

次世代ファイアウォールの機能概要

アプリケーション動作および使用状況パターンの近年の変化により、従来のファイアウォールでは攻撃を防御しきれなくなっています。ユーザはあらゆる場所からアプリケーションにアクセスして業務を行うことが増えています。これらの多くのアプリケーションでは、ハイポート、ホップポート、および暗号化を使用してユーザアクセスの簡略化や合理化を図り、ファイアウォールをバイパスしています。サイバー犯罪者は、このような束縛のないアプリケーションの使用状況を悪用してターゲットを絞った新しい種類の巧妙な悪意あるソフトウェアを拡散しています。その結果、ポートおよびプロトコルに依存する従来のファイアウォールでは、ネットワーク上を行き来するアプリケーションや脅威を識別、制御できなくなっています。

アプリケーションの利用状況を管理し、すべてのユーザのデジタル資産を保護しようとする試みの結果、ローカルおよびリモートの二重のセキュリティポリシーが生まれ、スタンドアロンのファイアウォールヘルパーまたはシートメタルが一体化されたファイアウォールヘルパーの業界が支持しています。このようなアプローチでは、正確で完全なトラフィック識別が行われず、管理が煩雑です。また複数のスキャンプロセスによって遅延が発生するばかりか、ポリシーが一貫性を欠き可視化と制御能力の問題の解決にはなりません。可視化および制御能力を再構築するには、次世代のファイアウォールだけが実現できる、安全なアプリケーションの使用を実現する完全に新しいアプローチが必要です。

次世代ファイアウォールには、次の機能が含まれます。

- ポートではなくアプリケーションを識別 — プロトコル、暗号化手法、セキュリティ回避手法にかかわらずアプリケーションを特定し、すべてのセキュリティポリシーの基礎として識別情報を使用します。
- IP アドレスだけでなくユーザを識別 — ユーザがどこにしようと、エンタープライズディレクトリのユーザ情報やグループ情報を、可視化、ポリシー作成、レポート作成、およびフォレンジック調査に利用します。
- リアルタイム脅威防御 — 危険なアプリケーション、脆弱性、悪意あるソフトウェア、高リスク URL、悪意あるファイル、コンテンツによる絶え間ない攻撃から保護します。
- ポリシー管理を簡略化 — 使いやすいグラフィカルツールと統合されたポリシーエディタを使用してアプリケーションを安全に利用できるようにします。
- リモートユーザにもセキュリティポリシーを適用 — 社内ユーザや在宅勤務ユーザによらず、すべてのユーザを、物理的境界から論理的境界まで一貫したセキュリティで保護します。
- マルチギガビットのスループットを実現 — 専用のハードウェアとソフトウェアアーキテクチャにより、すべてのサービスを使用した状態でも低遅延のマルチギガビットパフォーマンスを実現します。

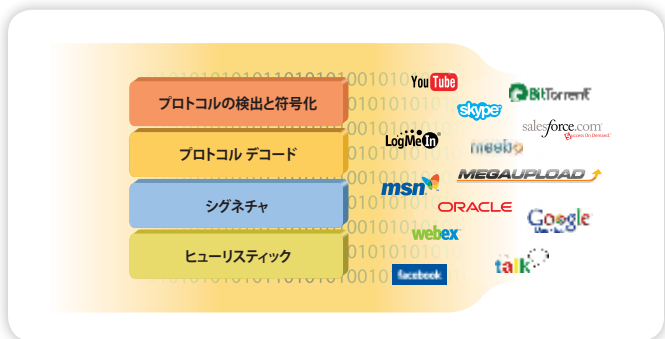
Palo Alto Networks の次世代ファイアウォールに採用されている 3 種類の独自の識別技術 (App-ID™、User-ID、Content-ID) によって、アプリケーション、ユーザ、およびコンテンツを可視化して制御します。これらの識別技術は、すべての Palo Alto Networks ファイアウォールに搭載されており、デバイスの統合により総所有コストを大幅に削減しながらアプリケーションの使用状況を安全に制御します。



