PaloAltoNetworks.NetSec-Pro-JPN.v2026-09-21.q35

試験コード： NetSec-Pro-JPN
試験名称： Palo Alto Networks Network Security Professional (NetSec-Pro日本語版)
認証ベンダー： Palo Alto Networks
無料問題の数： 35
バージョン： v2026-09-21
ページの閲覧量 :104
問題集の閲覧量 :354
https://www.jpnshiken.com/shiken/PaloAltoNetworks.NetSec-Pro-JPN.v2026-09-21.q35.html

質問: **1**
モバイル ユーザー トラフィックの Prisma Access 脅威ログを確認できるアプリケーションはどれですか (2 つ選択してください)。
A. Prisma Cloud ダッシュボード
B. Strata Cloud Manager (SCM)
C. Strataロギングサービス
D. サービス接続ファイアウォール
正解: **(**正解を表示します**)**
Threat logs for Prisma Access mobile users can be reviewed in both Strata Cloud Manager (SCM) and Strata Logging Service. Prisma Cloud and service connection firewalls are not directly tied to mobile user traffic logs.
Prisma Access logs are available in the Strata Cloud Manager and can also be sent to the Strata Logging Service for detailed analysis and threat visibility.

質問: **2**
Prisma Access で使用できるゾーンはどれですか?
A. クライアントレスVPN
B. インターゾーン
C. イントラゾーン
D. DMZ
正解: **(**正解を表示します**)**
In Prisma Access, the interzone security policy rule is available and plays a crucial role in controlling traffic between zones.
You can configure an interzone rule to control traffic that flows between different zones in Prisma Access, enabling granular security policy enforcement.
This ensures comprehensive control of traffic crossing security boundaries in the cloud-delivered architecture.

質問: **3**

AWS 用の Cloud NGFW を構成するために使用できるツールはどれですか (2 つ選択してください)。
A. コルテックス XSIAM
B. Prisma Cloud 管理コンソール
C. パノラマ
D. クラウドサービスプロバイダーの管理コンソール
正解: **(**正解を表示します**)**
Cloud NGFW for AWS can be configured using Panorama for centralized management, as well as the AWS management console for native integration and configuration.
You can configure Cloud NGFW for AWS using Panorama for centralized security management, or directly through the AWS management console to deploy and manage security services for your AWS resources.

質問: **4**
ネットワークセキュリティエンジニアは、Strata Logging Service のデータをセキュリティオペレーションセンター (SOC) が使用するツールに転送し、詳細な調査を行いたいと考えています。これは、Palo Alto Networks Zero Trust のどのベストプラクティスステップに当てはまりますか？
A. トランザクションのマッピングと検証
B. 実装
C. 標準と設計
D. レポートとメンテナンス
正解: **D (**コメントを発表する**)**
The "Report and Maintenance" step of the Zero Trust model emphasizes ongoing monitoring, analysis, and reporting to ensure the environment remains secure over time.
The Report and Maintenance phase includes continuous monitoring, log forwarding, and sharing of security telemetry to third-party tools to maintain and validate Zero Trust implementation.
By forwarding logs to SOC tools, the engineer ensures comprehensive visibility and proactive threat hunting.

質問: **5**
NGFW のどのコンポーネントがアクティブ/パッシブ設計ではサポートされますが、アクティブ/アクティブ設計ではサポートされませんか?
A. 単一のフローティングIPアドレス
B. DHCPクライアントの使用
C. ルートベースの冗長性
D. レイヤ3でのARP負荷分散の設定
正解: **A (**コメントを発表する**)**

Single floating IP address (also known as a floating IP or shared IP) is supported only in an active/passive HA pair. In active/active HA, both firewalls are forwarding traffic simultaneously and thus do not share a single floating IP.
In active/passive HA, a single floating IP address is used for seamless failover.
Active/active HA requires separate IP addresses and does not support a single floating IP.
This simplifies failover in active/passive deployments by using a single shared IP that moves to the active peer upon failover.

