



It's Time to Fix the Firewall

今こそファイアウォールを”修復”しよう

企業ネットワークセキュリティ基盤となるファイアウォールの再構築

2009年2月

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408-738-7700
www.paloaltonetworks.com

目次

概要	3
新種のアプリケーションとその脅威は非常に捕まえにくい	4
個人用アプリケーションの普及	4
業務用アプリケーションが個人用アプリケーションを模倣している	4
脅威の進化: 動機の変化とアプリケーションとの深い結びつき	5
IT はもう制御不能である	5
従来のポートブロック方式のファイアウォールは効果がない	6
ファイアウォールの救済は失敗した	7
追加型の DPI (Deep Packet Inspection) のアプローチには基本的な欠陥がある	7
ファイアウォール補完製品の導入では問題を解決できず、 複雑でコストのかかる装置を無益に増加させる	7
今こそファイアウォールを修復しよう	8
Palo Alto Networks と次世代ファイアウォールのご紹介	8
可視性と制御を取り戻す独自の識別技術	9
App-ID – ポートやプロトコル、SSL 暗号化に左右されずにアプリケーションを識別する	9
User-ID – IP アドレスだけではなく、ユーザー単位、グループ単位に可視性と制御を実現する	10
Content-ID – 高性能なコンテンツスキャンは、脅威や不正なウェブコンテンツ、 慎重に取り扱うべきデータの漏洩を防ぐ	10
高性能な SP3 アーキテクチャが「妥協のないセキュリティ」を提供する	12
エンタープライズ向けのソリューションを実現するその他の機能	13
企業セキュリティの新たな基盤	14

Copyright 2009, Palo Alto Networks, Inc. 無断複写・転載を禁じます。Palo Alto Networks、Palo Alto Networks ロゴ、PAN-OS、App-ID は米国における Palo Alto Networks, Inc. の商標です。仕様はすべて予告なく変更される場合があります。本文書内の誤りや本文書中の情報更新義務に関し、Palo Alto Networks はいかなる責任も負わないものとします。Palo Alto Networks は、本出版物を予告なく変更、修正、権利譲渡、または他の何らかの方法で改訂する権利を留保します。

概要

この 15 年間、ポートをブロックする方式のファイアウォールが企業ネットワークセキュリティの基盤 (cornerstone) となってきました。しかし、高速に進化していくアプリケーションとその脅威に対して、この種のファイアウォールはまさに石 (stone) のように佇んでいるだけでした。近年のアプリケーションとその脅威が、この種のファイアウォールを簡単にすり抜けてしまうことは明らかとなっています。このため、各企業は「ファイアウォールを補完する製品」を導入し、アプリケーションとその脅威に対応しようとしてきました。しかし、アプリケーションとその脅威は簡単にそれらをすり抜けてしまうため、有効な対策とはならず、結果、企業の IT 部門はさらに複雑な問題とコストを抱えています。

Palo Alto Networks はファイアウォールを修復するために設立され、白紙の状態からアプリケーションやユーザー、コンテンツといった主要な要素に可視性と制御を与えます。高性能なアーキテクチャで構成された Palo Alto Networks の次世代ファイアウォールにより、企業は不要なリスクを冒すことなく、新種のアプリケーションを安全に使用できるようになります。ファイアウォールの修復により、企業は多くの可視性と制御を手に入れ、リスクを減らすことが可能です。またファイアウォールを修復する更なるメリットとして、企業は複雑さやコストが低下することで、合理的でよりシンプルなネットワークセキュリティが得られます。

新種のアプリケーションとその脅威は非常に捕まえにくい

この数年、アプリケーションとその脅威の全体像には多くの重大な変化がありました。

個人用アプリケーションの普及

まず、はじめにユーザー中心のアプリケーションが普及しました。インターネット専用で当初から個人間のコミュニケーション向けに作られたアプリケーションとして、インスタントメッセージやピアツーピアのファイル共有、ウェブメールや近年大量に出現したソーシャルネットワークサイトなどが挙げられます。問題は企業ネットワークにおいて、たとえ企業がポリシー上使用を禁止していたとしても、実際にはこれらのアプリケーションは間違いなく使用されてしまうことです。これらのアプリケーションは非常に人気があるだけでなく、ファイアウォールなどの従来の利用防止策を、自らの通信方法を動的に変更し回避するように作られています。よく知られている手段として次のようなものがあります。

