PA-5450

PA-5450

パロアルトネットワークスの機械学習 (ML) を活用した次世代ファイアウォール (NGFW) プラットフォームである PA-5450 は、ハイパースケール データ センター、インターネット エッジ、およびキャンパス セグメンテーションの導入向けに設計されています。このプラットフォームは、189 Gbps の脅威防御スループットという驚異的なパフォーマンスを、セキュリティ サービスが有効な状態で発揮できます。さらに、スケーラブルなモジュール設計の、ニーズの増加に応じてパフォーマンスを拡張できます。また、管理とライセンスにシングルシステム アプローチを採用することで、シンプルさを確保しています。

特長

- 世界初の ML を活用した NGFW
- Gartner Magic Quadrant ネットワーク ファイアウォール部門で 11 回連続リーダー評価
- Forrester Wave: Enterprise Firewalls, Q4 2022 でリーダーに選出
- サービス プロバイダや企業による 5G 変革とマルチアクセス エッジ コンピューティング (MEC) の保護を目的に構築された、5G ネイティブなセキュリティを提供
- 追加のセンサーを導入することなく、管理対象外の IoT デバイスを含むすべてのデバイスの可視性とセキュリティを強化
- アクティブ/アクティブとアクティブ/パッシブの両モードで高可用性をサポート
- セキュリティ サービスにより予測可能なパフォーマンスを発揮
- Panorama ネットワーク セキュリティ管理による集中管理をサポート
- Strata™ Cloud Manager によってセキュリティ投資を最大限活用し、ビジネスの中断を防ぐ

世界初の ML を活用した NGFW は、未知の脅威を阻止し、モノのインターネット (IoT) を含むすべてを可視化して保護し、ポリシー推奨の自動化によってエラーを削減します。PA-5450 を制御するのは、PAN-OS® です。このソフトウェアは、パロアルトネットワークスのすべての NGFW で採用されています。PAN-OS は、アプリケーション、脅威、コンテンツなど、全トラフィックをネイティブに分類し、場所やデバイスの種類に関わらずトラフィックをユーザーと関連付けます。業務遂行に欠かせない要素である、アプリケーション、コンテンツ、およびユーザーをセキュリティ ポリシーの基礎に据えることで、セキュリティ体制を強化するとともに、インシデントの応答時間を短縮します。

主要なセキュリティ機能と接続機能

ML を活用した次世代ファイアウォール

- ファイアウォールの中核に機械学習 (ML) を組み込むことで、ファイルベース攻撃に対するシグネチャレスの防御をインラインで実施し、未知のフィッシング攻撃を特定して即座に阻止することができます。
- クラウドベースの ML プロセスを活用することで、シグネチャと命令を即座に NGFW へ配信します。
- 動作分析を使用して、IoT デバイスを検出し、ポリシーを推奨します。これは、NGFW にネイティブで統合されているクラウド型サービスです。
- ポリシーを自動推奨することで、時間が節約され、人的ミスが少なくなります。

完全なレイヤー 7 の検査により、すべてのアプリケーションをすべてのポートで常に識別して分類

- 使用されているポート、プロトコル、セキュリティの回避技術、暗号化 (TLS/SSL) に関わらず、ネットワークを通過するアプリケーションを識別します。SaaS Security サブスクリプションによって新規アプリケーションを自動的に検出・管理することで、SaaS の急増に対応します。
- 許可、拒否、スケジュール、検査、帯域制御の適用などのあらゆるセキュリティ ポリシーを、ポートではなくアプリケーションを基に決定します。
- 自社開発のアプリケーション向けにカスタム App-ID™タグを作成できます。また、新規アプリケーション向けの App-ID の開発をパロアルトネットワークスに依頼することも可能です。
- アプリケーション内のすべてのペイロード データ (ファイルやデータ パターンなど) を識別して悪意のあるファイルをブロックし、データ漏えいを阻止します。
- 標準およびカスタムのアプリケーション使用状況レポート、たとえば、ネットワーク上の承認済みおよび未承認のすべての Software-as-a-Service (SaaS) トラフィックに対する洞察を提供する SaaS レポートを作成します。
- 組み込みの Policy Optimizer を使用して、従来のレイヤー 4 ルール セットから App-ID ベースのルールに安全に移行できます。また、移行後はルール セットをより安全かつ簡単に管理できます。