質問: **6**
永続的な VM シリーズ ファイアウォールをフレキシブル VM に移行するための展開プロファイルを作成するときに必要な 2 つの構成はどれですか。(2 つ選択してください。)
A. 構成タイプとして 固定 vCPU モデル」を選択します。
B. 永続 VM と同じ数の vCPU を割り当てます。
C. 永続 VM と同じセキュリティ サービスのみを許可します。
D. 管理用に仮想 Panorama を展開します。
正解: **(**正解を表示します**)**
When migrating from a perpetual VM-Series firewall license to a flexible VM licensing model, two critical steps are needed:
Allocate same number of vCPUs ?This ensures that the VM-Series capacity remains consistent and avoids resource bottlenecks.
When migrating perpetual VM-Series licenses to flexible VM licensing, allocate the same vCPU and memory resources to ensure equivalent performance.
Limit to same security services ?Flexible licensing requires maintaining the same security services to preserve licensing compliance.
Ensure that you allow only the same security services on the flexible VM instance as were licensed on the perpetual VM.

質問: **7**
Cloud NGFW のセキュリティポリシーを作成するときに、AWS マネジメントコンソールでポリシーはどのように評価されますか?
A. 管理者はルールの順序を設定して、評価される順序を決定します。
B. 評価中にスタック内を上下にドラッグできます。
C. 管理者はルールの優先度を設定して、ルールが評価される順序を決定します。
D. 評価される順序で作成する必要があります。
正解: **(**正解を表示します**)**
Cloud NGFW Security Policies in the AWS Console are evaluated in the exact creation order ?they do not have explicit rule priority fields.
In AWS, security rules are evaluated in the order they are created. To ensure the correct evaluation logic, create them in the desired order from top to bottom.

Unlike Panorama, AWS-native management of Cloud NGFWs uses creation order as the evaluation sequence.

質問: **8**
ファイアウォール管理者は、最も時間効率の高い方法で 300 個の一意の URL のリストをブロックするにはどうすればよいでしょうか。
A. アプリケーション フィルターを使用して App-ID をブロックします。
B. アプリケーション グループを使用して App-ID をブロックします。
C. リストをカスタム URL カテゴリにインポートします。
D. 複数の定義済み URL カテゴリをブロックします。
正解: **(**正解を表示します**)**
For large lists of specific URLs, creating a custom URL category and importing the list is the most efficient approach for granular URL filtering.
You can create custom URL categories to define specific URLs or patterns and enforce policies for these categories. This is the most efficient way to handle large sets of URLs. This approach saves time compared to manual rule creation or using generic application filters.

質問: **9**
セグメント化されたネットワーク アーキテクチャ全体でユーザー エクスペリエンスを最適化し、ブランチとキャンパス間の安全な接続を維持するための最も効果的な方法を実装するアクションはどれですか。
A. 各ブランチおよびキャンパス ファイアウォールにサイト間トンネルを確立し、各部門に個別の VLAN を用意します。
B. すべてのブランチおよびキャンパス ファイアウォールを単一の共有ブロードキャスト ドメインを使用するように構成します。
C. ネットワーク パフォーマンス メトリックに基づいてすべてのトラフィックをルーティングし、ゾーン保護プロファイルを使用するように SD-WAN を実装します。
D. すべてのブランチ トラフィックのルーティングを処理するために単一のキャンパス ファイアウォールを構成します。
正解: **(**正解を表示します**)**
SD-WAN solutions optimize application experience and provide secure, dynamic connectivity across distributed locations by leveraging real-time path metrics (latency, jitter, loss).
By implementing SD-WAN, traffic is routed intelligently based on real-time network performance metrics. Zone protection profiles ensure security while maximizing application performance.
Key advantage:
Secure connectivity and best user experience across campuses and branches.

