誰にでもわかる次世代ファイアウォール

Next-Generation Firewalls

FOR DUMMIES®

学べること:

- 「良い」アプリケーションと「悪い」アプリケーションを区別する
- アプリケーションで使用されるファイアウォール回避テクニックを識別する
- 効果的なアプリケーションおよびネットワーク制御を実装する

Brought to you by

paloalto NETWORKS

the network security company™

Lawrence C. Miller, CISSP

パロアルトネットワークスについて

パロアルトネットワークスは、ネットワーク セキュリティを専門とする企業です。パロアルトネットワークスの次世代ファイアウォールを導入すれば、アプリケーションやコンテンツの可視性をこれまでにないレベルに高め、最大 20Gbps でパフォーマンスの低下なく、しかもIPアドレスだけでなくユーザごとにきめ細かいポリシーによる制御を実現できます。特許出願中のApp-ID™テクノロジによりパロアルトネットワークスのファイアウォールは、ポート、プロトコル、回避テクニック、SSL暗号化などには関係なくアプリケーションを正確に識別、制御してコンテンツをスキャンすることで、脅威を阻止し、情報漏洩を防止します。企業は、初めてWeb 2.0を採用している環境において、完全な可視性と制御を維持しながら、デバイス統合を通して総所有コスト (TCO) を大幅に削減することができます。詳細については、http://www.paloaltonetworks.comをご覧ください。

誰にでもわかる次世代ファイアウォール®

著者: Lawrence C. Miller, CISSP

Wiley Publishing, Inc.

誰にでもわかる次世代ファイアウォール®

発行元
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774 USA

ISBN: 978-1-118-09768-7

Manufactured in the China

10 9 8 7 6 5 4 3 2 1

発行者からのお知らせ
当社のその他の製品およびサービスの概要については、当社のビジネス開発部門 (米国、317-572-3205) に問い合わせてください。各企業または組織向けのカスタムのFor Dummies (「誰にでもわかる」シリーズ) 書籍を作成する方法の詳細については、`info@dummies.biz` に問い合わせてください。製品またはサービスに対するFor Dummiesブランドのライセンス取得については、`BrandedRights&Licenses@Wiley.com` に問い合わせてください。

取得、編集、およびメディア 開発
シニア プロジェクト エディタ: Zoë Wykes
編集マネージャ: Rev Mengle
ビジネス開発担当者:
Karen Hattan
カスタム発行プロジェクト スペシャリスト:
Michael Sullivan

構成サービス
シニア プロジェクト コーディネータ: Kristie Rees
レイアウトおよび図: Carl Byers,
Carrie A. Cesavice, Cheryl Grubbs
校正者: Rebecca Denoncour
パロアルトネットワークスからの特別な支援:
Chris King

目次

はじめに

インターネットから押し寄せる新しい脅威が、かつてないほど急速な広がりを見せています。次第にその標的を「ファイアウォール対応」アプリケーションやアプリケーション層の脆弱性に移していくに従って、従来のファイアウォールでは企業ネットワークを十分に保護できなくなっています。

アプリケーションと脅威は急速に進化しているにもかかわらず、従来のセキュリティ テクノロジの進化は停滞してしまっています。その結果、企業の安全を維持しようと努めているIT部門は、可視性が低下し制御する術を失っています。

アプリケーションの可視性と制御を取り戻し、ネットワークや情報資産に対する保護能力を高めようと努力を続けているにもかかわらず、ほとんどの組織は依然として苦しい立場に置かれています。革新的なソリューションが存在しないため、今日のセキュリティの課題に完全には対処できていないのです。

その結果さまざまな単一機能のアプライアンスを組み合わせることになりますが、これはコストがかかる上に複雑です。ソリューションとしては決して望ましくない方法であるといえます。しかし、組織はより少ないコストと労力で、より大きな成果を上げる必要に迫られています。今日の厳しい経済環境下では、複雑でコストのかかるソリューションは受け入れられないのです。

ネットワーク セキュリティに対するまったく新しい、革新的なアプローチが必要です。ファイアウォールを再発明するときが来ました。

本書について

本書では、次世代ファイアウォールの概要について詳細に説明します。ここでは、ネットワーク セキュリティの進化、Enterprise 2.0アプリケーションの登場とそれに関連する脅威、従来のファイアウォールの欠点、および次世代ファイアウォールに見られる高度な機能について検証します。

前提条件

本書では、読者がネットワーク セキュリティの知識を持っていることを前提にしています。そのため、主に組織のセキュリティの課題に対処するための新しいソリューションを評価している技術分野の読者向けに記述されています。

本書の構成

本書は、6つの短い章と付録で構成されています。各章の簡単な概要を以下に示します。

第1章: ネットワーク セキュリティの進化を理解する

最初に、ファイアウォールがネットワーク セキュリティで果たしてきた役割と、今日のネットワーク セキュリティのいくつかの課題について調べます。

第2章: アプリケーションと脅威のトレンドを定義する

第2章では、企業でのアプリケーションの開発と使用に影響を与えるいくつかの傾向について説明します。ビジネス上のメリットのほか、さまざまなアプリケーションに関連したセキュリティ上のリスクや、新しい脅威がEnterprise 2.0アプリケーションの「ネットワーク接続性確保機能」をどのように悪用しているかについて説明します。

第3章: 従来のセキュリティ インフラの課題を認識する

第3章では、従来のポート ベースのファイアウォールと不正侵入防御システムが、最近登場した新しい脅威から企業を保護するには不十分である理由について解説します。

第4章: 次世代ファイアウォールで問題を解決する

第4章では、次世代ファイアウォールの先進的な機能や特徴について詳しく説明します。次世代ファイアウォールとは何か、それに該当しないもの、および組織にとっての次世代ファイアウォールのメリットについて説明します。

第5章: 次世代ファイアウォールの導入

第5章では、セキュリティ ポリシーおよび制御の重要性と、これらのポリシーおよび制御の実装における次世代ファイアウォールの役割について説明します。また、組織の特定の技術的要件を定義したり、ネットワーク上での次世代ファイアウォールの導入を計画したりする場合に役立ついくつかのヒントも提供します。

第6章: 次世代ファイアウォールのための10の評価基準

ここでは、あのお馴染みの*For Dummies* (「誰にでもわかる」シリーズ)十選の形式で、次世代ファイアウォールを選択する場合に考慮する必要のある10の機能および基準を示します。

用語集

最後に、読者が本書のどこかで技術的な用語または省略形がわからなくなった場合に備えて、それらのすべてを調べるのに役立つ用語集を添付しています。

本書で使用しているアイコン

本書の全体を通して、特に注目すべき重要な情報への注意を促すためにアイコンを使用している場合があります。残念ながら、素晴らしい解説者である池上 彰氏にこれらの情報を指摘してもらうことができないため、こちらで代わりにそれを行っています。

このアイコンは、覚えておく価値があると思われる情報または概念を示しています。そのため、知ったかぶりをして面倒だと思うのではなく、この情報を絶対に忘れないようにしてください。

ここで、ヒトゲノムのマップや常温核融合の秘密が見つかるわけではありません (ひょっとしたら可能性があるかも) が、技術オタクに磨きをかけたいのなら注目してください。このアイコンでは、専門用語の背景にある専門用語について説明します。

お読みいただき、ありがとうございます。本書をぜひお楽しみください。著者への気遣いもお忘れなく。真面目な話、このアイコンは、読者が時間をある程度節約でき、頭痛からも解放してくれる可能性のある役立つ提案や有効な価値ある情報を指摘します。

司令官により緊急発令 ... いやいや、実際にはそれほど危険ではありません。とは言え、このアイコンは、潜在的な落とし穴や混同しやすい概念を指摘します。

どこから読み始めるか

千里の道も一歩からとは、よく言われることです。でも、72ページから成る本書は、リビングルームの中で体験することのできる、どちらかと言うと短期間の (ただし有益な) 小旅行です。

流れがわからなくなったり、結末が台無しになったりする心配はありません。本書の各章は独立して記述されているため、好きなところから読み始めて、いつでも興味のある章に移動することができます。もちろん、従来の方法がよければ、単純にページをめくって先頭から読み進めることも可能です。

第1章

ネットワーク セキュリティの進化を理解する

この章で学ぶこと

- ポート ベースのファイアウォールが時代後れになった理由を理解する
- 情報漏洩の問題に対処する
- 法令順守を達成する

インターネットの黎明期から、ウイルス対策ソフトウェアがPC セキュリティにおいて必須の存在になってきたのとまったく同様に、ファイアウォールはネットワーク セキュリティにおいて必須の存在になってきました。

今日のアプリケーションと脅威のトレンドでは、従来のポート ベースのファイアウォールは、企業ネットワークや機密データを保護するうえでほとんど効果がないと見なされています。今日のアプリケーションの多くは、ビジネスやプライベートの用途を問わずネットワーク上で動作し、ネットワークを介したコミュニケーションによりユーザに様々なメリットをもたらします。しかし、最近では新しい脅威や情報漏洩、コンプライアンス非順守などのリスクの要因にもなってきています。

この章では、従来のファイアウォールの動作の仕組みと、それが今日のアプリケーションや脅威の課題を解決できない理由、および情報漏洩とコンプライアンスの課題によってネットワーク セキュリティやより優れたファイアウォールの必要性について説明します。

従来のファイアウォールが効果的でなくなった理由

ファイアウォールは、信頼できるネットワーク (社内LANなど) と信頼できないネットワークまたはパブリック ネットワーク (インターネットなど) の間のトラフィック フローを制御します。今日、一般的なファイアウォールは、ポート ベース (またはパケット フィルタリング) ファイアウォールか、またはこの基本的なファイアウォールの何らかの変種 (ステートフル インスペクションなど) です。これらのファイアウォールが普及している理由には、運用や保守が比較的単純なこと、一般に安価であること、スループットが優れていること、20年以上にわたって普及してきたことなどがあります。

インターネット時代の急速な技術革新のペースからすると、20年前に開発されたポート ベースのファイアウォールが使用しているテクノロジは非常に古いものです。実際、ネットワーク セキュリティは、しばしば暗黒時代にたとえられます。つまり、ネットワークゲートウェイが城壁にたとえられ、ファイアウォールが跳ね橋のようにアクセスを制御します。そして、上か下のどちらかの状態にあるつり上げ橋のように、ポート ベースのファイアウォールは、ネットワーク トラフィックを制御するための選択肢として許可またはブロックの2つだけしかありません。

ポート ベースのファイアウォール (およびその変種) は、発信元/宛先IPアドレスとTCP/UDPポート情報を使用して、ネットワークまたはネットワーク セグメント間のパケットの通過を許可するかどうかを判断します。ファイアウォールは、IPパケット内のTCPヘッダの最初の数バイトを検査して、SMTP (ポート25) やHTTP (ポート80) などのアプリケーション プロトコルを特定します。

ほとんどのファイアウォールは、ルールで明示的にブロックされていない限り、信頼できるネットワークから発信されたすべてのトラフィックは信頼できないネットワークへの通過できるように設定されています。たとえば、特定のネットワーク情報がインターネットに誤って転送されることがないように、SNMP (Simple Network Management Protocol) が明示的にブロックされている可能性があります。これは、発信元または宛先IPアドレスには関係なく、UDPポート161と162をブロックすることによって達成されます。

静的ポートの制御は、比較的簡単です。ステートフル インスペクション ファイアウォールは、適切に定義された複数のポート (FTPポート20と21など) を使用する動的アプリケーションに対応しています。信頼できるネットワーク上のコンピュータまたはサーバが、信頼できないネットワーク上のコンピュータまたはサーバとセッションを開始す

る場合は、接続が確立されます。ステートフル インスペクション ファイアウォール上では、信頼できないネットワーク上のコンピュータまたはサーバからの応答または返信を許可するための動的なルールが一時的に作成されます。そうでない場合は、返信トラフィックを明示的に許可するか、またはファイアウォール上でアクセス ルールを手動で作成する必要があります (これは通常、現実的ではありません)。

すべての人がルールに従って行動する限り、これらはすべて適切に機能します。残念ながら、これらのルールはどちらかと言うとガイドラインであり、インターネットを使用している人がすべて適切に行動するとは限りません。

今やインターネット上でやりとりされるトラフィックの大半はエンタープライズ ネットワークにも流れ込んできています。これはWebサーフィンだけではありません。インターネットは、ネットワーク ユーザが個人的な目的とビジネスでの目的の両方のためにアクセスする新世代のアプリケーションを生み出しました。これらのアプリケーションの多くがビジネスの生産性向上に役立っている一方で、その他のアプリケーションによって大量の帯域幅が消費され、不必要なセキュリティ上のリスクが生じ、さらにビジネス上の責任が増加しています。また、これらのアプリケーションの多くには、従来のポート ベースのファイアウォールを回避するための、標準以外のポートの使用、ポートホッピング、トンネリングなどの「ファイアウォール回避」のテクニックが組み込まれています。

IT部門は、ポート ベースのファイアウォールの欠陥を、プロキシ、不正侵入防御システム、URLフィルタリングなどの、コストのかかる複雑な機器で補完しようと努力してきましたが、残念ながら今日のアプリケーションと脅威のトレンドを考慮すると、これらのすべての対策はあまり効果的ではありません。

情報漏洩の問題の大きさ

機密データまたは個人データの大規模な漏洩問題は、頻発しています。偶発的および意図的な情報漏洩の数多くの例が頻繁にニュースの見出しを飾り、大手小売業者による数万のクレジット カード番号の流出や、政府機関、健康管理組織、または雇用主による社会保障番号の漏洩が明らかになっています。たとえば、2008年12月には、禁止されているピアツーピア (P2P) ファイル共有アプリケーションによって、24,000名の米国陸軍兵士の個人情報のデータベースがインターネット上で公開されました。残念ながら、このような出来事は他にもいくつかあります。米国陸軍のウォルターリード陸軍病院、Marine Oneで働く米国政府の請負業者や、およびファイザー社も以前、同じような被害を受けました。これらのいずれの場合も、機密データは、ポリシーでは明示的に禁止されているが、技術的に規制することが難しかったアプリケーションを通じて漏洩しています。

情報漏洩防御 (DLP) テクノロジは万能薬としてさかんに宣伝され、多くのIT部門の注意を引いてきました。しかし、残念ながら、ほとんどの場合、対象となるデータセットの範囲、サイズ、および分散性を考慮した場合、データの場所や所有者の検出だけでは課題の克服は困難です。この課題に加えて、アクセス制御、レポート、データの分類、休止中のデータと移動中のデータの比較、デスクトップとサーバ エージェント、暗号化などに関連した多くの考慮すべき項目があります。その結果、組織内の多くのDLP対策の進捗は遅くなり、ほとんどの場合、最終的には頓挫してしまいます。

多くのDLPソリューションは、すでに扱いにくくなっている製品に、多すぎる情報セキュリティ機能を (さらに、ストレージ管理の要素さえも) 組み込もうとしています。言うまでもなく、この範囲の拡大によって、複雑さや、時間、そして機器管理コストや人件費等の経費が追加されます。そのため、DLPテクノロジは多くの場合、煩雑なうえ、不完全であり、多くの組織にとって高価なことは言うまでもなく、過剰とも言える高度なスキルが必要になります。

