能により、ネットワークの分離とルーティング ポリシーの制御が可能になります。
* この記述は文書化された機能と矛盾しています。
* 検証：
* 「動的ルーティング用の仮想ルータでBGPを構成する」(docs.paloaltonetworks.com/pan-os/10-2
/pan-os-networking-admin/bgp/configure-bgp)。
* 結論: 誤り - PAN-OS は BGP と分離技術をサポートしています。該当しません。
オプションB: 複数のeBGP自律システムを作成することで対処できます
* 分析：
* eBGP: それぞれ固有の AS 番号を持つ異なる AS 間で使用されます (例: AS 65001、AS 65002)。
* 単一の組織内で複数の eBGP AS を作成するには、次のものが必要です。
* 各内部セグメントに一意の AS 番号 (パブリックまたはプライベート) を割り当てます。
* 各セグメントを個別の AS として扱い、eBGP を介して他のセグメントと外部的にピアリングします。
* 課題:
* 内部的には、これは単一のネットワークでは実用的ではなく、外部ピアリング (例:
たとえば、ISP など)。
* 複雑な管理とパブリック/プライベート AS 番号の割り当てが必要であり、内部分離には適していません。
* 内部 AS 管理用に設計された iBGP またはコンフェデレーションを活用しません。
* PAN-OS は eBGP をサポートしていますが、このアプローチは内部ネットワーク分離の目的と一致しません。
* 検証：
* 「eBGP ピアは異なる AS を接続します」(docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp/bgp-concepts)。
* 結論: 可能だが非現実的であり、内部分離のための意図された BGP ソリューションではありません。最適ではありません。
オプションC: BGPコンフェデレーションで対処できる
* 説明: BGP コンフェデレーションは、単一の AS をサブ AS (それぞれプライベート コンフェデレーション メンバー AS 番号を持つ) に分割し、統合された外部 AS を維持しながら iBGP フルメッシュ要件を削減します。
* 分析：
* 仕組み:

* 単一の AS (例: AS 65000) がサブ AS (例: 65001、65002) に分割されます。
* 各サブ AS 内では、iBGP フルメッシュまたはルートリフレクタが使用されます。
* サブ AS 間は eBGP のようなピアリング (コンフェデレーション EBGP) で接続されますが、外部的には 1 つの AS として表示されます。
* 分離：
* 各サブ AS は、独自のルーティング ポリシーを持つ一意の BGP 環境 (部門、サイトなど) を表すことができます。
* サブ AS 内のファイアウォールは iBGP 経由でピアリングし、サブ AS 間ではコンフェデレーション EBGP を使用します。
* PAN-OS サポート:
* 「ネットワーク > 仮想ルーター > BGP > コンフェデレーション」でコンフェデレーションメンバー AS 番号を使用して設定できます。
* 複数のパブリック AS 番号を使用せずにセグメント化を必要とする大規模な内部ネットワークに最適です。
* 利点：
* 内部 BGP 管理を簡素化します。
* 独自の内部 BGP 環境に対する顧客のニーズに応えます。
* 検証：
* 「BGP 連合は、AS をサブ AS に分割することでフルメッシュの負担を軽減します」(docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp/bgp-confederations)。
* 「固有の内部ルーティング ドメインをサポートします」(knowledgebase.paloaltonetworks.com)。
* 結論: サポートされた実用的なソリューションで要件に直接対処します。適用可能。
オプションD: BGPが機能するには内部で完全にメッシュ化されている必要があるため、対処できません。
* 分析：
* iBGP フル メッシュ: 従来の iBGP では、AS 内のすべてのルータが相互にピアリングする必要があり、スケーリングが不十分です (n(n-1)/2 接続)。
* 緩和策: PAN-OS は代替手段をサポートしています:
* ルート リフレクタ: iBGP ピアリングを集中管理します。
* コンフェデレーション: AS をサブ AS に分割します (オプション C を参照)。
* この声明はこれらの機能を無視し、BGP の制限により分離が防止されると誤って主張しています。
* 検証：
* 「コンフェデレーションとルート リフレクタによりフルメッシュの必要性がなくなる」(docs.paloaltonetworks.com/pan- os/10-2/pan-os-networking-admin/bgp/bgp-confederations)。
* 結論: 誤り - PAN-OS はフルメッシュの制約を克服します。該当なし。
ステップ3: 推奨の根拠

* オプション C を選んだ理由は?
* アライメント: コンフェデレーションにより、単一の外部 AS を維持しながら、内部ネットワークを固有の BGP 環境 (サブ AS) に分離できるため、顧客のニーズに完全に一致します。
* スケーラビリティ: iBGP フルメッシュの複雑さを軽減し、大規模またはセグメント化された内部ネットワークに最適です。
* PAN-OS サポート: BGP 構成で明示的に実装され、ドキュメントによって検証されています。
* 他の人はなぜダメなのか?
* A: False - PAN-OS は BGP と分離をサポートしています。
* B: eBGP は外部 AS 用であり、内部分離用ではありません。連合ほど実用的ではありません。
* D: BGP の機能を誤って伝えています。コンフェデレーションやルート リフレクタではフル メッシュは必要ありません。
ステップ4：検証済みの参照
* BGP コンフェデレーション: 「内部セグメンテーションのために AS をサブ AS に分割する」(docs.paloaltonetworks)。
com/pan-os/10-2/pan-os-networking-admin/bgp/bgp-confederations を参照してください。
* PAN-OS BGP: 「ルーティングの柔軟性のために eBGP、iBGP、およびコンフェデレーションをサポートします」(paloaltonetworks)。
com、PAN-OS ネットワーク ガイド)。
* ユースケース: 「コンフェデレーションは大規模な内部ネットワークに適しています」(knowledgebase.paloaltonetworks.com)。

最新問題**: 18**
APIに関して、顧客のRFPには「ベンダーのファイアウォールソリューションは、2時間後にAPIキーを無効化する強制メカニズムを備えたAPIを提供する必要があります」と記載されています。回答ではこの条項にどのように対応すればよいでしょうか？
A. はい - これは API キーのデフォルト設定です。
B. いいえ - PAN-OS XML API はキーをサポートしていません。
C. いいえ - API キーは作成できますが、時間に基づいて非アクティブ化する方法はありません。
D. はい - デフォルト設定を制限なしから 120 分に変更する必要があります。
Answer: (解答を表示する**)**
Palo Alto NetworksのPAN-OSは、ファイアウォールのRESTful APIおよびXMLベースのAPIとのやり取りにおいて、認証用のAPIキーをサポートしています。デフォルトではAPIキーに有効期限は設定されていませんが、管理者は特定の要件（例えば2時間後に時間ベースで無効化するなど）に合わせてAPIキーの有効期限を設定できます。これは、コンプライアン

スやセキュリティの観点から、APIキーを無期限にアクティブにしておくべきではない場合に特に役立ちます。
オプションの評価は次のとおりです。
* オプションA: APIキーのデフォルト設定には有効期限が含まれていないため、これは誤りです。デフォルトでは、明示的に設定しない限り、APIキーは無期限に有効です。
* オプションB: PAN-OSはAPIキーを完全にサポートしているため、これは誤りです。APIキーはファイアウォールAPIへのアクセス管理に不可欠であり、安全な認証方法を提供します。
* オプションC: これは誤りです。PAN-OSは明示的に設定することでAPIキーの有効期限をサポートします。デフォルトでは「有効期限なし」ですが、有効期限（例2時間）を設定する機能も利用可能です。
* オプションD（正解）RFP条項への正しい回答は、デフォルトのAPIキー設定を変更し、有効期限を120分（2時間）に設定することです。これは、時間に基づいてAPIキーの無効化を強制するという顧客要件と一致しています。管理者は、PAN-OS管理インターフェースまたはCLIを使用してこれを設定できます。
API キーの有効期限を設定する方法 (手順):
* ファイアウォール上の Web インターフェイスまたは CLI にアクセスします。
* デバイス > 管理 > API キーの有効期間設定 (GUI) に移動します。
* 希望する有効期限を設定します (例: 120 分)。
* または、CLI を使用して API キーの有効期限を設定します。
deviceconfig system api-key-expiry <時間（分）> を設定します
専念
* show コマンドを使用するか、API 呼び出しをテストして構成を確認し、設定された期間後にキーが期限切れになることを確認します。
参考文献:
Palo Alto Networks API ドキュメント: https://docs.paloaltonetworks.com/apis 構成ガイド: API キーの有効期限の管理

