paloalto NETWORKS®

the network security company™

プロキシを使わない、より効果的なURLフィルタリングとは？

2013年10月

プロキシの登場

ファイアウォールはポジティブ コントロール モデルでネットワーク アクセスを管理し、ポリシーで定義された特定のトラフィックだけがネットワークへのアクセスを許可され、それ以外はすべて拒否されます。最初は、多くの場合ルーターとして アクセス制御リスト（ACL）がこの機能を担っていましたが、このような原始的なアプローチは、指定されたパケットのフィルタとより深いレベルのアクセスがコントロール可能なステートフル インスペクション型のファイアウォール デバイスに取って代わられました。残念なことに、これら従来のファイアウォールには共通の欠点があります。すべてのポートやプロトコル上のネットワークを横断するアプリケーション全部を確認できないことです。プロキシベースのデバイスを使用することで、従来のファイアウォールでは確認できなかった少数のアプリケーションやプロトコルまで詳細に確認できるようになりました。

プロキシによるソリューションは、ソフトウェアかアプライアンスかに関わらず、トラフィックのソースと接続先の間で仲介役としての役割を担います。プロキシは限られた少数のアプリケーションやプロトコルへのアプリケーションのセッション接続を遮断、終了した後に、最初に対象とした接続先への接続を再初期化します。この処理により、プロキシは特定のトラフィックを転送して、ファイルのウイルス スキャンやユーザがアクセス可能なウェブサイトの決定など、セキュリティ上の決定を実行できます。

ステートフル型のファイアウォールにはこの重要な機能が欠けていたため、多くの組織で、可視化を高めてウェブ トラフィックをコントロールするためにプロキシベースのデバイスが導入されました。既存の古いファイアウォールに専用のプロキシを追加することにより、URLフィルタリングやプロキシ キャッシュによってウェブを高速化できるようになりました。

時代による変化

時間とともにプロキシベースのデバイスは進化して、侵入防止システム（IPS）やウイルス対策（AV）機能を搭載し、成長し続ける多くのセキュリティ「補完製品」の一部となりました。各「補完製品」が確認できるネットワーク トラフィックには限界があり、独立型のプロキシベースの URL フィルタリング デバイスも例外ではありません。プロキシを URL フィルタリング デバイスとして導入した場合も特定のトラフィックのみを対象としているため、すべてのウェブ トラフィックとネットワーク間の最新アプリケーションを識別することはできません。

さらに、これまでにプロキシによる URL フィルタリング ソリューションを導入することで得られたメリットも分かりにくくなっています。例えば、プロキシベースのデバイスの機能はパフォーマンス向上のためのウェブ キャッシュにまで広がっていますが、近年のウェブ コンテンツは非常に動的になっているため、キャッシュが保持できるのはウェブページの最新コンテンツのごく一部分にすぎません。最近では、接続スピードの大幅な高速化に、インターネット回線の価格下落も伴い、プロキシ キャッシュ機能の重要性も以前ほどではありません。

実際、多くの組織は、根本的な問題があるにもかかわらず、プロキシにはまだメリットがあると考えています。ウェブベースやネットワークベースのアプリケーションの爆発的な増加に加え、脅威の変化に伴い、このような組織はプロキシを導入した本来の理由を再評価する時機を迎えています。ネットワーク セキュリティの専門家は、プロキシベースの製品や独立型 URL フィルタリングが持つ主な問題として、次のような点を挙げています。

プロキシと独立型 URL フィルタリングの問題点

コンテクストの不足

独立型のプロキシベースの URL フィルタリング ソリューションは、今日に至るまで孤立、分離されたままのツールです。というのも、ネットワーク トラフィックの全体を確認できないことや、ネットワーク上の他のセキュリティ デバイスと比べるとその役割が限定的であることが理由の一部です。その主要な役割はファイアウォールなどの他のデバイスからウェブ トラフィックを受信して、リクエストを定義されたウェブサイトのグループや URL のカテゴリごとに分類して、ユーザのアクセスを許可/拒否するポリシーを決めることです。ただし、このプロキシベースのデバイスや他のセキュリティ デバイスによるポリシーから得られた情報には統一性が欠けています。例えば、管理者は独立型の URL フィルタリング デバイスを使って詳細で広範囲にわたるネットワーク セキュリティ ポリシーを作成することができません。URL デバイスでは、ファイアウォール上のすべての接続ログ、ウイルス対策デバイスが検出した悪意のあるファイル、IPS ボックスが検出した脅威に対して、ポリシーを考慮に入れることができません。接