質問: **10**
悪意のあるドメインや誤って構成されたドメインから保護するための NGFW セキュリティ ポリシーの構成に必要な 2 つのセキュリティ サービスはどれですか (2 つ選択してください)。
A. 高度な脅威防止
B. SaaS セキュリティ
C. 高度なワイルドファイア
D. 高度なDNSセキュリティ
正解: **A,D (**コメントを発表する**)**
Protecting against malicious and misconfigured domains requires two critical services:
Advanced Threat Prevention
Provides signature-based and advanced analysis to identify threats, including DNS-based attacks.
Advanced Threat Prevention enables the NGFW to detect and prevent exploits and malware- based communications, including those leveraging DNS.
Advanced DNS Security
Specifically designed to detect and sinkhole malicious and misconfigured DNS queries.
DNS Security uses real-time intelligence to block DNS-based threats, protect against data exfiltration, and automatically sinkhole suspicious domain lookups.
By combining these services in security policies, NGFWs ensure robust protection against domain- based threats and misconfigurations.

質問: **11**
Strata Logging Service は、Prisma Access を使用している企業の増え続けるログ保持ニーズをどのように解決しますか?
A. ログの分散収集と保存により、復元力が向上します。
B. 物理データ ストレージ領域の自動選択により、導入時間が短縮されます。
C. ビジネスの成長に合わせて、新しい場所の容量ニーズに合わせて拡張できます。
D. Prisma Access 用に購入したライセンス帯域幅を使用してトラフィックをログに記録すると、オーバーヘッドが削減されます。
正解: **(**正解を表示します**)**
The Strata Logging Service offers scalable log storage to accommodate data growth, which ensures organizations can retain logs for compliance and threat hunting as their environments expand.
The Strata Logging Service is designed to scale dynamically to accommodate growing log retention needs, allowing enterprises to maintain comprehensive visibility as they expand their network footprint.

質問: **12**

Prisma Access データ プレーン ソフトウェアのアップグレード中に継続性とセキュリティを維持するために最も効果的な手順はどれですか?
A. 構成をバックアップし、オフピーク時にアップグレードをスケジュールし、ネットワーク全体への展開を試みることなく段階的なアプローチを使用します。
B. Strata Cloud Manager (SCM) を使用して、すべての場所で動的なアップグレードを自動的かつ同時に実行し、ネットワーク全体の均一性を確保します。
C. 競合を防ぐためにアップグレード中はすべてのセキュリティ機能を無効にし、完了後にスムーズなロールアウト プロセスを確保するために再度有効にします。
D. アップグレードを営業時間のピーク時に実行し、ユーザーから報告された問題に迅速に対応し、ロールアウト後にすぐにトラブルシューティングできるようにします。
正解: **(**正解を表示します**)**
To minimize disruptions, it is recommended to perform Prisma Access upgrades during non- business hours and in a phased manner, starting with less critical sites to validate the process before moving to critical locations. Backup configurations and validate the system's readiness to avoid data loss and maintain service continuity.

質問: **13**
SSL インバウンド インスペクションが有効な場合、ファイアウォールはどのように動作しますか?
A. クライアントと内部サーバー間で透過的に動作します。
B. 受信および送信の SSH 接続を復号化します。
C. クライアントと外部サーバー間のトラフィックを復号化します。
D. クライアントと内部サーバー間の仲介者として機能します。
正解: **D (**コメントを発表する**)**
SSL Inbound Inspection allows the firewall to decrypt incoming encrypted traffic to internal servers (e.g., web servers) by acting as a man-in-the-middle (MITM). The firewall uses the private key of the server to decrypt the session and apply security policies before re-encrypting the traffic.
SSL Inbound Inspection requires you to import the server's private key and certificate into the firewall. The firewall then acts as a man-in-the-middle (MITM) to decrypt inbound sessions from external clients to internal servers for inspection.