最新問題**: 19**
顧客の RFP に応答しているときに、システム エンジニア (SE) が「PANW ファイアウォールは、ゼロ トラスト原則の一環としてトランザクションのマッピングをどのように可能にするのか」という質問を受けました。SE がこの質問に答えるために使用できる 2 つの説明はどれですか。(2 つ選択してください。)
A. ゼロ トラストをイデオロギーとして強調し、ゼロ トラストの原則にどのように準拠するかは顧客が決定することを強調します。
B. 悪意のないトラフィックを検証するための復号化とセキュリティ保護の重要性を強化します。
C. すべてのトラフィック フローを可視化できるように、NGFW をネットワークに配置する方法を説明します。

D. ユーザー、アプリケーション、およびデータ オブジェクトを使用して、Palo Alto Networks NGFW セキュリティ ポリシーがどのように構築されるかについて説明します。
Answer: (解答を表示する**)**
ゼロトラストとは、暗黙の信頼を排除し、デジタルインタラクションのあらゆる段階を継続的に検証することで、インフラストラクチャとデータを保護する戦略的フレームワークです。Palo Alto NetworksのNGFWは、トランザクションの監視、IDの検証、最小権限アクセスの適用など、ゼロトラストの原則に準拠したネイティブ機能を備えて設計されています。以下の説明は、お客様の質問に効果的に答えています。
* 選択肢A :ゼロトラストをイデオロギーとして強調するのは正確ですが、この回答では、Palo Alto Networksのファイアウォールがトランザクションのマッピングをどのように促進するかを直接説明していません。文脈は示されていますが、質問の技術的な側面に対応するには不十分です。
* オプションB：復号とセキュリティ保護は悪意のあるトラフィックを特定する上で重要ですが、ゼロトラスト・フレームワークにおけるトランザクションのマッピングに特有のものではありません。この回答は、可視性やポリシー適用といったより広範な概念ではなく、セキュリティ機能のサブセットに焦点を当てています。
* オプションC（正解）NGFWをネットワークに導入することで、ユーザー、デバイス、アプリケーションを経由するすべてのトラフィックフローを可視化できます。これにより、ファイアウォールはトランザクションをマッピングし、ネットワークのセグメント化、すべてのトラフィックの検査、アクセス制御といったゼロトラスト原則を適用できます。App-ID、User-ID、Content-IDなどの機能により、ファイアウォールはトラフィックフローに関するきめ細かなインサイトを提供し、トランザクションの識別とセキュリティ確保を容易にします。
* オプションD（正解）Palo Alto Networks NGFWは、ゼロトラスト原則に準拠するため、ユーザー、アプリケーション、データオブジェクトに基づいたセキュリティポリシーを使用します。IPアドレスやポート番号に依存せず、アプリケーションの挙動、ユーザーのID、関連するデータの機密性に基づいてポリシーが適用されます。このマッピングにより、許可されたユーザーのみが特定のリソースにアクセスできるようになります。これはゼロトラストの基盤となります。
参考文献:
* ゼロトラストフレームワーク: https://www.paloaltonetworks.com/solutions/zero-trust
* ゼロトラストのセキュリティポリシーのベストプラクティス: https://docs.paloaltonetworks.com

最新問題**: 20**
見込み顧客は、ポート 53 経由のデータの流出、データの侵入、およびコマンド アンド コントロール (C2) アクティビティを阻止することに懸念を抱いています。
システム エンジニアはどのサブスクリプションを推奨する必要がありますか?
A. 脅威防止

B. DNSセキュリティ
C. App-IDとデータ損失防止
D. 高度な脅威防止と高度なURLフィルタリング
Answer: B (メーッセージを残す)
オプションC: BGPコンフェデレーションで対処できる
説明: BGP コンフェデレーションは、単一の AS をサブ AS (それぞれプライベート コンフェデレーション メンバー AS 番号を持つ) に分割し、統合された外部 AS を維持しながら iBGP フルメッシュ要件を削減します。
分析：
仕組み:
単一の AS (例: AS 65000) はサブ AS (例: 65001、65002) に分割されます。
各サブ AS 内では、iBGP フル メッシュまたはルート リフレクタが使用されます。
サブ AS 間では、eBGP のようなピアリング (コンフェデレーション EBGP) によって接続されますが、外部的には 1 つの AS として表示されます。
分離：
各サブ AS は、独自のルーティング ポリシーを持つ一意の BGP 環境 (部門、サイトなど) を表すことができます。
サブ AS 内のファイアウォールは iBGP 経由でピアリングし、サブ AS 間ではコンフェデレーション EBGP を使用します。
PAN-OS サポート:
「ネットワーク > 仮想ルーター > BGP > コンフェデレーション」でコンフェデレーション メンバー AS 番号を使用して設定できます。
複数のパブリック AS 番号を使用せずにセグメント化する必要がある大規模な内部ネットワークに最適です。
利点：
内部 BGP 管理を簡素化します。
独自の内部 BGP 環境に対する顧客のニーズに応えます。
検証：
「BGPコンフェデレーションは、ASをサブASに分割することでフルメッシュの負担を軽減します」（docs.paloaltonetworks.com）
/pan-os/10-2/pan-os-networking-admin/bgp/bgp-confederations）。
「固有の内部ルーティング ドメインをサポートします」
(knowledgebase.paloaltonetworks.com)。
結論: 裏付けのある実用的なソリューションで要件に直接対応します。適用可能です。
オプション D: BGP が機能するには内部で完全にメッシュ化されている必要があるため対処できません。分析:
iBGPフルメッシュ: 従来のiBGPではAS内のすべてのルータが相互にピアリングする必要があり、スケーリングが不十分です(n(n-
1)/2接続)。

緩和策: PAN-OS は代替手段をサポートしています:
ルート リフレクタ: iBGP ピアリングを集中管理します。
コンフェデレーション: AS をサブ AS に分割します (オプション C を参照)。
この声明はこれらの機能を無視し、BGP の制限が分離を妨げていると誤って主張しています。
検証：
「コンフェデレーションとルート リフレクタによりフルメッシュの必要性がなくなります」(docs.paloaltonetworks.com/pan-os/10-2/pan- os-networking-admin/bgp/bgp-confederations)。
結論: 誤ったPAN-OSはフルメッシュの制約を克服します。該当しません。
ステップ3: 推奨の根拠
オプション C を選ぶ理由は何ですか?
調整: コンフェデレーションにより、単一の外部 AS を維持しながら、内部ネットワークを固有の BGP 環境 (サブ AS) に分離できるため、顧客のニーズに完全に一致します。
スケーラビリティ: iBGP フルメッシュの複雑さを軽減し、大規模またはセグメント化された内部ネットワークに最適です。
PAN-OS サポート: BGP 構成で明示的に実装され、ドキュメントによって検証されています。
他の人はなぜダメなのか？
A: False - PAN-OS は BGP と分離をサポートしています。
B: eBGP は外部 AS 用であり、内部分離用ではありません。連合ほど実用的ではありません。
D: BGP の機能を誤って伝えています。コンフェデレーションやルート リフレクタではフル メッシュは必要ありません。
ステップ4：検証済みの参照
BGP 連合：「内部セグメンテーションのために AS をサブ AS に分割する」（docs.paloaltonetworks.com）
/pan-os/10-2/pan-os-networking-admin/bgp/bgp-confederations）。
PAN-OS BGP: 「ルーティングの柔軟性のために eBGP、iBGP、およびコンフェデレーションをサポートします」(paloaltonetworks.com、PAN-OS ネットワーク ガイド)。
ユースケース: 「コンフェデレーションは大規模な内部ネットワークに適しています」(knowledgebase.paloaltonetworks.com)。

最新問題**: 21**
システムエンジニア（SE）が、Strata Cloud Manager（SCM）によって管理されるNGFWを企業にデモンストレーションし、成功を収めました。その後の価値実証（POV）計画フェーズにおいて、CISOは、セキュリティポリシーがCritical Security Controls（CSC）などの業界標準をどの程度満たしているか、あるいは満たすべく進んでいるかを示すテスト、そして企

