PA-2000 シリーズ

PA-2000 シリーズ次世代ファイアウォールの主要機能

APP-ID™ 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時識別

- 使用されているポートや暗号化（SSL または SSH）、セキュリティ回避技術に関わらず、アプリケーションを識別します。
- 許可、拒否、スケジュール、スキャン、帯域制御の適用などのセキュリティポリシー決定の要素として、ポートではなくアプリケーションを使用します。
- 不明なアプリケーションを、ポリシー コントロール、脅威のフォレンジック、カスタム App-ID の作成、または App-ID 開発用のパケット キャプチャが行えるよう分類します。

USER-ID™ と GLOBALPROTECT™ であらゆる場所のあらゆるユーザに安全なアプリケーション使用ポリシーを拡張

- Active Directory、LDAP、eDirectory Citrix、Microsoft Terminal Services とエージェントレスに統合します。
- XML APIにより、NAC、802.1X ワイヤレス、およびその他の非標準ユーザ リポジトリと統合します。
- Microsoft Windows、Mac OS X、Linux、Android、または iOS プラットフォームを実行しているローカルおよびリモートのユーザに一貫したポリシーを導入します。

CONTENT-ID™ と WILDFIRE™ で既知および未知のあらゆる脅威に対して保護

- 一般的な脅威回避技法が実装されているかに関わらず、すべてのポートでエクスプロイト、マルウェア、スパイウェアを含む様々な既知の脅威をブロックします。
- ファイルや機密データの無許可の転送を制限し、仕事とは関係ない Web の利用を制御します。
- 不明なマルウェアを識別して 100 以上の悪意ある動作について分析を行い、自動的にシグネチャを作成して次の更新時に配信します。

PA-2050

PA-2020

Palo Alto Networks™ PA-2000 シリーズは PA-2050 と PA-2020 の 2 つの高パフォーマンス プラットフォームで構成されています。これらのプラットフォームはどちらも高速インターネット ゲートウェイでの導入を目的としています。PA-2000 シリーズはネットワーキング、セキュリティ、脅威からの保護と管理のための専用のプロセッサとメモリを使用してネットワーク トラフィック フローを管理します。

高速バックプレーンはデータプレーンと管理プレーンに分離されているため、トラフィックの負荷とは無関係に常に管理アクセスを行うことができます。PA-2000 シリーズの管理要素は、セキュリティに特化した専用のオペレーティング システムである PAN-OS™ で、これによって企業は App-ID、User-ID、Content-ID、GlobalProtect、WildFire を使用してアプリケーションを安全に使用できます。

パフォーマンスと容量[1]	PA-2050	PA-2020
ファイアウォール スループット（App-ID 対応）	1 Gbps	500 Mbps
脅威防御スループット	500 Mbps	200 Mbps
IPSec VPN スループット	300 Mbps	200 Mbps
新規セッション/秒	15,000	15,000
最大セッション	250,000	125,000
IPSec VPN トンネル/トンネル インターフェイス	2,000	1,000
GlobalProtect（SSL VPN）同時ユーザ	1,000	500
SSL 復号化セッション	1,000	1,000
SSL インバウンド証明書	25	25
バーチャル ルータ	10	10
バーチャル システム（基本/最大[2]）	1/6	1/6
セキュリティ ゾーン	40	40
最大ポリシー数	5,000	2,500

[1] パフォーマンスと容量は最適なテスト条件のもと PAN-OS 5.0 で測定されています。

[2] 別途追加ライセンスを購入いただくことで、基本の仮想システム数に、仮想システム数を追加可能です。

PA-2000 シリーズの次世代ファイアウォールの詳細な説明については、www.paloaltonetworks.com/literature をご覧ください。

paloalto NETWORKS

the network security company™

ハードウェア仕様

I/O

- PA-2050: 10/100/1000 x 16 ポート、SFP オプティカル ギガビット x 4 ポート
- PA-2020: 10/100/1000 x 12 ポート、SFP オプティカル ギガビット x 2 ポート

管理 I/O

- 10/100/1000 アウトオブバンド管理ポート x 1 ポート、RJ-45 コンソール ポート x 1 ポート

ストレージ容量

- 160GB HDD

電源(平均/最大消費電力)

- 250W (105W/120W)

最大 BTU/HR

- 409

入力電圧(入力周波数)

- 100-240VAC (50-60Hz)

最大消費電流

- 3A@100VAC

平均故障間隔(MTBF)

- 7.3 年

最大突入電流

- 70A@230VAC; 35A@115VAC

ラック マウント可能(寸法)

- 1U、19 インチ標準ラック 4.45cm(高さ) x 43.2cm(奥行)x 43.2cm(幅)

重量(スタンドアロン デバイス/出荷時)

- 6.8kg/9.7kg

安全規格

- UL、CUL、CB

EMI

- FCC Class A、CE Class A、VCCI Class A、TUV

認証

- FIPS 140 レベル 2、Common Criteria EAL2、ICSA、UCAPL

環境

- 動作温度 32 ～ 122 F、0 ～ 50 ℃
- 動作時以外の温度 -4 ～ 158 F、-20 ～ 70 ℃

ネットワーキング

インターフェイス モード:

- L2、L3、タップ、バーチャル ワイヤ(トランスペアレント モード)

ルーティング

- モード: OSPF、RIP、BGP、スタティック
- フォワーディング テーブル サイズ(デバイス/VRごとのエントリ):
  5,000/2,500 (PA-2050)、2,500/2,500 (PA-2020)
- ポリシーベース フォワーディング
- PPPoE (Point-to-Point Protocol over Ethernet)
- マルチキャスト: PIM-SM、PIM-SSM、IGMP v1、v2、v3