App-ID: すべてのアプリケーション、すべてのポート、すべての時刻を常時識別

正確なトラフィック識別はファイアウォールの中核になり、セキュリティポリシーの基盤になります。従来のファイアウォールではトラフィックをポートとプロトコルで識別しました。これは、1か所においてネットワークを守るのに十分なメカニズムでした。現在では、動的なポート変更、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従来の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は、ファイアウォールがトラフィックストリームを検出すると同時に複数の識別メカニズムを適用し、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することにより、従来のファイアウォールの問題であるトラフィック識別可視化の限界を解決します。

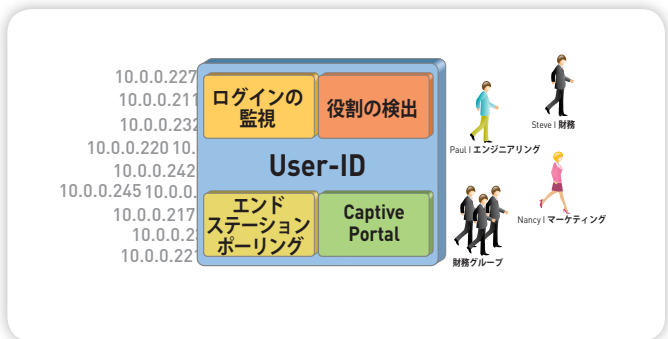
管理者が設定した従来のポートベースのポリシーに対してIPSシグネチャを適用する後付けの手法とは異なり、App-IDは、自動的に最大4つのトラフィック識別メカニズムを使用してアプリケーションを識別します。App-IDは継続的にアプリケーション状態を監視し、トラフィックを再識別し、使用されているさまざまな機能を特定します。セキュリティポリシーにおいてアプリケーションの処理方法、つまり、ブロック、許可、または安全な使用（スキャン、埋め込まれた脅威のブロック、許可されていないファイル転送やデータパターンの検査、QoSを使用したトラフィックシェーピング）を決めます。



User-ID: ユーザおよびグループによるアプリケーションの使用

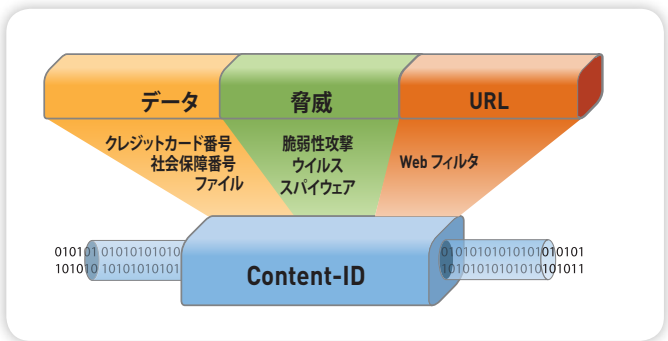
従来、セキュリティポリシーはIPアドレスに基づいて適用されてきましたが、ユーザやコンピューターの使用がますます多様化すると、IPアドレスだけではユーザアクティビティを監視および管理するメカニズムとして不十分になりました。User-IDを使用することによって、ユーザベースアプリケーションまたはグループベースアプリケーションの使用ポリシーをMicrosoft Windows、Apple Mac OS X、Apple iOS、およびLinuxユーザ間に適用できます。

ユーザ情報は、エンタープライズディレクトリ (Microsoft Active Directory、eDirectory、Open LDAP) およびターミナルサービス製品 (Citrix、Microsoft Terminal Services) から収集できます。また、Microsoft Exchange、Captive Portal、およびXML APIとの統合により、組織は、通常はドメイン外部に存在するApple Mac OS X、Apple iOS、UNIXユーザにまでポリシーを適用できます。