- ポートホッピング、これはポートやプロトコルをセッション中にランダムに変化させることをいいます
- 標準でないポートの使用、たとえば Yahoo! Messenger を TCP ポート 5050 番の代わりに TCP ポート 80 番で使用するを指します
- 広く利用されているサービスの内側をトンネルさせる方法、たとえば、ピアツーピアのファイル共有であったり、Meebo のようなインスタントメッセージのクライアントを HTTP 上で使用することを指します
- SSL による暗号化で通信内容を隠す方法。

業務用アプリケーションが個人用アプリケーションを模倣している

互いに密接に関連した 2 つの変化が事態をより複雑化させています。第一の変化は、これらの次世代アプリケーションが単なる個人間のコミュニケーションツール以上に非常に有用であることが証明されたことです。最近では世界中の企業でこれらのアプリケーションが正式に業務用として日常的に利用され、主要な業務を加速し、顧客サービスを向上し、調整やコミュニケーションの向上、従業員の生産力の向上を補助する役割をおおむね担っています。

第二の変化は新種の多くの業務用アプリケーションが上記で述べた個人用アプリケーションと同種の回避技術を利用して作られるようになったことです。特に顧客やパートナー、企業自身のセキュリティや運用を取り扱う部門にとって、最小限の混乱で容易に業務運用を可能にしたい場合にこの方法は非常に有益です。ただし、意図しない IT の副作用でネットワーク通信の制御がまったく利かなくなるため、非常に問題になります。

他の関連した傾向として、企業向けアプリケーションが Web 化していることが挙げられます。管理稼働やコストを削減してアクセスの容易性を向上させるために、標準的なクライアントサーバーアプリケーションは着実に Web 技術を利用したものに生まれ変わってきています。そして、従来のアプリケーションの多くは徐々に Salesforce.com や WebEx、Google Apps のようなホスト型で Web ベースのサービスに取って代わられています。その結果、HTTP と HTTPS のトラフィックはすべての企業で扱うトラフィックのおよそ 3 分の 2 を占めるようになりました。それ自体は問題ではありませんが、従来のセキュリティインフラに内在する弱点をさらに悪化させています。特に古いソフトウェアにとって、この一般的なプロトコルの上に乗る多くの上位アプリケーションが正式に業務目的で利用されているかどうかを見分けることは不可能です。

脅威の進化: 動機の変化とアプリケーションとの深い結び付き

脅威の全体像に目を向けると、こちらにも大きな変化がありました。具体的には、ハッキングの動機が名声を得る目的から、実際に金銭的に利益を得る目的へと変化し、これはハッカーが上述の回避行動を中心に考えて行動していることを意味します。その際、一般的にハッカーはアプリケーション層に脅威となるプログラムを構築する手段をとります。これにより、ハッカーのプログラムが、大多数の企業のセキュリティをすり抜けることが可能になります。これは企業のセキュリティがネットワーク層に対する攻撃への防御手段として設計されているためです。

今日のハッカーはユーザー中心のアプリケーションの普及度にも注目しています。これは SANS Institute がインスタントメッセージやピアツーピアのプログラムを SANS が選ぶ上位 20 位のセキュリティリスクに常に挙げていることからわかります。これらのアプリケーションはその人気の高さからハッカーの格好の標的となるだけでなく、これらアプリケーションの持つ回避技術によってハッカーが企業ネットワークへ「制限なく」進入できるようになります。

IT はもう制御不能である

アプリケーションとその脅威の全体像の変化により、IT は制御不能になりました。現実的には、ほとんどの会社でセキュリティインフラにより優良で望ましいアプリケーションと悪質で望まないアプリケーションとを効果的に区別することが不可能で、適切な手段も残されていません。1 つの手段として、業務を通常どおり継続し、次世代アプリケーションによる通信をチェックなしに許可することにより望ましいアプリケーションの動作を保障する方法があります。一方、手持ちのツールを使用して悪質で望まないアプリケーションの通信の切断を試みる方法もあります。しかし、後者の方法は成功するとはいいがたく、優良なアプリケーションの通信までも切断してしまう傾向があります。

この状況を修復するため、企業は次に挙げるトラフィックを識別する可視性と知能を持つことが必要です。

- 正式な業務目的で利用されているアプリケーションと対応しているネットワークトラフィック
- 正式な業務目的で利用されている可能性もあるが、許可されていない活動で使われている可能性もあるアプリケーションと対応しているネットワークトラフィック
- 正式な業務に利用されているが、悪意のあるソフトウェアやその他の脅威を防ぐためにブロックすべき通信トラフィック

