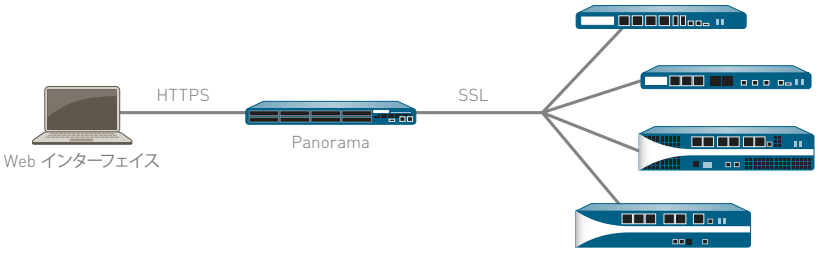
PANORAMA

Panorama は Palo Alto Networks の次世代ファイアウォールに対して、一元化されたポリシーとデバイス管理を提供します。

- ネットワーク上のアプリケーション、ユーザ、潜在的なセキュリティ インパクトの概要をグラフィカルに表示します。
- ローカル ポリシーと併用するコーポレート ポリシーを一元化された環境に導入することで、柔軟性を提供します。
- デバイス レベル、または役割ベースの管理によってグローバルに、管理制御に適したレベルを割り当てます。
- ネットワーク トラフィック、セキュリティ インシデント、管理上の変更を一元的に分析、調査、および報告します。



大企業では通常、ネットワーク全体にいくつものファイアウォールが導入されており、その複雑さや個々のデバイス間の互換性の欠如によって、それらの管理や運用プロセスには手間がかかります。その結果、管理の手間とそれに伴う費用が増えています。

Panorama は Palo Alto Networks の次世代ファイアウォールを一元管理することができます。一元化された環境で、管理者はファイアウォールを通過するアプリケーション、ユーザ、コンテンツに関するインサイト（知見）を得ることができます。ネットワーク上で何が発生しているのかを把握し、安全なアプリケーション実行ポリシーを適用することで、管理の手間を最小化しながら保護と制御機能を最大化することができます。管理者は長期的に集約したデータや、ファイアウォールに保存されているデータを使用して分析、レポートの作成、フォレンジックを行うことができます。

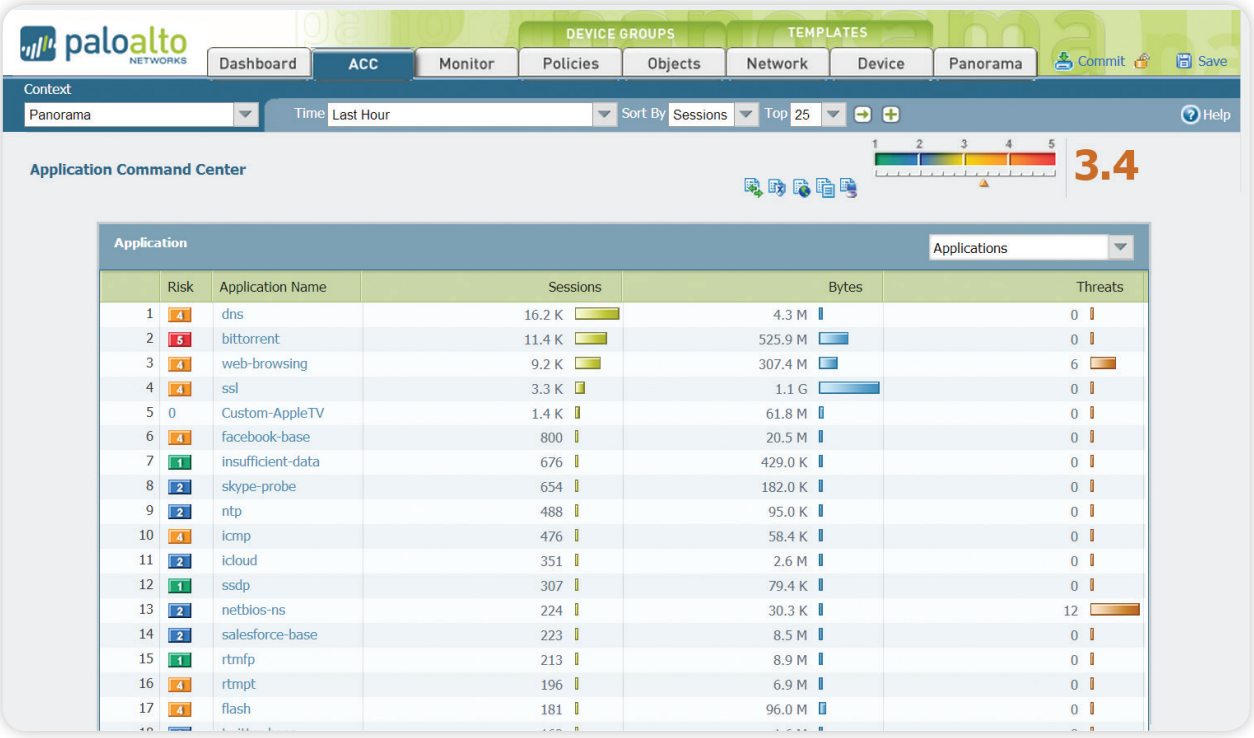
Panorama と各々のデバイスは、同一の Web ベースの外観と操作性を提供することで、操作習得にかかる時間とタスクの実行の遅れを最小化することができます。Palo Alto Networks は一貫性を重視した管理哲学に従い、競合他社よりもはるかに高い優位性を提供します。