さらに、現在市販されているDLPテクノロジの標準的な実装はアプリケーションの制御に対応していないため、許可されていないP2Pファイル共有アプリケーションによって引き起こされた最近の侵害の多くを防御できなかったと考えられます。

一部の組織は、大規模にデータの検出や分類およびカタログ化を含むDLPを実装する必要があります。しかし、ほとんどの組織にとって、機密データの漏洩に最もよく使用されるアプリケーションの制御、およびクレジット カードや社会保障番号などの個人データまたは機密データが許可なく転送されることを阻止することが最低限必要なことであると言えます。分界点が内部と外部の間、または内部ユーザとデータセンタ内の内部リソースの間のどちらにあるかにかかわらず、その制御を信頼の境界 (ネットワークゲートウェイ) で実施することが理想です。ファイアウォールは理想的な場所に位置していて、異なるネットワークやネットワーク セグメントに転送されるすべてのトラフィックを監視しています。残念ながら、従来のポートおよびプロトコルベースのファイアウォールはアプリケーションや、ユーザ、およびコンテンツを認識していないため、このいずれについても対応できません。ファイアウォールを使用して情報漏洩に効果的に対処するには、組織は以下のことを実行する必要があります。

- ネットワーク上のアプリケーションを制御することによって、情報漏洩の手段を制限する
- ネットワーク上で必要なアプリケーションを検査して、機密データまたは個人データを調べる
- これらのアプリケーション トランザクションを開始しているユーザと、その理由を把握する
- 偶発的または意図的な情報漏洩を防止するための適切な制御ポリシーとテクノロジを実装する

企業がゲートウェイで機密データまたは個人データのフローを制御できれば、頻繁にニュースになっている情報漏洩事故の多くを回避できます。残念ながら、従来のファイアウォールで構成されている従来のネットワーク セキュリティ インフラでは、事故を回避するには装備が不十分であると言えます。

コンプライアンスは任意事項ではない

情報セキュリティやデータ保護の要件を義務付けている規制が全世界で400を超えている現在、どこの組織もコンプライアンスを達成し、維持しようと努力を続けています。これらの規制の例としては、米国ではHIPAA、FISMA、FINRA、およびGLBAが、ヨーロッパではEUデータ保護法 (DPA) があります。

皮肉なことに、今日の最も広範囲に及ぶ、おそらく最も効果的で最もよく知られたコンプライアンス要件は政府規制にさえなっていません。クレジットカード業界データ セキュリティ標準 (PCI DSS) は、ID盗難や詐欺的なカード使用から企業、銀行、および消費者を保護するために、主要なクレジットカード ブランド (American Express、MasterCard、Visaなど) によって作成されました。また、経済がクレジットカードのトランザクションにますます依存するに従って、カード保持者のデータが消失するリスクは増加する一方であり、コンプライアンスが目的かどうかは別にしても、データを保護するためのあらゆる努力が重要になっています。

PCI DSSは、処理されるトランザクションの数や量には関係なく、支払いカード (クレジット カードやデビット カードなど) 情報を転送、処理または格納するすべてのビジネスに適用可能です。

コンプライアンスを満たしていない企業には、軽微な違反の場合は1月あたり最大25,000ドル(約212万円)の罰金、実際に財務データの消失または盗難が発生した違反の場合は最大500,000ドル(約4,250万円)の罰金、カード処理の承認の取り消し (これによって事業の運営はほぼ不可能になる) を含む厳しいペナルティが課されることがあります。

コンプライアンス要件はほぼ完全に、情報セキュリティに関するベスト プラクティスに基づいていますが、セキュリティとコンプライアンスは同じものではないことに注意する必要があります。ビジネスがPCIに準拠しているかどうかには関係なく、データの侵害には高いコストがかかる場合があります。米国の独立系調査会社であるForrester社が実施した調査によると、侵害の1レコードあたりの概算コスト (罰金、クリーンアップ、機会の損失、その他のコストを含む) は、規模が小さく規制対象ではない企業の場合で90ドル(8000円弱)から明確な規制対象となる企業で305ドル(約26,000円)に及びます。

セキュリティとコンプライアンスは関連していますが、同一のものではありません。

PCI DSSバージョン1.2は、12の一般的な要件と、200を超える特定の要件で構成されています。12の一般的な要件のうち、次の内容が、特にファイアウォールおよびファイアウォール関連の要件に対応しています。

- **要件 1:** カード保持者のデータを保護するために、ファイアウォールを導入し、適切な設定管理を行うこと。
- **要件 5:** ウイルス対策ソフトウェアを導入し、定期的なアップデートを行うこと。
- **要件 6:** 安全性の高いシステムとアプリケーションを開発し維持すること。
- **要件 7:** カード保持者のデータへのアクセスを、ビジネス上必要な場合にのみに制限すること。
- **要件 10:** ネットワーク資源やカード保持者のデータに対する全てのアクセスを追跡および監視すること。
- **付録 F:** ネットワークセグメントの分割によりPCI DSSの範囲を減らし、企業はカード保持者のデータを格納、処理、または転送するシステムを他のネットワークから分離すること。

第2章

アプリケーションと脅威のトレンドを定義する

この章で学ぶこと

- アプリケーションを良い、悪い、またはその両方として識別する
- 接続性を確保するための手法を理解する
- 今日の脅威の速度と高度化を認識する

以前は、ネットワーク セキュリティは比較的単純で、すべてが多かれ少なかれ白か黒、つまり明らかに悪いか明らかに良いかのどちらかに分類することができました。ビジネス アプリケーションが許可すべき良いトラフィックを構成する一方で、その他の非常に多くのアプリケーションはすべて、ブロックすべき悪いトラフィックを構成していました。

現在、このアプローチでの問題として、アプリケーションが次の傾向を示している点が挙げられます。

- ますます「グレー」になっている。アプリケーションを単純に良いまたは悪いとして分類することが難しくなっている。
- ますます回避的、つまりファイアウォールでは制御が難しくなっている
- 今日のサイバー犯罪者や脅威の開発者にとって利用されるインフラになっている。

この章では、進化するアプリケーションと脅威のトレンド、ユーザ アプリケーションとビジネス アプリケーションの曖昧な区別、および今日のビジネスにとってのこれらの多くのアプリケーションの戦略的な性質 (および、それに関連するリスク) について明らかにします。

アプリケーションは完全に良いわけでも、完全に悪いわけでもない

この10年の間に、アプリケーションは組織にとって劇的な変化を遂げてきました。企業の生産性を高めるアプリケーションには、意志の疎通や意志決定を迅速化するためのコミュニケーション機能を中心として、数多くの個人およびコンシューマ向けのアプリケーションとの連携や機能統合が行われています。企業のICTよりもコンシューマ向けのICTが先行している「コンシューマ化」と呼ばれる傾向によって、企業のインフラと個人・コンシューマ向けテクノロジとの協調や融合は促進されています。米国のIT調査会社であるガートナー社によれば、このコンシューマ化は2015年にかけてIT部門に影響を与える最も重要な傾向になります。

コンシューマ化のプロセスは、企業のITソリューションより強力または高機能で、より便利で、より安価で、よりすばやくインストールでき、より簡単に使用できるコンシューマーテクノロジやアプリケーションをユーザが見つけたときに発生します。これらのユーザ中心の「ライフスタイル」アプリケーションやテクノロジを使用すると、各個人が、仕事以外のことを処理したり、オンラインの顔を維持したりすることができます。この一般的な例には、Google Docs、インスタント メッセージング、およびWebベースの電子メールがあります。Enterprise 2.0アプリケーションでは、ビジネスでの使用と個人的な使用の従来の区別がなくなります。たいていは、ソーシャルネットワークに使用される同じアプリケーションが、仕事に関連する目的にも使用されています。そして、仕事と私生活の境界が曖昧になるに従って、ユーザは実質的に、職場でこれらの同じツールを使用できるようになることを求めます。

この要求に応えて、テクノロジ ベンダおよび開発者は、規模の経済性による恩恵と、口コミによる宣伝を中心としたバイラル マーケティングによる広範なメリットを受けています。比較的少数の企業顧客への大量の販売ではなく、文字どおり数億の個々のユーザへの少量の販売には次の意味があります。

- 購入サイクルの短縮。購入が企業の決定ではなく、個人的な選択になります。
- 標準や相互運用性ではなく、機能や使いやすさに焦点が置かれます。
- 大規模かつ、ほぼ瞬時のユーザ フィードバックに基づいて、製品が絶えず迅速に機能強化されます。

Enterprise 2.0アプリケーションの採用はIT部門ではなく、ユーザによって促進されています。容易にアクセスできることに加え、今日のナレッジ ワーカーがその使用に慣れているという事実は、コンシューマ化の傾向が継続するこ

とを示しています。Appopedia社 (www.theappgap.com) によって「企業における迅速なコラボレーション、情報の共有、出現および統合機能を提供するWebベースのテクノロジから成るシステム」と定義されている Enterprise 2.0 アプリケーションは、今や世界を魅了しています。ほとんど検索、リンク、およびタグ付けに焦点を絞ったいくつかのアプリケーションとして開始されたものが、オーサリング、ネットワーク、および共有を可能にする多数のアプリケーションに急速に移行しています。

第一世代のEnterprise 2.0アプリケーションの例には次のものがあります。

- SocialtextなどのWiki
- Bloggerなどのブログ ツール
- NewsGatorなどのRSSツール
- Cogenzなどの企業内ブックマークおよびタグ付けツール
- AOL Instant Messenger (AIM) などのメッセージング ツール

第二世代のEnterprise 2.0アプリケーションの例には次のものがあります。

- SharePointなどのコンテンツ管理ツール
- MegaUpload.comなどのブラウザ ベースのファイル共有ツール
- Facebookなどの複雑なソーシャル ネットワーク
- YouTubeなどの公開ツール
- Skypeなどのユニファイド メッセージング ツール
- Twitterやソーシャル ブックマークなどの投稿ツール

これらのアプリケーションで技術革新と採用のサイクルがいかに急速に促進されてきたかについて、世界中の347組織の分析結果に基づいて考えてみます 。

- 2008年4月の開始から18か月以内に、企業内においてFacebookチャットの利用率がYahoo! IMやAIMを追い越しました。これはEnterprise 2.0アプリケーションの普及がEnterprise 1.0アプリケーションに比べて着実に進行していることを示す良い例と言えます。
- 2009年3月から2009年9月までの間に、Google Docsの企業への浸透率は33%から82%に増加しました。
- その同じ期間に、企業におけるTwitterの使用はセッション数で252%、帯域幅で775%と急増しました。

コンシューマ化の傾向をビジネスプロセスの中でどのように活用したらよいかと言う点に対して自信がない多くの組織の反応は２つです。ひとつは、職場での使用を単純に無視することによって、これらの技術やEnterprise 2.0アプリケーションを黙認する。もしくは、その使用を明示的に禁止はしても、従来のファイアウォールとセキュリティテクノロジでは技術的に制御できない。これらの2つのアプローチはどちらも理想的とは言えず、いずれの場合も組織にとっていくつかのリスクを招きます。

- ビジネス運営上重要な役割を果たしているが、少数のユーザにしか知られず、個人向けの技術やアプリケーションに完全に依存し、組織の文化やポリシーに沿わない暗黙的なワークフロープロセスが作成される。
- 暗黙的であるために組織として対処される事も少なく、パッチ未適用で脆弱性を伴う。ユーザを狙った脅威が存在するために、脆弱性がそのアプリケーション内に存在するかどうかにかかわらず、ネットワークおよびコンピューティングインフラ全体に新たなリスクが発生する。
- これにより、組織がHIPAA、FINRA、PCI DSSなどの規制要件を満たすことができなくなり、準拠していないためのペナルティが課せられる。
- 従業員は外部プロキシや暗号化されたトンネル、およびリモートデスクトップ アプリケーションを利用する事によりファイアウォールなどのセキュリティ装置による制御を回避することができるため、セキュリティおよびリスクマネージャが、管理しようとしているリスクを確認することが困難になる。

アプリケーションが多様化しているだけでなく、これらのアプリケーションを良いまたは悪いとして明確に、分類できないことも大きな課題であると言えます。多くは明らかに良く (低リスク、ハイリターン)、その他は明らかに悪い (高リスク、ローリターン) にもかかわらず、その殆どはその中間のどこかに位置しています。その上、これらのアプリケーションが位置づけは、システムの構成やユーザまたはセッションに応じて変動する場合があります 。

たとえば、ソーシャル ネットワーク アプリケーションを使用して製品ドキュメントを見込み客と共有することは「良い」(中リスク、ハイリターン) に分類されますが、同じアプリケーションを使用して次に予定しているリリースの詳細を、競合他社の従業員を含む「友達リスト」に転送することは「良くない」(高リスク、ノーリターン) に分類されます。

実際に、多くの組織は現在、さまざまなソーシャル ネットワーク アプリケーションを使用して、人材募集、研究開発、マーケティング、カスタマ サポートなどの広範囲の正当なビジネス機能のために利用しています。さらに、「従業員に優しい」作業環境を提供し、やる気を向上させるための方法として、ライフスタイル アプリケーションの使用をある程度まで許可しようとしている組織も多数あります。

ビジネスを保護しながらFacebookの使用を許可する

従業員がFacebookを使用して自分の仕事を完了するようになるに従って、個人の世界から企業の世界にその影響が急速に広がっています。同時に、多くの組織は、約5億人のFacebookユーザを対象に調査を実施したり、対象を絞ってマーケティングを実行したり、製品のフィードバックを収集したり、認知度を高めたりするチャンスとして見ています。結果として、Facebookは組織の収支を改善する上で一定の効果を発揮する場合が多いと言えます

ただし、Facebookの使用を正式に有効にした場合、組織ではいくつかの課題が発生することになります。多くの組織は、業務におけるFacebookの利用頻度、またその使用目的を認識していません。ほとんどの場合、特定の使用方法を規定するポリシーは存在しないか、またはポリシーを規定しても実際に適用することは技術的な理由から非常に困難です。ユーザは「とりあえずクリック、考えるのは後」という精神状態で操作する傾向にあり、これにより、重大なセキュリティ上のリスクが発生します。

エンド ユーザによって企業に持ち込まれるすべてのアプリケーションと同様に、Facebookを黙認すると、脅威の拡大、データの消失、企業の評判の低下などを招く可能性があります。また、Facebookはビジネスにおいて重要な役割を果たす可能性があり、禁止するとユーザが代わりのアクセス手段 (プロキシや回避ツールなど) を探し始める可能性があるため、盲目的にブロックすることは必ずしも適切な対応であるとは言えません。組織は、体系化されたプロセスに従ってFacebookの適切な使用ポリシーを規定し、有効にして、適用しながら、同時にネットワーク リソースを保護する必要があります。

(続き)

(続き)