続や各デバイスが検出したアクティビティを確認する集中型のシステムがなければ、ネットワークやセキュリティの管理者はコンテクストが不足したばらばらの情報を与えられるだけです。

また、コンテクスト不足は文字通り高くつくのです。継続中のメンテナンス サポート契約、高額な設備のアップグレード、ユーザごとのライセンス料で貴重な IT セキュリティ予算が使い果たされてしまいます。ところが、セキュリティ チームから見ると、支払った金額に対して、ネットワークの状態が分かりやすくなるわけではありません。

すべてのポートやプロトコル間の可視性の不足

ほとんどのプロキシがサポートしているアプリケーションやプロトコルは一部のアプリケーション（メッセージングやメディア ストリーミングなど）や特定のプロトコル（HTTP［ポート80］、HTTPS［ポート443］、FTP［ポート21］など）に限られています。このように、プロキシベースのデバイスは異なるプロトコルで実行するアプリケーションを区別できないだけでなく、非標準ポートを使用しているアプリケーションも識別できません。多くのアプリケーションは意図的にウェブベースとなっていて、ポート80や443を使用しており、ポートベースのファイアウォール経由で確実に接続でき、利便性も向上しています。ただし、セキュリティの観点から見ると、プロキシベースのデバイスはすべてのポートやプロトコル間の可視性が不足しているため、1つのオープンなポート間を横断するすべてのアプリケーションを正確に識別したり、アプリケーションのポリシーを決定したりできません。同様に、Skype や BitTorrent などの一部のアプリケーションは、ネットワーク上の利用可能なポートを動的に探して利用することができます。ポート ホッピング技術を実装すると、これらのアプリケーションはプロキシベースのデバイスの限られた可視性とセキュリティ能力を迂回することができます。

プロキシベースの URL フィルタリング デバイスはアプリケーションを区別できないだけでなく、回避技術に対する防御能力も限られています。エンドユーザは従来の URL フィルタリングやプロキシベースのデバイスを簡単に回避できる無数のツールを自由に使うことができます。PHProxy や CGIproxy から ProxEasy、Guardster、その他の匿名化アプリケーションまで、様々な公開プロキシ サーバーがあります。さらに、トラフィックの暗号化によって、指定されたエンドユーザがセキュア シェル（SSH）トンネルや SOCKS プロキシ内での使用や、Tor や Hamachi などのアプリケーションを経由することで、実際のアプリケーション利用状況を比較的簡単に隠すことができるようになっています。実際、あるセキュリティベンダーのナレッジベースの記事では、セキュリティ迂回ツール、Ultrasurf クライアントは Ultrasurf ネットワークに接続する際に、TCP を UDP トラフィックに動的に切り替えるため、プロキシベースのソリューションではブロックできないとはっきりと認めています

パフォーマンスの低下

セキュリティ機能の実行は従来からコンピューターに負荷のかかる作業ですが、プロキシベースのデバイスは、ソース クライアント、プロキシ デバイス、接続先サーバ間で追加のプロキシ接続を確立するのにかなり負荷の高い作業であるため、大量のリソースを必要とします。この処理要求にプロキシ接続による待ち時間が加わったため、プロキシベースのデバイスは高速の処理能力や高い拡張性を必要としない所でのみ導入されるに留まりました。プロキシの配置をネットワーク上のごく一部のトラフィックに限定すれば役立つこともありますが、そうでない場合、組織のネットワーク全体のパフォーマンスが著しく低下する恐れがあります。