従来のポートブロック方式のファイアウォールは効果がない

粒度の細かいアクセス制御を実行する機能が、従来の企業ファイアウォールには求められてきました。通信トラフィックの流れを制御できる性能を生かして、従来のファイアウォールは企業セキュリティの大黒柱として、信頼度のレベルの異なるドメイン間に境界を設けるために利用されており、たとえばインターネットゲートウェイや、パートナー企業との接続、最近ではデータセンターとの論理的な入り口部分においての利用が挙げられます。

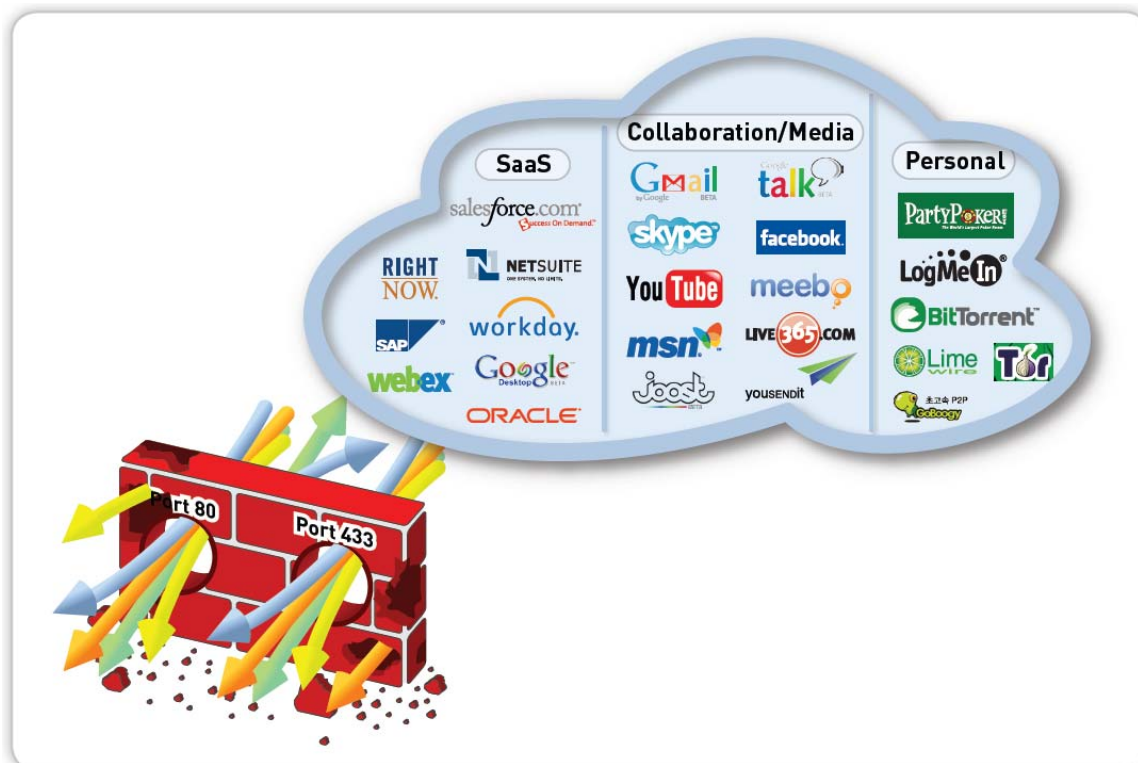


図 1: ポートブロック方式のファイアウォールではアプリケーションを判別、制御できない

しかし、問題は大半のファイアウォールが遠視眼であることです。通信の一般的な形式は判別できますが、実際に起きている詳細な通信を判別できません。なぜなら従来のファイアウォールは、アプリケーション層のサービスにおけるトラフィックの流れはポート番号と紐付いていることを想定して動作するからです。各サービスに対応したポートがある(例: TCP ポート 80 番は HTTP に対応する)という慣例に従い、ユーザーの要件を満たすことはありません。このため、同一のポートやサービスを使用する異なるアプリケーションを区別することもできません。

結果、従来の「ポートブロック方式」のファイアウォールは基本的に次世代アプリケーションには通用しません。ポートホッピングやプロトコルトンネリング、標準でないポートの使用といった、よく利用される回避技術に太刀打ちできません。このため、上述の可視性と知能への取り組みを始めることさえできません。これらの製品や、同様な制限のある他の競合製品に頼りつづける企業のネットワークは、アメリカ開拓期の西部そのものとなり果て、ユーザーはあらゆるアプリケーションを使ってどんなことでも実現できてしまいます。