1. **誰がFacebookを使用しているかを見つけます**。マーケティングまたは販売部門によって「企業内」Facebookの運用がすでに確立されている場合も多く存在するため、IT部門はどのソーシャル ネットワーク アプリケーションが使用されているか、誰がそれらのアプリケーションを使用しているか、および関連するビジネス目標を明確にすることが重要です。Facebookを使用している、又は必要としているビジネス グループに会い共通の企業目標を話し合うことにより、IT部門は「常にノーと言う」イメージから「ビジネス上必要な物は許可」 する役割に移行することができます。
2. **企業のFacebookポリシーを規定します**。Facebookの使用パターンが特定されたら、組織は、企業、競合について何を発言または投稿すべきか、あるいはすべきでないかを議論する必要があります。Facebookに関連したセキュリティ上のリスクについてユーザを教育することは、ビジネス目的の使用を促進するためのもう一つの重要な要素です。組織は、ソーシャル ネットワークによってもたらされる潜在的な脅威からユーザと組織の両方をより適切に保護するために、「とりあえずクリック、考えるのは後」という精神状態を「考えてから、クリックする」という態度に変化させる必要があります。
3. **ポリシーを監視および適用するためのテクノロジを使用します**。これらの各議論の結果は、エンタープライズ環境でFacebookを安全に使用するために、IT部門がセキュリティ ポリシーをどのように適用するかの説明を行い、文書化する必要があります。

ソーシャル ネットワークの使用ポリシーの文書化と適用は、組織が従業員のやる気を向上させながら、収支を改善するのに役立ちます。さらにこの取り組みがIT部門と各ビジネスグループとの間に一般的に存在する溝を埋めるのに役に立つことでしょう。

米国の著名なコンサルティング会社であるマッキンゼー・アンド・カンパニー社とECM(エンタープライズ・コンテンツ・マネジメント)に関する国際団体であるAIIMの調査によると、企業はEnterprise 2.0アプリケーションおよびテクノロジの使用に測定可能なメリットがあることを認めています。特定のメリットには、アイデアを共有する能力の向上、知識の専門家へのより迅速なアクセス、および移動や運用、通信の各コストの削減が含まれます。

そのため、今日のネットワークセキュリティソリューションはアプリケーションの種類を区別できるだけでなく、その他ユーザ情報など関連情報を適切に識別し、その結果に応じて実行するアクションを変更できる機能が必要です。

アプリケーションはファイアウォールでは止められない

「アプリケーションの種類を区別すること」は簡単に思えますが、いくつかの理由から、実際には簡単ではありません。どのような環境でもアクセスして使用できるよう、多くのアプリケーションは通信方法を動的に調整することによって、従来のファイアウォールを回避するように最初から設計されています。つまり、エンド ユーザにとって、アプリケーションはいつでも、どこからでも使用できます。ファイアウォール等のセキュリティ装置を回避する一般的な手法には主に次のものがあります。

- **ポート ホッピング：** ポート/プロトコルが、1つのセッションの中でランダムに変更されます。
- **標準以外のポートの使用：** Yahoo! Messengerの標準のTCPポート (5050) の代わりに、TCPポート80 (HTTP) を介してYahoo! Messengerを実行するなど。
- **一般に使用されるサービス内のトンネリング：** P2Pによるファイル共有や、Meeboなどのインスタント メッセンジャー (IM) クライアントがHTTPを介して実行されている場合など。
- **SSL暗号化による隠ぺい：** たとえば、TCPポート443 (HTTPS) 経由でアプリケーショントラフィックが隠ぺいされます。

パロアルトネットワークス社による「アプリケーションの使用およびリスク レポート」2010年春版によると、分析された741の固有のアプリケーションのうち、65%がネットワーク環境に依存せず接続性を確保するためにこれらの技術を使用して設計されていることがわかりました。図2-1は、過去18か月間 (半年に1度の「アプリケーションの使用およびリスク レポート」がカバーしている期間) で、ネットワーク接続性確保技術を使用するアプリケーションがかなり増加していることを示しています。

多くの標準クライアント サーバ アプリケーションが、Webテクノロジを利用するように再設計されています。図2-1では、このレポートで分析された、ネットワーク接続性の確保に重点を置いたアプリケーションの30% (149) がクライアント サーバ ベースであること、つまり「ネットワーク接続性の確保機能を持つ」アプリケーションは常にブラウザを使用しているという概念と矛盾する事実が示されています。同時に、企業はますます、Salesforce.com、WebEx、Google Appsなどのクラウド ベースのWebサービスを採用しています。これらはたいていブラウザで開始されますが、その後すぐによりクライアント サーバ的な動作 (リッチ クライアント、独自仕様のトランザクションなど) に切り替わります。

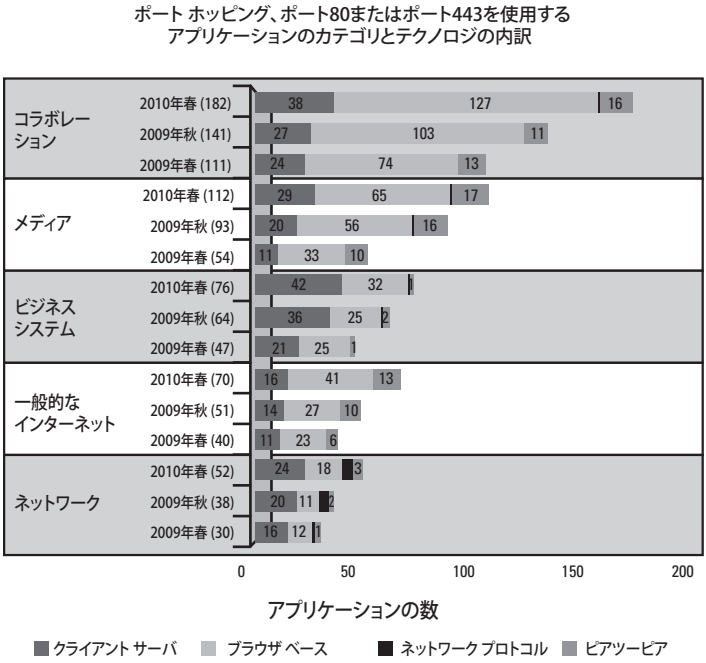


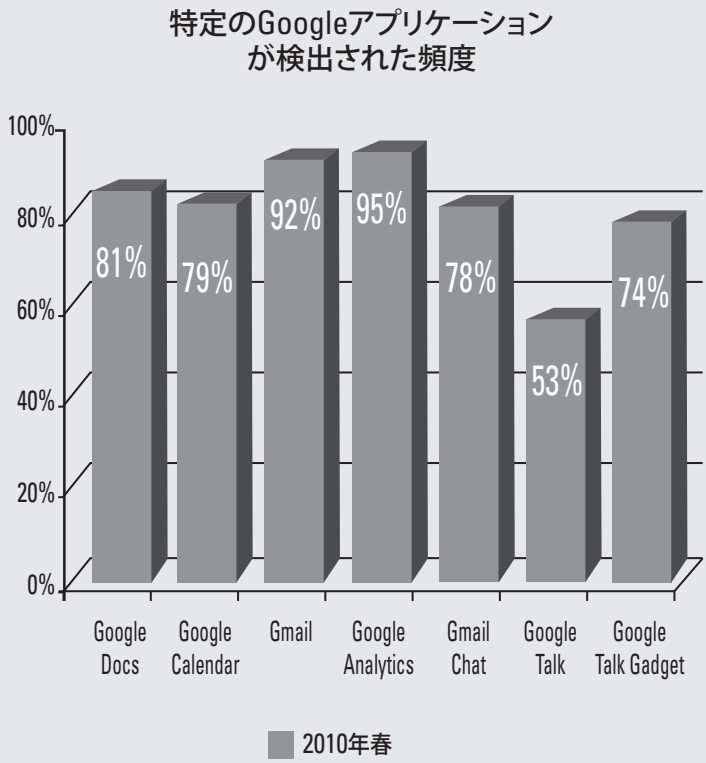
図2-1: アクセス性「機能」を持つアプリケーションのかなりの増加

Googleアプリケーション: Enterprise 2.0の典型か?

Googleが公開しているアプリケーションの多くは、ある程度まで、Enterprise 2.0 (ビジネス目的で使用されるWeb 2.0およびインターネット ベースのアプリケーション) の典型といえるでしょう。パロアルトネットワークス社による「アプリケーションの使用およびリスク レポート」2010年春版では、生産性 (Google Docs、Analytics、Calendar)、ソーシャル ネットワーク (Orkut)、通信 (Gmail、Gtalk、Voice)、およびエンターテイメント (YouTube、Picasa) という、広い機能範囲をカバーする22のGoogleアプリケーションが識別されています。これらのアプリケーションは、この調査に参加している組織で、かなり高い頻度で検出されました (次の図を参照)。

パロアルトネットワークス社の「アプリケーションの使用およびリスクレポート」2009 年秋版と比較すると、Enterprise 2.0 アプリケーションの使用増加の傾向が読み取れます。

- Google Docs は、組織あたり帯域が 55%、セッション消費が42%増加しました。
- Google Calendar は、組織あたり帯域が 18%、セッション消費が30%増加しました。
- Google Talk Gadget の帯域が 56% 急増したのに対して、Google Talk は 76% 低下しました。Google Talk Gadget は、クライアント サーバ ベースのGoogle Talkと同じ機能を実行する、フラッシュ ベースのブラウザ プラグインです。最も大きな違いは、ブラウザ ベースであるため、エンド ユーザによるアプリケーション インストールがデスクトップ制御によって制限される環境であっても簡単に使用できるという点にあります。



最後に、多くの新しいビジネス アプリケーションは、これらの同じテクニックを使用して、運用をより容易にしています。たとえば、RPCとSharepointがポート ホッピングを使用しているのは、検出を回避したり、アクセス性を高めたりするためではなく、ポート ホッピングがプロトコルまたはアプリケーションそれぞれの機能にとって重要であるためです。

多くのアプリケーションが私たちのイメージとは異なり、ポート ホッピングが可能なアプリケーションで多く検出されたものは、個人的に使用するアプリケーションだけではなくビジネスで使用するアプリケーションも多く含まれます(図2-2を参照)。これらのうち、ブラウザ ベースは3つだけ(Sharepoint、Mediafire、およびOoyla) であり、他はピアツーピアまたはクライアント サーバです。

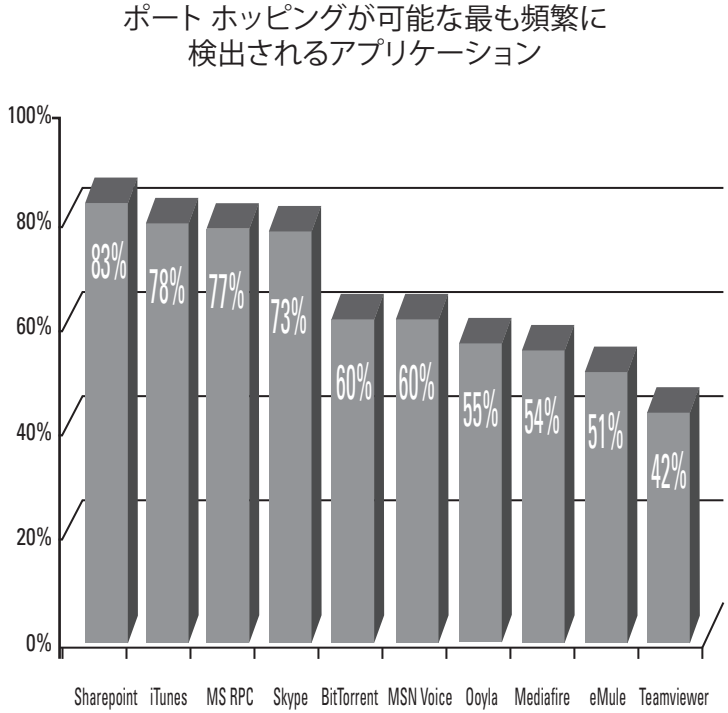


図2-2: 多く検出されたポート ホッピングが可能なアプリケーション

結果として、HTTPとHTTPSは現在、すべての企業トラフィックの約３分の２を占めています。これは、それ自体では問題になりませんが、従来のセキュリティ インフラの固有の問題を悪化させることは間違いありません。特に、HTTPやHTTPS上で動作するさまざまな上位アプリケーションは (正当なビジネス目的でサービスを提供しているかどうかにかかわらず)、古いネットワーク セキュリ

ティソリューションではほぼ区別が付きません。アプリケーションが劇的に進化し、組織はネットワーク通信に対する制御を失っているのです。

脅威が一緒にやって来る

アプリケーション層への攻撃が増え続けていることも、もう一つの心配事です。プリケーションを直接狙う攻撃は、これまでネットワーク層の保護を重視して構築されてきた多くの企業防衛網を通過できます。アプリケーションでのトンネリングのように、アプリケーション開発者が使いやすさの向上や利用範囲拡大のために使用する(前のセクションで説明した)ものと同じ手法を攻撃開発者は悪用し、ネットワークに侵入します。これらの攻撃や他の最新アプリケーションに組み込まれている回避技術は、企業ネットワークへ脅威が自由に侵入するために利用されています。したがって新種のマルウェアや不正侵入の80%以上が、ネットワーク装置やサービスではなく、アプリケーションの脆弱性を悪用するのは当然といえます。ユーザのアプリケーションへの信頼と、これらすべての要因が組み合わさって最悪の状況が生み出されます。また、ハッカーの動機は、知名度を上げることから金儲けに変化しています。今日の最も重要な目的は情報を盗むことです。そのため、誰かの邪魔をするだけの攻撃や害のない脅威を考え出すのはハッカーの興味の対象ではなくなりました。盗みを成功させるには、素早く気づかれないようにしなければなりません。

洗練さよりスピード(新しい脅威の生成スピード、修正スピード、拡大スピード)を優先するハッカーにとっての目的は、新たな脆弱性が発表されたら直ちに新しい脅威を開発し、実行し、素早くまん延させることです。パッチを当てるとか、アンチウイルスソフトウェアや不正侵入防御のような脅威シグネチャに依存するといった受動的な対抗手段では、このように生成されたゼロデイ攻撃やゼロデイに近い攻撃を防ぐことができない可能性が高くなります。

主に脅威開発Webサイト、ツール キット、フレームワークを広範囲に利用できることによって、この素早いアプローチが促進されています。これらのリソースを用いて、(少なくともシグネチャ ベースの対応策の観点から見て)「既知の」脅威を「未知の」脅威に容易に、かつすばやく変換できるようになりました。脅威のコードをわずかに変更するか、またはまったく新しい拡大と攻撃のメカニズムを追加し一般に複合脅威と呼ばれるものを作成することによって、変換が行われます。

Mariposa: その脅威の実態

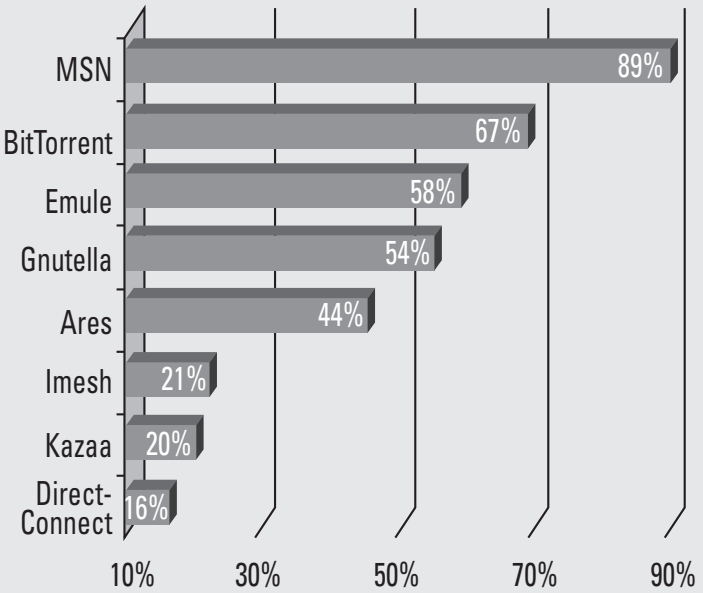
2010年7月28日、米国連邦捜査局(FBI) は、これまでに検出された犯罪ボットネットの中で最大級の「Mariposa」の作成者とされるスロベニア人ハッカーの逮捕を発表しました。