アプリケーション対応の遅れ

プロキシベースの製品は、次々と開発される最新アプリケーションや既存のアプリケーション、プロトコルのアップデートに追いつくことで精一杯です。新しいアプリケーション プロキシの作成は非常に複雑な作業で、メーカーによっては数か月から数年かかる場合があります。新しいプロトコルやアプリケーションを導入、解析して、クライアントとサーバーのトランザクションやレスポンスがどのように処理されているか完全に理解しなければなりません。従来より、中に含まれているプロトコルには接続のための専用プロキシが必要で、専用プロキシがない場合、メーカーが考えうるすべてのシナリオを再現するためのプロキシを作成するのは大変困難です。プロキシでモデリングと再現を行った後で、新しいアプリケーション プロキシを何度もテストして、接続が切れないことや、サポート対象のアプリケーションに悪影響を与えないことを確認する必要があります。このような時間と労力を考えると、非常に動的な

インターネット コンテンツや、絶えずアップデートと改良を続ける Web 2.0 のアプリケーションに追いつくことは不可能と言うよりありません。

複雑な実装手順

ウェブ トラフィックのフィルタリングを目的とした効果的なツールとなるためには、組織の全ユーザがプロキシベースのデバイスにトラフィックと接続リクエストを送る必要があります。プロキシ転送の実行には主に2種類ありますが、どちらも複雑な実装手順が必要で、独自の問題点もあります。

明示型プロキシ

明示型プロキシの導入には、ウェブ トラフィックがプロキシ アプライアンスやセキュリティ デバイスへ向けられることを確認するために、社内のそれぞれのノートパソコンやワークステーションのウェブブラウザを IT 部門が設定する必要があります。多くの企業では手動の方法を利用するプロキシ自動設定（PAC）ファイル、Microsoft のグローバル ポリシー オブジェクト（GPO）で強化したシステム ポリシー、あるいはウェブ プロキシ自動発見（WPAD）プロトコルを導入しています。ただし、WPAD ファイルに設定ミスがあった場合、攻撃者によりユーザの端末が不正な設定ファイルへとリダイレクトされる恐れがあります。また、制限が厳しすぎる GPO の場合、ユーザから IT 担当者へ送信されるトラブル チケットが増加する可能性があります。また、企業のプロキシポリシーを迂回するために使用されるモバイル デバイスなどは、組織がエンドポイントを把握、コントロールできないため、さらなる問題点に直面しています。

暗示型プロキシ

暗示型、あるいは透過型プロキシの導入には、ネットワーク上のトラフィックの一部しか確認できないために、複雑さ、待ち時間、追加の管理機器のすべてがつきものです。暗示型プロキシでは、ウェブ トラフィックを直接プロキシ アプライアンスに誘導するためのウェブ キャッシュ通信プロトコル（WCCP）を使用するため、通常 IT 部門でスイッチやルーターを再設定する必要があります。多くのプロキシ アプライアンスは、ウイルス対策スキャンなど一部の検査タスクを、インターネット コンテンツ適合プロトコル（ICAP）経由で追加の分離型アプライアンスへ通過させます。これにより構成が 複雑化するだけでなく、別の管理コンソールを必要とするツールがもう一つ増えることにもなります。プロキシ デバイスがトラフィックをウイルス対策スキャン アプライアンスへ転送するのに時間がかかり、そのトラフィックを許可/拒否するかの応答を待って接続をオープンにするため、処理全体がシステムのパフォーマンスに影響を与えます。

パロアルトネットワークス®を導入して、プロキシ問題を解決

すべてのネットワーク トラフィックの確認ができない、コンテクストが不足している、ネットワークのパフォーマンスに影響する、実装や維持が困難、ユーザによるインターネット セキュリティ強化対策の迂回を防ぐことができないようなセキュリティ ソリューションを組織は導入すべきではありません。幸い、パロアルトネットワークス®は大企業から中小企業まで、すべての企業向けのネットワークセキュリティの問題点を理解することに重点を置いています。パロアルトネットワークスでは、独立型URL フィルタリングなど、プロキシベースのセキュリティ ソリューションにつきものの根本的な問題に対応するネットワーク セキュリティ プラットフォームを一から開発しています。