ファイアウォールの救済は失敗した

従来のファイアウォールの不十分な機能への対処として、2つの方法が最もよくとられますが、その意図や目的をまったく達成できず失敗に終わっています。

追加型の DPI (Deep Packet Inspection) のアプローチには基本的な欠陥がある

従来のファイアウォール製品ベンダーの多くは、詳細パケット検査 (DPI) の性能を組み込むことで製品の制御機能を修復しようとしています。一見すると、この方式でアプリケーション層の可視性と制御を得るのが合理的なアプローチに見えますが、大半の場合、(a) 機能が「追加型」であることと、(b) そもそも追加される元となる基礎部分が脆弱であることから、得られるセキュリティ効果の増分は小さくなります。言い換えると、新機能は組み込み型というよりは統合型であり、ポートブロック方式のファイアウォールはアプリケーションを認識する能力がないため、いまだに最初の全トラフィックの分類のために利用されています。これは次のような問題と制限を含んでいます。

- 検査すべきトラフィックが必ずしもすべて検査されるわけではありません。ファイアウォールはアプリケーションのトラフィックを正確に分類できず、DPI の対象とすべきかどうかの判断を誤る場合があります。
- ポリシー管理が複雑になります。個々のアプリケーションに適用されるルールは製品の DPI 部分に含まれるため、必然的に「ネスト構造」となり、製品そのものが上位レベルの外向けのアクセス制御ポリシーとして動作します。
- 不十分な性能が妥協を生みます。システムリソースや CPU の非効率な使用や、メモリー消費の激しいアプリケーション層の機能が基盤プラットフォームにかなりの負担を掛けます。この状況に対処するため、管理者は高度なフィルタリングを選択して導入するだけになります。

ファイアウォール補完製品の導入では問題を解決できず、複雑でコストのかかる装置を無益に増加させる

他に選択肢がないため、企業はファイアウォールの弱点を、大半がスタンドアロン型の装置である、追加のセキュリティ製品を導入してカバーしようと試みました。侵入防止装置やウィルス対策用ゲートウェイ、Web フィルタリング製品、たとえばインスタントメッセージ対応のセキュリティ製品などに代表されるアプリケーション特化型の製品は、人気製品のごく一部にすぎません。ただしその効果は残念ながら DPI によるアプローチと同様で、追加するたびに複雑さを増すものばかりです。

すべてのトラフィックを検査できない理由は、ファイアウォール補完製品はすべてのトラフィックを観測することができず、従来のファイアウォールで失敗してきたポートベースやプロトコルベースでの分類手法に頼るものや、一定のアプリケーションしかカバーしないものであるためです。ポリシー管理はアクセス制御のルールや検査の要求条件が数台のコンソールにまたがることを考えると、一層大きな問題です。全体の遅延が比較的大きくなる点では性能面でも問題があります。

そして、装置の無益な増加が問題となります。次々と製品をネットワークに追加した結果、装置数、構成の複雑さ、保持にかかる総合的な費用は上昇し続けます。必要となる製品自体の費用とインフラの費用に加え、サポート契約や維持契約、コンテンツ契約費用、設備費用 (例: 電力、空調、フロアスペースなど) を含む運用経費が絶えず発生し、IT の生産性や研修、ベンダー管理に関連するソフト費用も発生することはいうまでもありません。結果、費用がかかり、扱いにくく非効率で、維持困難なものとなります。

今こそファイアウォールを修復しよう

ファイアウォールはネットワークの重要な合流点に直列に配置されることから、すべてのトラフィックを監視可能で、トラフィック制御を行うには理想的な装置であることは明らかなです。その課題は、これまで述べてきたように、従来のファイアウォールが最新世代のアプリケーションとその脅威に無力であることです。ただしこれは問題の一部にすぎません。問題のもうひとつの側面は、この状況を修復するためにファイアウォールの弱点を補うことだけに着目した方法しか実現されていないことです。優秀さからは程遠いこれらのアプローチでは、疑問が残ります。なぜ、根本的に問題を解決しようとしないのでしょうか。

非常に効果的で最新型のファイアウォールに必要とされる、次のような本質的な機能要件に取り組んだ製品を提供して、上述のファイアウォール補完製品を不要にしましょう。

- ポートやプロトコル、回避技術や SSL 暗号化に左右されずアプリケーションを特定する能力
- アプリケーションおよび各アプリケーションの個々の機能に対し粒度の細かい可視性とポリシー制御を提供する能力
- ユーザーを正確に特定し、その後ユーザー情報をポリシー制御の要素として利用する能力
- アプリケーション層で動作するものも含めたさまざまな脅威をリアルタイムに防御する能力
- ギガビット単位のトラフィックに対応し、直列に配置してもパフォーマンスにほとんど影響を与えない能力