Content-ID: 許可されたトラフィックの保護

今日のほとんどのアプリケーションには大きな利点がありますが、現代の悪意あるソフトウェアおよび脅威を呼び込む道具としても使用されているのが現状です。Content-IDとApp-IDを併用すると、ネットワークを保護する二面解決策になります。App-IDを使用して不要なアプリケーションを識別してブロックした後、管理者は、脆弱性攻撃、最近の悪意あるソフトウェア、ウイルス、ボットネット、その他のマルウェアが、ポート、プロトコル、回避手法に関係なくネットワークに拡散されるのをブロックすることによって、許可されたアプリケーションを安全に有効にすることができます。Content-IDの制御機能は包括的なURLデータベースにも対応し、Webの利用やデータフィルタリング機能を制御します。



安全なアプリケーションの使用

App-ID、User-ID、Content-ID をシームレスに統合することにより、基本的な許可または拒否だけではない一貫したアプリケーション使用ポリシーを、多くの場合アプリケーションの各機能のレベルにまで適用できます。GlobalProtect™ によって、本社のユーザを保護するのと同じポリシーが、ユーザがどこにいるかに関係なく、すべてのユーザに適用され、ネットワークの外側にいるユーザの論理的境界を確立できます。

安全なアプリケーション使用を可能にするポリシーは、App-ID により決定されるアプリケーション識別から始まります。このアプリケーション識別情報は User-ID を使用して関連するユーザにマッピングされます。トラフィックコンテンツは Content-ID により、脅威、ファイル、データ パターン、および Web アクティビティがスキャンされます。これらの結果は ACC に表示され、管理者はほぼリアルタイムでネットワークの動作を知ることができます。このとき、ポリシー エディタでは、ACC で表示されたアプリケーション、ユーザ、およびコンテンツに関する情報を利用して、不要なアプリケーションをブロックする一方、他のアプリケーションを安全な方法で許可して使用できるようにします。最後に、アプリケーション、ユーザ、およびコンテンツを基準にした詳細な分析、レポート作成、またはフォレンジックを再度実行できます。

Application Command Center: 知識は力

ACC は、ログ データベースの分析をグラフィカルに総括することにより、ネットワークを通過するアプリケーション、利用しているユーザ名、およびセキュリティに対する潜在的な影響を浮き彫りにします。ACC は動的に更新され、App-ID が実行する継続的なトラフィックの識別を利用します。アプリケーションがポートまたは動作を変更した場合、App-ID は引き続きトラフィックを監視して、結果を ACC に表示します。ACC に表示される新規または見慣れないアプリケーションは、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、主要な機能、動作特性、およびユーザを表示できます。URL カテゴリ、脅威、およびデータに関する追加の可視化データは、ネットワーク アクティビティの包括的なイメージを補完します。ACC を使用して、管理者は、ネットワーク内外を通過するトラフィックの詳細情報をすばやく把握し、その情報を確かなセキュリティ ポリシーに反映できます。

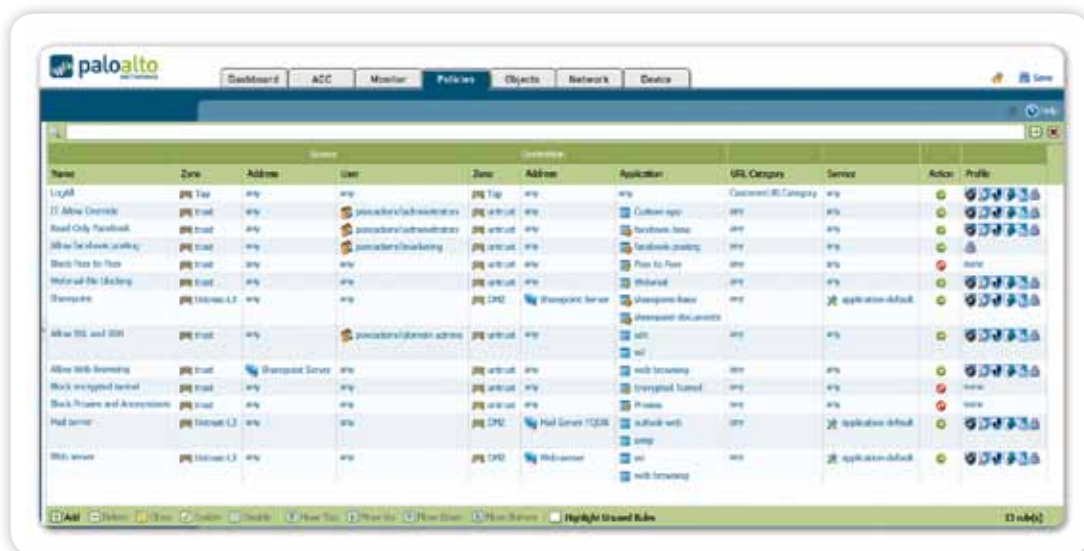
ポリシー エディタ: 安全な使用ポリシーに取得情報を反映
管理者は、ネットワークを通過するアプリケーション、利用しているユーザ名、および潜在的なセキュリティ リスクの種類を知ることができるため、アプリケーション、アプリケーション機能、およびポートベースの使用ポリシーを体系的かつ管理された方法で導入できます。ポリシーは、オープン (許可) から、モデレート (特定のアプリケーションまたは機能を使用して、スキャン、トラフィック シューピング、スケジューリングなど)、クローズ (拒否) の範囲で対応します。例を以下に示します。