包括的プラットフォーム

次世代ファイアウォールと脅威の防御テクノロジーを組み合わせた、パロアルトネットワークスの次世代セキュリティ プラットフォームは、企業データ ネットワークのための、アプリケーション、ユーザ、コンテンツに関する高い可視性とコントロールを実現しています。App-ID™ や User-ID などの一元化されたテクノロジーが使用中のアプリケーションをユーザと共に識別する一方、Content-ID と Wildfire™ のテクノロジーがアプリケーションのトラフィックに潜む脅威を絶えず監視、ブロックします。セキュリティ管理者はこれらのテクノロジーを利用して、論理的なアプリケーションベースのセキュリティ ポリシーを作成し、すべてのトラフィックをアプリケーション、ユーザ、コンテンツごとに分類できるようになります。これまでのファイアウォールや「補完製品」では対応できなかった部分です。そして、最も重要なのは、パロアルトネットワークス セキュリティ プラットフォームが最初に実行するタスクは、採用されているポート、プロトコル、セキュリティ 回避技術に関係なく、アプリケーションの正確な識別することで、これがファイアウォールのセキュリティ ポリシーの基礎となりま

す。パロアルトネットワークスのプラットフォームは常に最新アプリケーションや脅威に関する情報をアップデートするだけでなく、WildFire のクラウドベースの仮想環境で収集したマルウェアの情報もアップデートします。

パロアルトネットワークスのネットワーク セキュリティ テクノロジーの導入は簡単で、多くの「補完製品」ボックスも、従来の URL フィルタリングなどの独立型デバイスも必要ありません。一つのポリシーで、追加的な防御やコントロールが可能なすべてのパロアルトネットワークスのセキュリティプロファイルを、URL フィルタリング、ウイルス対策、脆弱性の防御などのポリシーのトラフィックに集中させることができます。管理者は、管理コンソールで1つ以上のセキュリティ プロファイルを指定するだけで、詳細なセキュリティ ポリシーを作成できます。

パロアルトネットワークスのプラットフォームは従来のファイアウォールに匹敵する能力も備えているため、ネットワークのすべてのトラフィックを監視できます。パロアルトネットワークスのセキュリティ プラットフォームは、高い柔軟性のレイヤー1（Virtual Wire）、レイヤー2、レイヤー3導入モードと共に、豊富なネットワーク機能（静的および動的ルーティング機能など）を利用できるので、ネットワーク エンジニアはあらゆる既存のネットワーク アーキテクチャ デザインにもネットワーク セキュリティ プラットフォームを簡単に導入することができます。シングルパスのソフトウェア エンジンを、ネットワーク、セキュリティ、脅威の防御、管理機能の機能ごとの処理に使用する専用のハードウェア プラットフォームと組み合わせることで予測可能な高速パフォーマンスが実現します。

動的で、コンテクスチュアルなポリシー

アプリケーション、ユーザ、コンテンツの完全な可視性と制御により、セキュリティ管理者は動的でコンテクスチュアルなポリシーの作成に利用するデータにアクセスすることができます。それに対し、従来の独立型 URL フィルタリング デバイスはネットワークのごく一部しか確認できず、ウェブサイトを定義済みの URL カテゴリに分類することに重点を置くに留まります。パロアルトネットワークスのテクノロジーが IT 企業に提供している共有情報が、URL フィルタリング デバイスには欠けています。

パロアルトネットワークスの URL フィルタリングのセキュリティ プロファイルは他のすべてのプロファイルと同時に動作しますので、それによってネットワーク トラフィックから得たコンテクストを利用して脅威に対する完全な防御ネットワークを作成できます。例えば、パロアルトネットワークスの App-ID テクノロジーは URL フィルタリングを補うのに最適で、ネットワーク アクティビティの制御を強化し、同時に URL フィルタリングの回避ツールの使用も防ぎます。アプリケーション、ユーザの身元、アプリケーションの発行元やユーザの場所を特定することは、URL フィルタリングや脅威に対する防御セキュリティ プロファイルと組み合わせた時に、ポリシー強化の強力な武器となります。最終的には、セキュリティ管理者が特定の URL カテゴリに対しトラフィックをブロックしたり許可するだけの方法から、安全なトラフィックを可能にするポリシーを自由に作成できるようになります。