業が購入した機能を効果的に活用していることをどのように検証できるかを示すテストを要求しました。
POV テストのタイムライン中に、SE は POV が CISO の要求を満たすことをどのように確認する必要がありますか?
A. 最後に、POV でセキュリティ ライフサイクル レビュー (SLR) を実行し、顧客向けのレポートを作成します。
B. 最初は、顧客と協力して、必要な情報に関するカスタム ダッシュボードとレポートを作成し、顧客の必要に応じてレポートを取得できるようにします。
C. 最後に、顧客は、ベスト プラクティス、CDSS の採用、および NGFW 機能の採用という SCM ダッシュボードから情報を取得します。
D. 最初は、コンプライアンスに準拠し、テスト対象の CDSS サブスクリプションの機能を有効にするように設計された PANhandler ゴールデン イメージを使用します。
Answer: B (メーッセージを残す**)**
SEはSCMによって管理されるNGFWのデモンストレーションを実施しました。CISOは、POV（セキュリティ監査）による業界標準（CSCなど）への進捗状況の検証と、購入した機能（Advanced Threat PreventionなどのCDSSサブスクリプションなど）の有効活用の検証を求めています。SEは、テスト期間中にPOVが測定可能な証拠を提供できるようにする必要があります。それでは、選択肢を検討してみましょう。
ステップ1: CISOの要求を理解する
* 業界標準 (例: CSC): インターネット セキュリティ センターの重要なセキュリティ コントロール (例: CSC 1: デバイスのインベントリ、CSC 4: 安全な構成) では、可視性、脅威の防止、ポリシーの適用が求められますが、NGFW と SCM はこれらに対応できます。
* 機能の使用率: ライセンスされた機能 (App-ID、脅威防止、URL フィルタリングなど) がアクティブで有効であることを確認します。
* POV 目標: テスト タイムライン内で検証可能な進捗状況と使用率のメトリックを提供します。
参考資料: Strata Cloud Manager の概要 (docs.paloaltonetworks.com/strata-cloud-manager)、CIS Critical Security Controls (www.cisecurity.org/controls)。
ステップ2: SCM機能を定義する
Strata Cloud Manager (SCM): Palo Alto NGFW 用のクラウドベースの管理プラットフォームで、セキュリティ体制、ポリシーのコンプライアンス、サブスクリプションの使用状況を監視するためのダッシュボード (ベスト プラクティス、機能の採用など) とカスタム レポートを提供します。
セキュリティ ライフサイクル レビュー (SLR): リアルタイムの POV の進捗状況ではなく、セキュリティ ギャップのトラフィック ログを分析する、カスタマー サポート ポータル (SCM ではありません) を介して生成されるレポート。
ダッシュボードとレポート: SCM は、ポリシーの有効性と機能の採用に関するリアルタイムの分析情報を提供するために、事前に構築されたカスタマイズ可能なビューを提供します。

参考: SCM ダッシュボードとレポート (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports)。
ステップ3: 各オプションを評価する
A) 最後に、POV でセキュリティ ライフサイクル レビュー (SLR) を実行し、顧客向けのレポートを作成します。
説明: SLR は 7 ～ 30 日間のトラフィック ログを分析し、遡及的なセキュリティ態勢評価 (ブロックされた脅威、ポリシーのギャップなど) を提供します。
プロセス: POV の終了が近づいたら、ログをカスタマー サポート ポータル (サポート > セキュリティ ライフサイクル レビュー) にアップロードし、レポートを生成して共有します。
制限事項:
SLR はポイントインタイム分析であり、POV タイムライン中のリアルタイムの進捗状況トラッカーではありません。
POV 後のログ収集が必要となり、フィードバックが遅れます。
SCM で機能の使用状況の進行状況や CSC の調整が直接表示されません。
適合: 「POV タイムライン中」の要件を満たしていません。POV 後の分析に適しています。
参考: セキュリティ ライフサイクル レビュー ガイド (support.paloaltonetworks.com、ログインが必要です)。
B). 最初は、顧客と協力して、必要な情報に関するカスタムダッシュボードとレポートを作成し、顧客の必要に応じてレポートを取得できるようにします。
説明: SCM では、ポリシーコンプライアンス (CSC の調整) や機能の使用状況 (脅威防止のヒットなど) などの指標に合わせてカスタマイズされたカスタム ダッシュボードとレポート (モニター > ダッシュボードまたはレポート) を使用できます。
プロセス：
POV の開始時に、CISO と協力してメトリックを定義します (例: CSC 6 の場合は「ATP によってブロックされた脅威」、機能の採用の場合は「App-ID の使用」)。
SCM でカスタム ダッシュボードを構成します (ダッシュボード > ダッシュボードの追加 > カスタム)。
スケジュールされたレポートまたはオンデマンド レポートを設定します (レポート > カスタム レポート)。
顧客が POV 全体の進捗状況を監視できるようにします。
利点：
タイムライン中のポリシーの有効性と機能の使用状況をリアルタイムで確認できます。
CSC (ブロックされたマルウェア イベントなど) と一致し、サブスクリプションの ROI を表示します。
顧客が独自に結果を検証できるようにします。
適合: POV タイムライン内で CISO の要求を完全に満たします。
参考: SCM カスタム ダッシュボード (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/custom-dashboards)。

C) 最後に、顧客は SCM ダッシュボードからベスト プラクティス、CDSS 導入、NGFW 機能導入に関する情報を取得します。
説明: SCM は事前に構築されたダッシュボードを提供します。
ベスト プラクティス: セキュリティ標準に対するポリシーの整合性を評価します。
CDSS の採用: サブスクリプションの使用状況 (ATP、URL フィルタリングなど) を追跡します。
NGFW 機能の採用: App-ID や User-ID などの機能を監視します。
制限事項:
「終わりに近づく」まで待つと可視性が遅れ、進行中の進捗状況の追跡ができなくなります。
事前に構築されたダッシュボードは、カスタマイズしないと、CSC または特定の顧客のニーズに完全には一致しない可能性があります。
適合性: 有用だが不完全。POV 全体にわたるプロアクティブなセットアップとリアルタイムの監視が欠けている。
参考: SCM 事前構築済みダッシュボード (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/prebuilt-dashboards)。
D). 最初は、コンプライアンスに準拠し、テスト対象の CDSS サブスクリプションの機能を有効にするように設計された PANhandler ゴールデン イメージを使用します。
説明: PANhandler は、コンプライアンスのための「ゴールデン イメージ」(NIST、CIS ベンチマークなど) を含む Skillet (構成テンプレート) を管理するためのツールです。
プロセス: POV の開始時に Skillet を適用し、コンプライアンス設定と CDSS 機能を使用して NGFW を構成します。
制限事項:
NGFW を構成しますが、POV 中に進行状況や使用率は確認しません。
CISO が結果を追跡するためのレポートやダッシュボードの統合がありません。
適合: 環境は設定されていますが、検証要件を満たしていません。
参考: PANhandler Skillets (github.com/PaloAltoNetworks/panhandler)。
ステップ4：最適なアプローチを選択する
B が最も強力な選択肢です。
プロアクティブ: 最初から開始し、POV 全体にわたってメトリックが追跡されるようにします。
カスタマイズ可能: ダッシュボード/レポートを CSC (CSC 6 の脅威検出など) および機能の使用 (ATP イベントなど) に合わせてカスタマイズします。
検証可能: 顧客が必要に応じてレポートを取得できるようにし、タイムライン内で CISO の要求を満たします。
なぜA、C、Dではないのですか?
A: SLR はリアルタイムではなく遡及的であり、「進行中」という側面が欠けています。
C: 事前に構築されたダッシュボードは便利ですが、カスタム オプションよりも遅く、柔軟性が低くなります。

D: ゴールデン イメージは構成されますが、進行状況や使用率は確認されません。
ステップ5: Palo Altoドキュメントによる検証
SCM カスタム ダッシュボード: リアルタイムのカスタマイズされた監視をサポートします (SCM ドキュメント)。
SLR: POV プログレッシブではないポスト分析ツール (サポート ポータル ドキュメント)。
事前構築されたダッシュボード: カスタマイズは限定的 (SCM ドキュメント)。
PANhandler: レポートではなく構成に重点を置いています (PANhandler ドキュメント)。
したがって、検証された答えは B です。

最新問題**: 22**
見込み顧客が Palo Alto Networks 製品を評価し、既存のアーキテクチャにどのように適合するかを判断するために使用できる 3 つのツールはどれですか。(3 つ選択してください)
A. 概念実証（POC）
B. ポリシーオプティマイザー
C. セキュリティライフサイクルレビュー (SLR)
D. 究極のテストドライブ
E. 遠征
Answer: A,C,D (メーッセージを残す**)**
Palo Alto Networks製品を評価する際、見込み顧客は既存のアーキテクチャ内での互換性、パフォーマンス、そして価値を評価できるツールを必要とします。以下のツールが最も関連性の高いものです。
* なぜ「概念実証（POC）」なのか（正解A）？概念実証とは、お客様が自社の環境に直接パロアルトネットワークス製品を導入し、テストできる実践的な評価方法です。これにより、実際のパフォーマンス、互換性、運用への影響を評価できます。
* なぜ「セキュリティライフサイクルレビュー（SLR）」なのか（正解C）？SLRは、短期間の評価期間中に収集されたデータに基づいて、お客様のネットワークセキュリティ体制に関する詳細なレポートを提供します。お客様のネットワークにおけるリスク、脆弱性、そしてアクティブな脅威を明らかにし、パロアルトネットワークスのソリューションがそれらのリスクにどのように対処できるかを示します。SLRは、お客様のアーキテクチャにおける製品の価値を正当化するための強力なツールです。
* 「Ultimate Test Drive」（正解D）とは？Ultimate Test Driveは、Palo Alto Networksが提供するガイド付きハンズオンワークショップで、見込み顧客が管理された環境で製品の機能や性能を体験できます。本番環境ネットワークに導入せずに製品を評価したいお客様に最適です。
* 「ポリシーオプティマイザー」（オプションB）をお勧めしないのはなぜですか？ポリシーオプティマイザーは、製品の導入後に、未使用または過度に緩いルールを特定することでセキュリティポリシーを改善するために使用されます。導入前の評価には設計されていません。