質問: **14**
Panorama から次世代ファイアウォールにプッシュできるコンテンツ更新は 2 つありますか? (2 つ選択してください。)
A. 高度なURLフィルタリング
B. アプリケーションと脅威
C. ワイルドファイア
D. GlobalProtectデータファイル
正解: **B,C (**コメントを発表する**)**

Applications and threats
Panorama can push application and threat signature updates to managed firewalls, ensuring consistent application and threat visibility.
Panorama uses dynamic updates to distribute the latest application and threat signature packs to all managed firewalls.
WildFire
Panorama also distributes WildFire signature updates to firewalls for real-time malware detection.
WildFire updates provide the latest malware signatures to enhance detection and prevention, and can be deployed to all managed firewalls via Panorama.

質問: **15**
IoT セキュリティを機能させるには、どの 2 種類のログを Strata Logging Service に転送する必要がありますか?
（2つ選択してください。）
A. ワイルドファイア
B. 強化されたアプリケーション
C. 脅威
D. URLフィルタリング
正解: **B,C (**コメントを発表する**)**
For IoT Security to accurately classify and monitor IoT devices, the following logs must be forwarded to Strata Logging Service:
Enhanced application logs - provide detailed application usage and behaviors, essential for profiling device types and roles.
Enhanced Application logs provide additional context on IoT device behavior and usage patterns, and must be forwarded to Strata Logging Service for IoT Security to build accurate Device-ID profiles.
Threat logs - essential for detecting suspicious or malicious activities by IoT devices.
Threat logs are critical for identifying potential exploits or suspicious activities involving IoT devices and are required for accurate threat visibility within IoT Security.
These logs collectively ensure accurate device classification and real-time threat visibility.

質問: **16**
SSL受信検査が有効になっている場合、ファイアウォールはどのように動作しますか？
A. 受信および送信の SSH 接続を復号します。
B. クライアントと外部サーバー間の通信を復号します。
C. クライアントと内部サーバーの間で透過的に動作します。
D. クライアントと内部サーバーの間で、仲介役として機能します。
正解: **(**正解を表示します**)**

有効的な**NetSec-Pro-JPN**問題集はJPNTest.com提供され、**NetSec-Pro-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**NetSec-Pro-JPN**試験問題集を提供します。JPNTest.com NetSec-Pro-JPN試験問題集はもう更新されました。ここで**NetSec-Pro-JPN**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/NetSec-Pro-JPN-mondaishu 　**126**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
ネットワークセキュリティエンジニアがPrisma Accessでセキュリティポリシーを作成しましたが、そのポリシーには送信元アドレスにネゲートリージョンが含まれています。ネゲートリージョンによる接続の損失を防ぐには、どのような構成が適切でしょうか？
A. サービスをアプリケーションのデフォルトに設定します。
B. 宛先アドレスが &any」である否定されたリージョンのセキュリティ ポリシーを作成します。
C. セキュリティ ポリシーに動的アプリケーション グループを追加します。
D. プライベート IP アドレスを含むすべてのリージョンを送信元アドレスに追加します。
正解: **(**正解を表示します**)**
Negated source addresses exclude traffic from the specified region. To avoid accidental connectivity loss for traffic from that region, create a separate Security policy to explicitly permit it.
When you use a negated region in a Security policy rule, ensure to create an additional Security policy to permit traffic from the excluded (negated) region to avoid unintentional drops.

質問: **18**
どのサブスクリプションが、データ フィルタリング プロファイルの基準に一致するファイル形式ベースではないトラフィックをクラウド サービスに送信して判定を下しますか。
A. エンタープライズ DLP
B. 高度なURLフィルタリング
C. SaaS セキュリティ インライン
D. 高度なWildFire
正解: **(**正解を表示します**)**
Enterprise DLP uses cloud analysis to inspect and classify sensitive data in non-file-based formats (e.g., in-line data streams, SaaS communications).
Enterprise DLP inspects data in non-file-based traffic flows, forwarding suspicious data patterns to the cloud for classification and verdicts.
The other services focus on file-based scanning (WildFire), URL access control (Advanced URL Filtering), or inline SaaS application controls (SaaS Security Inline).

