次世代ファイアウォールの概要

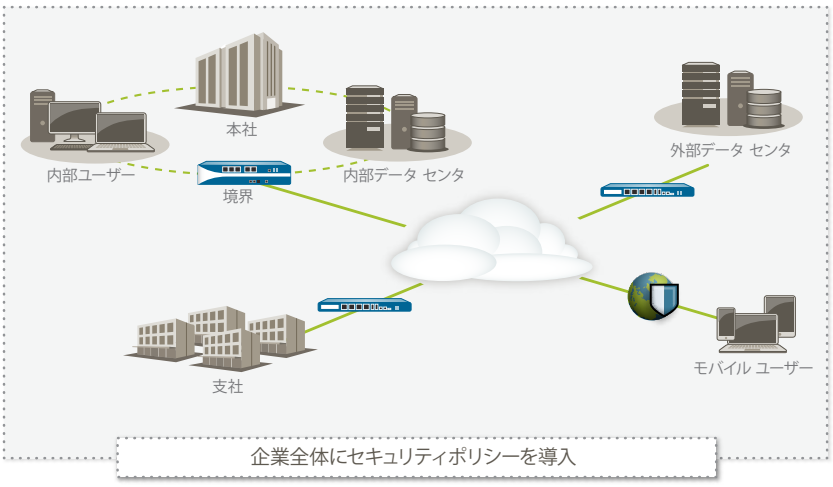
アプリケーションや脅威をめぐる状況、ユーザの行動、ネットワーク インフラストラクチャの根本的な変化によって、従来のポートベースのファイアウォールが提供していたセキュリティの効果は徐々に失われつつあります。ユーザは様々な種類のデバイスを使用してあらゆるタイプのアプリケーションにアクセスしており、その多くは業務のために使用しています。その一方でデータセンタの拡張、仮想化、モバイル、クラウド中心の取り組みの結果、アプリケーションへのアクセスを可能にしながら同時にネットワークを保護するための方法は、再考を余儀なくされています。

従来の対応にはファイアウォールに加え、増大し続けるポイントテクノロジのリストを使用してすべてのアプリケーション トラフィックを遮断する試みが含まれますが、これはビジネスの妨げとなる可能性があります。あるいは、すべてのアプリケーションを許可するという方法もありますが、これも同じようにビジネスとセキュリティのリスクを増大させるため容認できるものではありません。ここで問題なのは、従来のポートベースのファイアウォールでは、たとえアプリケーション ブロックを追加したとしても、これらいずれのアプローチに対しても代わりの選択肢を提供できないということです。すべてを許可することとすべてを拒否することの間でバランスをとるには、主要なファイアウォール セキュリティ ポリシー基準としてアプリケーション アイデンティティやアプリケーションの使用者、コンテンツの種類などビジネス関連エレメントを考慮して、安全にアプリケーションを使用できるようにする必要があります。