一元化された可視性: Application Command Center

Panorama が提供している Application Command Center（ACC）を使用することで、管理者は管理対象になっているすべての Palo Alto Networks デバイスのアプリケーション、URL、脅威、データ（ファイルとパターン）をグラフィカルに表示することができます。ACC は各デバイスから動的にデータを取得し、ネットワーク上のアプリケーション、そのアプリケーションを利用しているユーザ、さらに潜在的な脅威に関する最新のデータを管理者に提供します。管理者は一度のクリックでアプリケーションの説明とその主な機能、そのアプリケーションを利用しているユーザを表示することで、新しいアプリケーション、または見慣れないアプリケーションを調査することができます。

URL カテゴリおよび脅威に関する追加のデータにより、ネットワーク アクティビティをあらゆる角度から包括的に確認できます。管理者は、ACC から提供される情報に基づいてポリシーに関する決定を下し、潜在的なセキュリティ脅威に迅速に対応できます。

paloalto NETWORKS
the network security company™



Application Command Center はアプリケーション トラフィックに関するグローバルおよびローカルなビューを提供し、ドリルダウン（もぐり込み検索）によって現在のアクティビティの詳細を把握できます。

グローバルなポリシー制御: 安全性を確保したアプリケーション

アプリケーションを安全に使用できるようになると、特定のアプリケーションへのアクセスが許可され、特定の脅威防御ポリシーとファイル、データ、または URL フィルタリング ポリシーを適用できます。Panorama により管理者は一元化された環境でルールを管理することができるので、ネットワーク上の全てのファイアウォールでアプリケーションを安全に管理することができます。

Panorama ベースの共有ポリシーでは、ローカル デバイス ルールによってセキュリティと柔軟性を維持しながら、社内要件または規制要件へのコンプライアンスを確保できます。ポリシーとオブジェクトに対して一元管理とローカル管理を組み合わせることで、グローバル レベルでの一貫したセキュリティと、ローカル レベルでの柔軟性のバランスを上手にとることができます。

管理者はディレクトリ サービスの統合によって、ユーザ情報に基づいたアプリケーションを安全に有効化するポリシーを導入することができます。また、アプリケーション固有の脅威防御機能を実装して、コンテンツとネットワークを保護することもできます。IP アドレスではなくユーザ情報に基づいたアプリケーションを安全に有効化する単一のポリシーを設定することで、企業や組織は必要なポリシー数を大幅に減少させることができます。ディレクトリ サービスとの統合によるもう 1 つのメリットは、日常的に発生する従業員の追加、移動に伴う管理オーバーヘッドの大幅な削減です。従業員を 1 つのグループから別のグループに移動する際も、セキュリティ ポリシーの安定性が維持できます。