詳細は『App-ID 技術概要』をご覧ください。

使用中のデバイスや所在地に関わらず、ユーザーにセキュリティを適用すると同時に、ユーザー アクティビティに基づくポリシーを導入

- IP アドレスだけでなく、ユーザーやグループに基づいて可視化、セキュリティ ポリシー、レポート、フォレンジックを利用できます。
- ワイヤレス LAN コントローラ、VPN、ディレクトリ サーバ、SIEM、プロキシなどのリポジトリを簡単に統合して、ユーザー情報を活用できます。
- ファイアウォールにダイナミック ユーザー グループ (DUG) を定義して、ユーザー ディレクトリに変更が適用されるのを待たずに、時間制限付きセキュリティ アクションを実行できます。
- ユーザーの所在地 (オフィス、自宅、移動先など) や使用中のデバイス (iOS/Android モバイル デバイス、macOS/Windows/Linux PC、Citrix/Microsoft VDI、ターミナル サーバ) に関わらず、一貫したポリシーが適用されます。

- アプリケーションを変更することなくアプリケーションのネットワーク レイヤーに多要素認証 (MFA) を導入。外部 Web サイトへの企業認証情報の漏洩や、盗まれた認証情報の再利用を防ぎます。
- ユーザーの行動に基づいて動的なセキュリティ アクションを提供し、疑わしいユーザーや悪意のあるユーザーを制限します。
- ID ベースのセキュリティを実施する全く新しいクラウドベース アーキテクチャ「Cloud Identity Engine」を採用。ユーザーやユーザーの ID ストアの所在に関わらず、ユーザーの認証と認可を一貫して提供することで、ゼロ トラスト セキュリティ体制への移行を加速させます。

詳細は『Cloud Identity Engine ソリューション概要』をご覧ください。

暗号化トラフィックに隠蔽された悪意のあるアクティビティを阻止

- TLS 1.3 や HTTP/2 を使用するトラフィックなど、インバウンドとアウトバウンド両方の TLS/SSL 暗号化トラフィックを検査し、ポリシーを適用します。
- 暗号化されたトラフィックの量や TLS/SSL バージョン、暗号スイートなど、TLS トラフィックに対する優れた可視性を復号なしで提供します。
- 従来の TLS プロトコル、安全でない暗号、誤って設定されている証明書の使用を制御して、リスクを軽減します。
- 復号機能を簡単に導入できます。また、証明書がピン留めされているアプリケーションなどの問題を、組み込みのログを使用してトラブルシューティングできます。
- プライバシーとコンプライアンスの確保を目的として、URL カテゴリ、送信元ゾーンと宛先ゾーン、アドレス、ユーザー、ユーザー グループ、デバイス、ポートを基に復号機能を柔軟に有効化/無効化できます。
- ファイアウォールから送られた復号トラフィックのコピーを作成して (復号ミラーリング)、トラフィック収集ツールに送信し、フォレンジック、履歴調査、データ損失防止 (DLP) に利用できます。
- Network Packet Broker を使用してサードパーティ セキュリティ ツールにすべてのトラフィック (復号済み TLS、未復号 TLS、非 TLS) をインテリジェントに転送することで、ネットワーク パフォーマンスを最適化し運用経費を削減できます。

いつ、どこで、どのように復号を行って脅威を阻止し、企業を保護できるかは、復号に関するホワイト ペーパーをご覧ください。

Strata Cloud Manager による AI を活用した統一的な管理と運用

ネットワーク障害を防止 : 導入の正常性を予測し、予測分析によって最長 7 日先までの容量ボトルネックを予防的に特定して、業務の中断を予防します。

セキュリティをリアルタイムに強化 : 弊社および業界のベストプラクティスに基づく、AI を活用したポリシー分析とリアルタイム コンプライアンス チェック。

シンプルで一貫したネットワークセキュリティ管理と運用を実施 : あらゆるフォーム ファクタ (SASE、ハードウェア / ソフトウェア ファイアウォール、セキュリティ サービスなど) の設定とセキュリティ ポリシーを管理して一貫性を確保し、運用経費を削減することができます。