「Butterfly Bot」と呼ばれるコンピュータ ウイルスで構成されるMariposaボットネットは、Webサイトや金融機関のパスワードを盗み、世界の約200か国におよぶ800～1,200万台ものコンピュータを感染させたと推測されています。Defence Intelligence 社の CEO である Christopher Davis 氏によると、「Fortune 1000 企業のうち、この危険にさらされた企業のリストより、危険にさらされていなかった企業のリストを提供する」方が簡単とのことです。ネットワークに対する損害や、盗まれた実際のデータの被害総額はまだ計算中であり、ボットの作成者が逮捕されたにもかかわらず、そのボットを購入した世界中の犯罪者が今でも、何の疑いも持たない数百万の被害者からデータを盗んでいます。

Mariposaは、Ares、BearShare、Direct Connect、eMule、iMesh、Kazaa、Gnutella、Bit Torrent (LimeWire クライアント経由)、Shareaza の 9 種類の P2Pネットワークにまたがって自身を拡散します。基本的には、P2P ネットワークごとに、このボットの実行可能ファイルを提供している Mariposa フォルダ共有フィードが存在します。また、P2P アプリケーションに加えて、MSN インスタント メッセージングも拡散手法として使用されます。次の図は、パロアルトネットワークス社のアプリケーションおよび脅威調査チームが実施した 363 組織の分析で検出された最も一般的な Mariposa スプレッダーを示しています。

363 組織のより詳細な分析によって、いくつかの驚くべき統計が明らかになりました。

検出された上位のMariposaスプレッダー



- 312の組織 (86%) に、Mariposaで使用されるP2Pアプリケーションが1つ以上確認できました。
- 各組織で、9つのP2Pアプリケーションのうち平均して3つが検出されました。
- Mariposaを拡散できるP2Pアプリケーションによって消費される合計の帯域は 17.3 TBで、組織あたり平均55GB でした。
- P2Pスプレッダーによるセッションの消費は 5.55 億で、組織あたり平均180万セッションでした。
- MSNは、322の組織 (89%) で検出されました。組織あたり 2.8 GB の帯域、67,400 セッションのリソースが消費されていました。

89% の組織でMSNが検出され、85% を超える組織で平均3つのP2Pアプリケーションが検出されたことを考慮すると、多くの組織が脅威にさらされていると推測できます。

Mariposa ボットネットは、実際の脅威が現在広く普及している多くのアプリケーションにタダ乗りしているだけでなく、マイレージ(大きな恩恵)まで得ている明確な例です。

今日の脅威の多くは、ネットワークやシステム上で密かに動作することにより、機密データまたは個人データを密かに収集し、可能性な限り長く検出されずに済むように設計されています。このアプローチは、盗まれたデータの価値を保持するのに役立ち、さらに同じ攻撃や攻撃経路を繰り返し使用できるようにします。その結果、脅威はますます高度になってきました。たとえば、ルートキットに多くみられるカーネル レベルの攻撃は、他の種類のマルウェアの存在を効果的に隠ぺいすることにより、キーストロークの傍受のような、きわめて悪質な処理を永続的に実行できるようにします。

対象を絞った攻撃や、「Aurora」などの、特定の組織または個人に対するAPT (Advanced Persistent Threat: 高度で永続的な脅威) も、もう一つの懸案事項です。特定の装置、システム、アプリケーション、設定、さらには特定の組織または場所に採用されているスタッフさえもハッカーに利用され、長期間にわたって機密データを密かに収集するためにカスタマイズされた攻撃メカニズムを開発します。Verizon社の「2010年データ侵害調査レポート」によると、データ侵害の70%が外部のエージェントに起因しています。

脅威の増え続ける速度と高度化に対抗するため、アプリケーション層における広範囲の可視性と制御を備えた対応策が求められています。

第3章

従来のセキュリティ インフラの課題を認識する

この章で学ぶこと

- 従来のポート ベースのファイアウォールの弱点を調査する
- 不正侵入防御の欠点を検証する
- デバイス スプロールに対処する

アプリケーションと脅威のトレンドが急速に変化するに従い、多くの組織では、IT部門が制御を失っています。既存のセキュリティ インフラでは、良い (望ましい) アプリケーションと悪い (望ましくない) アプリケーションを効果的に区別できなくなっているため、ほとんどのIT部門は、セキュリティに対して柔軟性がなく、防御もできない「オール オア ナッシング」のアプローチをとらざるを得なくなっています。

- 寛大な立場をとる。これは、重要なアプリケーションのアクセス性を確保するためのアプローチですが、企業ネットワーク上の望ましくないアプリケーションや脅威も許可されてしまいます。
- 高いレベルのセキュリティを維持するために、単純に「ノー」と言うと、ビジネスの敏捷性や生産性が制限されたり、ユーザやビジネス部門が離反したり、セキュリティ制御を回避するためのバックドアがユーザによって作成されたりするおそれがあります。

代わりに、ビジネス単位やエンド ユーザからの正当な要求に自信を持って「イエス」と言うために、IT部門には、きめ細かな制御を働かせ、個々のアプリケーションのレベルまでの徹底的な保護を提供する能力が必要です。残念ながら、従来のネットワーク セキュリティ インフラはこの傾向に追随できず、この機能を提供することはできません。

この章では、新しいアプリケーションと脅威のトレンドに対して、ファイアウォールなどの従来のセキュリティ デバイスのどこが問題なのか、について説明します。

ファイアウォールにいったい何が起こったのか?

今では、ファイアウォールに関心がある人など誰もいないことにお気付きですか? かつて一時期、ファイアウォールはネットワーク内の最も重要なセキュリティ デバイスでした。いったい何が起こったのでしょうか。

答えはやや月並みですが、インターネットがすべてを変えてしまいました。数年前までは、ほとんどのファイアウォールが企業ネットワーク内外のトラフィックの制御にとても役立っていました。アプリケーション トラフィックが概ね正常に動作していたのはそのためです。電子メールは一般にポート25を通して流れ、FTPはポート20に割り当てられ、さらに「Webサーフィン」全体がポート80を利用していました。誰もが「ポート + プロトコル = アプリケーション」というルールに従って行動し、ファイアウォールがすべてを制御していました。ポートをブロックすると、アプリケーションがブロックされました。まさに正確で単純です。

残念ながら、今日のインターネットはそんな単純なものではありません。今日、インターネットは、企業ネットワーク上のトラフィックの70%以上を占めています。それは、ポート80のWebサーフィンだけではありません。通常、その20 ～ 30%はポート443上の暗号化されたSSLトラフィックです。さらに悪いことに、都合の良いルールを押し通す新しいインターネット アプリケーションが多く存在します。これらのアプリケーションは他のプロトコル内に自身を包み、自身に属していないポートをこっそり通過し、SSLトンネルの内部に自身を埋め込みます。つまり、まったく以前のようなお行儀の良い動作ではありません。

これらのアプリケーションはすべて、ビジネスに何らかのリスクをもたらします。そして、ファイアウォールを検出されずにすり抜けることができる賢い、新しい脅威のホストとして動作します。その間、既存のファイアウォールはすでに存在しないルールに依然として従っているため、何も問題ないかのように、ただそこに置かれているだけです。

ポート ベースのファイア ウォールはビジョンに欠ける

重要なネットワーク接続部にインラインで配置されるファイアウォールは、すべてのトラフィックを監視し、きめ細かなアクセス制御を提供する理想的な装置です。ただし、問題は、ほとんどのファイアウォールが「木を見て森をみず」ならぬ「森を見て木を見ず」である点にあります。つまり、一般的な全体像は見えますが、実際に発生していることをより細かく見ることはできません。これは、ファイアウォールが、パケットのヘッダで使用されているポート番号に基づいて、特定のトラフィック ストリームが関連付けられているアプリケーション層のサービスを推測することによって動作すること、また通常はパフォーマンスを向上させるために、セッション内の最初のパケットのみを参照して処理中のトラフィックの種類を特定するためです。ファイアウォールは、特定ポートが特定サービスに対応する (たとえば、TCPポート80がHTTPに対応する) という (要件ではなく) 慣習に依存しています。そのため、同じポート/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 (図3-1を参照)。

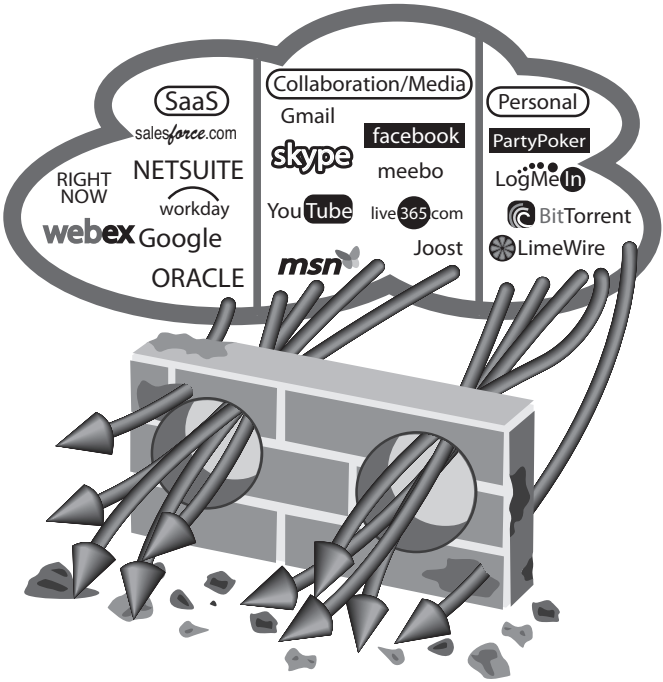


図3-1: ポート ベースのファイアウォールはアプリケーションを監視または制御できない

その結果、従来の「ポート ベース」のファイアウォールでは、基本的に何も見えなくなりました。ポート ホッピング、プロトコル トンネリング、標準以外のポートの使用などの一般的な回避テクニックを識別できないことに加え、これらのファイアウォールは単純に、各ネットワーク トラフィックが次のどの場合に該当するかを識別するための可視性やインテリジェンスに欠けています。

- ビジネスを目的にサービスを提供するアプリケーションに対応している。
- ビジネスを目的にサービスを提供しているが、場合によっては、承認されていない行動に使用されてしまっているアプリケーションに対応している 。
- ビジネス活動に対応しているにもかかわらず、マルウェアやその他の種類の脅威が含まれているため、ブロックすべきである。

これ以外に、これらのファイアウォールの制御モデルは一般に、きめ細かな制御ができません。これらのファイアウォールはトラフィックのブロックと許可は可能です。ですが、あるアプリケーションに存在する特定の機能を許可したり、許可するが帯域制御ポリシーを適用したり、許可するが脅威や機密データを検査したり、ユーザ、グループ、または時刻によって許可したりすることはできません。結果、企業が最終的には使いたいすべての「グレー」アプリケーションへのより適切に使用するためのソリューションとなりえません。

実際、従来のファイアウォールの一般的なよくある手法は、どの点から見ても完全に失敗しているといえるでしょう。

後付けの機能は基本的に欠陥を含んでいる

従来のファイアウォールベンダーの多くが、DPI (Deep Packet Inspection: 詳細パケット検査) 機能を組み込むことによって、この欠点を修正しようとしてきました。この方法でアプリケーション層の可視化と制御のための手段とすることは妥当なアプローチのように見えます。ただし、追加機能は「後付け」され、さらに後付けするときの元になる基礎が脆弱であるため、ほとんどの場合、非効率なセキュリティとなってしまいます。つまり、新しい機能は統合されるというより、付け足されるだけであり、アプリケーションの認識が完全に欠落しているポート ベースのファイアウォールが依然として、すべてのトラフィックの最初の分類に使用されます。これによりもたらされる問題と制限には、次のものがあります。

- **ネットワーク上に存在すべきでないアプリケーションがネットワークへの侵入を許可されてしまう**。
- **検査されるべきアプリケーションが必ずしもすべて検査されるとは限らない**。ファイアウォールがアプリケーション トラフィックを正確に分類できないため、どのセッションをDPIエンジンに渡すべきか不明確になります。
- **ポリシー管理がきわめて複雑になる**。製品のDPI機能においては、個々のアプリケーションをどのように処理するかというルールは基本的に「ネスティング構造」になります。このルールは、上位レベルのアクセス制御ポリシーの一部として動作します。
- **パフォーマンスが出なくなる**。アプリケーション層の機能がシステム リソースやCPUとメモリを集中的に使用することにより、基になるプラットフォームにかなりの負担が生じます。この状況を回避するために、管理者は高度なフィルタリング機能をすべて使用することはできず、選択的に実装することしかできません。

ファイアウォールの「補完製品」が役に立たない

ここ数年にわたり企業は、多くの補完的なセキュリティ ソリューションを、たいていはスタンドアロン アプライアンスの形式で実装することによって、ファイアウォールの欠陥を埋め合わせようとしてきました。不正侵入防御システム、アンチウイルス ゲートウェイ、Webフィルタリング製品、アプリケーション固有のソリューション (たとえば、インスタント メッセージング セキュリティのための専用プラットフォーム) などは、ほんの一部にすぎません。残念ながら、その結果はDPIアプローチの結果にがっかりするほど似ているだけでなく、さらに別の問題が加わります。

これらのファイアウォールの補完製品はすべてのトラフィックを監視できないか、従来のファイアウォールで失敗したのと同じポートおよびプロトコル ベースの分類方式に依存しているか、限られた一連のアプリケーションのみをカバーしているため、検査されるべきアプリケーションがすべて検査されるとは限りません。アクセス制御のルールや検査の要件が複数の管理画面に分散し、複数のポリシー モデルが使われる場合は、ポリシー管理がさらに大きな問題になります。また、レイテンシーが比較的長くなり、パフォーマンスも問題です。

次に、いわゆるデバイス スプロール化（無秩序に拡張されること）の問題があります。「ソリューション」が増え続けることにより、デバイスの台数、複雑性、TCO (総所有コスト) のすべてが上昇し続けます。製品自体に加え、膨大な運用経費が加わります。これらの経費には、IT部門の生産性、トレーニング、ベンダ管理などに関連するコストは言うまでもなく、サポート/メンテナンス契約、コンテンツ サブスクリプション、および施設のコスト (電力、冷却、フロア スペースなど) が含まれます。これには、厄介で、非効率的な、さらにコストのかかる努力が必要になります。