トラフィックの監視: 分析、レポート作成、およびフォレンジック

Panorama ではローカル デバイス管理レベルと同一の、強力なモニタリングおよびレポート作成ツールを持っています。そして、アクティビティの集約ビューを提供することで可視性をさらに向上させます。管理者によるクエリの実行や、レポート作成の際、Panorama は管理しているファイアウォールや、Panorama に転送されたログから、最も最新のデータを動的に収集します。すべてのデバイスの最新情報にアクセスできることで、管理者は発生中のセキュリティ インシデントだけでなく、プロアクティブに対処して、コーポレートの資産を保護することができます。

- **ログ ビューワ:** Panorama の管理者はセル値をクリック、またはエクスプレッション ビルダーを使用してソートの基準を定義し、動的なログ フィルタリングで、個々のデバイスや全デバイスのログ アクティビティをすぐに表示することができます。結果を保存して後日クエリに使用することも、分析用にエクスポートすることもできます。
- **カスタム レポート機能:** 特定の要件に合わせて、あらかじめ定義されたレポートをそのまま使用することも、カスタマイズすることも、1 つのレポートにまとめることもできます。
- **ユーザ アクティビティ レポート:** Panorama のユーザ アクティビティ レポートには、各ユーザが使用したアプリケーション、アクセスした URL カテゴリや Web サイト、特定期間中にアクセスした全 URL が表示されます。Panorama は保護されているファイアウォール、使用している IP アドレスやデバイスに関係なく、ユーザ アクティビティを集約したレポートを作成します。

Panorama の管理アーキテクチャ

Panorama によって、企業や組織は一元化された監視と制御の両方を提供するモデルを使用して、Palo Alto Networks ファイアウォールを管理することができます。Panorama は一元化された管理を行うためのツールをいくつか提供しています。

- **テンプレート:** Panorama はテンプレートによって、共通のデバイスとネットワーク コンフィグレーションを管理します。テンプレートを使用してコンフィグレーションの一元管理を行い、管理対象の全ファイアウォールに変更をプッシュすることができます。この方法によって、各ファイアウォールに対する同じ変更を多くのデバイスで繰り返し行う必要がなくなります。たとえば、同じ変更をデバイスごとに行うのではなく、数百のファイアウォールに対して DNS と NTP の共通の設定をプッシュすることができます。

- **デバイス グループ:** Panorama はデバイス グループごとに共通のポリシーやオブジェクトを管理します。デバイス グループを使用して、共通の要件を持つ多数のデバイスのルールを一元管理することができます。デバイス グループでのデバイスのグループ化の一例として、地理的（ヨーロッパと北米など）、または機能的（境界またはデータセンタ）なものが挙げられます。デバイス グループ内では、バーチャル システムは物理ファイアウォールと同じレベルで、個別のデバイスとして扱われます。これによって、デバイス上の異なるバーチャル システムでルールを共有することができます。