クラウド提供型セキュリティ サービスによる高度な脅威の検出と防御

サイロ化したセキュリティ ツールを使用する従来のアプローチは、セキュリティ ギャップの発生、セキュリティ チームの負担増大、業務生産性の低下などの問題の原因となります。業界最先端の次世代ファイアウォールとシームレスに統合されたパロアルトネットワークスのクラウド提供型セキュリティ サービスは、6 万 5,000 社の顧客の間で脅威インテリジェンスを共有して、あらゆる攻撃経路からの既知および未知の脅威をリアルタイムに阻止します。ネットワーク全体のセキュリティ ギャップを解消し、インライン AI を活用したセキュリティ サービスを利用して、あらゆる場所でリアルタイム防御を提供します。

サービス内容 :

- **Advanced Threat Prevention**: インライン AI を利用した検出によって既知および未知のエクスプロイト、コマンドアンドコントロール (C2) 攻撃を阻止。従来型 IPS ソリューションと比べてゼロデイ インジェクション攻撃を 60% 多く、高度な回避技術を用いたコマンドアンドコントロールトラフィックを 48% 多く阻止します。
- **Advanced WildFire®**: 業界最大の脅威インテリジェンスとマルウェア防御エンジンを利用して、既知/未知のマルウェアや高度な回避型マルウェアを競合他社の 180 分の 1 の時間で自動的に阻止し、ファイルの安全を確保します。
- **Advanced URL Filtering**: 既知と未知の脅威をリアルタイムに防御する業界初の機能で、悪意のあるサイトの 88% を他社の 48 時間以上前に阻止。安全なインターネット アクセスを確保し、Web ベース攻撃を 40% 多く防ぎます。
- **DNS Security**: インフラを変更することなく DNS 攻撃に対するカバー範囲を 68% 改善し、コマンドアンドコントロールやデータ窃盗に DNS を悪用した攻撃の 85% を阻止します。
- **Enterprise DLP**: あらゆるクラウド提供型エンタープライズ DLP の 2 倍のカバー範囲で、データ侵害リスクを最小化し、ポリシー違反のデータ転送を阻止し、エンタープライズ環境全体で一貫したコンプライアンスを可能にします。
- **SaaS Security**: 業界唯一の次世代 CASB によって SaaS の急増に先手を打ち、すべてのプロトコルですべてのアプリケーションを自動的に可視化して保護します。
- **IoT Security**: 業界で最もスマートなセキュリティをスマート デバイスに導入してあらゆる「モノ」を保護することで、20 倍高速なゼロ トラスト デバイス セキュリティを実施します。

シングルパス アーキテクチャを使用した独自のパケット処理アプローチ

- ネットワーキング、ポリシー検索、アプリケーションの識別とデコード、シグネチャ マッチングを、すべての脅威とコンテンツに対してシングルパスで実行します。これにより、1 つのセキュリティ デバイスで複数の機能の実行に必要なオーバーヘッドが大幅に減少します。
- ストリームベースの統一されたシグネチャ マッチングを使用したトラフィックのスキャンでは、シングルパスですべてのシグネチャを確認するため、遅延の発生を回避できます。
- セキュリティ サブスクリプションを有効にした場合でも、安定した予測可能なパフォーマンスを発揮できます (表 1 の「Threat Prevention のスループット」は、複数のサブスクリプションを有効にした場合の測定値です)。

SD-WAN 機能の有効化

- SD-WAN を、既存のファイアウォールで有効にするだけで簡単に導入できます。
- SD-WAN を安全に実装できます。この機能は、業界をリードするパロアルトネットワークスのセキュリティ機能にネイティブに統合されています。
- 遅延、ジッター、パケット損失を最小限に抑えることで、卓越したエンドユーザー エクスペリエンスを提供します。