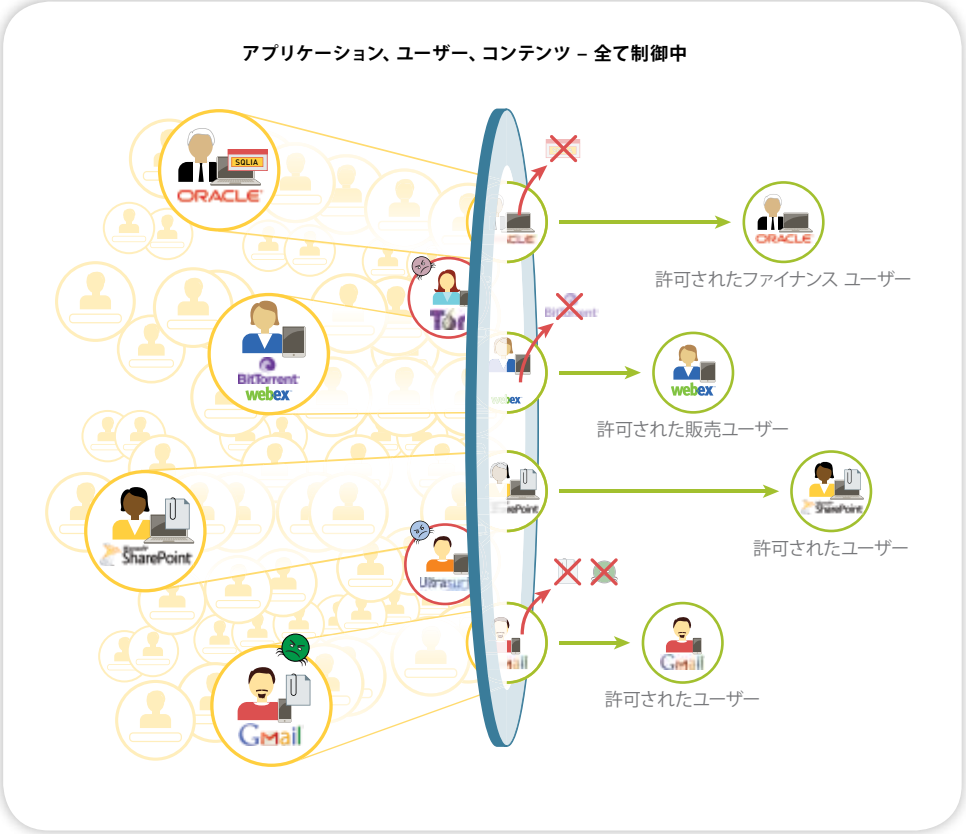
安全なアプリケーション利用を実現するための要件:

- **ポートではなくアプリケーションで通信を識別** - ファイアウォールに到達した時点でトラフィックを識別し、プロトコルや暗号、回避技法に関係なくアプリケーションを識別します。その識別情報をすべてのセキュリティ ポリシーのベースとして使用します。
- **場所やデバイスに関係なく、IP アドレスではなくユーザ を識別** - エンタープライズ ディレクトリやその他のユーザストアからのユーザおよびグループの情報を使用して、場所やデバイスに関わらずすべてのユーザに対して一貫したポリシーを導入します。
- **既知および不明のあらゆる脅威に対して防御。既知および不明のあらゆる脅威に対して防御 -** 既知の脆弱性攻撃、マルウェア、スパイウェア、悪意ある URLから保護し、標的型の未知のマルウェアがないかトラフィックの分析を行い、その対応シグネチャを自動配信します。
- **ポリシー管理を簡略化** - 使いやすいグラフィカルなツール、統合ポリシー エディタ、テンプレート、デバイス グループによって、安全なアプリケーション利用を実現し、管理負荷を低減します。

安全なアプリケーション利用ポリシーは、導入場所に関わらずセキュリティを向上します。インターネットの境界では不要なアプリケーションを幅広くブロックし、許可されたアプリケーションについては既知と不明のどちらのアプリケーションも脅威がないか調査することで、脅威の及ぶ範囲を減らすことができます。データセンタでは従来型か仮想型のデータセンタかに関わらず、許可されたユーザによってのみデータセンタ アプリケーションが使用されるようにすることで、コンテンツを脅威から保護し、バーチャル インフラストラクチャの動的な性質がもたらすセキュリティ上の問題に対応します。エンタープライズの支社やリモート ユーザは、本社で導入されているものと同じポリシーでのセキュリティが実現できるため、ポリシーの一貫性が確保できます。



paloalto NETWORKS
the network security company™



アプリケーション利用によってビジネスを強化

Palo Alto Networks 次世代ファイアウォールによって安全なアプリケーション利用を実現すれば、ネットワークを通過するアプリケーションの急速な増加にともなうビジネスおよびセキュリティ上のリスクに対応できます。ローカル、モバイル、およびリモートのユーザまたはユーザ グループに対してアプリケーションを有効化し、既知および不明の脅威に対してトラフィックを保護することで、ビジネスを拡大させながらセキュリティ レベルを向上できます。