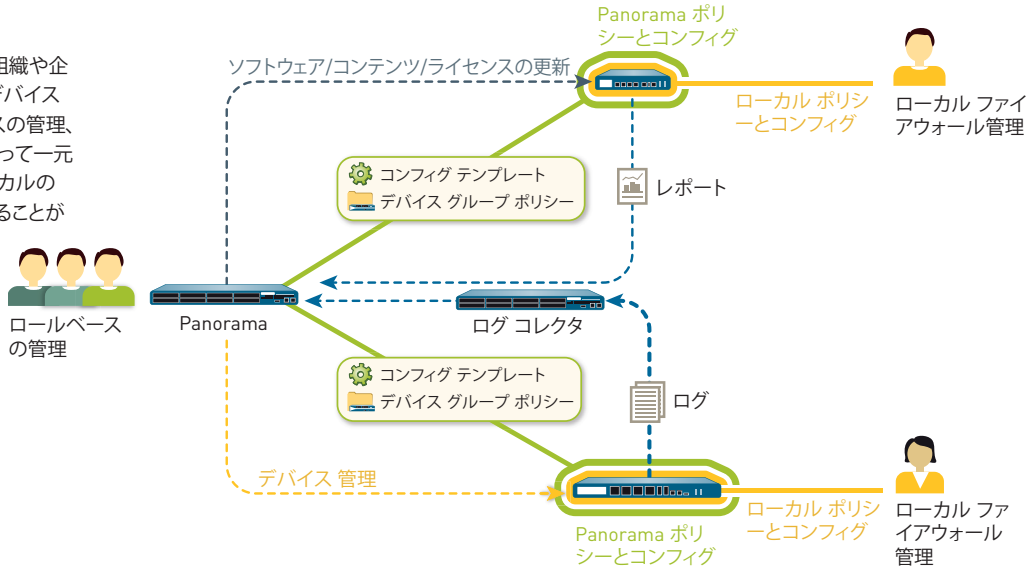
  企業や組織は共有ポリシーを使用して一元化された制御を行いながら、ファイアウォール管理者には自治権を与えて、ローカルでの要件に必要な細かい調整を行えるようにすることができます。デバイス グループ レベルでは、管理者は基準との照合に使用する最初のルール セット（プレルール）と最後のルール セット（ポストルール）として定義される共有ポリシーを作成できます。プレルールとポストルールは管理対象ファイアウォールごとに表示することができますが、Panorama から、定義されている管理者上の役割の範囲内でのみ編集できます。ローカル デバイス ルール（プレルールとポストルールの間にあるルール）は、ローカル管理者、またはローカル ファイアウォール コンテキストに切り替えた Panorama 管理者のいずれでも編集できます。また、組織や企業は Panorama 管理者が定義した共有オブジェクトを使用し、ローカルに管理されているデバイス ルールによって参照することもできます。

- **役割ベースの管理:** 企業や組織は役割ベースの管理機能を使用して、スタッフごとに機能レベルで管理アクセス権限（有効、読み取り専用、無効、非表示）を付与することができます。各管理者の業務に関連したタスクへの適切なアクセスを提供すると共に、他のアクセスは非表示または読み取り専用とすることができます。たとえばこの種のアクセス コントロールを使用して、セキュリティ管理やネットワーク管理など、エンタープライズ内で異なるタスクを担当するスタッフに対して、異なる役割を定義することができます。管理者によるすべての変更は、変更時刻、管理者名、使用したインターフェイス（Web UI、CLI、Panorama）、コマンド、または実行した動作と共にログに記録されます。

- **ソフトウェア、コンテンツ、ライセンス更新管理:** 導入規模が拡大すると、組織や企業の多くは、更新を整然とダウンストリーム ボックスに確実に送信したいと考えます。たとえば、ソフトウェアの更新を一元的に検証した後に、Panorama から本番のファイアウォールに一斉に配信したいというセキュリティ チームもあるでしょう。Panorama を使用すれば、ソフトウェアの更新、コンテンツ（アプリケーションの更新、アンチウイルス シグネチャ、脅威シグネチャ、URL フィルタリング データベースなど）、およびライセンスの更新プロセスを一元管理することができます。

テンプレート、デバイス グループ、役割ベースの管理、更新管理により、組織や企業はすべての管理機能、可視化ツール、ポリシー作成、レポート機能、ログに対する適切なアクセス権限を、グローバルおよびローカルの両方のレベルで付与することができます。

Panorama により、組織や企業はテンプレート、デバイス グループ、役割ベースの管理、および更新管理によって一元化された管理とローカルの管理のバランスをとることができます。



柔軟な導入

組織や企業は Panorama をハードウェア アプライアンス、またはバーチャル アプライアンスとして導入することができます。

ハードウェア アプライアンス

高性能な専用ハードウェアに Panorama を導入したいと考えている、または大量のログ データ用に Panorama の管理とログ機能を分離したいと考えている組織や企業は、M-100 ハードウェア アプライアンスを使用することができます。M-100 上での Panorama の稼働には、以下の導入方法があります。