シングルパス アーキテクチャを使用した独自のパケット処理アプローチ

- ネットワーキング、ポリシー検索、アプリケーションの識別とデコード、シグネチャ マッチングを、すべての脅威とコンテンツに対してシングルパスで実行します。これにより、1 つのセキュリティ デバイスで複数の機能の実行に必要なオーバーヘッドが大幅に減少します。
- ストリームベースの統一されたシグネチャ マッチングを使用したトラフィックのスキャンでは、シングルパスですべてのシグネチャを確認するため、遅延の発生を回避できます。
- セキュリティ サブスクリプションを有効にした場合でも、安定した予測可能なパフォーマンスを発揮できます (表 1 の「Threat Prevention のスループット」は、複数のサブスクリプションを有効にした場合の測定値です)。

PA-5450 のアーキテクチャ

PA-5450 では、ネットワーキング、セキュリティ、管理の各主要機能に適した種類および量の処理能力を利用できるようにするため、拡張性に優れたアーキテクチャが採用されています。デバイスは 1 つの統合システムとして管理されるため、空いているすべてのリソースをデータ保護のために簡単に使用できます。PA-5450 は、ネットワーキング カード (NC)、データ処理カード (DPC)、管理処理カード (MPC) の 3 つのサブシステムに処理要求をインテリジェントに分配します。それぞれのサブシステムが、高いコンピューティング能力と大容量の専用メモリを備えています。

PA-5450 には、NC と DPC 用に合計 6 つのスロットが用意されています。

ネットワーキング カード

ネットワーク接続を確立するために、PA-5450 には NC (PA-5400-NC-A) が最低 1 枚必要です。2 枚目の NC を利用するには、システムに少なくとも 2 枚の DPC が必要です。最大 2 枚の NC を搭載できます。NC は、パケットの入口タスクおよび出口タスクの実行専用です。

各 PA-5400-NC-A には複数の接続ポートが用意されています (表 3: 100/1000/10G 銅線 x 4 ポート、1G/10G SFP/SFP+ x 12 ポート、40G/100G QSFP28 x 2 ポート)。

データ処理カード

PA-5450 はパケット処理とセキュリティ処理に DPC (PA-5400-DPC-A) を使用します。6 つのスロットに DPC を最低 1 枚、最大 5 枚配置できます。

管理処理カード

MPC サブシステム (PAN-PA-5400-MPC-A) は、PA-5450 をあらゆる面から制御する専用の接続先として機能します。

表 1: PA-5450 のパフォーマンスと容量

	PA-5400-DPC-A 1 台	PA-5450 設定済みシステム *
ファイアウォールのスループット (appmix)†	75 Gbps	200 Gbps
Threat Prevention のスループット (appmix)‡	55 Gbps	189 Gbps
IPsec VPN のスループット§	17 Gbps	85 Gbps||
最大セッション数#	20M	100M||
新規セッション/秒**	725,000	3.6M||
仮想システム (基本/最大)††	—	25/225

注 : PAN-OS 11.1 で測定した値です。

* 特に明記しない限り、すべてのテストはネットワーキング カード 2 枚とデータ処理カード 4 枚を搭載した状態で行われました。

† ファイアウォールのスループットは、App-ID とロギングが有効な状態で、appmix トランザクションを利用した場合の測定値です。

‡ Threat Prevention のスループットは、App-ID、IPS、アンチウイルス、アンチスパイウェア、WildFire、DNS Security、ファイル ブロック、ロギングが有効な状態で、appmix トランザクションを利用した場合の測定値です。