質問: **19**
VM シリーズ ファイアウォールでセキュリティ ポリシーを構成する場合、どのアクション セットが最も包括的なセキュリティ ポリシーの適用を保証しますか?
A. ポートベースのポリシーを構成し、脅威ログを毎週チェックし、ソフトウェアの更新を毎年実施し、復号化を有効にします。
B. User-ID と App-ID を使用してポリシーを構成し、復号化を有効にし、ルールに適切なセキュリティ プロファイルを適用し、動的更新で定期的に更新します。
C. ファイアウォールによって提供されるすべてのデフォルト ポリシーを構成し、ポリシー オプティマイザーを使用し、インシデントの発生後にセキュリティ ルールを調整します。
D. すべての悪意のある受信トラフィックに対してブロック ポリシーを構成し、すべての送信トラフィックに対して許可ポリシーを構成し、動的更新で定期的に更新します。
正解: **(**正解を表示します**)**
A comprehensive security approach uses:
- User-ID for identity-based policies
- App-ID for application-based security
- Decryption to inspect encrypted traffic
- Security profiles to enforce protections
- Dynamic updates to ensure up-to-date threat coverage
For comprehensive security, combine User-ID, App-ID, decryption, and security profiles. Keep the firewall updated with dynamic content updates to maintain the strongest security posture.
This ensures real-time, identity-aware, and application-centric security enforcement.

質問: **20**
Strata Cloud Manager (SCM) でカスタム Prisma Access レポートを作成するために必要な手順は何ですか?
A. サポート チケットを開きます。
B. Cloud Identity Engine を設定します。
C. PDF 概要レポートを生成します。
D. ダッシュボードを構成します。
正解: **(**正解を表示します**)**
To create custom Prisma Access reports within SCM, you first configure a dashboard that aggregates the relevant logs and analytics. This allows you to define the data points you want to include.
Dashboards in SCM can be customized to include Prisma Access data sources, enabling you to create and generate reports that meet specific business and security requirements. Once configured, you can export the dashboard as a custom report.
Use the dashboard's data visualization to create custom reports for Prisma Access, which can be exported as PDFs for distribution.

質問: **21**
エンジニアが Strata Cloud Manager (SCM) を使用して VM シリーズ ファイアウォールを一括更新できるようにするには、どのアクションを実行すればよいですか。
A. 更新グループ化ルールの作成
B. ソフトウェア更新のスケジュール設定
C. デバイスのグループ化ルールの作成
D. ターゲットOSバージョンの設定
正解: **C (**コメントを発表する**)**
Device grouping rules in SCM allow administrators to organize firewalls into logical groups and collectively manage updates or configuration pushes across those groups.
SCM allows you to create device group rules, enabling streamlined management and collective updates of multiple NGFW instances.
This approach ensures consistency in software versions and configuration baselines across large deployments.

質問: **22**
NGFW は、新しいセッション設定が正当か不正かを判断するためにどの機能を使用しますか?
A. SYNビット
B. SYNクッキー
C. ランダム早期検出 (RED)
D. SYNフラッド保護
正解: **B (**コメントを発表する**)**
To prevent SYN flood attacks, the NGFW uses SYN cookies to validate legitimate session establishment.
SYN cookies allow the firewall to verify the legitimacy of new session requests without allocating resources until the handshake is completed. This prevents SYN flood attacks from exhausting system resources.
SYN cookies mitigate resource exhaustion by ensuring only legitimate connections are established.

質問: **23**
リモートユーザーアクセスに関する問題のトラブルシューティングに役立つログの種類はどれですか？(2つ選択してください)
A. 脅威ログ
B. HIPマッチログ
C. ゾーン保護ログ
D. GlobalProtect ログ
正解: **(**正解を表示します**)**

HIP Match Logs: Host Information Profile (HIP) Match Logs provide information about the health and compliance status of the connecting endpoint, which helps troubleshoot access issues due to client posture or security policy compliance failures.
GlobalProtect Logs: These logs are specific to the GlobalProtect VPN and provide detailed information about user connection attempts, authentication status, errors, and other VPN-specific events which are essential for diagnosing remote user access problems.