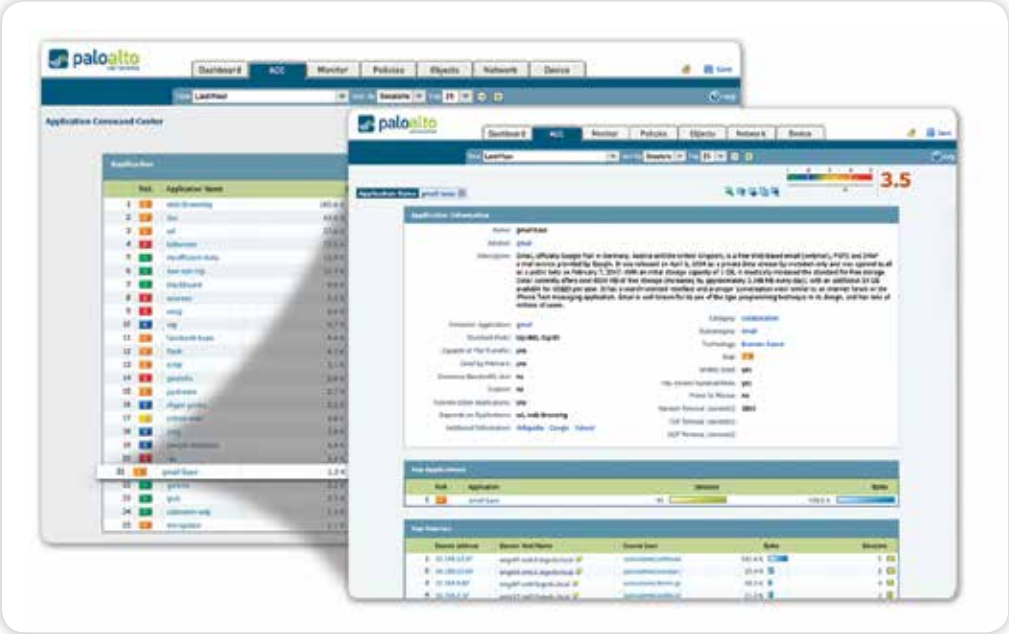
- **すべてのアプリケーションをすべてのポートで常時識別。**トラフィックの正確な識別はあらゆるファイアウォールの中心で、その結果はセキュリティ ポリシーの基礎となります。現在では、ポートホッピング、SSL や SSH による暗号化、80 番ポートの使用、ハイポートの使用などによって、アプリケーションはポートベースのファイアウォールを容易にバイパスできるようになりました。App-ID では、トラフィックがファイアウォールに到達するとすぐに複数の識別メカニズムをトラフィック ストリームに適用することで、従来のファウォールを悩ませていたトラフィック識別の可視化における制約に対処し、使用されているポートや暗号（SSL または SSH）、回避技術に関係なく、ネットワークを通過するアプリケーションを正確に識別します。ポートとプロトコルだけでなく、どんなアプリケーションがネットワークを通過しているかについての正確な情報は、セキュリティ ポリシーの決定すべてにとっての基礎となります。不明なアプリケーションは通常トラフィックの中でわずかな割合しか占めていませんがリスクの可能性は高く、自動的に分類して組織的な管理を行います。これにはポリシー コントロール、調査、脅威のフォレンジック、カスタム App-ID の作成、または Palo Alto Networks App-ID 作成用のパケット キャプチャが含まれます。

- **IP アドレスだけでなくユーザとデバイスをポリシーに統合** - デバイスや場所に関係なくアプリケーションとユーザ識別に基づきセキュリティ ポリシーを作成し管理することは、ポートと IP アドレスだけに依存するよりもネットワーク保護の方法として効果的です。幅広いエンタープライズ向け ディレクトリサービスとの統合によって、アプリケーションにアクセスする Microsoft Windows、Mac OS X、 Linux、Android、または iOS ユーザの識別が提供されます。出張中のユーザやリモートで作業するユーザは、ローカルまたは企業ネットワークで使用されているポリシーと同じ一貫したポリシーでシームレスに保護されます。ユーザのアプリケーション アクティビティに対する可視化と制御を組み合わせることで、ユーザがアクセスしている場所や方法に関係なく、OracleやBitTorrent、Gmailまたはネットワークを通過するその他のアプリケーションを安全に使用することができます。