Palo Alto Networks と次世代ファイアウォールのご紹介

セキュリティ関連の専門家で ステートフルインスペクションの共同発明者であり、最新世代のアプリケーションとその脅威に対する功績で知られている Nir Zuk により 2005 年に Palo Alto Networks は設立されました。一流の投資家とネットワークセキュリティ業界に経験豊富な経営陣のもと、Palo Alto Networks の技術者はファイアウォールを「根本的に修復する」ことにより、企業のファイアウォールに有用性を取り戻す作業を開始しました。弊社の技術陣は白紙の状態から、企業ネットワークを通過する、新旧を問わないすべてのアプリケーションに対して可視性と制御を有効にするため、トラフィック分類にアプリケーションを中心としたアプローチを行いました。この努力の結果が Palo Alto Networks の次世代ファイアウォールであり、前項で述べた本質的な機能要件をすべて満たした、市場で唯一のファイアウォール製品です。

この差異と次世代ファイアウォールの市場をリードする能力の鍵となるのは、3 つの革新的な識別技術と高性能な設計、堅牢な企業クラスのソリューションを生み出す付加機能の連携です。

可視性と制御を取り戻す独自の識別技術

Palo Alto Networks の次世代ファイアウォールは、高次元の可視性と制御を達成するために 3 つの独自の技術、App-ID、User-ID、Content-ID を利用します。これらの技術により、不透明で間違いの多いポートやプロトコルといった要素に頼ることなく、企業は業務に関連する項目であるアプリケーション、ユーザー、コンテンツに着目してポリシー制御を行うことができます。

App-ID – ポートやプロトコル、SSL 暗号化に左右されずにアプリケーションを識別する

App-ID は特許申請中のトラフィック分類技術で、次世代ファイアウォールの中核を担います。4 つの特徴的な技術を利用し、ネットワーク上で通信される 800 以上のアプリケーションを、ポート、プロトコル、SSL 暗号化、回避技術に左右されることなく正確に識別することが可能です。

アプリケーションプロトコルの検知と解釈 この最初のステップではアプリケーションプロトコル (例: HTTP) を判定し、SSL が使用されていれば、解析できるようトラフィックを解釈します。すべての識別技術により処理された後は必要であれば再暗号化を行います。

アプリケーションプロトコルの復号化 この技術は最初に検知したアプリケーションプロトコルが「本物」か、それとも本当のアプリケーションを隠すためのトンネル (例: Yahoo! Instant Messenger は HTTP で偽装されている可能性があります) かを判定します。

アプリケーションの定義形式 このステップでは、さまざまなアプリケーションの定義形式データから、通信されているアプリケーションの独自の性質や通信方法の特徴を割り出し、ポートやプロトコルに依らないアプリケーションの識別を正確に行います。たとえば、ファイル送信がインスタントメッセージのセッション内で行われていたり、会議用アプリケーション内でデスクトップ共有が行われたりする場合が挙げられます。

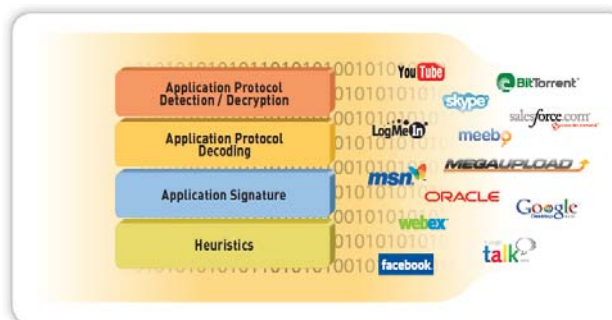


図 2: App-ID はポート、プロトコル、回避技術、SSL 暗号化に左右されることなくアプリケーションを識別する

経験則 定義形式分析を回避したトラフィックに対して、経験則、動作特性による解析処理を適用します。これにより、ピアツーピア通信であったり独自の暗号化技術を使った VoIP ツールなどのトラブルを起こしやすいアプリケーションの識別を可能にします。

アプリケーションの識別は問題の一部にすぎないことから、Palo Alto Networks ではアプリケーションブラウザにより App-ID を補完します。この強力な調査ツールにより、管理者は 800 以上のアプリケーションの情報から、それらをどう制御するかを判断できます。アプリケーション情報はカテゴリ別、サブカテゴリ別に関連可能で、基盤となる技術、ファイル送信能力、知られている脆弱性、検知を回避する能力、帯域を消費する性質、悪意のあるソフトウェアを送信する性質、悪用される可能性を含んだアプリケーションの特徴を表示可能です。

App-ID により、IT 部門は、ネットワーク上を行き交うアプリケーションを効果的に制御するポリシーを作成、強化するのに必要な可視性と知能を得ることができます。