ポリシーの実例

パロアルトネットワークスの次世代セキュリティ プラットフォームで既に組み込まれている次世代のセキュリティ テクノロジーを利用したポリシーの実例をいくつかご紹介します。ウェブ リクエストを単に「ブロック」したり「許可」したりするだけでなく、これらの詳細なポリシーにより企業はネットワークを保護し、安全に業務を行うことができます。

- 特定の地域や「マルウェア」と分類されたウェブサイトを除き、App-ID や User-ID を利用して、特定の個人やグループごとにインターネット アクセスを認証する–ユーザのデバイスが既知のマルウェアやフィッシング ダウンロード サイトにアクセスするのを防ぐ
- 「金融サービス」と分類されたすべてのウェブサイトは暗号化されたままで、既知のマルウェア サイトは暗号解読されるように、URL フィルタリング セキュリティ プロファイルを利用して SSL 暗号化ポリシーを実装する–トラフィックを保護すると同時に、ユーザの銀行情報に対するプライバシーを保護する

- 特定のユーザに1つの URL カテゴリーでのオンライン ストレージ ツールへのアクセス権を付与するが、Microsoft ドキュメントのアップロードや実行ファイルのダウンロードを防ぐために、セキュリティ プロファイルをブロックするファイルを適用する–企業の機密情報とマルウェアと思われるソフトウェアを制御する
- URL カテゴリごとにメディア ストリーミングを許可するが、App-ID 経由で YouTube や NicoNico Douga アプリケーションの使用を明示的にブロックする–回線容量を節約し、従業員の時間の無駄を防ぐ
- 人気イベント（オリンピックや FIFA ワールドカップなど）開催時のピークタイムのアクセスを、User-ID、QoS 、カスタマイズした App-ID シグネチャ経由で、特定のユーザやグループごとに絞り込む–業務関連の使用と職場の文化のバランスを取る

顧客事例

プロキシが不要に

世界的なコンサルティング会社を顧客に持つ某有名テクノロジー企業は、現在ネットワーク周辺機器に高可用性（HA）のパロアルトネットワークス PA-5020 セキュリティ プラットフォーム2台を使用して、およそ8,000人のユーザを守っています。これらのアプライアンスは顧客の既存の高速スイッチアとスムーズに統合され、独立型のプロキシベース URL フィルタリング デバイスの前面に配置されました。パロアルトネットワークスのセキュリティ プラットフォームの導入から7か月後、ネットワーク開発コンサルタントはプロキシ アプライアンスがセキュリティ警告を一切記録していないことに気づきました。調査の際に、パロアルトネットワークスの装置がすべてのマルウェアを捕捉し、脅威からネットワークを保護し続けていることが分かったのです。

そこで、注意深く状況を考慮した結果、プロキシベースのアプライアンス（図1を参照）の接続を解除して、使用停止することを決定したということです。この決定により、プロキシ テクノロジーを搭載したデバイスを取り外してネットワーク アーキテクチャが簡略化されただけでなく、不要なプロキシ ハードウェアの今後のアップグレードに伴うサポートの更新費用をなくすことで運営経費や資本経費の節約にもつながりました。