- **既知および未知のあらゆる脅威から防御** - 現在のネットワークを保護するためには、既知のエクスプロイト、マルウェア、スパイウェアだけでなく、まったく未知の標的型の脅威がやって来る状況に対処することが必要です。このプロセスではまず、特定のアプリケーションを許可して他をすべて拒否することでネットワークの攻撃の元となる通信を減らします。これは「Deny-all-else（一部以外すべて拒否）」戦略を通じて黙示的に行うか、または明確なポリシーを使用して行います。次に、許可されたすべてのトラフィックに統合的な脅威防御検査を適用し、既知のマルウェア サイトや脆弱性攻撃、ウイルス、スパイウェア、および悪意ある DNS クエリを一度の処理で検知しブロックします。バーチャル サンドボックス環境で未知のファイルを実行し 100 を超える悪意ある動作を直接監視することで、カスタムまたは不明なマルウェアを積極的に分析し識別します。新しいマルウェアが検出されると、感染ファイルと関連するマルウェア トラフィックに対するシグネチャが自動的に生成され配信されます。すべての脅威防御分析でアプリケーションとプロトコルの詳細なコンテキストを使用し、たとえ脅威がトンネルや圧縮コンテンツ、ハイポートなどでセキュリティの回避を試みたとしても、常に検出できるようにします。

導入と管理の柔軟性

安全なアプリケーション利用は、専用のハードウェア プラットフォームまたは仮想マシンのいずれかで実現可能です。ハードウェアまたは仮想マシンである複数の Palo Alto Networks ファイアウォールを導入する場合は、Panorama を利用できます。Panorama はトラフィック パターンの可視化やポリシーの導入、レポートの生成、コンテンツ更新の配信を中央から提供する中央管理のためのオプション製品です。



アプリケーションの可視化 : アプリケーション アクティビティを正確でわかりやすい形式で表示します。フィルタの追加および削除で、アプリケーション、機能、利用者の詳細情報を把握できます。

安全なアプリケーション利用のための包括的アプローチ

安全なアプリケーション利用にあたっては、ネットワークを保護しビジネスを成長させる包括的なアプローチが必要で、それにはまずネットワーク上のアプリケーションについて、プラットフォームや場所に関わらず誰が使用しているかや、そのアプリケーションが運んでいるものがあればその内容など、詳細な情報が必要です。ネットワーク アクティビティのより詳細な情報があれば、ビジネスに関連するアプリケーション、ユーザ、コンテンツというエレメントに基づく、より意味のあるセキュリティ ポリシーを作成できます。インターネットの境界、従来型または仮想型のデータセンタ、支社やリモート ユーザなど、ユーザの場所、そのプラットフォーム、ポリシーの導入場所などは、ポリシーの作成方法にとってはほとんど、あるいはまったく関係ありません。つまり、どんなアプリケーションやユーザでも、どんなコンテンツでも安全に使用することが可能になります。

具体的な情報による厳密なセキュリティ ポリシー

セキュリティのベスト プラクティスでは、ネットワーク上に何があるかをより完全に把握することが、より厳密なセキュリティ ポリシーの実施に役立つとされています。たとえば、ポートベースの幅広い一連のトラフィック分類と異なり、どのアプリケーションがネットワークを通過しているかを正確に把握できれば、管理者は不要なアプリケーションをブロックしながら、ビジネスを推進するアプリケーションを具体的に許可することができます。IP アドレスだけでなく利用者が誰かを把握することでさらにポリシーの基準が追加され、これによってポリシーの指定がより明確になります。