従来のIPSは今日の脅威に適していない

IPS (Intrusion Prevention System: 不正侵入防御システム) は、システムやアプリケーション内に存在する脆弱性を狙った攻撃を検出してブロックします。警告のみを行うIDS (Intrusion Detection System: 不正侵入検知システム) とは異なり、IPSシステムは、検出された攻撃を積極的にブロックするためにインラインに設置するように設計されています。IPSの主要機能の1つは、シグネチャをより正確に適用するためにプロトコルをデコードする機能です。これにより、IPSシグネチャをトラフィックの適切な部分に適用できるようになるため、シグネチャのみのシステムでは多く発生していた誤検知の割合が低減されます。ほとんどのIPS製品が、トラフィック分類の最初のパスとしてポートとプロトコルを使用していることに注意する必要があります。今日のアプリケーションの回避的な特性を考慮した場合、これはアプリケーションの誤った識別につながる可能性があります。また、IPSシステムは主に攻撃に焦点を絞っているために通常は、個別のアプライアンスとして、またはファイアウォールとIPSの組み合わせとして、ファイアウォールとともに展開されます。

IPSは、「見つけ次第止める」アプローチを使用して脅威を阻止するように設計されています。アプリケーションを制御するようには設計されていません。しかし、脅威を阻止するためでさえ、IPS には独自の欠陥があります。

新しいアプリケーションと脅威のトレンドを考慮して、組織もまた、従来の不正侵入防御システム (IPS) を再検証しています。主要なIPSベンダは、IPSの次のいくつかの基本的要素にわたって差別化しようと努力しています。

- **サーバとデータセンタの保護**。検出手法や防御手法はごく少数で、ほとんどのIPS製品がそれらすべてをサポートしています。これらの手法には、プロトコル アノマリ検知、ステートフル パターン マッチング、統計アノマリ検知、ヒューリスティック分

析、無効または不正な形式のパケットのブロック、IPデフラグメンテーションとTCP再構築 (回避への対抗のため) などがあります。また、ほとんどのIPSベンダは (攻撃に対応したシグネチャではなく) 脆弱性に対応したシグネチャを使用し、パフォーマンスを向上させるためにサーバからクライアントへの保護を無効にしています。

- **調査とサポート**。これは、実際の調査ベンダがどれだけ努力しているか、新しい攻撃や脆弱性から企業を保護するためにどれだけ迅速に対応できるかという点にたどり着きます。その多くはIPSベンダの調査チームの活動から成り、確かに違いは存在するものの、調査の多くは複数の業界調査の専門家にアウトソーシングされています。その他の (誰が調査を実施するかには関係なく) 重要な側面は、最近登場した新しい脅威から顧客を保護するために、ベンダがタイムリーな更新を提供できるかどうかという点です。
- **パフォーマンス**。企業は明らかに、IPSのパフォーマンスの問題に敏感になっています。最近のInfonetics社による調査では、企業が「アウト オブ バンド（インラインではないワンアームの構成）」でIPSを構築しようとさせている主な要因として、トラフィック/アプリケーションのレイテンシーの増加と帯域幅/パフォーマンスを挙げています。つまり、スループットやレイテンシーにおいての企業の期待に答えられるかどうかが、顧客の一番の関心事なのです。

ただし、防御が成熟するに従って、攻撃者は進化します。ファイアウォールなどの不正侵入検知および防御システムが、比較的よく知られた従来のテクニックを使っている場合、新しい攻撃は、次に示すような既知の弱点を悪用できます。

- **アプリケーションが運ぶ脅威**。脅威の開発者は、アプリケーションを攻撃対象と転送経路の両方に使用します。アプリケーションは、この両方の方法のための格好の舞台を提供します。アプリケーションが運ぶ脅威には、よく知られているもの (たとえば、Koobface、Boface、Fbactionなどの、ソーシャル ネットワーク間を移動する脅威の多く) と、そうでないもの (MSN MessengerとP2Pファイル共有アプリケーションを使用して広がるMariposaなど) があります。攻撃者はおかまいなしに、アプリケーションに便乗して、クライアントへの攻撃を開始します。
- **暗号化された攻撃経路**。脅威で使用される別の重要なテクニックに、暗号化があります。セキュリティ研究者は長年にわたり、さまざまな脅威が暗号化を使用する可能性があることを警告してきました。ユーザ主導のアプリケーションは暗号化された攻撃の侵入に利用されています。あまりにも多くのユーザがHTTPSは「安全」だと考えているため、ユーザは簡単に騙されて暗号化されたリンクをクリックしてしまい、暗号化された脅威は企業の防御を

なんなく通過してしまいます。信頼のレベルがきわめて高いソーシャル ネットワークでは、これがますます簡単になっています。密接に関連するもう1つの経路が、圧縮です。従来のIPSでは圧縮解除できず、そのため、圧縮されたコンテンツをスキャンできません。

ここでの共通のテーマは、これらのより新しい脅威を防御するために必要な制御のレベルです。つまり、アプリケーションとコンテンツの制御、SSLの復号化、および脅威を見つけるためのコンテンツの圧縮展開のすべてが、IPSが従来から行っているレベルをはるかに超えています。IDS (不正侵入検知システム) から移行するために費やした努力にもかかわらず、IPSは消極的なセキュリティ モデルにとどまり、またそのように設計されているという制限があります。簡単に言うと、IPSは「見つけ次第止める」モデルに依存しています。このモデルは、アプリケーション間を移動するような新しい脅威に対抗するにはあまり適していません。また、すべてのトラフィックを暗号化解除したり、分類したりできるアーキテクチャやプラットフォームにも適していません。

積極的なセキュリティ モデルは、良性、適正、または必要であることがわかっているすべての通信を明示的に許可し、その他のすべての通信を除外することによって動作します。消極的なセキュリティ モデルは、好ましくない通信やコンテンツのみを分類しようと努力し、悪いことがわかっている通信やコンテンツに対する対応策を使用することによって動作します。

情報漏洩に関する話題

過去2年間の情報セキュリティ関係の最大規模のニュース記事には、アプリケーションを介した組織の部外秘または機密データの漏洩が含まれます (たとえば、米国政府機関や請負業者、製薬メーカー、小売業者など)。ほとんどの場合、データの漏洩に使用されたアプリケーションは明示的に禁止されていましたが、従来のファイアウォールとIPSではそのポリシーを強制的に適用できていませんでした。これらの目立ったセキュリティ侵害を考慮すれば、組織が、このような厄介な出来事からの保護に役立つ、より優れたソリューションを探し始めているのも無理はありません。

UTMは複数の機能を無理やり詰め込んだ製品にすぎない

UTM (Unified Threat Management: 統合脅威管理) デバイスは、従来の手法を利用しつつセキュリティの課題に対する別の新しいアプローチです。UTM ソリューションは、セキュリティ ベンダが展開のコストを削減するために、自社のステートフル ファイアウォールに不正侵入防御やアンチウイルスのアドオンを後付けして生まれました。UTM 製品は、各機能を専門とする専用機器より優れた機能を実行するわけではまったくありません。代わりに、複数の機能を1つのデバイスに統合することによって、顧客に利便性を提供します。残念ながら、UTM には不正確である、管理しにくい、サービスを有効にするとパフォーマンスが低下するといった評判があるため、UTMは、失われる機能、管理性、またはパフォーマンスのマイナス面よりデバイス統合の価値の方が重要な環境に追いやられています。

UTM ソリューションの主な利点は、デバイス数を増加させることなく比較的適切に対処できることです。すべての「補完機能」を個別のデバイスとして展開する代わりに、UTM では、そのすべてが1つの物理パッケージに含まれています。

しかし、それでどうなるのでしょうか。その結果は実際、後付けのアプローチと何も変わらず、そのために同じ欠陥を露呈しています。不十分なアプリケーション分類と検査では盲点が基本的な問題として残り、複数の追加の対応策に対処しなければならないことによりパフォーマンスやポリシー管理の問題が発生しています。

ファイアウォールを修復するときが来た

従来のポート ベースのファイアウォールは実際のところ、ネットワークの境界が崩壊しインターネット アプリケーションが爆発的に増加している今日においては、すでにどのような価値も提供していません。

しかし、皆さんは、もうすでにわかっています。なぜ、その目に余る欠陥を、不正侵入防御システム、プロキシ、アンチウイルス、スパイウェア対策、URLフィルタリング、その他多くのより特殊なアプライアンスで埋め合わせるよう強要されたかを。確かに、これらのツールにより価値はある程度徐々に増えますが、特に困難な経済状況の下、その追加コストと複雑さを正当化することは難しくなっています。

セキュリティ アプライアンスの数が増えたからといって、必ずしもセキュリティが強化されるわけではありません。複雑さと不整合が、実際に組織のセキュリティにとって害になる場合があります。

Cigna社の最高情報セキュリティ責任者 (CISO) であるCraig Shumard氏は、2009年2月の雑誌「Network World」とのインタビューで、自分の組織内の増え続けるセキュリティ製品の山を「持続不可能」と呼び、それを「ピサの斜塔」にたとえて次のように話しています。「15～25、あるいはそれ以上のセキュリティ製品を引き続き運用することはできません ... この環境に新しいセキュリティ製品を追加し続けて、それらが効果的に使用されるはとても思えません」。明らかに、それは拡張性のない戦略です。さらに重要なことに、これらのどの追加製品からも、ネットワーク上で実行されているアプリケーションに必要な可視性と制御は提供されません。

いよいよ、中核の問題に対処するときが来ました。ファイアウォールの修復です。何と言っても、ファイアウォールはネットワーク内の最も重要な場所に位置しており、実際に、ネットワークを出入りするすべてのトラフィックに対する可視性と制御の集中管理されたポイントであるべきです。

第4章

次世代ファイアウォールで問題を解決する

この章で学ぶこと

- アプリケーション、ユーザ、およびコンテンツを識別する
- 次世代ファイアウォールと従来型ファイアウォールのパフォーマンスを比較する
- 次世代ファイアウォールのセキュリティとビジネス上のメリットを認識する

ほとんどの企業のネットワーク セキュリティは細分化され、分割されていて、ビジネス リスクや、増え続けるコストが課題となっています。従来のネットワーク セキュリティ ソリューションは、アプリケーション、脅威、およびネットワークのトレンドの変化について行くことができませんでした。さらに、その欠陥を埋め合わせるために提案された対応策も、その大部分は効果的でないことが実証されています。ネットワーク セキュリティを最初から作り直すときが来ました。

この章は次世代ファイアウォール (NGFW) に関する章であり、次世代ファイアウォールとは何か、それに該当しないもの、および組織にとっての次世代ファイアウォールのメリットについて説明します。

次世代ファイアウォール

法人ネットワーク セキュリティの基盤としてのファイアウォールを復活させるために、次世代ファイアウォールは「その中心にある問題を修正」します。白紙状態から始め、エンタープライズ ネットワーク上で実行されているすべての種類のアプリケーション (Web 2.0、Enterprise 2.0、および従来のアプリケーションを含む) の可視性と制御を有効にするために、次世代ファイアウォールはアプリケーションを識別し、トラフィックを分類します。効果的な次世代ファイアウォールのための不可欠な機能要件として、次の能力があります。

- 最初に、ポート、プロトコル、回避テクニック、またはSSL暗号化には関係なく、アプリケーションを識別する。
- アプリケーション (個々の機能を含む) の可視化、きめ細かなポリシー ベースの制御を提供する。
- ユーザを正確に識別した後、ポリシー制御のための属性として使用する。
- 広範囲の脅威 (アプリケーション層で動作している脅威を含む) に対するリアルタイム保護を提供する。
- 従来のファイアウォールとネットワーク不正侵入防御機能を単に統合するのではなく、融合する。
- マルチギガビットのインライン展開を、無視できるレベルのパフォーマンス低下で実現する。

従来のファイアウォールの標準的な機能には、パケット フィルタリング、ネットワークおよびポート アドレス変換 (NAT)、ステートフル インスペクション、仮想プライベート ネットワーク (VPN) のサポートなどが含まれます。標準的な不正侵入防御機能には、脆弱性および脅威に対応したシグネチャ、ヒューリスティックなどが含まれます。

NGFWの特長は、従来のファイアウォールで実行されるすべての機能を、革新的な識別テクノロジ、高性能、およびエンタープライズ クラスの基礎的な機能を用いて実行する能力です。

アプリケーション識別

ポートとプロトコルの確立は、アプリケーション識別における重要な最初の手順ですが、それだけでは不十分です。ネットワーク通信サービスにのみ依存するのではなく、堅牢なアプリケーション識別および検査により、現在使用されている特定のアプリケーションに基づいて、ファイアウォールを通過するセッション フローをきめ細かく制御することが可能になります (図4-1を参照)。

アプリケーション識別は、NGFWの中心に位置するトラフィック解析エンジンによって実行されます。それには、ポート、プロトコル、暗号化、または回避テクニックには関係なく、ネットワーク上のアプリケーションを特定するための多元的なアプローチが必要になります。NGFWで使用されるアプリケーション識別テクニック (図4-2を参照) には次のものがあります。

- **アプリケーション プロトコルの検出と復号化**。アプリケーション プロトコル (たとえば、HTTP) を特定し、SSLが使用されている場合は、さらに分析できるようにトラフィックを復号化します。このトラフィックは識別テクノロジで特定され、再び暗号化されます。
- **アプリケーション プロトコルのデコード**。最初に検出されたアプリケーション プロトコルが「実際のプロトコル」なのか、または実際のアプリケーションを隠ぺいするためのトンネルとして使用されているのか (たとえば、HTTPの内部にYahoo! Instant Messengerが存在する可能性があります) を判定します。
- **アプリケーション シグネチャ**。コンテキスト ベースのシグネチャが、使用されているポートやプロトコルには関係なく、アプリケーションを正しく識別するためのプロパティやトランザクション特性を探します。これには、アプリケーション内の特定の機能 (IM セッション内のファイル転送など) を検出する能力が含まれます。

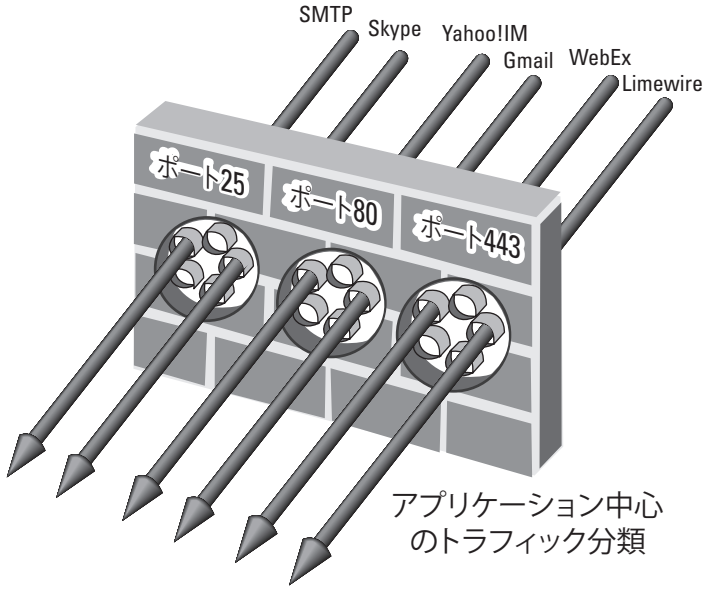


図4-1: アプリケーション中心のトラフィック分類では、使用されているポートやプロトコルには関係なく、ネットワーク全体を流れる特定のアプリケーションを識別します。