* Expedition」オプションE）をお選びにならないのはなぜですか？Expeditionは、サードパーティ製ファイアウォールまたは既存のPalo Alto Networksファイアウォールからの設定変換を支援する移行ツールです。お客様のアーキテクチャにおける製品の適合性を評価するためのツールではありません。
参考: Palo Alto Networks SLR ドキュメントと Ultimate Test Drive の概要では、製品評価におけるこれらのツールの役割が確認されています。

最新問題: **23**
顧客がシステム エンジニア (SE) に、ファイアウォールで有効になっている Cloud-Delivered Security Services (CDSS) サブスクリプションが増えてもスループット パフォーマンスが低下しないと Palo Alto Networks が主張できる理由を尋ねました。
顧客の懸念に対処するために SE が説明する必要がある 2 つの概念はどれですか? (2 つ選択してください。)
A. 並列処理
B. 高度なルーティングエンジン
C. シングルパスアーキテクチャ
D. 管理データプレーンの分離
Answer: C,D (メーッセージを残す**)**
* シングルパスアーキテクチャ（回答C）：
* Palo Alto Networks ファイアウォールはシングル パス アーキテクチャを使用します。つまり、ファイアウォールは、有効になっているすべてのセキュリティ サービスに対してトラフィックを 1 回処理します。
* これにより、脅威防止、URL フィルタリング、WildFire などの複数のサービスに対する検査プロセスの重複が回避されます。
* ファイアウォールは、1 回のトラフィック検査パスで、追加の CDSS サブスクリプションが有効になっている場合でも、パフォーマンスを低下させることなくすべてのセキュリティ ポリシーを適用します。
* 管理データプレーンの分離（回答D）：
* Palo Alto Networks ファイアウォールでは、管理プレーンとデータ プレーンが分離されています。
* 管理プレーンは構成、ログ記録、およびその他の管理タスクを処理し、データ プレーンはトラフィックの処理と転送のみに焦点を当てます。
* このアーキテクチャ設計により、追加のクラウド配信セキュリティ サービスを有効にしても、スループットに影響が出たり、トラフィック処理の効率が低下したりすることはありません。
* 並列処理をしない理由（回答A）
* 並列処理は有益ですが、より多くのサービスが利用可能になった際に、一貫したスループットを維持するための主要な要素ではありません。ここで鍵となるのはシングルパス アーキテクチャです。

* 高度なルーティング エンジンを使用しない理由 (回答 B):
* 高度なルーティングエンジンは、CDSSサブスクリプションを有効にする際のスループット維持とは直接関係ありません。ルーティングプロトコルとトラフィックエンジニアリングに有効です。
Palo Alto Networks ドキュメントからの参照:
* シングルパスアーキテクチャのホワイトペーパー
* 管理およびデータプレーンの概要

最新問題: **24**
DNS ベースの脅威を阻止するために何が使用されますか?
A. DNSプロキシ
B. バッファオーバーフロー保護
C. DNSトンネリング
D. DNSシンクホール
Answer: D (メーッセージを残す)
DNSトンネリング、フィッシング、マルウェアのコマンドアンドコントロール（C2）活動といったDNSベースの脅威は、攻撃者がデータを盗み出したり、悪意のある通信を確立したりするためによく利用されます。Palo Alto Networksのファイアウォールは、これらの脅威に対処するための複数のメカニズムを提供しており、その中でもDNSシンクホールは最適な手法です。
* なぜ「DNSシンクホール」なのか（正解D）？DNSシンクホールは、悪意のあるドメインへのDNSクエリを内部IPアドレスまたはルーティング不可能なIPアドレスにリダイレクトすることで、悪意のあるドメインとの通信を効果的に防止します。ユーザーまたはエンドポイントが悪意のあるドメインに接続しようとすると、シンクホールDNSエントリによってトラフィックがブロックされるか、制御された宛先にルーティングされます。
* DNS シンクホールは、C2 サーバーに接続しようとするマルウェアをブロックしたり、データの流出を防いだりするのに特に効果的です。
* 「DNSプロキシ」（オプションA）ではダメな理由とは？DNSプロキシは、エンドポイントからのDNSクエリを上流のDNSサーバーに転送するために使用されます。ネットワークのDNS設定の一部として使用できますが、DNSベースの脅威を積極的に阻止することはできません。
* 「バッファオーバーフロー保護」（オプションB）ではダメですか？バッファオーバーフロー保護は、ソフトウェアの脆弱性を悪用するなど、メモリ関連の攻撃を防ぐための手法です。DNSベースの脅威防御とは無関係です。
* 「DNSトンネリング」（オプションC）ではないのはなぜですか？DNSトンネリング自体はDNSベースの脅威の一種であり、攻撃者はDNSクエリと応答内に悪意のあるトラフィックをエンコードします。このオプションは脅威そのものを指し、それを阻止する方法を指しているわけではありません。

参考: Palo Alto Networks の DNS セキュリティ ドキュメントでは、DNS シンクホールが DNS ベースの脅威を阻止するための重要なメカニズムであることが確認されています。

最新問題: **25**
顧客がシステム エンジニア (SE) に、ファイアウォールで有効になっている Cloud-Delivered Security Services (CDSS) サブスクリプションが増えてもスループット パフォーマンスが低下しないと Palo Alto Networks が主張できる理由を尋ねました。
顧客の懸念に対処するために SE が説明する必要がある 2 つの概念はどれですか? (2 つ選択してください。)
A. 並列処理
B. 高度なルーティングエンジン
C. シングルパスアーキテクチャ
D. 管理データプレーンの分離
Answer: A,C (メーッセージを残す**)**
お客様からの質問は、Palo Alto Networks Strataハードウェアファイアウォールが、脅威防御、URLフィルタリング、WildFire、DNSセキュリティなどのクラウド配信型セキュリティサービス（CDSS）サブスクリプションの増加に伴い、どのようにスループット性能を維持するかという点に焦点を当てています。従来のファイアウォールでは、セキュリティ機能を追加するとパフォーマンスが低下することがよくありますが、Palo Alto Networksは独自のアーキテクチャを活用することで、この影響を最小限に抑えています。システムエンジニア（SE）は、ファイアウォールのスループット維持能力の基盤となる2つの重要な概念、「並列処理」と「シングルパスアーキテクチャ」について説明する必要があります。以下は、Palo Alto Networksのドキュメントに基づいて検証された詳細な説明です。
ステップ1 :クラウド配信型セキュリティサービス（CDSS）とパフォーマンスに関する懸念事項を理解する CDSSサブスクリプションは、クラウドベースの脅威インテリジェンスと高度なセキュリティ機能をPAN-OSに統合することで、Strataハードウェアファイアウォールの機能を強化します。例として、以下のものが挙げられます。
* 脅威の防止: エクスプロイト、マルウェア、コマンド アンド コントロール トラフィックをブロックします。
* WildFire: クラウド内の未知のファイルを分析してマルウェアを検出します。
* URL フィルタリング: Web トラフィックを分類して制御します。
従来、他のファイアウォールでこのようなサービスを有効にすると、各機能が個別のパケットスキャンや追加のハードウェアリソースを必要とするため、処理オーバーヘッドが増加し、遅延やスループットの低下につながります。Palo Alto Networksは、シングルパスパラレルプロセッシング（SP3）アーキテクチャに基づく革新的な設計により、一貫したパフォーマンスを実現していると主張しています。

最新問題: **26**
デバイス ID はどの 3 つのポリシーで使用できますか? (3 つ選択してください。)