- グラフィカルで協力な可視化ツールとの組み合わせによって管理者は、アプリケーション アクティビティやセキュリティに対する潜在的な影響をより詳細に把握でき、より具体的な情報に基づいたポリシーの決定を行うことができます。アプリケーションはその状態の変化に応じて継続的に識別され、グラフィカル サマリが動的に更新されて、使いやすい Web ベースのインターフェイスに情報が表示されます。
- 新しいアプリケーションや不明なアプリケーションをシングル クリックですばやく調べて、アプリケーションの説明、動作特性、およびそのユーザを表示できます。
- URL カテゴリ、脅威、およびデータ パターンに関するデータの追跡によって、ネットワーク アクティビティの包括的な把握を実現します。
- 通常どのネットワーク上でもわずかな割合しか占めないものの潜在リスクの高い不明なアプリケーションも個別で分類されて、内部のアプリケーションであるか、識別を必要とする商用アプリケーションであるか、あるいは脅威であるかが判断されます。

アプリケーションの利用とリスクの削減

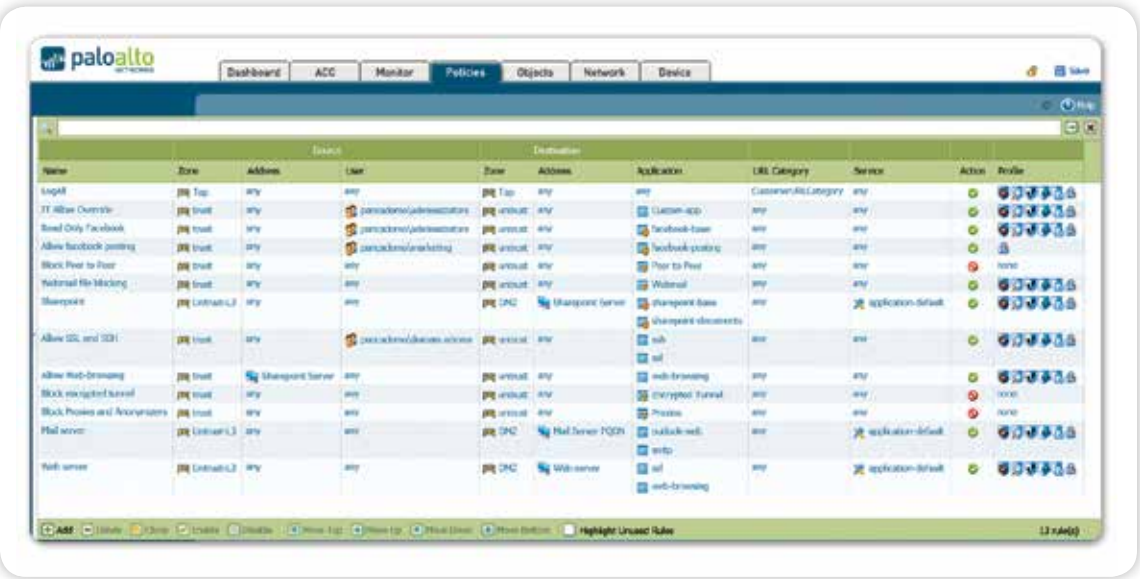
安全なアプリケーション利用を実現するためのポリシーでは、すべてを盲目的に許可するのではなく、リスクが高いけれどもビジネスの制約につながるすべてのアプリケーションを拒否と許可の間でバランスをとる必要があり、そのためアプリケーション/アプリケーション機能、ユーザおよびグループ、コンテンツを含むポリシーの条件を活用することができます。

支社やモバイル、リモート ユーザを含む境界では、使用ポリシーはすべてのトラフィックを識別してからユーザアイデンティティに基づき選択的にトラフィックを許可し、その後、脅威がないかトラフィックをスキャンすることに重点を置きます。ポリシーの例を以下に示します。