- **ヒューリスティック**。シグネチャ分析による識別を逃れるトラフィックには、ヒューリスティック (または振る舞い) 分析が適用され、独自仕様の暗号化を使用するP2PまたはVoIPツールなどの厄介なアプリケーションの識別が可能になります。

図4-2: ポート、プロトコル、回避テクニック、またはSSL暗号化には関係なく、アプリケーションを識別するために使用されるNGFWテクニック。

アプリケーションを正確に識別するためのテクノロジを用意することは重要ですが、情報に基づいたポリシー決定を行うことができるように、アプリケーションのセキュリティへの影響を理解することも同様に重要です。IT管理者に、既知の脆弱性、検出を回避する能力、ファイル転送機能、帯域幅の消費、マルウェアの転送、誤用の可能性などのアプリケーションに関する知識を提供するために、各アプリケーションと、その動作やリスクに関する情報を含むNGFWソリューションを探してください。

ユーザ識別

ユーザ識別のテクノロジは、特定のユーザIDにIPアドレスをリンクすることにより、ユーザごとのネットワーク活動の可視化と制御を可能にします。Microsoft Active Directory (AD) などのLDAPディレクトリとの緊密な統合により、この目的を次の2つの方法でサポートします。最初に、ログイン監視、エンド ステーション ポーリング、およびキャプティブ ポータル（Web認証）の組み合わせを使用して、ユーザとIPアドレスの関係を定期的に検証および保持します。次に、ADと通信して、役割やグループ割り当てなどの関連するユーザ情報を取得します。それにより、これらの詳細情報を次の目的に使用できます。

- 具体的に誰が、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、および脅威のトラフィックに責任を負っているかについての可視性を得る。
- アクセス制御ポリシー内の変数としてユーザ識別情報の使用を可能にする。
- トラブルシューティング/インシデントへの対応やレポートを促進する。

ユーザ識別により、IT部門は、アプリケーションの使用をインテリジェントな方法で制御するのに役立つ別の強力なメカニズムを手に入れることができます。たとえば、通常であればブロックされるソーシャル ネットワーク アプリケーションを、それを使用する必要がある個人またはグループ (人事部門など) に対して有効にすることができます (図4-3を参照)。

コンテンツ識別

コンテンツ識別は、次世代ファイアウォールに、許可されたトラフィック内の脅威のリアルタイムの防御、Webサーフィン活動の制御、ファイルおよびデータ フィルタリングなどの、エンタープライズ ファイアウォールではできなかった機能を提供します。

- **脅威防御**。このコンポーネントは、利用されているアプリケーション トラフィックには関係なく、スパイウェア、ウイルス、および脆弱性攻撃がネットワークに侵入するのを防御します。
    - **アプリケーション デコーダ**。データ ストリームを前処理し、そこに特定の脅威が含まれていないかどうかを検査します。

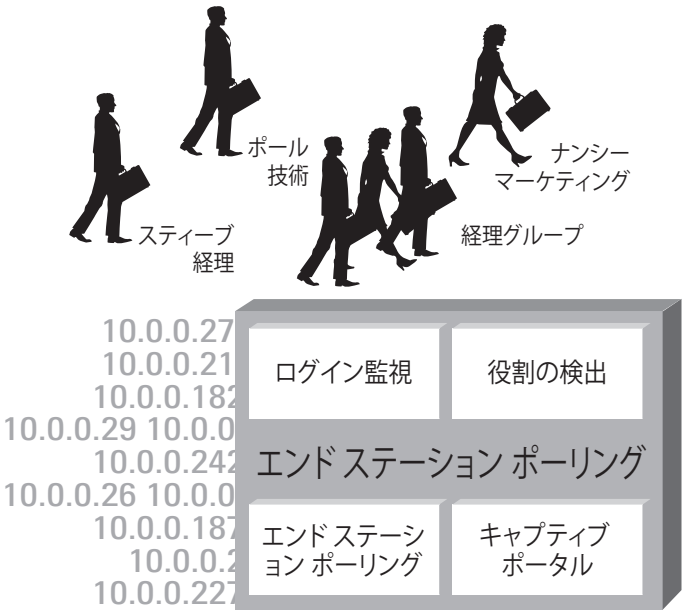


図4-3: ユーザ識別は、ユーザ ベースのポリシー、レポート、およびフォレンジックのためのエンタープライズ ディレクトリを統合します。

- **ストリーム ベースのウイルスおよびスパイウェア スキャン**。ファイル全体がメモリに格納されるまで待たず、ファイルの最初のパケットを受信したらすぐにトラフィックをスキャンするため、スループットが最大化され、処理遅延が最小限に抑えられます。
- **脅威防御のシグネチャフォーマットを統一**。脅威の種類ごとに個別のスキャン エンジンを使用する必要性がなく、パフォーマンスが向上します。ウイルス、スパイウェア、および脆弱性攻撃をすべて、1回のパスで検出できます。
- **脆弱性攻撃からの保護 (IPS)**。トラフィックの正規化とデフラグメンテーションのための堅牢なルーチンに、最も広範囲の既知および未知の両方の脅威からの保護を提供するためのプロトコル アノマリ、動作アノマリ、およびヒューリスティック検出メカニズムが加わります。

- **URLフィルタリング**。必須ではないものの、URLフィルタリングは、コンテンツの分類に使用されることがあります。統合された、標準のURLデータベースにより、管理者は、従業員やゲストユーザのWebサーフィン活動を監視および制御することができま

す。ユーザ識別と組み合わせて使用されるWeb使用ポリシーをユーザごとに設定することもできます。これにより、企業は法律、規制、および生産性に関連する一連のリスクからさらに保護されます。

- **ファイルおよびデータ フィルタリング**。ファイルおよびデータ フィルタリングでは、詳細なアプリケーション検査を利用して、許可されていないファイルやデータの転送のリスクを軽減するポリシーの適用を可能にします。これには、(拡張子だけに基づくのではなく) 実際の種類でファイルをブロックする機能や、クレジット カード番号などの機密のデータ パターンの転送を制御する機能が含まれます。これは、アプリケーション識別の精度を補完するものです。これにより、個々のアプリケーション (IMなど) 内のファイル転送を制御する機能が多くのアプリケーションに提供されます。

コンテンツ識別により、IT部門は、脅威を阻止し、インターネットの不適切な使用を削減し、さらに情報漏洩の防止に役立つ機能のすべてを、膨大な追加製品や様々なリスク対策アプライアンスに投資することなく手に入れることができます (図4-4を参照)。

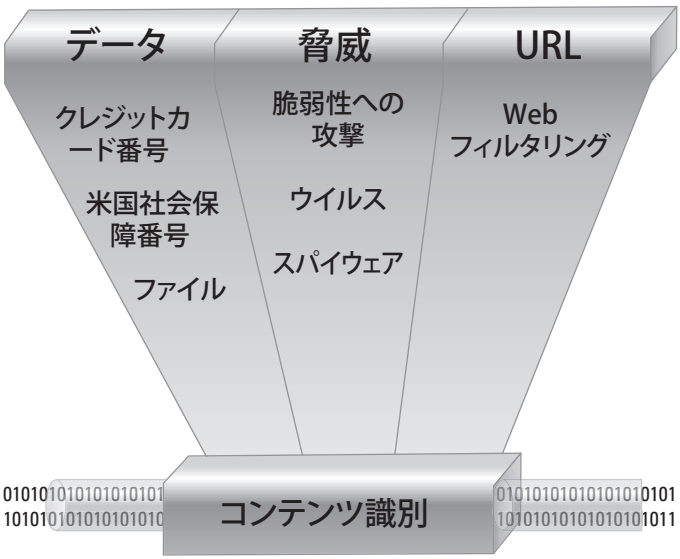


図4-4: コンテンツ識別は、脅威、機密データ、およびURLフィルタリングに対するコンテンツ スキャンを統合します。

ポリシー制御

使用されている「アプリケーションの識別」、それを使用している「ユーザの識別」、およびその使用目的つまり「コンテンツの識別」は、ネットワークを流れるトラフィックの学習における重要な最初の手順です。そのアプリケーションの処理内容、使用しているポート、基になるテクノロジ、およびその動作の学習は、そのアプリケーションの処理方法について情報に基づいた決定を下すために必要な次の手順です。使用の全体像が得られたら、組織は、従来のポート ベースのファイアウォールで使用可能なアクションである単純な「許可」または「拒否」よりきめ細かく、かつ適切な広範囲のアクションを含むポリシーを適用できます。これは、アプリケーション、ユーザ、およびコンテンツ識別を組み合わせた、次世代ファイアウォールのセキュリティモデルによって可能になります。従来のポート ベースのファイアウォールにもセキュリティ モデルはありますが、インテリジェンスに欠けています。その他のセキュリティ デバイスには何らかのインテリジェンスがある可能性がありますが、セキュリティ モデルはありません。NGFWにおけるポリシー制御オプションの例には、次のものがあります。

- 許可または拒否する
- 許可するが、攻撃、ウイルス、その他の脅威をスキャンする
- スケジュール、ユーザ、またはグループに基づいて許可する
- 暗号化解除して検査する
- QoSによる帯域制御を適用する
- ポリシー ベースのフォワーディングを適用する
- 特定のアプリケーション機能を許可する
- 上記の任意の組み合わせ

高性能なアーキテクチャ

広範囲にわたる一連のアプリケーション認識およびコンテンツ検査機能が用意されていても、パフォーマンスの制約のためにIT管理者がそれらの機能を完全に使用できなければ、ほとんど価値はありません。そのため、高性能を提供するように最初から設計された次世代ファイアウォールを選択することが重要です。問題は、これらの機能がリソースを集中的に使用するという点だけではありません。多くのアプリケーションにおけるレイテンシーの影響は言うまでもなく、今日のセキュリティ インフラが処理すべきトラフィック量も膨大に存在します。すべてのアプリケーションと脅威検査機能が同時に使用された場

合でも、高い負荷の下で、決められたスループットと妥当なレイテンシーを持続させる必要があります。これが、セキュリティの観点から見た場合の理想的な構成です。

従来の (特に、後付けの機能を含む) セキュリティ製品の場合は、高レベルの各セキュリティ機能が独立に実行されます。このマルチパス アプローチでは、低レベルのパケット処理ルーチンを相当な回数繰り返す必要があります。システム リソースが非効率的に使用され、かなりの処理遅延が発生します (図4-5を参照)。

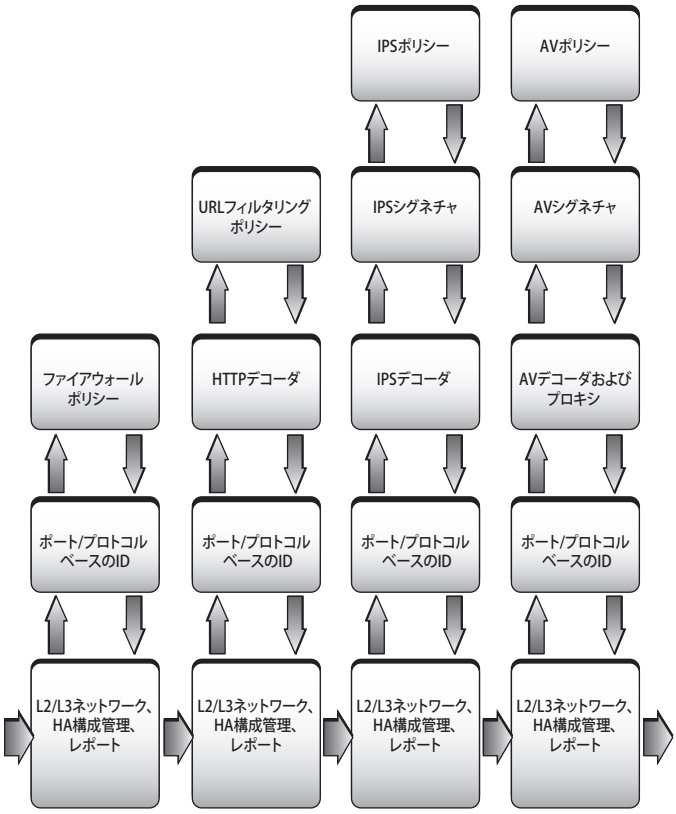


図4-5: 従来のマルチパス アーキテクチャ

これに対して、シングルパス アーキテクチャを使用するNGFWでは、パケットの繰り返し処理が不要なので、ハードウェアにかかる負荷が軽減され、処理遅延が最小限に抑えられます。個別のデータとコントロール プレーンを保持するカスタマイズされたハードウェア アーキテクチャなどのその他の技術革新が、エンタープライズ クラスのソリューションを提供します (図4-6を参照)。

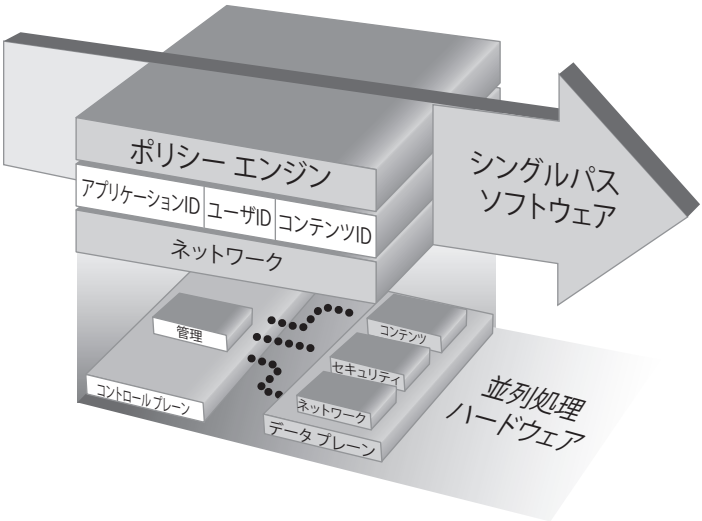


図4-6: シングルパス並列処理アーキテクチャと完全に独立したコントロールおよびデータ プレーンによって、エンタープライズ パフォーマンスが提供されます。

次世代ファイアウォールと似て異なる製品とは

次世代ファイアウォールに似た機能を実行する多くのネットワーク ベースのセキュリティ製品が入手可能ですが、それらの製品は同じものではありません。それらの例を次に示します。

- **統合脅威管理 (UTM)**。UTMアプライアンスは、ポート ベースのファイアウォール機能や、基本的な不正侵入防御などの複数のセキュリティ機能を持っています。UTMソリューションは一般に、高性能を発揮するようには設計されておらず、通常は小規模な環境にのみ適しています 。

- **プロキシ ベースの製品**。プロキシ (ファイアウォールとキャッシュの両方) は発信元と宛先の間に位置しており、トラフィックを傍受し、アプリケーション セッションを終了した後、再び起動して対象の宛先に送信することによってそのトラフィックを検査します。プロキシは、クライアントに代わって宛先との接続を確立することにより、ネットワーク上のコンピュータをプロキシの背後に隠します。ただし、各個別のアプリケーションに独自のプロキシが必要なため、限られた数のアプリケーションしかサポートできません。
- **Webアプリケーション ファイアウォール (WAF)**。WAFは、Webアプリケーションを検査して、潜在的なコーディング エラーによるセキュリティ上の問題がないかどうかを監視するように設計されています。WAFでは、OSIスタック全体ではなく、レイヤ7のみを検査します。