A. セキュリティ
B. 復号化
C. ポリシーベース転送 (PBF)
D. SD-WAN
E. サービス品質 (QoS)
Answer: (解答を表示する**)**
デバイスIDは、Palo Alto Networksファイアウォールの機能で、デバイス固有の属性（MACアドレス、デバイスタイプ、オペレーティングシステムなど）に基づいてデバイスを識別します。デバイスIDは、複数のポリシータイプで使用でき、きめ細かな制御が可能です。各オプションへの適用方法は以下の通りです。
* オプションA: セキュリティ
* デバイス ID は、セキュリティ ポリシーで使用して、デバイスの種類または ID に基づいてルールを適用できます。
たとえば、特定のデバイス タイプ (IoT デバイスなど) のトラフィックを許可またはブロックするポリシーを作成できます。
* これは正解です。
* オプションB: 復号化
* デバイスIDは復号ポリシーでは使用できません。復号ポリシーは、デバイス属性ではなく、トラフィックの種類、証明書、その他のSSL/TLS属性に基づいて作成されます。
* これは誤りです。
* オプションC: ポリシーベース転送（PBF）
* デバイスIDはPBFポリシーで使用でき、識別されたデバイスに基づいてトラフィックの転送を制御できます。例えば、特定のデバイスタイプからのトラフィックを特定のISPまたはVPNトンネル経由でルーティングできます。
* これは正解です。
* オプションD: SD-WAN
* SD-WANポリシーでは、トラフィックステアリングにパス品質（レイテンシ、ジッターなど）やアプリケーション情報などの指標を使用します。デバイスIDはSD-WANポリシーで使用される基準ではありません。
* これは誤りです。
* オプションE: サービス品質 (QoS)
* デバイスIDはQoSポリシーで使用でき、特定のデバイスに対してトラフィックシェーピングや帯域幅制御を適用できます。例えば、IoTデバイスや特定のエンドポイントから発信されるトラフィックの優先順位付けや帯域幅制限が可能です。
* これは正解です。
参考文献:
* デバイスIDに関するPalo Alto Networksのドキュメント

最新問題: 27
境界ファイアウォールに当てはまる説明を 3 つ選んでください。

A. ネットワークの外側のエッジに対するネットワーク層保護
B. 持続的に500ワット未満の電力使用
C. 柔軟なリソース割り当てによる仮想化データセンターの東西トラフィックのセキュリティ保護
D. 主にネットワークに出入りする南北トラフィックのセキュリティを確保します
E. 外部からの攻撃に対する防御
Answer: A,D,E (メーッセージを残す)
境界ファイアウォールは、従来、ネットワークを外部の脅威から保護するためにネットワークの境界に導入されています。
不正アクセスのブロック、トラフィックフローの検査、機密リソースの保護など、様々な保護機能を提供します。オプションの適用方法は以下の通りです。
* オプションA（正解）：境界ファイアウォールは、ネットワークに出入りするトラフィックを外側のエッジでフィルタリングおよび検査することで、ネットワーク層の保護を提供します。これが境界ファイアウォールの主な役割の一つです。
* オプション B: 電力使用はファイアウォールの機能的またはアーキテクチャ的な側面ではなく、境界ファイアウォールの目的を説明する場合には無関係です。
* オプションC：East-Westトラフィックのセキュリティ保護は、仮想化環境またはセグメント化された環境内におけるトラフィックの横方向（East-West）移動を監視するデータセンターファイアウォールとより密接に関連しています。境界ファイアウォールは、North-Southトラフィックに重点を置きます。
* オプションD（正解）：境界ファイアウォールは主に、ネットワークに出入りするトラフィック（North-Southトラフィック）を保護します。これにより、受信トラフィックと送信トラフィックがセキュリティポリシーに準拠していることが保証されます。
* オプション E (正解): 境界ファイアウォールは、DDoS 攻撃、悪意のある IP トラフィック、その他の不正アクセス試行などの外部攻撃を防ぐ上で重要な役割を果たします。
参考文献:
Palo Alto Networks ファイアウォール展開ユースケース:
https://docs.paloaltonetworks.com North-South トラフィック制御のセキュリティ リファレンス アーキテクチャ。

最新問題**: 28**
システムエンジニア（SE）が、Strata Cloud Manager（SCM）によって管理されるNGFWを企業にデモンストレーションし、成功を収めました。その後の価値実証（POV）計画フェーズにおいて、CISOは、セキュリティポリシーがCritical Security Controls（CSC）などの業界標準をどの程度満たしているか、あるいは満たすべく進んでいるかを示すテスト、そして企業が購入した機能を効果的に活用していることをどのように検証できるかを示すテストを要求しました。
POV テストのタイムライン中に、SE は POV が CISO の要求を満たすことをどのように確認する必要がありますか?

A. 最後に、POV でセキュリティ ライフサイクル レビュー (SLR) を実行し、顧客向けのレポートを作成します。
B. 最初は、顧客と協力して、必要な情報に関するカスタム ダッシュボードとレポートを作成し、顧客の必要に応じてレポートを取得できるようにします。
C. 最後に、顧客は、ベスト プラクティス、CDSS の採用、および NGFW 機能の採用という SCM ダッシュボードから情報を取得します。
D. 最初は、コンプライアンスに準拠し、テスト対象の CDSS サブスクリプションの機能を有効にするように設計された PANhandler ゴールデン イメージを使用します。
Answer: B (メーッセージを残す)
SEはSCMによって管理されるNGFWのデモンストレーションを実施しました。CISOは、POV（セキュリティ監査）による業界標準（CSCなど）への進捗状況の検証と、購入した機能（Advanced Threat PreventionなどのCDSSサブスクリプションなど）の有効活用の検証を求めています。SEは、テスト期間中にPOVが測定可能な証拠を提供できるようにする必要があります。それでは、選択肢を検討してみましょう。
ステップ1: CISOの要求を理解する
* 業界標準 (例: CSC): インターネット セキュリティ センターの重要なセキュリティ コントロール (例: CSC 1: デバイスのインベントリ、CSC 4: 安全な構成) では、可視性、脅威の防止、ポリシーの適用が求められますが、NGFW と SCM はこれらに対応できます。
* 機能の使用率: ライセンスされた機能 (App-ID、脅威防止、URL フィルタリングなど) がアクティブで有効であることを確認します。
* POV 目標: テスト タイムライン内で検証可能な進捗状況と使用率のメトリックを提供します。

最新問題**: 29**
顧客が完了させた評価の利点を示すために、システム エンジニアが使用する必要がある 2 つのツールはどれですか。
A. ベストプラクティス評価 (BPA)
B. セキュリティライフサイクルレビュー (SLR)
C. ファイアウォールのサイズ設定ガイド
D. 黄金の画像
Answer: A,B (メーッセージを残す)
お客様がPalo Alto Networksソリューションの評価を終えた後、評価中に得られた結果とメリットについて詳細な分析を提供することが重要です。最適なツールは以下の2つです。
* なぜ「ベストプラクティスアセスメント（BPA）」なのか（正解）？BPAは、お客様のファイアウォール設定をパロアルトネットワークスが推奨するベストプラクティスに照らし合わせて評価します。セキュリティ体制を強化するために設定を改善できる領域を浮き彫りにします。これは、パロアルトネットワークスのベストプラクティスの導入が業界標準に準拠し、セキュリティパフォーマンスを向上させることを示す優れたツールです。

* なぜ「セキュリティライフサイクルレビュー（SLR）」なのか（正解B）？SLRは、評価中に収集されたデータに基づいて、お客様のセキュリティ環境に関する洞察を提供します。ネットワークで観測された脆弱性、リスク、悪意のあるアクティビティを特定し、パロアルトネットワークスのソリューションがこれらの問題にどのように対処できるかを示します。SLRレポートは、明確なビジュアルと指標を用いて、評価のメリットをよりわかりやすく示します。
* 「ファイアウォール サイジング ガイド」（オプション C）はいかがでしょうか？ファイアウォール サイジング ガイドは、お客様のネットワーク規模、パフォーマンス要件、その他の基準に基づいて適切なファイアウォール モデルを推奨するための販売前ツールです。評価のメリットを示すものではありません。
* 「ゴールデンイメージ」（オプションD）をご利用にならないのはなぜですか？ゴールデンイメージとは、特定のユースケースでファイアウォールを導入するための事前設定済みテンプレートを指します。運用効率の向上には役立ちますが、顧客評価の結果やメリットを示すツールではありません。
参考: ベスト プラクティス アセスメント (BPA) とセキュリティ ライフサイクル レビュー (SLR) に関する Palo Alto Networks のドキュメントでは、評価のメリットを紹介する上でのその役割が確認されています。

最新問題**: 30**
送信された資格情報が有効な企業資格情報であるかどうかを判断するために NGFW が使用する 2 つの方法は何ですか? (2 つ選択してください。)
A. グループマッピング
B. LDAPクエリ
C. ドメイン資格情報フィルター
D. WMIクライアントプローブ
Answer: B,C (メーッセージを残す**)**
* LDAP クエリ (回答 B):
* Palo Alto Networks NGFW は、LDAP ディレクトリ (Active Directory など) を照会して、送信された資格情報が企業ディレクトリと一致するかどうかを検証できます。
* ドメイン資格情報フィルター (回答 C):
* ドメイン資格情報フィルター機能により、送信された資格情報が有効な企業資格情報と照合され、資格情報の不正使用が防止されます。
* なぜAではないのか:
* グループ マッピングは、ポリシー適用のためのユーザー グループを識別するために使用されますが、送信された資格情報は検証しません。
* なぜDではないのか:
* WMI クライアント プローブはユーザー識別に使用されますが、送信された資格情報を検証する方法ではありません。
Palo Alto Networks ドキュメントからの参照:

* 資格情報盗難防止

最新問題: **31**
Policy Optimizer を使用すると、システム エンジニアは NGFW に対して何ができるようになりますか?
A. 新しいポリシー作成に関するベストプラクティスを推奨する
B. クラウド配信セキュリティサービス (CDSS) サブスクリプションとファイアウォールの未使用ライセンスを表示します。
C. 未使用のアプリケーションを含むセキュリティポリシールールを識別する
D. サードパーティベンダーからポリシーをインポートするための移行ツールとして機能する
Answer: C (メーッセージを残す**)**
ポリシーオプティマイザーは、管理者がPalo Alto Networks次世代ファイアウォール（NGFW）におけるセキュリティポリシーの効率性と有効性を向上させるために設計された機能です。未使用または過度に許容されているポリシーを特定し、設定を合理化および最適化することに重点を置いています。
* 「未使用のアプリケーションを含むセキュリティポリシールールを特定する」（正解）理由：Policy Optimizerは既存のセキュリティポリシーを可視化し、未使用または古いアプリケーションを含むルールを特定します。例えば：
* ルールによって使用されなくなったアプリケーションが許可されているかどうかを検出できます。
* 過剰な権限を持つルールを識別し、管理者がルールを調整してセキュリティとパフォーマンスを向上できるようにします。これらの問題に対処することで、ポリシー オプティマイザーは攻撃対象領域を減らし、ファイアウォールの全体的な管理性を向上させます。
* 「新しいポリシー作成に関するベストプラクティスを推奨する」（オプションA）ではダメですか？Policy Optimizerは、新しいポリシーの作成ではなく、既存のポリシーの最適化に重点を置いています。ポリシーの改良時にベストプラクティスを適用することは可能ですが、新しいポリシーの作成を推奨することはPolicy Optimizerの目的ではありません。
* 「クラウド配信型セキュリティサービス（CDSS）サブスクリプションとファイアウォールの未使用ライセンスを表示する」（オプションB）を選択しないのはなぜですか？Policy Optimizerはライセンス管理や追跡には対応していません。未使用ライセンスの特定はPolicy Optimizerの機能範囲外です。
* 「サードパーティベンダーからのポリシーをインポートするための移行ツールとして機能する」（オプションD）はなぜダメなのでしょうか？Policy Optimizerは移行ツールとしては機能しません。Palo Alto Networksはサードパーティ製ファイアウォールの移行ツールを提供していますが、これはPolicy Optimizerの機能とは別です。

最新問題: **32**
Palo Alto Networks AIOps for NGFW の機能と購入オプションを明確に説明している 2 つの文はどれですか (2 つ選択してください)。
A. 商用エディションとエンタープライズ エディションの 2 つのライセンス レベルで提供されます。
B. 無料バージョンとプレミアム バージョンの 2 つのライセンス レベルで提供されます。
C. テレメトリ データを使用して問題を予測、予防、または特定し、機械学習 (ML) を使用してプロセスを調整および強化します。
D. 問題を予測、防止、または特定するためにログ データを Advanced WildFire に転送し、機械学習 (ML) を使用してプロセスを改善し、適応します。
Answer: B,C (メーッセージを残す)
Palo Alto Networks AIOps for NGFW は、テレメトリ データと機械学習 (ML) を活用して、プロアクティブな運用分析情報、ベスト プラクティスの推奨事項、問題の防止を提供するクラウド配信サービスです。
* なぜ 無料版とプレミアム版の 2 つのライセンス層で提供される」のですか (正解 B)。AIOps for NGFW は次の 2 つの層で利用できます。
* 無料レベル: 追加費用なしで、基本的な運用上の洞察とベスト プラクティスを提供します。
* プレミアム レベル: AI を活用した予測、プロアクティブな問題防止、強化された ML ベースの推奨事項などの高度な機能を提供します。
* テレメトリデータを用いて問題を予測、予防、または特定し、機械学習（ML）を用いてプロセスを調整・強化する」（正解C）理由は何ですか？AIOpsは、NGFWからのテレメトリデータを用いて運用傾向を分析し、潜在的な問題を予測し、問題が発生する前に解決策を提案します。MLは、実世界のデータから学習することでこれらの洞察を継続的に洗練させ、時間の経過とともに精度と有効性を高めます。
* 商用エディションとエンタープライズ エディションの 2 つのライセンス レベルで提供されます」(オプション A) ではダメですか? これは誤りです。AIOps のライセンス モデルは、 商用」エディションと 「エンタープライズ」エディションではなく、 無料」および 「プレミアム」レベルに基づいているためです。
* 問題を予測、防止、または特定するためにログデータをAdvanced WildFireに転送し、機械学習（ML）を使用してプロセスを改善し、適応させる」（オプションD）ではダメなので

しょうか？AIOpsはAdvanced WildFireに依存しません。代わりに、NGFWから直接テレメトリデータを取得し、運用およびセキュリティ分析を実行します。
参考: NGFW 向け AIOps に関する Palo Alto Networks のドキュメントでは、その機能とライセンス構造が確認されています。

最新問題: **33**
顧客が完了させた評価の利点を示すために、システム エンジニアが使用する必要がある 2 つのツールはどれですか。
A. ベストプラクティス評価 (BPA)
B. セキュリティライフサイクルレビュー (SLR)
C. ファイアウォールのサイズ設定ガイド
D. 黄金の画像
Answer: A,B (メーッセージを残す**)**
お客様がPalo Alto Networksソリューションの評価を終えた後、評価中に得られた結果とメリットについて詳細な分析を提供することが重要です。最適なツールは以下の2つです。
* なぜ「ベストプラクティスアセスメント（BPA）」なのか（正解A）？BPAは、お客様のファイアウォール設定をパロアルトネットワークスが推奨するベストプラクティスに照らし合わせて評価します。セキュリティ体制を強化するために設定を改善できる領域を浮き彫りにします。これは、パロアルトネットワークスのベストプラクティスの導入が業界標準に準拠し、セキュリティパフォーマンスを向上させることを示す優れたツールです。
* なぜ「セキュリティライフサイクルレビュー（SLR）」なのか（正解B）？SLRは、評価中に収集されたデータに基づいて、お客様のセキュリティ環境に関する洞察を提供します。ネットワークで観測された脆弱性、リスク、悪意のあるアクティビティを特定し、パロアルトネットワークスのソリューションがこれらの問題にどのように対処できるかを示します。SLRレポートは、明確なビジュアルと指標を用いて、評価のメリットをよりわかりやすく示します。
* 「ファイアウォール サイジング ガイド」（オプション C）はいかがでしょうか？ファイアウォール サイジング ガイドは、お客様のネットワーク規模、パフォーマンス要件、その他の基準に基づいて適切なファイアウォール モデルを推奨するための販売前ツールです。評価のメリットを示すものではありません。
* 「ゴールデンイメージ」（オプションD）をご利用にならないのはなぜですか？ゴールデンイメージとは、特定のユースケースでファイアウォールを導入するための事前設定済みテンプレートを指します。運用効率の向上には役立ちますが、顧客評価の結果やメリットを示すツールではありません。

最新問題: **34**
鉱業会社に所属するシステムエンジニア（SE）の取り組みがきっかけとなり、同社は危険な状況下でロボットや遠隔操作車両を使用するオペレーションに革新的な設計を取り入れる取り組みの一環として、パロアルトネットワークスに関心を示しました。ディスカバリー