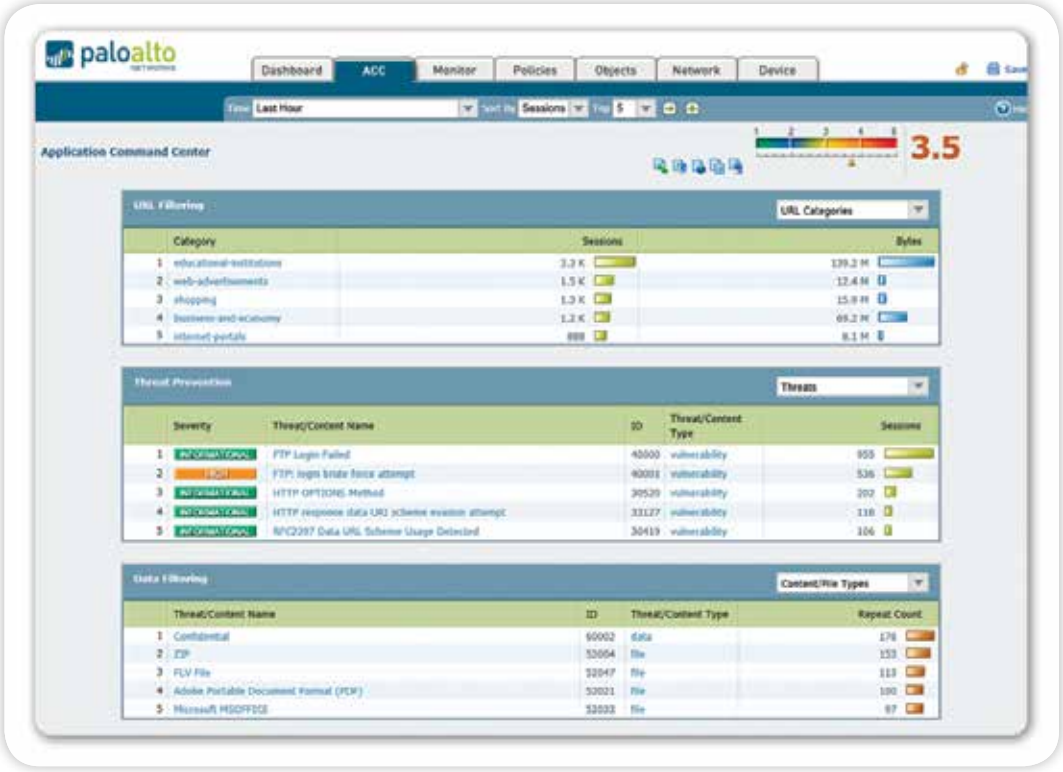
- Web メールやインスタント メッセージングの使用を選択した少数の種類に制限する。SSL を使用するものは復号化し、脆弱性攻撃がないかトラフィックを調査して、不明のファイルを WildFire にアップロードして分析およびシグネチャ作成を行う。
- ストリーミング メディア アプリケーションとWeb サイトは許可するが、QoS とマルウェア防御を適用して VoIP アプリケーションへの影響を制限し、ネットワークを保護する。
- ユーザ全員が「ブラウズ」できるよう許可することで Facebook を制御し、すべての Facebook ゲームとソーシャル プラグインをブロックし、マーケティング部門からの投稿の場合のみ Facebook を許可する。すべての Facebook トラフィックをスキャンし、マルウェアや脆弱性攻撃がないか確認する。
- ビジネス関連の Web サイトへのトラフィックを許可してスキャンを行い、明らかに仕事とは無関係な Web サイトへのアクセスをブロックすることで Web の利用を制御し、カスタマイズされたブロック ページによって疑わしいサイトへのアクセスに対して指導を行う。
- GlobalProtect によってローカル、モバイル、またはリモートのすべてのユーザに同じポリシーをトランスペアレントに導入し、一貫したセキュリティを実施する。
- 黙示的なDeny-all-else（他をすべて拒否）戦略の使用か、P2P や サーカムベンタ、または特定の国からのトラフィックなどの不要なアプリケーションを明示的にブロックすることで、ビジネスおよびセキュリティ上のリスクをもたらすアプリケーション トラフィックを削減する。

従来型、仮想型、またはそれらを組み合わたタイプのデータセンタでは、使用ポリシーの例はアプリケーションの承認、不正アプリケーションの捜索、データの保護が中心になります。