- 財務グループへのアクセスを制限して Oracle データベースの保護、標準ポート間のトラフィックの強要、トラフィックにおけるアプリケーションの脆弱性の検査を実行する。
- 標準ポート間のリモート管理アプリケーション (SSH、RDP、Telnet) のセットを定義して、IT グループのみがこれらのアプリケーションを使用できるようにする。
- 特定の Web メールやインスタント メッセージングの使用を許可するが、それぞれのファイル転送機能をブロックする企業ポリシーを定義および適用する。
- Microsoft SharePoint Administration の使用を管理チームのみに許可し、Microsoft SharePoint Documents へのアクセスを他のユーザすべてに許可する。
- Web 使用ポリシーを導入することで、明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し、カスタマイズされたブロック ページを使用して適切なサイトへのアクセスを指導する。

アプリケーションの可視性
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。フィルタを追加および削除して、アプリケーション、機能、およびユーザの詳細情報を把握できます。



統一されたポリシーエディタ
 使い慣れたロックアンド
 フィールドによって、アプリケー
 ション、ユーザ、およびコンテ
 ントを制御するためのポリシー
 の迅速な作成と導入を実現。



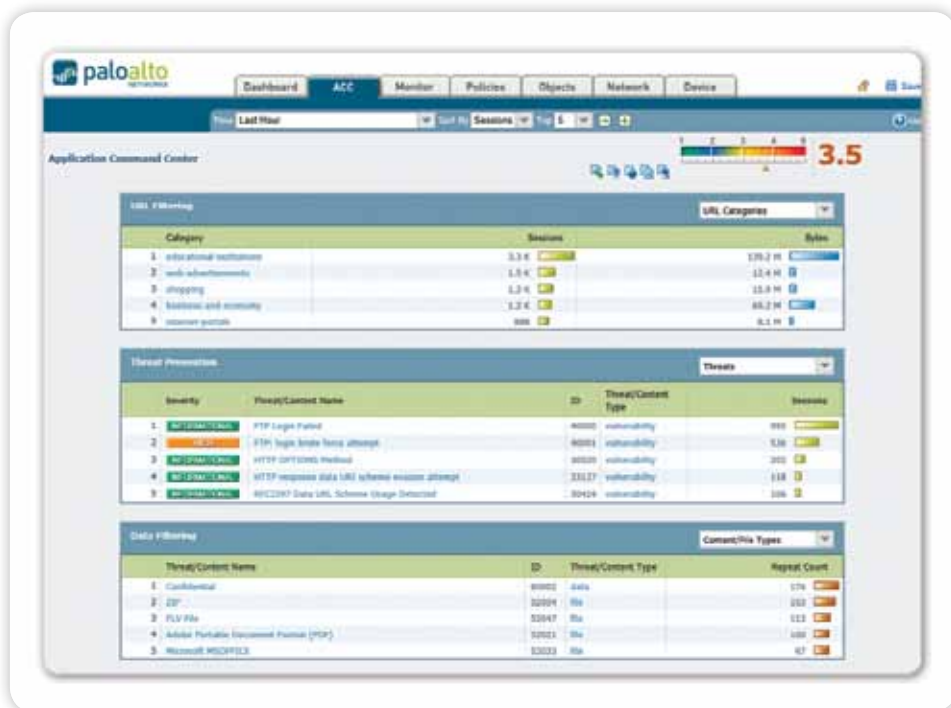
- QoS ポリシーを適用することで、帯域幅を大量に消費するメディア アプリケーションおよび Web サイトを許可する一方で、VoIP アプリケーションに対する影響を制限する。
- ソーシャル ネットワーキングおよび Web メール サイトの SSL トラフィックを復号化し、悪意あるソフトウェアおよび攻撃をスキャンする。
- ユーザ承認を行い、ゼロデイ攻撃によるドライブバイダウンロードを防止してから、まだ識別されていない Web サイトからの実行ファイルのダウンロードを許可する。
- 特定国からのすべてのトラフィックを拒否するか、P2P ファイル共有、検閲回避ツール、外部プロキシなどの不要なアプリケーションをブロックする。