User-ID – IP アドレスだけではなく、ユーザー単位、グループ単位に可視性と制御を実現する

Palo Alto Networks のファイアウォールの標準機能である User-ID 技術は、IP アドレスを特定のユーザー識別情報と紐付けることにより、ネットワークアクティビティの可視性と制御をユーザー単位に実現できます。Microsoft Active Directory (AD) と密接に連携することにより、Palo Alto Networks User Identification Agent は 2 つの方法でこの目的を達成します。まず、ユーザーと IP アドレスの紐付けを、ログイン監視、エンドステーションポーリング、Captive Portal 技術を組み合わせて利用することで確認し、維持します。次に AD のドメインコントローラと通信し、職務や組織属性といったユーザー情報を抽出します。これらの詳細情報により次のことが可能になります。

- ネットワーク上のすべてのアプリケーション、コンテンツ、脅威となるトラフィックを発生させているユーザーへの可視性を増幅させます。
- ユーザー識別情報をアクセス制御ポリシーの変数として利用することができます。
- トラブル対応やインシデントに対するレスポンスを容易にし、レポート内で使用することが可能です。

User-ID により、IT 部門はアプリケーションの使用を知的に制御する、もう 1 つの強力な機構を手に入れます。たとえば、ソーシャルネットワークのアプリケーションは、ともすればその危険な特徴からブロックされますが、人事部のように利用したい正式な理由がある組織および個人に対して有効にすることが可能です。

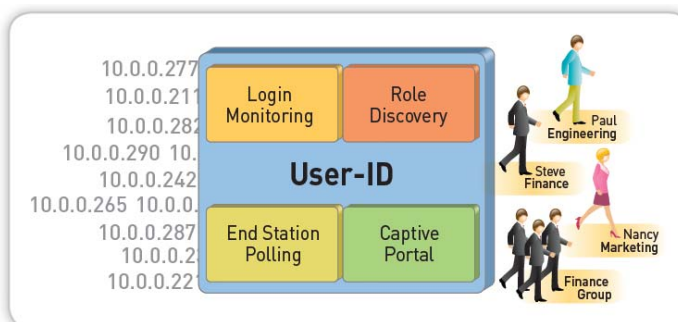


図 3: User-ID はユーザー単位のポリシーとレポート作成のため、企業ディレクトリを統合する

Content-ID – 高性能なコンテンツスキャンは、脅威や不正なウェブコンテンツ、慎重に取り扱うべきデータの漏洩を防ぐ

他の技術同様、Content-ID も Palo Alto Networks の次世代ファイアウォールに既存の企業ファイアウォールではなかった新たな可能性をもたらします。この技術は、許容トラフィック内でリアルタイムに脅威を防ぎ、ウェブ閲覧に対する粒度の細かい制御を実現し、ファイルやデータのフィルタリングを行います。

脅威の防御 Content-ID にあるこの機能部分は、スパイウェアやウイルス、アプリケーションの脆弱性からネットワークが占有されることを防ぐ、数種類の革命的な機能を具備しており、攻撃されるアプリケーションの新旧、種類は問いません。

- **アプリケーション復号化** Content-ID は App-ID のこの機能部分を利用し、データの流れに対して、あらかじめこの処理を通した後、脅威の特定を行います。
- **データの流れに応じたウイルス、スパイウェアのスキャン** ファイルの最初のパケットが到着した段階でトラフィックをすぐにスキャンし、ファイル全体がメモリーに展開されるまで待機しないことで、遅延を最小化し、スループットを最大化します。

- **脅威の定義形式の統一** それぞれの脅威に別々のスキャン機構を使用しないことで、性能を高めています。ウイルスやスパイウェア、脆弱性を突いた攻撃はすべて単一の工程で検知可能です。
- **脆弱性攻撃への防御 (IPS)** トラフィックの正規化と断片化したデータの合成を堅牢な方式で常時実施し、異形なプロトコルや動作の検知機構、経験則による検知機構を用いて、既知か未知かを問わないさまざまな脅威から総合的に防御します。

URL フィルタリング 完全に統合された組み込み型の URL データベースを利用し、管理者は従業員および他ユーザーのウェブ閲覧の監視制御が可能です。User-ID と組み合わせることにより、ウェブ利用のポリシーをユーザー単位に設定することも可能で、さらには法や規制、生産性に関連した広範囲なリスクから企業を守ります。