- Oracle ベースのクレジット カード番号リポジトリを独立したセキュリティ ゾーンに切り離し、トラフィックが標準ポートを通過するよう強制し、アプリケーションの脆弱性がないかトラフィックを調査して、財務グループへのアクセスを制御する。
- 標準ポート間のリモート管理アプリケーション（SSH、 RDP、Telnet）の固定セットを定義して、IT グループのみがデータセンタにアクセスできるようにする。
- Microsoft SharePoint Administration の使用を管理チームのみに許可し、Microsoft SharePoint Documents へのアクセスは他のユーザすべてに許可する。



統一されたポリシー エディタ: 使い慣れたルック アンド フィールによって、アプリケーション、ユーザ、およびコンテンツを制御するためのポリシーの迅速な作成と導入を実現します。



コンテンツと脅威の可視化: URL アクセス先、脅威、およびファイル/データ転送アクティビティを正確でわかりやすい形式で表示します。フィルタを追加および削除して、個々のエレメントの詳細情報を把握できます。

アプリケーションの保護

安全なアプリケーションの利用とは、特定のアプリケーションへのアクセスを許可し、次に特定のポリシーを適用して既知の脆弱性攻撃や既知および未知のマルウェアやスパイウェアをブロックし、ファイルやデータ転送、Web閲覧の活動を制御することを意味します。ポートホッピングやトンネリングなど一般的な脅威の回避技法は、App-ID のデコーダによって生成されるアプリケーションおよびプロトコルのコンテキストを使用して脅威防御ポリシーを実行することで対応します。これとは逆に、UTM ソリューションでは各機能、ファイアウォール、IPS、AV、URL フィルタリングで脅威防御への多段モジュール型のアプローチをとり、通信のコンテキスト情報を共有せずに毎回一からトラフィックをスキャンするため、回避的動作の影響を受けやすくなっています。

- **既知の脅威のブロック:** IPS およびネットワーク型アンチウイルス/アンチスパイウェア。統一されたシグネチャ形式とストリームベースのスキャニング エンジンで、ネットワークを幅広い脅威から保護できます。侵入防止システム（IPS）機能がネットワークおよびアプリケーション層の脆弱性攻撃、バッファ オーバフロー、DoS 攻撃、ポート スキャンをブロックします。アンチウイルス/アンチスパイウェア保護機能によって、多数のマルウェアをブロックし、また、マルウェアによって生成されるコマンド アンド コントロール トラフィック（C&C） 通信、PDF ウイルス、圧縮ファイルや Web トラフィック（圧縮 HTTP/HTTPS）内に隠れたマルウェアをブロックします。すべてのポートですべてのアプリケーションにわたりポリシーベースの SSL 復号化を行うことで、マルウェアが SSL で暗号化されたアプリケーション上を移動するのを防ぎます。
- **未知で、標的型のマルウェアをブロック:** Wildfire™。不明な、またはターゲットを絞ったマルウェアを WildFire によって識別し分析します。WildFire はクラウドベースのバーチャル サンドボックス環境で不明なファイルを直接実行し監視します。WildFire は100 を超える悪意ある動作を監視し、その分析結果は警告として管理者に即座に提供されます。オプションで提供されるで提供される WildFire サブスクリプションは、強化された保護、ログ、レポート機能を提供します。サブスクリプションを契約されると、世界のどこで新しいマルウェアが検出されても 1 時間以内にシグネチャが配信され保護されることになり、新しいマルウェアの拡散が影響を及ぼす前に効果的に阻止します。またサブスクリプション契約者は、統合された WildFire ログおよびレポート機能にアクセスでき、分析用に WildFire クラウドにサンプルを送信できる API も利用可能になります。