コールの結果、同社は制御プログラムを実行するクラウドベースのアプリケーションに接続する無線塔を用いて、プライベートモバイルネットワーク経由で機械への制御信号を受信する予定であることが確認されました。
SE が推奨すべき 2 つのソリューション セットはどれですか?
A. 5G セキュリティを有効にして設計し、オンサイト マシンに送信されるコマンドでクラウド コンピューティングが侵害されないようにする。
B. クラウドベースのアプリケーションを、それをホストするクラウド サービス プロバイダーへの外部アクセスから保護するために、クラウド NGFW を組み込むこと。
C. マシンの可視性を確保し、ネットワークに接続された他のデバイスが識別され、リスクと動作のプロファイルが与えられるようにするために、IoT セキュリティを組み込むこと。
D. 設計に高度な保護を確実に適用するために、高度な CDSS バンドル (高度な脅威防止、高度な WildFire、および高度な URL フィルタリング) を調達します。
Answer: (解答を表示する**)**
* 5Gセキュリティ（回答A）：
* このシナリオでは、マイニング会社は、ロボットや車両の制御に低遅延と高帯域幅を確保するために 5G テクノロジーを活用したプライベート モバイル ネットワークで運営されます。
* Palo Alto Networks 5G Securityは、プライベートモバイルネットワークを保護するために特別に設計されています。5Gインフラストラクチャの脆弱性を悪用されるのを防ぎ、マシンに送信される制御信号が攻撃者によって侵害されないようにします。
* 主な機能には、ネットワーク スライシング保護、シグナリング プレーンのセキュリティ、安全なユーザー プレーン通信などがあります。
* IoTセキュリティ（回答C）：
* マイニング作業は、IoT デバイスである機械や遠隔操作車両に依存します。
* Palo Alto NetworksIoTセキュリティは以下を提供します:
* すべての IoT デバイス (ロボット、リモート車両、センサーなど) を検出するための完全なデバイス可視性。
* リスクプロファイルを作成し、機械の動作における異常を特定するための動作分析。
* これにより、IoT デバイスの安全な環境が確保され、デバイスが悪用されるリスクが軽減されます。
* クラウド NGFW を使用しない理由 (回答 B):
* クラウド NGFW はクラウドベースのアプリケーションを保護するために重要ですが、ここでの具体的な懸念事項は、クラウド サービスへの外部アクセスではなく、制御信号と IoT デバイスの保護です。
* プライベート モバイル ネットワークと IoT デバイスの保護要件により、5G セキュリティと IoT セキュリティの重要性が高まります。
* アドバンスド CDSS バンドルを選ばない理由 (回答 D):
* Advanced CDSS バンドル (Advanced Threat Prevention、Advanced WildFire、Advanced URL Filtering) は、Web トラフィックのセキュリティ保護と脅威の検出に不可欠ですが、プ

ライベート モバイル ネットワークや IoT デバイスのセキュリティ保護に関する特定の課題には対処していません。
* これらのサービスは設計を補完できますが、このユースケースでは主な焦点ではありません。
Palo Alto Networks ドキュメントからの参照:
* プライベートモバイルネットワーク向け5Gセキュリティ
* IoTセキュリティソリューション概要
* クラウド NGFW の概要

最新問題: **35**
セキュリティ エンジニアは、会社のオンプレミス Web サーバーの保護を任されていますが、Web アプリケーション ファイアウォール (WAF) を購入する権限がありません。
どの Palo Alto Networks ソリューションが、SQL インジェクション ゼロデイ、コマンド インジェクション ゼロデイ、クロスサイト スクリプティング (XSS) 攻撃、IIS エクスプロイトから企業を保護しますか?
A. 脅威防止とPAN-OS 11.x
B. 高度な脅威対策とPAN-OS 11.x
C. 脅威防止、高度な URL フィルタリング、PAN-OS 10.2 (およびそれ以降)
D. 高度な WildFire および PAN-OS 10.0 (およびそれ以降)
Answer: B (メーッセージを残す**)**
SQLインジェクション、コマンドインジェクション、XSS攻撃、IISエクスプロイトといった高度な脅威からWebサーバーを保護するには、ディープパケットインスペクション、行動分析、そしてゼロデイ攻撃のインライン防御機能を備えたソリューションが必要です。最も効果的なソリューションは、PAN-OS 11.xと組み合わせたAdvanced Threat Prevention (ATP)です。
* 「Advanced Threat Prevention と PAN-OS 11.x」（正解）を選ぶ理由：Advanced Threat Prevention（ATP）は、インラインディープラーニングモデルを用いてSQLインジェクション、コマンドインジェクション、XSS攻撃などの高度なゼロデイ脅威を検出・ブロックすることで、従来の脅威防御を強化します。PAN-OS 11.xでは、ATPの検出機能が拡張され、シグネチャベースの手法に依存せずに未知のエクスプロイトを検出できます。この機能は、専用のWAFが利用できないシナリオにおいてWebサーバーを保護するために不可欠です。
ATP には次のような利点があります。
* ディープラーニング モデルを使用したゼロデイ脅威のインライン防止。
* SQL インジェクションや XSS などの攻撃をリアルタイムで検出します。
* IIS などの Web サーバー プラットフォームの保護が強化されました。
* Palo Alto Networks 次世代ファイアウォール (NGFW) との完全な統合。
* 「脅威対策とPAN-OS 11.x」（オプションA）を選ばない理由は何ですか？脅威対策は、既知の脅威に対して主にシグネチャベースの検出に依存しています。基本的な保護機能は提供しますが、インラインディープラーニングなどの高度な手法を用いてゼロデイ攻撃をブ

ロックする機能は備えていません。ゼロデイSQLインジェクション攻撃やXSS攻撃に対しては、脅威対策だけでは不十分です。
* 「脅威防御、高度なURLフィルタリング、PAN-OS 10.2以降」(オプションC)を選択しないのはなぜですか？この組み合わせには、エクスプロイトに関連する悪意のあるURLをブロックするのに便利な高度なURLフィルタリングが含まれていますが、依然としてシグネチャベースの脅威防御に依存しています。この組み合わせでは、高度なインジェクション攻撃やXSS脆弱性に対するゼロデイ保護は提供されません。
* 「Advanced WildFireとPAN-OS 10.0 およびそれ以上)」(オプションD)をお勧めしません。Advanced WildFireは、サンドボックス環境でファイルと実行ファイルを分析してマルウェアを特定することに重点を置いています。マルウェアの特定には優れていますが、Webベースのインジェクション攻撃やWebサーバーを標的としたXSSエクスプロイトに対するインライン防御を提供するようには設計されていません。
参考：Palo Alto Networks Advanced Threat Preventionのドキュメントでは、インライン機械学習と行動分析を活用し、ゼロデイインジェクション攻撃やWebベースのエクスプロイトをブロックする機能が強調されています。これは、説明されているシナリオに最適なソリューションです。

最新問題: **36**
高度な DNS セキュリティに加えて、インライン機械学習 (ML) を活用している 3 つのクラウド配信セキュリティ サービス (CDSS) サブスクリプションはどれですか (3 つ選択してください)。
A. エンタープライズ DLP
B. 高度なURLフィルタリング
C. 高度なワイルドファイア
D. 高度な脅威防止
E. IoTセキュリティ
Answer: A,B,D (メーッセージを残す**)**
この疑問に答えるために、クラウド配信型セキュリティサービス（CDSS）の各サブスクリプションと、インライン機械学習（ML）におけるその役割を分析してみましょう。Palo Alto Networksは、複数のサブスクリプションにまたがるインラインML機能を活用することで、高度な脅威に対するリアルタイム保護を提供し、手動介入の必要性を軽減しています。
A: エンタープライズDLP（データ損失防止）
エンタープライズDLPは、機密データの漏洩を防ぐクラウド配信型のセキュリティサービスです。インライン機械学習を活用し、従来のデータパターンやシグネチャでは検出できない機密情報も、リアルタイムで正確に識別・分類します。このサービスはPalo Altoファイアウォールとシームレスに統合されており、ファイアウォールを通過する際にコンテンツを理解することで、データ漏洩のリスクを軽減します。
B: 高度なURLフィルタリング

高度なURLフィルタリングは、インライン機械学習を用いて悪意のあるURLをリアルタイムでブロックします。静的データベースに依存する従来のURLフィルタリングソリューションとは異なり、Palo Alto Networksの高度なURLフィルタリングは、機械学習を活用して、静的データベースにまだ分類されていない新しい悪意のあるURLを識別し、ブロックします。
このプロアクティブなアプローチにより、組織はフィッシングやマルウェアをホスティングする Web サイトなどの新たな脅威から保護されます。
C: 高度な山火事
Advanced WildFire は、ゼロデイマルウェアを検出して防止するように設計されたクラウドベースのサンドボックス ソリューションです。
Advanced WildFireはPalo Alto Networksのセキュリティ製品の重要な一部ですが、インライン機械学習ではなく、主に静的および動的分析を使用します。Advanced WildFireの機械学習ベースの分析は、ファイルがクラウドに送信されて処理された後にインラインで行われるため、この質問の範囲には該当しません。
D: 高度な脅威防止
Advanced Threat Prevention (ATP) は、インライン機械学習を用いてトラフィックをリアルタイムで分析し、未知のコマンドアンドコントロール (C2) トラフィックなどの高度な脅威をブロックします。このサービスは、従来の侵入防止システム (IPS) のアプローチに代わるものであり、ネットワークトラフィックをアクティブに分析し、悪意のあるペイロードをインラインでブロックします。このインライン機械学習機能により、ATP は難読化や回避技術を利用する脅威を確実に検知 ･ブロックできます。
E: IoTセキュリティ
IoTセキュリティは、ネットワークに接続されたIoTデバイスの検出と管理に重点を置いています。このサービスは、デバイスの挙動プロファイリングと異常検知に機械学習を活用していますが、リアルタイムのトラフィック検査にはインライン機械学習を活用していません。その代わりに、可視性を提供し、デバイスのリスクを特定することで、より一般的なレベルで動作します。
重要なポイント:
* エンタープライズ DLP、高度な URL フィルタリング、高度な脅威防止はすべて、インライン機械学習を利用してリアルタイムの保護を提供します。
* Advanced WildFire は ML を使用しますが、インラインではなく、クラウドで分析が実行されます。
* IoT セキュリティでは、インライン脅威検出ではなく、デバイス管理に ML を適用します。