質問**: 24**
Prisma Accessにおいて、サービスを中断することなくスムーズなアップグレードを保証する機能は何ですか？
A. バックアップベースのデプロイメント
B. マルチフェーズファームウェアステージング
C. ダウンタイムゼロのアップグレードアーキテクチャ
D. アップグレード前にすべてのポリシーを無効化します
正解**: (**正解を表示します**)**
Prisma Access is designed with mechanisms that allow upgrades to be performed without impacting network traffic or service availability, specifically leveraging phased, resilient upgrade processes with built-in failover and redundancy to guarantee continuous operation during upgrades. Disabling policies, backup-based deployment, and multi-phase firmware staging are not unique to Prisma Access's seamless upgrade capabilities.

質問**: 25**
Prisma SD-WAN を実装する分散型企業では、リモート サイトと本社間の最適なトラフィック フローを確保するために、最初にどの構成要素を実装する必要がありますか?
A. 各拠点に冗長化されたIONデバイスを展開します。
B. リアルタイムのパフォーマンス メトリックを使用して動的なパス選択を実装します。
C. すべてのブランチ オフィス間の静的ルートを構成します。
D. すべてのブランチ ロケーションでスプリット トンネリングを有効にします。
正解**: (**正解を表示します**)**
Dynamic path selection is the foundation of SD-WAN, leveraging real-time performance data to dynamically route traffic over the best available path.
Dynamic path selection continuously monitors performance metrics (loss, latency, jitter) and makes real-time routing decisions to ensure application SLAs are met across the WAN.
Establishing dynamic path selection first ensures the rest of the SD-WAN optimizations (e.g., failover, QoS) work effectively.

質問**: 26**
分散型エンタープライズ ネットワーク内の複数の場所にわたって安全かつ効率的な接続を確保するための 2 つの推奨事項は何ですか (2 つ選択してください)。

A. Prisma Access を使用して、ブランチ ユーザーに安全なリモート アクセスを提供します。
B. すべての場所で集中管理と一貫したポリシー適用を採用します。
C. ブランチ オフィスで働く請負業者向けに広範な VPN ポリシーを作成します。
D. ネットワーク管理を簡素化し、オーバーヘッドを削減するために、フラットなネットワーク設計を実装します。
正解**: A,B (**コメントを発表する**)**
Prisma Access for secure remote access
Prisma Access extends consistent security and optimized connectivity to branch locations, enabling secure access for mobile and branch users.
Centralized management for consistent policy enforcement
Centralized management using Strata Cloud Manager or Panorama ensures security policies and updates are uniformly applied across distributed locations, preventing policy drift and security gaps.
These two practices are foundational for modern, distributed enterprise networks to maintain security posture and performance.

質問**: 27**
組織が Advanced Threat Prevention サブスクリプションのインライン クラウド分析機能を使用していることを確認するために必要な手順はどれですか。
A. パフォーマンスへの影響を回避するためにスパイウェア対策を無効にし、外部の脅威インテリジェンスのみに依存します。
B. セキュリティ ポリシーで SSL 復号化を有効にして、暗号化されたトラフィックの脅威を検査および分析します。
C. スパイウェア対策セキュリティ プロファイルを更新または新規作成し、適切なローカル ディープ ラーニング モデルを有効にします。
D. 高度な脅威防止プロファイルをデフォルト設定で構成し、ネットワーク パフォーマンスに影響を与えないように、リスクの高いトラフィックのみに焦点を当てます。
正解**: C (**コメントを発表する**)**
To fully leverage inline cloud analysis in Advanced Threat Prevention, security profiles (e.g., anti- spyware) must be updated or newly created to enable local deep learning and inline cloud analysis models.
To activate inline cloud analysis, update your Anti-Spyware profile to enable advanced inline detection engines, including deep learning-based models and cloud-delivered signatures.
This ensures real-time protection from sophisticated threats beyond static signatures.