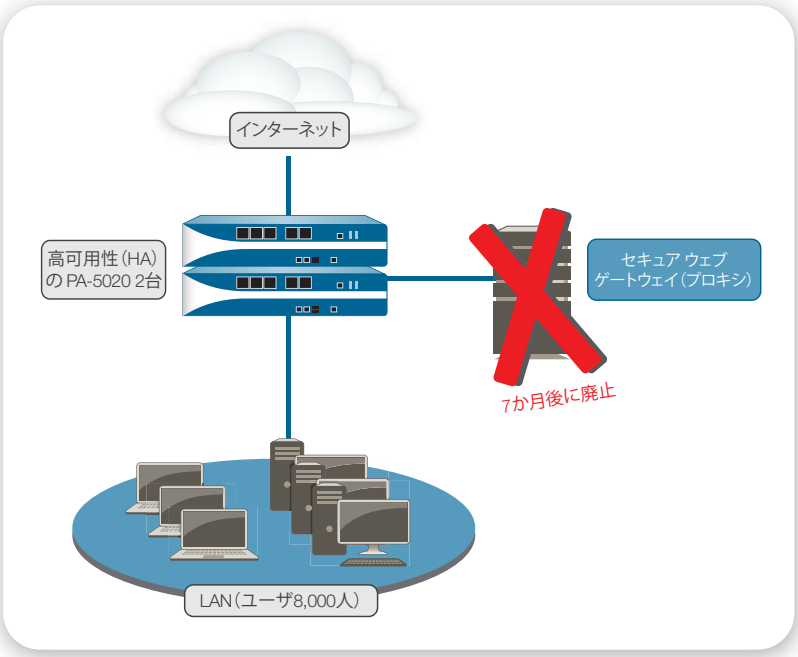

図1：顧客企業のネットワークで既存のプロキシ ソリューションの前面に導入されたパロアルトネットワークス 製品

本物のソリューションに時間は不要

1,000名の従業員を抱えるカナダの某エネルギー企業はネットワーク環境へのプロキシ デバイスの導入に悪戦苦闘していました。WCCP 実装を使用しているプロキシを使って、丸1年を費やしてきましたが、結果は満足のいくものとは言えず、6、7件の問題は全く解決されないままでした。パロアルトネットワークスはこの企業に解決策として、プラットフォームの評価を提案しました。レイヤー1（Virtual Wire）導入モードを使った装置を設置することで、パロアルトネットワークスのエンジニアはこの会社が1年間を費やしてきたプロキシの問題を解決することができました。しかも、たった半日で。この結果に納得していただき、各支社用にパロアルトネットワークスのハードウェア プラットフォームを、プラットフォームの管理にはパロアルトネットワークスの Panorama 集中管理コンソールを導入していただきました。

最初のプロキシ利用条件を再評価する

アプリケーションや脅威が絶えず進化を続ける中、一部の企業にとって、従業員の業務の妨げにならないようにネットワークを保護することは非常に困難になっています。多くのユーザが会社所有や個人所有の様々なデバイスでネットワークを利用して、多くの異なるネットワーク ポートやプロトコルと通信する新しいアプリケーションにアクセスすることで、問題が明らかになっています 。プロキシベースのデバイスは従来のファイアウォールの本来の性能をサポートし、ウェブ トラフィックに対する可視性と制御を高めるものですが、その可視性は HTTP（ポート80）や HTTPS（ポート443）など、一部のプロトコルに限定されています。パロアルトネットワークスはネットワーク内のプラットフォームの中心地から集められたアプリケーション、ユーザ、コンテンツ間で共有されているコンテクストを利用した動的ポリシーを駆使して、企業を守る次世代ネットワーク セキュリティ プラットフォームをご提供します。このプラットフォームにより、組織のユーザにきめ細やかなセキュリティを適用するための完全なネットワークの可視性とアプリケーションの安全な実行が、ポート、プロトコル、回避技術に関わらず可能になります。パロアルトネットワークスの次世代のセキュリティと脅威からの防御テクノロジーの導入により、IT 部門は独立型 URL フィルタリング ソリューションなどのプロキシベースのデバイスを利用するための当初の利用条件を着実に再評価できるようになります。詳細な情報、オンラインや訪問実演をご希望の方は、パルアルトネットワークスの認定パートナーにお問い合わせください。

paloalto NETWORKS®
the network security company™

〒102-0094
千代田区紀尾井町4番3号
泉館紀尾井町3F
電話番号：03-3511-4050
お問い合わせ先：
infojapan@paloaltonetworks.com
www.paloaltonetworks.jp