- **一元化:** このシナリオでは、Panorama のすべての管理およびログ機能を単一のデバイスに統合します（高可用性オプション付き）。
- **分散:** 組織や企業は管理およびログ機能を複数のデバイスに分散することができます。この構成では、マネージャとログ コレクタに機能を分けます。
  - **Panorama マネージャ**: Panorama マネージャは、管理対象の全デバイスのポリシーとデバイス コンフィグレーションに関連するタスクを処理します。マネージャはログ データをローカルに保存せず、別のログ コレクタを使用してログ データを処理します。マネージャはログ コレクタに保存されているデータを分析して、一元化されたレポートを生成します。
  - **Panorama ログ コレクタ:** ログを大量に記録、保存する必要がある組織や企業は、ログ コレクタ デバイス専用の Panorama を導入して、複数の管理対象ファイアウォールのログ情報を集約することができます。

管理とログ収集を切り離すことで、組織や企業は導入を最適化し、スケーラビリティの要件や、組織または地理的な要件に対応することができます。

バーチャル アプライアンス

Panorama を VMware ESX(i) 上のバーチャル アプライアンスとして導入し、組織や企業の仮想化への取り組みをサポートすることができます。また、制約のある、もしくはコストのかかるデータ センタ内のラック スペースを統合することもできます。バーチャル アプライアンスは、以下の 2 つの方法で導入できます。

- **一元化:** Panorama のすべての管理およびログ機能を単一のバーチャル アプライアンスに統合します（高可用性オプション付き）。
- **分散:** Panorama による分散ログ収集は、ハードウェアとバーチャル アプライアンスの混在に対応します。
  - **Panorama マネージャ:** バーチャル アプライアンスを Panorama マネージャとして使用し、管理対象の全デバイスのポリシーとデバイス コンフィグレーションに関連するタスクを処理します。
  - **Panorama ログ コレクタ:** Panorama ログ コレクタは M-100 を使用して導入することができ、大量のログ収集や処理タスクを実行します。バーチャル アプライアンスを Panorama ログ コレクタとして使用することはできません。

ハードウェア、またはバーチャル プラットフォームのいずれか、そして Panorama 機能の組み合わせ、または分離のいずれかを選択できることで、組織や企業は分散されたネットワーク環境内で、複数の Palo Alto Networks ファイアウォールを非常に柔軟に管理できます。

PANORAMA の仕様

サポートするデバイス数	最大 1,000
高可用性	アクティブ/パッシブ
管理者の認証	ローカル データベース RADIUS

M-100 管理アプライアンスの仕様

I/O

- (1) 10/100/1000、(3) 10/100/1000 (将来用)、(1) DB9 コンソール シリアル ポート

ストレージ

- M-100 1TB RAID: 2 x 1TB RAID 認証 HDD による 1TB の RAID ストレージ
- M-100 4TB RAID: 8 x 1TB RAID 認証 HDDによる 4TB の RAID ストレージ

電源(平均／最大消費電力)

- 500W/500W

最大 BTU/時

- 1,705 BTU/時

入力電圧(入力周波数)

- 100-240VAC (50/60Hz)

最大消費電流

- 10A (100VAC時)

平均故障間隔(MTBF)

- 14.5 年

ラック マウント可能(寸法)

- 1U、19 インチの標準ラック (高さ約 4.45 cm (1.75 インチ) x 奥行き約 58.42 cm (23 インチ) x 幅約 43.69 cm (17.2 インチ))

重量(スタンドアロン デバイス/梱包後)

- 約 12.1 kg (26.7 ポンド) /15.9 kg (35ポンド)

安全性

- UL、CUL、CB

EMI

- FCC Class A、CE Class A、VCCI Class A

環境

- 動作温度: 5～40℃、40～104°F
- 非動作温度: -40～65℃、-40～149°F

バーチャル アプライアンスの仕様

最小サーバー要件

- 40 GB のハード ドライブ
- 4 GB RAM
- Quad-Core CPU (2GHz+)

VMWARE サポート

- VMware ESX 4.1 以上

ブラウザ サポート

- IE v7 以上
- Firefox v3.6 以上
- Safari v5.0 以上
- Chrome v11.0 以上

ログ ストレージ

- VMware バーチャル ディスク: 最大 2TB
- NFS

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