質問**: 28**
Prisma SD-WAN 環境で音声品質の低下が発生した場合、どのような初期アクションが推奨されますか?

A. パス品質のしきい値を直ちに変更します。
B. パス パフォーマンスのリアルタイム分析を確認します。
C. すべての VoIP トラフィックをバックアップ パスに切り替えます。
D. ION デバイスの RMA を要求します。
正解: **(**正解を表示します**)**
Voice quality issues in SD-WAN deployments are typically linked to path performance metrics (latency, jitter, packet loss). Reviewing real-time analytics helps pinpoint root causes and appropriate mitigation.
When experiencing performance issues, the first step is to analyze real-time performance data.
Prisma SD-WAN provides path quality analytics to identify degradation and ensure informed troubleshooting.
This data-driven approach avoids unnecessary configuration changes.

質問: **29**
管理者は、既にクラウド配信型セキュリティサービス（CDSS）が有効になっているデータセンターNGFWに、追加のクラウド配信型セキュリティサービス（CDSS）を実装したいと考えています。NGFWのシングルパス並列処理（SP3）アーキテクチャにはどのような利点がありますか？
A. アプリケーション レベルでのトラフィック検査が可能になります。
B. パフォーマンスの低下は発生しません。
C. パフォーマンスはわずかに低下します。
D. 追加のセキュリティ検査デバイスをインラインで追加できます。
正解: **C (**コメントを発表する**)**
The SP3 architecture of Palo Alto NGFWs ensures that additional security services (CDSS) only cause a minor reduction in performance, as traffic is inspected once in a single pass.
The single-pass parallel processing (SP3) architecture performs application identification and security enforcement simultaneously in one pass, resulting in only minor performance impacts when enabling multiple security services.
Unlike traditional multi-pass engines, SP3 architecture optimizes performance while delivering comprehensive security.

質問: **30**
DNS インフラストラクチャの誤った構成を悪用し、トラフィックを悪意のあるドメインにリダイレクトする脅威アクターに対してリアルタイムの保護を提供するセキュリティ プロファイルはどれですか?
A. ウイルス対策
B. URLフィルタリング
C. 脆弱性保護

D. スパイウェア対策
正解: **(**正解を表示します**)**
The Anti-spyware profile includes DNS-based protections like sinkholing and detection of DNS queries to malicious domains, offering real-time protection against attacks that exploit DNS misconfigurations.
The Anti-Spyware profile protects against DNS-based threats by sinkholing DNS queries to malicious domains and detecting suspicious DNS activity, thus blocking data exfiltration and C2 communication.

質問: **31**
ネットワーク管理者は、エッジNGFW向けにPalo Alto NetworksのAdvanced Threat PreventionとAdvanced DNS Securityのサブスクリプションを取得し、セキュリティプロファイルを設定しています。Advanced DNS Securityサービスの初期設定には、どの手順を含める必要がありますか？
A. DNS-over-TLS / ポート 853 トラフィックを復号化する復号化ポリシー ルールを作成します。
B. 会社が所有するすべての FQDN のオーバーライドを作成します。
C. 悪意のある DNS クエリをシンクホールするための DNS セキュリティ署名ポリシー設定を構成します。
D. デフォルト設定で Advanced Threat Prevention を有効にし、リスクの高いトラフィックのみに焦点を当てます。
正解: **(**正解を表示します**)**
Advanced DNS Security uses a signature policy to sinkhole malicious DNS queries and prevent them from resolving.
The DNS Security service integrates with Anti-Spyware profiles, and you must configure signature policy settings to sinkhole malicious queries. This proactively stops traffic to known malicious domains.
Sinkholing ensures that DNS queries to malicious FQDNs are redirected to a safe IP, preventing compromise.