ユーザとグループに基づくアプリケーション管理を強固に統合し、許可されたトラフィックでさまざまな脅威をスキャンできるようになると、企業は、導入するポリシー数と共に日常的に発生する社員の追加、移動、および変更数を大幅に低減できます。

ポリシー エディタ : 使用するアプリケーションの保護
 アプリケーションを安全に使用できるようになると、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。Content-ID に含まれている各要素は、アプリケーション ベースで設定できます。

- 侵入防止システム (IPS): 脆弱性保護機能は、侵入防止システム (IPS) の豊富な機能を統合したものです。この機能を使用すると、ネットワーク層とアプリケーション層の脆弱性攻撃、バッファ オーバーフロー、DoS 攻撃、およびポート スキャンを防ぐことができます。
- ネットワーク アンチウイルス: ストリーム ベースのアンチウイルス保護機能は、圧縮ファイルまたは Web トラフィック (圧縮された HTTP/HTTPS) 内に隠れている PDF ウイルスや悪意のあるソフトウェアを含む、非常に多くのさまざまな悪意のあるソフトウェアをブロックします。ポリシーベースの SSL 暗号解読を使用すると、企業は、悪意のあるソフトウェアが SSL で暗号化されたアプリケーションを移動するのを防ぐことができます。
- URL フィルタ: 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 データベースにより、管理者はきめ細かい Web ブラウジング ポリシーを適用し、アプリケーションの可視化と制御ポリシーを補完し、さまざまな法規制、生産低下などのリスクから企業を守ることができます。
- ファイルとデータのフィルタ処理: 管理者は、データのフィルタ処理機能を使用すると、ファイル転送とデータ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。ファイルの転送とダウンロードは、ファイルの内部を調べることによって制御し (ファイルの拡張子だけを調べる手法とは異なります)、許可するかどうかを決めることができます。実行ファイルの自動ダウンロードをブロックすることができるので、ネットワークに悪意のあるソフトウェアが入り込むことを防ぐことができます。最後に、データのフィルタ処理機能は、クレジットカード番号や社会保障番号などの機密データ パターンを検出して制御できます。

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、個々の要素の詳細情報を把握できます。



悪意あるソフトウェアの検出と防止

悪意あるソフトウェアは、伸張性のあるネットワーク化されたアプリケーションに進化した結果、標的とするネットワークにたやすく侵入して支配する機会を攻撃者に与えるようになりました。悪意あるソフトウェアの威力が増すに従って、脅威が明らかになる前に即座に検出することが企業にとって不可欠となっています。Palo Alto Networks の次世代のファイアウォールは、実行ファイルとネットワークトラフィック両方を直接分析する多面アプローチによって、シグネチャをまだ確認できないような段階であってもネットワークを保護できます。