§ IPsec VPN のスループットは、ロギングが有効な状態で 64KB HTTP トランザクションを利用した場合の測定値です。

|| このテストはネットワーキング カード 1 枚とデータ処理カード 5 枚を搭載した状態で行われました。

最大セッション数は、HTTP トランザクションを利用した場合の測定値です。

** 新規セッション / 秒は、アプリケーション オーバーライドを有効にして、1 バイトの HTTP トランザクションを利用した場合の測定値です。

†† 基本数量に仮想システムを追加するには、別途ライセンスを購入する必要があります。

表 2: PA-5450 のネットワーキング機能
インターフェイス モード
L2、L3、タップ、バーチャル ワイヤ (透過的モード)
ルーティング
OSPFv2/v3(グレースフル リスタート有効)、BGP(グレースフル リスタート有効)、RIP、スタティック ルーティング
ポリシーベース フォワーディング
動的アドレス割り当てのため、PPPoE (Point-to-Point Protocol over Ethernet) と DHCP に対応
マルチキャスト : PIM-SM、PIM-SSM、IGMP v1、v2、v3
双方向転送検出 (BFD)
SD-WAN
パスの品質測定 (ジッター、パケット損失、遅延)
初期のパス選択 (PBF)
動的なパス変更
IPv6
L2、L3、タップ、バーチャル ワイヤ (透過的モード)
機能 : App-ID、User-ID、Content-ID、WildFire、SSL 復号
SLAAC
IPSec と SSL VPN
鍵交換 : 手動鍵、IKEv1、IKEv2 (事前共有鍵、証明書に基づいた認証)
暗号化 : 3DES、AES (128 ビット、192 ビット、256 ビット)
認証 : MD5、SHA-1、SHA-256、SHA-384、SHA-512
GlobalProtect® 大規模 VPN による構成と管理の簡素化 *
GlobalProtect のゲートウェイとポータルを用いた IPSec と SSL VPN トンネル経由のセキュア アクセス *
VLAN
デバイス/インターフェイスごとの 802.1Q VLAN タグ : 4,094/4,094
集約インターフェイス (802.3ad)、LACP
ネットワーク アドレス変換
NAT モード (IPv4): スタティック IP、ダイナミック IP、ダイナミック IP およびポート (ポート アドレス変換)
NAT64、NPTv6
追加の NAT 機能 : ダイナミック IP の予約、調整可能なダイナミック IP およびポートのオーバーサブスクリプション
高可用性 (HA)
モード : アクティブ/アクティブ、アクティブ/パッシブ、HA クラスタリング
障害検出 : パス モニタリング、インターフェイス モニタリング
モバイル ネットワーク インフラストラクチャ †
5G セキュリティ
GTP Security
SCTP Security

* GlobalProtect ライセンスが必要。

† 詳細については、機械学習 (ML) を活用した 5G 向けの次世代ファイアウォール (NGFW) データシートを参照してください。

表 3: PA-5450 のハードウェア仕様
PA-5400-NC-A ネットワーキング I/O
100/1000/10G 銅線 x 4 ポート、1G/10G SFP/SFP+ x 12 ポート、40G/100G QSFP28 x 2 ポート。システムに搭載する NC の枚数は最小 1 枚、最大 2 枚。NC を 2 枚使用する場合、2 枚以上の DPC を搭載する必要があります
PAN-PA-5400-MPC-A 管理 I/O
SFP/SFP+ MGT x 2 ポート、SFP/SFP+ HA1 x 2 ポート、HSCI HA2/HA3 QSFP+/QSFP28 x 2 ポート、 RJ45 シリアル コンソール x 1 ポート、Micro USB シリアル コンソール x 1 ポート
ストレージ容量
480 GB SSD、RAID1、システム ストレージ 4 TB SSD、ログ ストレージ (オプション)
最大 BTU/ 時
8,828
電源 (基本 / 最大)
2/4
AC 入力電圧 (入力周波数)
100 ～ 120 VAC & 200 ～ 240 VAC (50 ～ 60 Hz)
AC 電源出力
2,200 ワット/電源
最大消費電流
AC: 100 ～ 120 VAC、1 入力あたり最大約 14 A。200 ～ 240 VAC、1 入力あたり最大約 12.5 A
DC: 48 ～ 60 VDC、1 入力あたり最大 52 A
最大突入電流
AC: 35 A @ 230 VAC、35 A @ 120 VAC
DC: 50 A @ 72 VDC
ラックマウント (寸法)
5U、19 インチ標準ラック 高さ 22.2cm x 奥行き 76.8cm x 幅 44.1cm
最大故障間隔 (MTBF)
構成に依存。MTBF の詳細については、パロアルトネットワークスの代理店にお問合せください。
安全規格
cTUVus、CB
EMI
FCC Class A、CE Class A、VCCI Class A、KCC Class A、BSMI Class A
認定
paloaltonetworks.jp/legal-notices/trust-center/technical-certifications をご覧ください
環境
動作温度 : 0 ～ 50℃ (32 ～ 122°F)
非動作温度 : -20 ～ 70℃ (-4 ～ 158°F)

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
wwwpaloaltonetworks.jp

strata_ds_pa-5450_010424