ファイル、データのフィルタリング App-ID による徹底したアプリケーション検査を利用して、この機能ではファイルやデータの許可されていない転送のリスクを低減するためのポリシーを強化できます。ファイルを拡張子でなく実際の形式で判別してブロックしたり、クレジットカードやアメリカの社会保障番号のように慎重に取り扱うべきデータ形式の転送を制御したりできます。この機能は App-ID の粒度の細かさを補完するもので、他のアプリケーションは個々のアプリケーション (例: インスタントメッセージのクライアント) によるデータ転送しか制御できません。

結論として、Content-ID を用いれば、IT 部門はさまざまな製品の追加購入により装置を無益に増加させるリスクを負うことなく、脅威を既知か未知かを問わず防止し、インターネットの不適切な使用を低減させ、データの漏洩防止を支援することが可能となります。

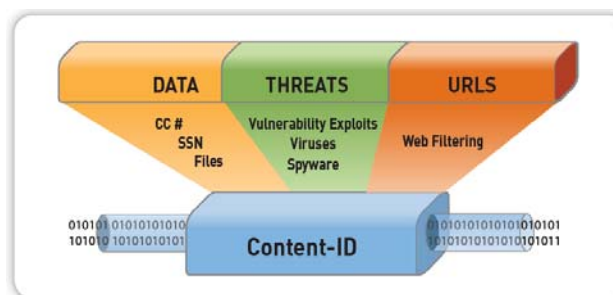


図 4: Content-ID は脅威、機密のデータに対するコンテンツスキャンと URL フィルタリングを一体化している

高性能な SP3 アーキテクチャが「妥協のないセキュリティ」を提供する

アプリケーション認識機能やコンテンツ検査機能を持った統合パッケージソフトを所有していても、性能的な制限から管理者がすべてを利用できないのでは、ほとんど意味がありません。問題は、もともとこれらの機能のリソース消費が激しいという点だけではありません。今日のセキュリティインフラは非常に大量のトラフィックを処理する必要があり、最近のアプリケーションの多くが、遅延にシビアであることもいうまでもありません。

Palo Alto Networks はこれらの課題を踏まえ、初めから高性能な製品の提供を目指しています。これは追加型の機能群を扱う競合製品には難しいことです。まず個々の機能の効率性をより高められるように最適化する方法を検討しました。この検討の結果、データの流れに応じたスキャン方法と、脅威の定義形式の統一を行いました。さらなる性能向上の実現を目指して、技術陣はシステムレベル、基盤レベルに効果的に手を加えました。具体的には、分岐のない単一工程を持つソフトウェア（パケットフロー）を持ち、機能的には並列に処理を行う機能を持つように次世代ファイアウォールを設計しました。この結果が Palo Alto Network の Single Pass Parallel Processing (SP3) アーキテクチャになります。

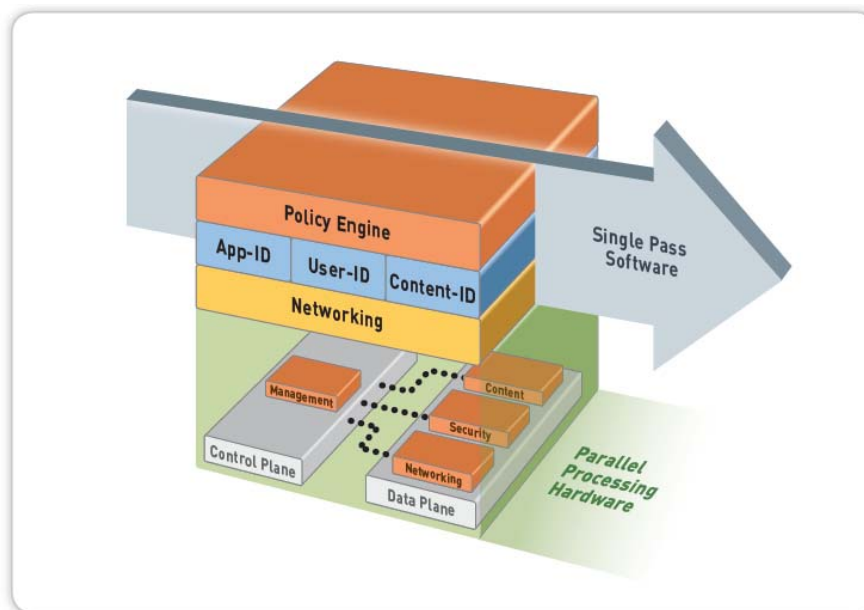


図 5: 単一工程、並列処理のアーキテクチャによりソフトウェアとハードウェアは一体になって企業のパフォーマンスを引き出す

従来のセキュリティ製品、特に追加型の機能を持つ製品では、高レベルのセキュリティ機能がそれぞれ独立して実行されていました。この複数工程を使ったアプローチでは、低レベルのパケット処理とトラフィックの再構築処理が無数に繰り返されます。システムリソースの使用効率は悪く、遅延も比較的大きくなります。対照的に、Palo Alto Networks の次世代ファイアウォールは単一の工程を使用しています。その処理モデルは意図的に高度に構造化され、本質的に直線的なつくりになっています。これにより、パケットやデータの流れを繰り返し処理する必要がなく、システムハードウェアへの負担は大幅に減少し、遅延も最小化します。