最新問題**: 37**
Policy Optimizer を使用すると、システム エンジニアは NGFW に対して何ができるようになりますか?
A. 新しいポリシー作成に関するベストプラクティスを推奨する

B. クラウド配信セキュリティサービス (CDSS) サブスクリプションとファイアウォールの未使用ライセンスを表示します。
C. 未使用のアプリケーションを含むセキュリティポリシールールを識別する
D. サードパーティベンダーからポリシーをインポートするための移行ツールとして機能する
Answer: C (メーッセージを残す)
ポリシーオプティマイザーは、管理者がPalo Alto Networks次世代ファイアウォール（NGFW）におけるセキュリティポリシーの効率性と有効性を向上させるために設計された機能です。未使用または過度に許容されているポリシーを特定し、設定を合理化および最適化することに重点を置いています。
* 「未使用のアプリケーションを含むセキュリティポリシールールを特定する」（正解）理由：Policy Optimizerは既存のセキュリティポリシーを可視化し、未使用または古いアプリケーションを含むルールを特定します。例えば：
* ルールによって使用されなくなったアプリケーションが許可されているかどうかを検出できます。
* 過剰な権限を持つルールを識別し、管理者がルールを調整してセキュリティとパフォーマンスを向上できるようにします。これらの問題に対処することで、ポリシー オプティマイザーは攻撃対象領域を減らし、ファイアウォールの全体的な管理性を向上させます。
* 「新しいポリシー作成に関するベストプラクティスを推奨する」（オプションA）ではダメですか？Policy Optimizerは、新しいポリシーの作成ではなく、既存のポリシーの最適化に重点を置いています。ポリシーの改良中にベストプラクティスを適用することは可能ですが、新しいポリシーの作成を推奨することはPolicy Optimizerの目的ではありません。
* 「クラウド配信型セキュリティサービス（CDSS）サブスクリプションとファイアウォールの未使用ライセンスを表示する」（オプションB）を選択しないのはなぜですか？Policy Optimizerはライセンス管理や追跡には対応していません。未使用ライセンスの特定はPolicy Optimizerの機能範囲外です。
* 「サードパーティベンダーからのポリシーをインポートするための移行ツールとして機能する」（オプションD）はなぜダメなのでしょうか？Policy Optimizerは移行ツールとしては機能しません。Palo Alto Networksはサードパーティ製ファイアウォールの移行ツールを提供していますが、これはPolicy Optimizerの機能とは別です。
参考: Palo Alto Networks Policy Optimizer のドキュメントでは、未使用または過度に広範なポリシー ルールを識別してファイアウォール構成を最適化するという主な機能が強調されています。

最新問題: **38**
PAN-OSのバージョンアップを行っている顧客のCIOは、「問題を発見し、サポート担当者と連携するには専門知識が必要ですが、運用チームはその専門知識を、ビジネスにとってより重要な業務に活用できます」と述べています。このアップグレードプロジェクトは、既存のNGFWの限界を示す適切なツールがなかったため、急いで開始されました。

Palo Alto Networks チームによる 2 つのアクションのうち、顧客に長期的なソリューションを提供するものはどれですか? (2 つ選択してください。)
A. 運用チームに、無料の機械学習を活用した NGFW ツール用の AIOps の使用を推奨します。
B. 運用チームがファイアウォールの作業について十分な情報を得て自信を持てるように、提案にトレーニングを含めることを提案します。
C. PAN-OS のアップグレードによって得られる新しい強化されたセキュリティ機能によって、アップグレードと容量に関する将来の問題が解決されることを CIO に通知します。
D. 既存のテクノロジー内で企業の問題に対処するために、Strata Cloud Manager (SCM) 内で AIOps Premium を提案します。
Answer: (解答を表示する**)**
お客様のCIOは、2つの主要な問題点を指摘しています。(1) 運用チームにはPAN-OSのアップグレードとサポート業務を効率的に管理するための専門知識が不足しており、重要な業務から注意が逸れています。(2) NGFWの容量を監視するツールが不足していたため、急いでアップグレードを実施せざるを得ませんでした。目標は、Palo Alto NetworksのStrataハードウェアファイアウォール向けソリューションを活用した長期的なソリューションを推奨することです。オプションBとD $trata Cloud Manager (SCM) 内のトレーニングとAIOps Premium）は、チームの能力を強化し、プロアクティブな管理ツールを提供することで、これらの問題に対処します。以下は、公式ドキュメントに基づいて検証された詳細な説明です。
ステップ1：顧客の課題を分析する
* 専門知識のギャップ :CIOは、問題を特定しサポートを提供するには、運用チームが十分に備えていない、または優先的に対応できない専門知識が必要であると指摘しています。Strata NGFW上のPAN-OSのアップグレードには、バージョン互換性チェック、アップグレード前の検証、トラブルシューティングといったタスクが含まれており、PAN-OSのツールとプロセスに関する知識が求められます。
* 容量の可視性: 急いでアップグレードを行ったのは、NGFW の容量 (CPU、メモリ、セッション制限など) が近づいていることを知らなかったためであり、監視や予測分析が不足していることを示しています。
長期的なソリューションでは、Palo Alto Networks の Strata ファイアウォールのエコシステムに合わせて、運用効率とプロアクティブな容量管理の両方に対処する必要があります。

最新問題: **39**
システム エンジニアは、高度な URL フィルタリングを使用してランサムウェアの URL から顧客を保護するために、どのカテゴリをブロックするプロファイルを作成する必要がありますか?
A. ランサムウェア

B. 高リスク
C. スキャンアクティビティ
D. コマンドとコントロール
Answer: A (メーッセージを残す**)**
Palo Alto Networks ファイアウォールで高度な URL フィルタリングを構成する場合は、ランサムウェア活動に関連する URL から顧客を保護するために、「ランサムウェア」カテゴリを明示的にブロックする必要があります。
ランサムウェアのURLには通常、ユーザーデータを暗号化して身代金を要求する悪意のあるコードやスクリプトがホストされています。「ランサムウェア」カテゴリをブロックすることで、システムエンジニアはユーザーがそのようなURLにアクセスするのを事前に防ぐことができます。
* なぜ「ランサムウェア」なのでしょうか (正解 A)? 「ランサムウェア」カテゴリは、ランサムウェアを配信したり、ランサムウェア操作をサポートしたりすることが知られている URL を含めるために、Palo Alto Networks によって特別にキュレーションされています。
このカテゴリをブロックすると、このリストに分類される URL にエンドユーザーがアクセスできなくなり、ランサムウェア攻撃のリスクが大幅に軽減されます。
* 「高リスク」オプションB）を選択しない理由：「高リスク」カテゴリには潜在的に悪意のあるサイトが含まれますが、対象範囲が広く、対象が限定されています。ランサムウェア特有のURLを必ずしもブロックできるとは限りません。「高リスク」には、評判の悪さや悪意のあるコンテンツのホスティングといった要因に基づいてフラグが付けられた幅広いウェブサイトが含まれます。「ランサムウェア」カテゴリほど対象が絞られていません。
* 「スキャンアクティビティ」オプションC）ではダメなのはなぜですか？「スキャンアクティビティ」カテゴリは、攻撃者による脆弱性スキャン、自動プロービング、または偵察に使用されるURLに焦点を当てています。このようなアクティビティはランサムウェア攻撃の前兆となる可能性がありますが、ランサムウェアのURLを直接ブロックするものではありません。
* 「コマンド＆コントロール」オプションD）ではダメなのはなぜですか？「コマンド＆コントロール」カテゴリは、マルウェアや侵害されたシステムが攻撃者との通信に使用するURLをブロックするように設計されています。一部のランサムウェアはコマンド＆コントロール（C2）サーバーを利用する場合がありますが、C2 URLのみをブロックしても、ランサムウェアのURL自体を直接ブロックすることはできません。
高度な URL フィルタリング プロファイルを使用し、「ランサムウェア」カテゴリをブロックすることにより、ファイアウォールはターゲットを絞った制御を適用し、ランサムウェア固有の脅威を軽減します。
参考：パロアルトネットワークスの高度なURLフィルタリングに関するドキュメントでは、「ランサムウェア」カテゴリは、ランサムウェアの脅威を防ぐための推奨されるベストプラクティスです。