- **WildFire™**: クラウドベースのアプローチを利用した WildFire は、従来は不可視であった悪意ある実行ファイルの動作を、安全な仮想化された環境で観察することによって明らかにします。WildFire は、Microsoft Windows の実行ファイルの悪意あるアクション（レジストリ値の変更、オペレーティングシステムのファイル改ざん、セキュリティメカニズムの無効化、実行プロセスへのコード挿入など）を検出します。この直接分析によって、保護メカニズムが機能しない場合でも悪意あるソフトウェアを迅速かつ正確に特定できます。結果は即座に管理者に通知されて適切な対策を促し、シグネチャが自動的に開発され、次のコンテンツ更新時にすべての顧客に提供されます。
- **ボットネットの動作の検出**: App-ID はアプリケーションレベルですべてのトラフィックを識別し、これによりネットワーク上の不明なトラフィックを明らかにします。このようなトラフィックは、悪意あるソフトウェアや他の脅威が存在する兆候となることが多くあります。ボットネット動作レポートでは、悪意あるソフトウェアサイトへの反復訪問、動的 DNS の使用、IRC、他の疑わしい振る舞いなどのボットネット感染を示すネットワーク動作が分析されます。感染の可能性のあるホストの一覧が結果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する必要があります。

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

セキュリティ ベスト プラクティスでは、管理者が前向きに継続して認識を深めて順応して法人資産を守ることとセキュリティ問題に敏感に対応し調査、分析、レポートを行うことをうまく両立させることが求められます。ACC とポリシー エディタを使用すると、アプリケーション使用ポリシーを積極的に適用できますが、豊富な監視ツールとレポート作成ツールは、Palo Alto Networks の次世代のファイアウォールを利用してアプリケーション、ユーザ、およびコンテンツを分析してレポートするために必要な手順を企業に提供します。

- **App-Scope**: App-scope は、ACC によって表示されるアプリケーションとコンテンツのリアルタイムビューを補完し、一定の期間のアプリケーション、トラフィック、および脅威アクティビティを動的に、ユーザがカスタマイズ可能な状態で表示します。
- **レポート作成機能**: 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 形式でエクスポートでき、スケジュールどおりに電子メールで送信することもできます。
- **ログ作成機能**: 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になります。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アーカイブしたり、さらに分析したりすることができます。
- **セッション追跡ツール**: 各セッションに関連付けられたトラフィック、脅威、URL、およびアプリケーションのすべてのログを集中的および相関的に表示して、フォレンジック調査またはインシデント調査の時間を短縮します。

グローバルな保護:あらゆる場所で一貫したセキュリティ
アプリケーションは、企業の変化の機動力となるだけではありません。自由に選択したデバイスにどの場所からでも簡単に接続してビジネスをしたいというエンドユーザが増えています。その結果、IT チームは、従来のような企業境界の外側にあるデバイスや場所にまでセキュリティを拡大しようと努めています。GlobalProtect、一貫したセキュリティ ポリシーを場所およびデバイスに関係なくすべてのユーザに適用することによってこの課題を解決します。

GlobalProtect、Microsoft Windows、Apple Mac OS X、Apple iOS などのさまざまなデバイスをサポートするトランスペアレントな VPN を使用してすべてのユーザに対して安全なアクセスを保証します。いったん接続すると、すべてのトラフィックをファイアウォールで識別し、使用ポリシーを適用してトラフィックの脅威をスキャンすると、ネットワークおよびユーザが保護されます。

また、グローバルな保護ではエンドユーザのデバイスの状態に基づいて追加の制御を適用できます。たとえば、デバイスのウイルス対策ソフトの有効期限が切れているか、またはディスク暗号化が有効になっていない場合、特定のアプリケーションやネットワークの保護区域へのアクセスは拒否される可能性があります。これによって、IT チームはエンドユーザが使用しているデバイスの種類に関係なく、アプリケーション使用を安全に運用できるだけでなく、一貫した次世代のセキュリティ アプローチを維持できます。

グローバルな保護
どんな場所にしようと、すべてのユーザに一貫した安全なアプリケーション使用ポリシーを実現します。