Palo Alto Networks SP3 アーキテクチャのその他の主な長所として、機能に特化した処理方式が挙げられます。どの次世代ファイアウォール装置にも、管理機能をサポートするために、専用の CPU やメモリー、ディスクを割り当てた制御プレーンがあります。他のすべての処理は独立したデータプレーンで実行されますが、データプレーンとしては次のような機構が挙げられます。

- 最初のパケット処理とネットワーク層の機能を扱うネットワークプロセッサ
- マルチコアのセキュリティプロセッサと、暗号化機能向けのハードウェアアクセラレーション
- コンテンツスキャン用のハードウェアエンジン

設計当初から高性能な製品を目指した結果、次世代ファイアウォールは App-ID、User-ID、Content-ID により実現される機能をすべて妥協することなく提供しており、すべてのサービスが伝送速度と同程度の少ない遅延で実現されている。

エンタープライズ向けのソリューションを実現するその他の機能

完全なソリューションとは、従来のファイアウォールの弱点を克服するだけでなく、設置や運用においても実際に企業が直面しているさまざまな問題を解決する必要があると Palo Alto Networks は常に考えています。この点に関して、既存のインフラとの互換性や、さまざまな使用方法をサポートする柔軟性、高い信頼性、そしていうまでもなくシンプルで使いやすいことが主な課題となります。このため、弊社の製品は次のような機能を満たす開発を行いました。

- L2/L3 スwitチング、ダイナミックルーティング (OSPF、RIPv2)、802.1Q VLAN、トランクポートをサポートする強固なネットワーク基盤
- ネットワークに組み込まない「可視性のみ」のモード、透過的な直列方式での運用、すべての機能を有効化した「ファイアウォール代替」設定などの柔軟な使用オプション
- すべての設定やセッション同期に対する動的または静的な高い可用性
- コマンドラインやウェブのインタフェース、同じ見え方、感じ方を共有可能な中央集中型のコンソール、syslog や SNMP のサポート、多様なロギングや通知機能などの直感的で柔軟なファイアウォールの管理

ネットワーク、統合、システム管理機能により、Palo Alto Networks の次世代ファイアウォールは IT 企業が求めていた堅牢な企業クラスのセキュリティソリューションを保証します。

企業セキュリティの新たな基盤

画期的な企業クラスのセキュリティ製品として、次世代ファイアウォールは企業に数々の大きな利益をもたらす機会を提供します。技術的な側面では、次に示す手法で、増加の一途をたどる広範囲な課題に最高情報責任者が取り組むのに役立ちます。

- 全ポートにまたがるすべてのアプリケーションに対してユーザー単位の可視性と制御を可能にします
- 悪意のあるソフトウェアやアプリケーションの脆弱性に対する攻撃をリアルタイムに防止します
- セキュリティインフラの複雑さとその管理を軽減します
- 高速で、性能に影響を与えることなく、最新のアプリケーションから防御するソリューションを提供します
- データの漏洩防止を支援します
- PCI コンプライアンスへの対応を簡単にします

もちろん業務的な側面からの検討も重要です。この点では、Palo Alto Networks の次世代ファイアウォールは次のような利点を持って企業を支援します。

- ネットワークトラフィックに対してほかに例を見ない認識能力と制御による、より良い、より徹底したリスク管理とコンプライアンスの達成
- 安全に最新のアプリケーションと技術を利用できる手段の提供による、企業の成長の促進
- 装置の連携、インフラのシンプル化、運用効率の向上の実現による、コスト削減

結論として、Palo Alto Networks は今日の企業がネットワークの制御を取り戻すために必要なものを正確に提供することで、企業は情報セキュリティに対する妥協がなくなり、コストのかかる装置の無益な増加を止め、収益を上げる業務に立ち返ることができます。アプリケーションとそれらを攻撃しようとする脅威に対して、他に例を見ない可視性と制御を提供することで、Palo Alto Networks の次世代ファイアウォールは企業セキュリティの新たな基盤の位置を占めようとしています。