- **ボットネット感染端末の洗い出し:** App-ID はすべてのポートですべてのアプリケーションを識別し、ネットワークに異常や脅威を及ぼすことが多い不明なトラフィックをすべて識別します。振る舞いベースのボットネットレポート機能では、既知のトラフィックと疑わしい DNS および URL クエリ、様々な異常なネットワーク動作の相互関係を比較し、マルウェアに感染した可能性が高いデバイスを明らかにします。その結果は感染が疑われるホストの一覧として表示されます。これらのホストはボットネットの感染源として調査できます。
- **許可されていないファイルおよびデータの転送を制限:** 管理者はデータのフィルタ処理機能を使用して、許可されていないファイルおよびデータの転送に関連したリスクを軽減するポリシーを適用できます。ファイルの転送では、通信の内部を調べることによってファイルタイプを識別でき（ファイルの拡張子だけを調べる手法とは異なります）、転送を許可するかどうかを判断できます。Drive-by-Download攻撃で通常よく見つかる実行ファイルをブロックすることができるため、不明なマルウェアの伝播からネットワークを保護できます。データのフィルタ処理機能によって、機密データ パターン（クレジット カード番号や社会保障番号、およびカスタム パターン）のフローを検出し制御できます。
- **Web** アクセスの制御製品内に完全統合されたカスタマイズ可能な URL フィルタリング エンジンにより、管理者はきめ細かい Web ブラウジング ポリシーを適用でき、アプリケーションの可視化と制御ポリシーを補完して、様々な法規制、生産低下などのリスクから企業を守ることができます。さらに、URL カテゴリーをポリシーに活用して、SSL 復号化、QoS、その他のルール ベースによりきめ細かい制御を提供できます。

管理と分析

セキュリティのベスト プラクティスでは管理者は、単一のデバイスであっても多数のデバイスであっても、プロアクティブにファイアウォールを管理することと、セキュリティ インシデントに敏感に対応し調査、分析、レポート作成することの間でバランスをとるよう求められます。

- **管理:** Palo Alto Networks の各プラットフォームは、コマンド ライン インターフェイス（CLI）またはフル機能を備えたブラウザベースのインターフェイスを使用して、個別に管理することができます。大規模な導入の場合は一元管理ソリューションとして Panorama をライセンス契約し導入でき、これによってグローバルな設定一元管理と、テンプレートや共有ポリシーなどの機能の使用によるローカル ポリシーの柔軟性の必要との間で、バランスをとることができます。SNMP および REST ベースの API などの 標準ベースのツールへの追加のサポートによって、サードパーティ管理ツールとの統合も可能です。デバイスの Web インターフェイスと Panorama インターフェイスのいずれを使用しても、ルック アンド フィールは全く同じであるため、一方から他方に切り換えた場合もとまどうことはありません。管理者は提供されたインターフェイスのいずれかを使用して、同期の問題に気を揉むことなくいつでも変更を行えます。すべての管理媒体でロールベースの管理がサポートされているため、特定の管理者に一部の機能だけを割り当てることが可能です。
- **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。レポートはすべて CSV 形式または PDF 形式で、スケジュールに合わせて実行したり電子メールで送信することができます。
- **ログ機能:** リアルタイムのログ フィルタ処理によって、ネットワークを通過した各セッションの迅速なフォ レンジック調査が可能です。ログ フィルタの結果は、CSV ファイルにエクスポートするか、syslog サーバーに送信してオフラインでアーカイブしたり、さらに分析したりできます。

専用のハードウェアまたはバーチャル プラットフォーム

Palo Alto Networks には、エンタープライズのリモート オフィス向けの PA-200 から、高速データセンタ向けの PA-5060 まで、あらゆる種類の専用ハードウェア プラットフォームがそろっています。プラットフォーム アーキテクチャはシングル パス ソフトウェア エンジンに基づき、ネットワーキング、セキュリティ、脅威防御、管理といった特定機能に特化した処理プロセッサを使用して高いパフォーマンスを提供します。また、ハードウェア プラットフォームで提供されるものと同じファイアウォール機能は、VM-Series バーチャル ファイアウォールでも利用できるため、インターネットの境界やリモート オフィスのファイアウォールに適用されたものと同じポリシーを使用して、仮想化およびクラウドベースのコンピューティング環境を保護することができます。

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