WAFがアプリケーションを保護するのに対して、NGFWはネットワークを保護します。

- **脆弱性およびパッチ管理**。脆弱性およびパッチ管理ソリューションは、ホストをスキャンしてソフトウェアやオペレーティング システムに既知の脆弱性がないかどうかを調べたり、パッチや更新がインストールされていることを確認したり、識別された脆弱性を修正したりします。これはNGFWの機能ではありません。
- **情報漏洩対策 (DLP)**。これらのソリューションは、識別されたパターン (クレジット カード番号など) に一致するデータの転送を防止します。これらのソリューションは、速度や処理遅延に関連したリアルタイムの要件がないネットワーク機能のために実装されます。
- **セキュアWebゲートウェイ**。これらのソリューションはURL分類を使用して、Webサイトへのユーザ アクセスに関連したポリシーを適用したり、悪意のあるWebサイトによって配信されたマルウェアをブロックしたりします。NGFWと比較すると、これらのソリューションは機能が限られており、ユーザによって容易にバイパスされます。
- **セキュア メッセージング ゲートウェイ**。これにはスパム フィルタやIMゲートウェイが含まれ、アンチスパムおよびアンチフィッシング保護、アンチウイルス スキャン、添付ファイル フィルタリング、コンテンツ フィルタリング、データ消失防御、ポリシー コンプライアンスおよびレポートが提供されます。NGFWとは異なり、これらの機能はリアルタイムには実行されず、レイテンシーの影響の少ない電子メールなどのアプリケーションに使用されます。

次世代ファイアウォールのメリット

従来のネットワーク セキュリティ インフラおよびソリューションに比べて、次世代ファイアウォールには多数のメリットがあります。そのいくつかを次に示します。

- **可視化と制御**。NGFWによって提供される可視化と制御の向上により、企業は、ポートやプロトコルなどの曖昧で、紛らわしい属性に依存しなくても、ポリシー制御のためにアプリケーション、ユーザ、コンテンツなどのビジネス関連の要素に焦点を絞ることができ、さらに許可されたアプリケーションのための脅威防御を提供しながら、リスクをより適切かつ綿密に管理するとともに、コンプライアンスを達成することができるようになります。
- **安全に「許可」する**。すべてのユーザに (現在の場所には関係なく) 整合性のある一連の保護およびイネーブルメント機能を提供することによって、広いカバー範囲を実現します。
- **簡略化**。多数のスタンドアロン製品の必要性をなくすことによって、ネットワーク セキュリティとその管理の複雑さを軽減します。この統合によって、サポート、メンテナンス、ソフトウェアサブスクリプション、電力、HVACなどの継続的な「ハード」運用経費、トレーニングや管理などの「ソフト」運用経費だけでなく、ハードの資産コストも削減されます。
- **ITとビジネスの調整**。IT部門に、広範囲にわたる一連の脅威からの保護を実現しながら、アプリケーションを識別してきめ細かく制御する能力を与えることにより、ビジネスを最適にサポートするために必要なアプリケーションに対して、IT部門が自信を持って「イエス」と言えるようにします。

第5章

次世代ファイアウォールの導入

この章で学ぶこと

- コンピュータやシステム利用者、そしてネットワークに対する適切な制御が出来る環境を実装する
- 最適なソリューションを選択するための要件を明確にする
- パフォーマンスとセキュリティを両立するネットワークを設計する

組織の全体的なセキュリティ戦略への影響を考慮せず、技術優先で実装される場合が多すぎます。この失敗を避けるために、組織のセキュリティポリシーが最新であることや、検討中の技術的な解決手段が包括的にセキュリティ戦略をサポートしていることを確認することが重要です。

さまざまな技術的解決手段を検討する場合は、組織の要件を明確に理解していることも重要です。Gartner社によると、エンタープライズファイアウォール市場における製品の差別化ポイントは少なく、そのために最終的な製品選択の決定のために、組織特有の要件に対応しているかという点を考える必要があります。

この章では、組織のセキュリティポリシーで考慮すべき各種の制御方法について説明した後、要件を定義し、ベンダへのRFPを作成するうえで調査する必要のある技術的要件の具体的な例を提供します。最後に、ネットワークや機密データを正しく分割管理することの重要性、およびモバイルユーザの対応方法について説明します。

組織全体のポリシーを通した安全な導入

どのように導入するかは、アプリケーション、動作、リスク、およびユーザの教育と知識に関する最優先課題です。Enterprise 2.0アプリケーションの場合、ユーザは以前からメリットに基づいて決定してきましたが、仕事に最適なアプリケーションの選択についてはさらに教育が必要性です。IT部門の役割はアドバイザーやよき指導者の役割、つまり、リスクや動作についてユーザにアドバイスし、一連の使用可能なアプリケーションのうちのどれが要件を解決するために最適になり得るかに関してユーザを指導することです。ただし、導入によってアプリケーションに関連したリスクの認識を高めることにもなります。その点では、ITワーカー自身が真のスーパーユーザ (とは言え、この用語の通常の意味とは異なりますが) になる必要があります。Enterprise 2.0のスーパーユーザは、アプリケーションの内部で「生活」し、一連の主要な作業をそのアプリケーションに依存しているユーザです。適切な行動をとろうとするならば、IT部門はEnterprise 2.0を本気で先入観なく採用する必要があります。それが達成されたら、IT部門は、Enterprise 2.0アプリケーションの使用に関連したすべてのリスク (その使用の社会的な影響や評判による影響に関係するリスクさえも含む) についてユーザを正しく教育することができます。

コーポレートガバナンスを効果的にするために、IT部門は、スマート ポリシーの定義において主要な役割を果たす必要があります。ただし、スマート ポリシーの有効性や関連性は従来のIT的な考え方と異なる場合があり、IT部門がこれらのポリシーの唯一の所有者にならないようにすることが重要です。この点は大きな物議をかもすように聞こえるかもしれませんが、Enterprise 2.0アプリケーションは「禁断の果実」になる傾向があります。また、Enterprise 2.0の採用は、そのほとんどがボトムアップ式に始まるにもかかわらず、経営幹部の理解と支援がなければそれほど成功しません。これは、いったんEnterprise 2.0アプリケーションの採用に成功すると、その使用を停止しようとしても、IT部門がそれに対する経営幹部の支援を当てにできなくなることを暗示しています。

多くの場合、コーポレートガバナンスに関する議論は、Facebookに代表されるソーシャルメディアなど、特定のEnterprise 2.0アプリケーションの使用中にユーザが引き起こした失敗の例とともに始められます。また、Enterprise 2.0アプリケーションの使用を管理する法律自体が存在しないという単純な理由から、IT部門がコンプライアンスに基づいた議論を追求することも賢い考えではありません。たとえば、株式取引などの規制の強い環境では、インスタントメッセージングの使用は記録や監査のルールに縛られる可能性があります。IT部門の役割は、各ツールの影響についてトレーダーを教育し、使用ポリシーの策

定に参加した後、その使用を監視および適用することです。この例では、そのポリシーによってトレーダーがFacebookチャットをインスタントメッセージングに使用することは防止できますが、代わりにMSNの使用が可能になる状況が発生する可能性があります。

コーポレートガバナンスとその管理作業が最も適切に機能するのは、組織全体ポリシーがIT部門、人事部門、経営幹部、ユーザという、Enterprise 2.0の展望における4つの主要な利害関係者によって策定されている場合です。明らかに、IT部門には果たすべき役割がありますが、それはそれほど頻繁に果たす厳密に定義された役割ではあり得ません。とは言え、アプリケーションや新技術導入者兼管理者としてのその役割について、のんびり構えているわけにもいきません。

アプリケーション制御を実装および適用する場合は、それを何よりも重要な企業セキュリティポリシーの一部にする必要があります。アプリケーション制御ポリシーを実装するプロセスの一部として、IT部門はEnterprise 2.0アプリケーションについて学ぶための一致団結した努力を行う必要があります。これには、それらのアプリケーションを意図したすべての目的に採用することや、必要な場合は、実際の動作を把握するためにラボ環境で事前にインストールまたは有効にすることが含まれます。その場合、仲間との議論や、Enterprise 2.0に重点を置いたWebサイト、掲示板、ブログ、開発者コミュニティなどが貴重な情報源になります。

従業員の教育

ほとんどの企業には、どのアプリケーションが許可され、どのアプリケーションが禁止されているかの概要を規定した、何らかの種類のアプリケーション使用ポリシーがあります。すべての従業員がこのポリシーの内容と、それに準拠しない場合の影響を理解していることを期待されていますが、次に示すような答えの得られない疑問がいくつかあります。

- 「悪い」アプリケーションがますます増えている現在、どのアプリケーションが許可され、どのアプリケーションが禁止されているかを従業員はどのように知ることができるのか。
- 承認されていないアプリケーションのリストはどのように更新され、従業員がそのリストの変更を知っていることを誰が保証するのか。
- 何を行うとポリシー違反になるのか。
- ポリシー違反の罰則はどのようなものか (解雇か、懲戒か)。

ポリシーガイドラインの策定は、何を許可し、何を禁止すべきかについて利害が一致しない部署間において相容れない意見が存在するため一般には困難です。この問題の中心には、ITセキュリティと人事部門という、通常はポリシーの策定に関与している2つの組織グループが、新技術の採用中にほとんど出る幕がないという事実があります。新技術や新しいアプリケーションが実装された後に、安全な使用のためのポリシーを策定することは簡単な作業ではありません。

文書化された従業員規定は、アプリケーション制御における重要な要素である必要がありますが、Enterprise 2.0アプリケーションの安全な実行において、単独のメカニズムとしての従業員の教育はほとんど効果を期待できません。

デスクトップ制御

デスクトップ制御は、IT部門に大きな課題を提示します。デスクトップ制御の精度や、その従業員の生産性への影響を慎重に検討する必要があります。従業員ポリシーと同様に、デスクトップ制御は企業におけるEnterprise 2.0アプリケーションの安全な実行において重要な部分であり、いくつかの理由から、単独で使用しても効果を期待できません。

ユーザが独自のアプリケーションをインストールできないようにするためのデスクトップ制御の徹底的な実行は、口で言うほど簡単な作業ではありません。

- リモートで接続されているラップトップ、インターネットのダウンロード、USBドライブ、電子メールのすべてが、承認されているかどうかは別にして、アプリケーションをインストールする手段になります。
- 管理者権限の完全な無効化は、実装が困難であることが実証されているだけでなく、場合によってはエンドユーザの能力を制限します。
- 現在ではUSBドライブでアプリケーションを実行できるため、事実上、ネットワークアクセスが許可された後でEnterprise 2.0アプリケーションにアクセスできます。

デスクトップ制御は、Enterprise 2.0アプリケーションを安全に実行にするための手段として、文書化された従業員規定を補完することができます。

ネットワーク制御

ネットワークレベルで必要なものは、Enterprise 2.0アプリケーションを識別し、それらのアプリケーションをブロックまたは制御する手段です。ネットワークレベルの制御を実装することによって、IT部門は、Enterprise 2.0アプリケーションを使用することによって発生する脅威や中断の可能性を最小限に抑えることができます。ネットワークレベルではいくつかの制御メカニズムを使用できますが、そのそれぞれに、有効性を低下させるある特定の欠点があります。

- ステートフルファイアウォールはネットワーク防御の最前線として使用でき、トラフィックのおおざっぱなフィルタリングと、異なるセキュリティゾーンをまたがるネットワークのセグメント化が可能になります。ステートフルファイアウォールの1つの欠点は、ネットワークとの間で送受信されるトラフィックを識別および制御するためにプロトコルとポート番号を使用していることです。このポート中心の設計は、使用するポート番号を変化させながら利用可能なポート番号を見つけるEnterprise 2.0アプリケーションの利用に対してほとんど効果がありません
- ファイアウォールと共に利用されるケースが多いIPSは、トラフィックのサブセットを検査し、既知の脅威や好ましくないアプリケーションをブロックすることにより、ネットワーク脅威の防御機能を向上させます。しかしIPS製品は幅広いアプリケーションや、すべてのポートにわたるすべてのトラフィックの検査に必要なパフォーマンスに欠けているため、残念ながら完全なソリューションと見なすことはできません。
- IPSテクノロジは通常、パフォーマンスの低下を避けるためにトラフィックの一部のみを検査するように設計されているため、今日の企業に必要な幅広いアプリケーションをカバーすることができません。そして最後に、ファイアウォールとIPSの組み合わせの場合、異なる管理インタフェースを持つ機器を個別に管理するという煩雑な作業が必要となります。簡単に言うと、現在の後付けのソリューションの１つであるIPSは、今日のアプリケーションの可視化と制御の要件を解決するために必要な精度、ポリシー、またはパフォーマンスを備えていません。
- プロキシソリューションはトラフィック制御のための別の手段ですが、これもまた、限定された一連のアプリケーションまたはプロトコルのみを検査するため、トラフィックの一部しか検査することができません。そのため、Enterprise 2.0アプリケーションは単純に、プロキシによってブロックされたポートを確認後、オープンされた次のポートに移行することができます。設計によ

り、プロキシは制御しようとしているアプリケーションのネットワーク動作を模倣する必要があるため、既存のアプリケーションに対する更新だけでなく、新しいアプリケーションのためのプロキシの開発に苦労しています。プロキシソリューションを悩ませる最後の問題は、プロキシがアプリケーションを終了した後、それを実際の宛先に転送する事によりスループット性能が必ずしも十分ではないという点です。

これらのいずれのネットワーク制御方法における共通の課題は、Enterprise 2.0アプリケーションを識別する機能がないこと、次にトラフィックの一部のみを検査する構造になっていること、そしてパフォーマンス面における問題を抱えていることです。

要件の定義およびRFPの策定

組織のセキュリティポリシーを作成または更新した後はいよいよ組織の要件を定義するときです。非常に高いレベルでは、検討対象のベンダに対するデューデリジェンスの実行がこれに含まれます。ソリューションを選定する可能性があるベンダについて、次に示すような質問を行う必要があります。

- そのベンダのビジョンはどのようなもので、そのビジョンをどれだけ実現しているか。
- どれくらい革新的か。
- 風土はどのようなものか。
- 開発プロセスはどのようなものか。品質保証プロセスはどのようなものか。
- 会社の規模および財務状態はどのようなものか。
- 会社は買収の対象となる可能性があるか。可能性がある場合、買収される理由として、その技術革新や独自仕様のテクノロジによる優位性をすばやく得るためか、または競合他社を壊滅させるためのどちらの可能性が高いか。
- インストール済み顧客ベースはどれくらいの大きさか。
- 自社の属する業界に他の顧客 (競合他社も含む) を持っているか。
- 顧客事例や顧客成功事例を持っているか。

次に、組織の技術的要件を定義します。幸いにも、必ずしもここで一からやり直す必要はありません。まず現在の組織のセキュリティポリシー (前のセクションを参照) を参照し、これらのポリシーを実装およびサポートするためにどのような機能が必要かを確認します。