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
- 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

アドレス割り当て

- デバイスに対するアドレス割り当て: DHCP クライアント/PPPoE/スタティック
- ユーザに対するアドレス割り当て: DHCP サーバ/DHCP リレー/スタティック

IPV6

- L2、L3、タップ、バーチャル ワイヤ(トランスペアレント モード)
- 機能: App-ID、User-ID、Content-ID、WildFire、SSL 復号化

VLANS

- デバイス/インターフェイスあたりの 802.1q VLAN タグ: 4,094/4,094
- 最大インターフェイス: 2,048 (PA-2050)、1,024 (PA-2020)
- アグリゲート インターフェイス (802.3ad)

NAT/PAT

- 最大 NAT ルール: 1,000
- 最大 NAT ルール(DIPP): 200
- ダイナミック IP およびポート プール: 254
- ダイナミック IP プール: 16,234
- NAT モード: 1:1 NAT、n:n NAT、m:n NAT
- DIPP オーバーサブスクリプション(ソースポートおよび IP ごとの一意の宛先 IP): 2
- NAT64

バーチャル ワイヤ

- 最大バーチャル ワイヤ: 1024 (PA-2050)、512 (PA-2020)
- バーチャル ワイヤにマッピングされるインターフェイスの種類: 物理およびサブインターフェイス

L2 転送

- ARP テーブル サイズ/デバイス: 2,500 (PA-2050)、1,000 (PA-2020)
- MAC テーブル サイズ/デバイス: 2,500 (PA-2050)、1,000 (PA-2020)
- IPv6 隣接テーブル サイズ: 1,000

セキュリティ

ファイアウォール

- アプリケーション、ユーザ、コンテンツに対するポリシーベースの制御
- フラグメント化されたパケットのプロテクション
- 偵察行為のスキャン プロテクション
- DoS（サービス妨害）/DDoS（分散サービス妨害）プロテクション
- 復号化: SSL（インバウンドおよびアウトバウンド）、SSH

WILDFIRE

- 100 以上の悪意ある動作について標的型および未知のファイルを識別し分析
- 新たに検出されたマルウェアに対してシグネチャを生成し自動的に配信
- 1 時間以内に WildFire シグネチャのアップデート配信、一体化されたロギング/レポーティング、WildFire API 経由で 1 日あたり最大 100 サンプルのプログラム提出と、ファイル ハッシュによる 1 日あたり最大 1000 のレポート クエリ（サブスクリプションが必要）

ファイルとデータのフィルタ処理

- ファイル転送: 60 以上の固有のファイルの種類に対する双方向制御
- データ転送: クレジットカード番号 および 米国社会保障番号 の不正転送の双方向制御
- ドライブバイ ダウンロード プロテクション

ユーザのインテグレーション（USER-ID）

- Microsoft Active Directory、Novell eDirectory、Sun One およびその他の LDAP ベースのディレクトリ
- Microsoft Windows Server 2003/2008/2008r2、Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services、Citrix XenApp
- XML API による非標準ユーザ リポジトリとの統合を助長

IPSEC VPN（サイトツーサイト）

- 鍵交換: 手動、IKE v1
- 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
- ダイナミック VPN トンネルの作成（GlobalProtect）

脅威防御（サブスクリプションが必要）

- アプリケーション、オペレーティング システムの脆弱性エクスプロイトからの保護
- ウイルス（HTML、Javascript、PDF および圧縮ファイルに埋め込まれたものを含む）、スパイウェア、ワームに対するストリームベースの保護

URL フィルタリング（サブスクリプションが必要）

- 事前定義済みおよびカスタムの URL カテゴリ
- 最近アクセスされた URL のデバイス キャッシュ
- セキュリティ ポリシーの一致条件としての URL カテゴリ
- 閲覧時間情報

サービス品質（QOS）

- アプリケーション、ユーザ、発信元、宛先、インターフェイス、IPSec VPN トンネル、その他多数のエレメントごとのポリシーベース トラフィック シェーピング
- 保証、最大値、優先帯域幅パラメータを備えた 8 つのトラフィック クラス
- リアルタイムの帯域幅モニタ
- ポリシーごとの diffserv マーキング
- QoS でサポートされている物理インターフェイス: 4

SSL VPN/リモート アクセス（GLOBALPROTECT）

- GlobalProtect ゲートウェイ
- GlobalProtect ポータル
- 伝送: SSL フォールバックを伴う IPSec
- 認証: LDAP、SecurID、ローカル DB
- クライアント OS: Mac OS X 10.6、10.7（32/64 ビット）、10.8（32/64 ビット）、Windows XP、Windows Vista（32/64 ビット）、Windows 7（32/64 ビット）
- サードパーティのクライアント サポート: Apple iOS、Android 4.0 以上、Linux 用 VPNC IPSec

管理、レポーティング、可視化ツール

- 統合 Web インターフェイス、CLI 集中管理（Panorama）
マルチ言語のユーザ インターフェイス
- Syslog、Netflow v9、 SNMP v2/v3
- XML ベース REST API
- アプリケーション、URL カテゴリ、脅威およびデータのグラフィカル サマリ（ACC）
- トラフィック、脅威、WildFire、URL、データ フィルタリングの各ログの閲覧、フィルタ、エクスポート
- 完全にカスタマイズ可能なレポート機能

PA-2000 シリーズ次世代ファイアウォールの詳細な説明については、www.paloaltonetworks.com/literature をご覧ください。

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com