有効的な**NetSec-Pro-JPN**問題集はJPNTest.com提供され、**NetSec-Pro-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**NetSec-Pro-JPN**試験問題集を提供します。JPNTest.com NetSec-Pro-JPN試験問題集はもう更新されました。ここで**NetSec-Pro-JPN**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/NetSec-Pro-JPN-mondaishu ⇑**126**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**

リモート ユーザー デバイスの姿勢に対するきめ細かなセキュリティの適用には、どの GlobalProtect 構成が推奨されますか?
A. すべてのモバイルユーザーに対するホスト情報プロファイル (HIP) チェックの構成
B. ユーザーが内部アプリケーションにアクセスする際に GlobalProtect を無効にすることをブロックするルールを構成する
C. 内部アプリケーションにアクセスしようとするすべてのユーザーに対して多要素認証 (MFA) を実装する
D. セッション終了時にすべての GlobalProtect セキュリティ ポリシーにログを適用します
正解: **(**正解を表示します**)**
Host Information Profile (HIP) checks are used in GlobalProtect to collect and evaluate endpoint posture (OS, patch level, AV status) to enforce granular security policies for remote users.
The HIP feature collects information about the host and can be used in security policies to enforce posture-based access control. This ensures only compliant endpoints can access sensitive resources.
This enables fine-grained, context-aware access decisions beyond user identity alone.

質問: **33**
NGFW に「default」という名前のセキュリティ プロファイル グループが作成されると何が起こりますか?
A. クライアントのリセットアクションによってドロップされたトラフィックにのみ適用されます。
B. デフォルトではトラフィックがすべてのセキュリティ チェックをバイパスすることを許可します。
C. 新しいポリシーの既存のセキュリティ プロファイル ルールをすべて否定します。
D. すべての新しいセキュリティ ルールに自動的に適用されます。
正解: **(**正解を表示します**)**
A security profile group named "default" is automatically applied to all new security rules unless a specific profile group is explicitly configured.
If a security profile group named `default' exists, it will be automatically applied to any newly created security policy rules to ensure consistent protection.
This behavior ensures that newly created policies are always protected by default security profiles, minimizing human error.

質問: **34**
NGFW ポリシーでは、低速パスでのみどのアクションが実行されますか?
A. セッション検索
B. レイヤー2～レイヤー4ファイアウォール処理
C. SSL/TLS 復号化
D. セキュリティポリシーの検索

正解: (正解を表示します)
In Palo Alto Networks' Single-Pass Parallel Processing (SP3) architecture, SSL/TLS decryption occurs only during the slow path when the firewall first encounters a new session.
SSL/TLS decryption, which requires CPU-intensive cryptographic operations, is performed during the slow path when establishing new sessions. Once decrypted, traffic is processed in the fast path for subsequent packets.
After the initial decryption in the slow path, decrypted traffic is handled by fast path for efficiency.

質問: 35
セキュリティ ポリシーのどの 2 つのコンポーネントを設定すると、業務時間外にサードパーティの請負業者が内部アプリケーションにアクセスできるようになりますか? (2 つ選択してください。)
A. アプリID
B. サービス
C. ユーザーID
D. スケジュール
正解: **C,D** (コメントを発表する)
To allow third-party contractors controlled access, security policies must combine user identification and time-based access controls:
User-ID
User-ID enables security policies to be based on user identity rather than IP addresses, ensuring precise policy enforcement for specific users such as contractors.
Schedule
Schedules allow policies to be active only during specific times, providing time-based access control (e.g., after business hours).
Together, they ensure that only authorized users (contractors) have access, and only when explicitly allowed.

有効的な**NetSec-Pro-JPN**問題集はJPNTest.com提供され、**NetSec-Pro-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**NetSec-Pro-JPN**試験問題集を提供します。JPNTest.com NetSec-Pro-JPN試験問題集はもう更新されました。ここで**NetSec-Pro-JPN**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/NetSec-Pro-JPN-mondaishu ¶126問、３０%ディスカウント、特別な割引コード: **JPNshiken**」