また、ファイアウォールやネットワークセキュリティの要件の多くの例が、ほぼどこにでも存在します。実際、データ保護に関連したほとんどの法令順守要件が、情報セキュリティに関するベストプラクティスに基づいています。組織がこれらのどの規制にも従っていない場合であっても、それらのベストプラクティスをガイダンスとして使用することができます。たとえば、クレジットカードまたはデビットカードを処理しているすべての組織に適用可能な支払いカード業界データセキュリティ標準 (PCI DSS) では、いくつかのファイアウォール要件が定義されていますが、そのすべてを容易に変更して組織の正式なRFPに組み込むことができます。

RFPでは、特定の機能要件を掘り下げて、アプリケーション識別、アプリケーションポリシー制御、脅威防御、管理、ネットワーク、ハードウェアなどのいくつかの要件に対応する必要があります。

- **アプリケーション識別**。ゲートウェイでアプリケーションを正確に識別する方法、およびアプリケーションの分類に使用されるメカニズムについて説明します。
    - 識別は、IPSまたはDPIテクノロジに基づいていますか。その場合は、ネットワークトラフィックのスキャン時に精度、完全性、およびパフォーマンスの問題が発生する可能性はどれぐらいですか。
    - トラフィック分類のメカニズムは、他のベンダに対してどのように差別化されていますか。
    - 未知のアプリケーションはどのように処理されますか。
    - カスタムのアプリケーション シグネチャはサポートされますか。
    - SSLで暗号化されたトラフィックは、どのように識別、検査、および制御されますか。
    - SSL制御では、個人的なトラフィック (バンキング、ショッピング、健康状態など) とその他のトラフィックがどのように詳細に識別されますか。
    - いくつのアプリケーションが識別されますか (リストを提供します)、またアプリケーション データベースを更新するためのプロセスはどのようなものですか (たとえば、ソフトウェア更新または動的な更新)。

- 新しいアプリケーションが必要な場合、そのアプリケーションをデバイスに追加するためのプロセスはどのようなものですか。
- エンド ユーザが識別や分析のためにアプリケーションを送信したり、カスタム アプリケーションを定義したりできますか。
- その製品はURLフィルタリングをサポートしていますか。URLフィルタリングデータベースについて説明します。データベースは、そのデバイスまたは別のデバイスのどちらに存在しますか。
- 収集されたアプリケーション情報を活用できるセキュリティ機能 (ドリルダウンの詳細やユーザ可視性機能を含む) があればすべて説明またはリストアップします。

- **アプリケーション ポリシー制御**。ポリシーベースのアプリケーション制御を実装するためのプロセス、すべてのアプリケーション ポリシー制御パラメータ (ユーザ、IPアドレス、日付/時刻など)、およびそれらのパラメータの使用方法について説明します。
  - 識別されたすべてのアプリケーションに対してポリシー制御を実装できますか。
  - 特定のユーザまたはグループに対してポリシー制御を実装できますか。
  - リモートアクセス環境はどのようにサポートされますか (たとえば、Citrixやターミナルサービス)。
  - アプリケーションデータベース内のすべてのアプリケーションに対してポートベースの制御を実装できますか。
  - このソリューションで従来のファイアウォールベースのアクセス制御を実行できますか。
  - ポリシー制御を単一の管理インタフェースから行うことができますか。
  - ユーザが、ポリシーに違反するURLまたはアプリケーションにアクセスしようとしたときに警告を表示させることは出来ますか。
- **脅威防御**。不正侵入防御機能およびアンチウイルスエンジンについて説明します。
  - ブロックできる脅威の種類をリストアップします。ブロックできるファイルの種類をリストアップします。
  - データフィルタリングはサポートされますか。
  - 脅威防御エンジンは、SSLで暗号化されたトラフィックの内部をスキャンできますか。圧縮されたコンテンツファイルの検査はサポートされていますか。

- **管理**。ネットワーク上のトラフィックを明確に把握可能な管理機能と可視化ツールについて説明します。
  - デバイス管理には個別のサーバまたはデバイスが必要ですか。
  - アプリケーション ポリシー制御、ファイアウォール ポリシー制御、脅威防御機能のすべてを同じポリシー エディタから有効にできますか。
  - ネットワーク上のアプリケーション、脅威、URLの概要ビューは、どのようなツールで提供されますか。
  - ログ視覚化ツールはありますか。
  - ネットワークがどのように使用されているかを把握したり、ネットワーク使用状況の変化を強調したりするためのレポート ツールを使用できますか。
  - このソリューションのロギングおよびレポート機能について説明してください。
  - デバイスが高トラフィック負荷状態にあるときに管理アクセスがどのように保証されるかについて記述してください。
  - 何らかの集中管理ツールが使用できますか。
- **ネットワーク**。ネットワーク統合および実装機能について説明します。
  - レイヤ2またはレイヤ3機能はありますか。
  - 802.1q VLANはサポートされますか？VLAN数はどれくらいですか？
  - ダイナミック ルーティングはサポートされますか (たとえば、OSPF、BGP、RIP)？
  - QoSまたはトラフィック シェーピング機能はありますか。
  - IPv6はサポートされますか？
  - IPSec VPNはサポートされますか？SSL VPNも使えますか？
  - どのような導入オプションが使用できますか (インライン、タップ、パッシブ等)？
  - 高可用性 (HA) 機能はありますか。
- **ハードウェア**。このソリューションはソフトウェア ベース、OEMサーバ、専用のアプライアンスのどれですか？アーキテクチャについて説明します。

導入の柔軟性に関する事項

パフォーマンスと効率を最大化するようにネットワークを設計することが重要です。NGFWをネットワーク上の最適な場所に正しく導入することも同様に重要です。セグメント分けは、ネットワークの正しい設計とファイアウォールの展開におけるキー コンセプトです。ネットワークのセグメント化にはさまざまな方法がありますが、次世代ファイアウォールでは、組織がデータセンタなどネットワークの重要なセクションを分離できるように、ハードウェアとソフトウェアに関連した独特なセグメンテーション機能の組み合わせが提供されます。

機密データや重要なネットワーク インフラ (この場合もたとえば、データセンタ) の分離を目的にしたセキュリティ ゾーンの概念は、大まかに言ってネットワーク セグメントに相当します (図5-1を参照)。セキュリティ ゾーンは、物理インタフェース、VLAN、IPアドレス範囲、またはそれらの組み合わせのための論理的なコンテナ（入れ物）です。各セキュリティ ゾーンに追加されたインタフェースはレイヤ2、レイヤ3、または混合モードに設定できるため、ネットワーク トポロジを変更しなくても幅広いネットワーク環境に導入できるようになります。

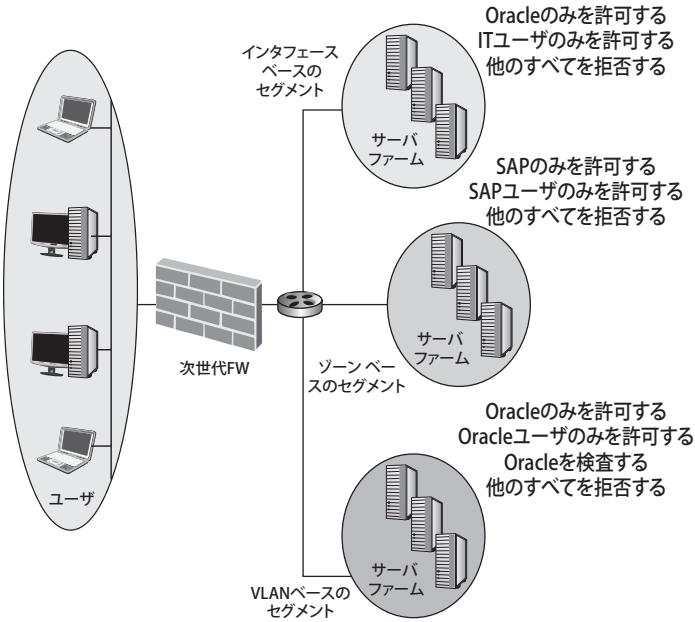


図5-1: ネットワーク セグメンテーションとセキュリティ ゾーン

ネットワークをセグメント化するためにさまざまな手法を使用できますが、セグメンテーションを機密データや重要なインフラの分離方法として見る場合は、いくつかの重要事項を考慮に入れる必要があります。

- **柔軟性**。セキュリティ目的でネットワークをセグメント化する場合は、ほとんどの企業ができれば避けたい作業である、ネットワーク アーキテクチャの変更が必要になることもあります。IPアドレス範囲、VLAN、物理インタフェース、またはそれらの組み合わせを使用してネットワークをセグメント化する機能は最も重要です。
- **ポリシー ベースのセキュリティ**。ポリシーは、IPアドレス、ポート、プロトコルだけでなく、使用しているユーザの識別や使用されているアプリケーションの識別に基づいていなければなりません。誰 (ユーザ) または何 (アプリケーションやコンテンツ) にセグメント内のアクセス権があるかを正確に認識して制御しなければ、IPアドレス、ポート、プロトコルに基づいた制御を容易に回避できるアプリケーションやユーザに機密データが公開されてしまう可能性があります。
- **パフォーマンス**。セグメンテーションとは、ビジネス上重要で、大量のトラフィックが発生することの多いネットワークで詳細なセキュリティ ポリシーを適用することを指します。つまり、セキュアなセグメントを提供するソリューションが、非常に高いセッション レートで最小レイテンシーのマルチギガビットで動作することが重要です。

モバイル ユーザおよびリモート ユーザに対応する

従来のファイアウォールでは、エンタープライズ ファイアウォールによって構築された境界を超えて、モバイル ユーザやリモート ユーザに対して可視化と制御を提供できないという技術的制限があります。この場合の次世代ファイアウォールにとっての課題は、完全に独立した一連のポリシーを管理することなく、ローカル ネットワーク上のユーザが受けるのと同程度の保護とアプリケーション使用を実現するソリューションを提供することです。また、次に示すような、この領域における現在の各ソリューションに関連した制限や欠点を回避するという課題もあります。

- **エンドポイント セキュリティ スイート**。配布方法やインストールに問題がある一方、機能がたくさんありすぎて、クライアント側のパフォーマンス、リソース要件、継続的な管理の点から見た課題が生じ得ます。
- **クラウドまたはCPEベースのプロキシ**。関連するWebサービスや製品は通常、特定のトラフィックの流れ (たとえば、ポート80/HTTPのみ) に特化しているため、サービスや対応策が制限される (たとえば、URLまたはマルウェア フィルタリングのみ) 場合があるだけでなく、プロキシ アーキテクチャに依存した誤動作を避けるために、たいていは多くのアプリケーションがフィルタを通過することを許可せざるを得ません。
- **VPNテクノロジを介した迂回中継**。IPSecベースか、SSLベースかはほとんど違いがありません。クライアント トラフィックが、VPNゲートウェイが配置されている複数のセンタ側サイトのいずれかに送り返されるため、待ち時間が増加することは避けられません。さらに大きな問題として、このトラフィックを識別およびフィルタリングするために使用されるネットワーク機器のアプリケーションの可視化と制御の能力が欠ける点があります。

これに対して、必要に応じてインストールできるクライアントを使ったソリューションは、より優れた代替手段になります。VPNベースのアプローチと同様に、リモート トラフィックはセキュアなトンネル経由で送信されます。違いは、ファイアウォールが組織のいずれかのハブ装置か、支社や支店の場所に導入されているか、またはパブリック/プライベート クラウド実装の一部として導入されているかには関係なく、最も近い次世代ファイアウォールへの接続が自動的に確立される点にあります。それによって待ち時間の影響は最小限に抑えられ、まるでユーザがリモートではなく、ローカル ネットワーク上で操作しているかのように、そのユーザのセッションが、アプリケーション、ユーザ、コンテンツ識別および検査テクノロジの全機能によって保護および制御されます。最終的には、リモート ユーザとモバイル ユーザに対して、オフィス内にいる場合と同程度のアプリケーションの実行および保護を提供する、実装しやすいソリューションが得られます。

第6章

次世代ファイアウォールのための10の評価基準

この章で学ぶこと

▶ 次世代ファイアウォールにどのような機能を求めるべきかを知る

この章では、RFPを作成した後、検討対象のベンダに求めるべきいくつかの答えについて説明します。注記: 次世代ファイアウォールの要件を定義するRFPをまだ作成していない場合は、「第5章」に戻ってください (寄り道せず、無条件に、直接「第5章」に戻ってください)。

ポートではなく、アプリケーションを識別する

ポート、プロトコル、SSL暗号化、その他の回避技術によらず、ファイアウォールによって参照された直後のアプリケーションを識別することにより、適切なポリシー制御が可能になります。

最後に、次世代ファイアウォールでは、ホストされたデータベースや「クラウド内の」データベースで発生する可能性のある待ち時間の問題を回避するために、デバイス上にできるだけ多くのアプリケーション シグネチャ ライブラリがインストールされていることが重要です。このライブラリをベンダからの新しいアプリケーション シグネチャまたはサブスクリプション サービスによって定期的に更新する必要があり、さらに必要に応じてシグネチャの更新を自動化する必要があります。

アプリケーション識別は、NGFWでのトラフィック分類の中核に位置しています。それは (すべてのポートにわたり、すべてのトラフィック上で) インテリジェントで、拡張可能、さらに広範囲に及び、しかも常に有効です。これに当てはまらない場合、それは次世代ファイアウォールではありません。

IPアドレスではなく、ユーザを識別する

エンタープライズ ディレクトリ サービス (Active Directory、LDAP、eDirectoryなど) とのシームレスな統合によって、管理者はネットワーク活動をIPアドレスだけでなく、ユーザやグループに結び付けることができます。アプリケーションおよびコンテンツ識別テクノロジとともに使用すれば、IT組織はユーザやグループの情報を、可視化、ポリシーの作成、アプリケーションに関するフォレンジック調査およびレポートに活用できます。

ユーザ識別は、特定ユーザの活動を監視および制御に役立ちます。これはかつて、きわめて簡単でしたが、企業がインターネット中心のモデルに移行するに従って困難になってきました。

従業員が世界中のほぼどこからでもネットワークにアクセスし、ユーザがゾーンからゾーンに移動するたびに内部無線ネットワークによってIPアドレスが再割り当てされ、さらにネットワーク ユーザが必ずしも企業の従業員であるとは限らない、とモバイル化が進んだことにより可視化の問題を複雑にしています。その結果、IPアドレスはもはや、ユーザの行動を監視および制御するためのメカニズムとして十分ではなくなっています。

ユーザとIPアドレスの関係を検証および保持し、ユーザを正確に識別するために、NGFWに次の機能を求めてください。

- **ログイン監視:** ユーザがドメインにログインしたときにIPアドレスをユーザやグループの情報に関連付けるために、ログイン動作が監視されます。
- **エンド ステーション ポーリング:** ユーザが、ドメインに再認証されることなくネットワーク内を移動したときにIPアドレス情報を検証して正確なマッピングを保持するために、アクティブな各PCがポーリングされます。
- **キャプティブ ポータル:** ホストがWebページ ベースの認証フォームを介してドメインの一部になっていない場合に、ユーザとIPアドレスを関連付けます。
- **導入の容易性:** 重要なインフラに影響を与えることなく、ユーザ識別を実行する必要があります。一部のソリューションでは組織内のすべてのドメイン コントローラにエージェントをインストールする必要があるため、パフォーマンスに影響を与えるだけでなく、導入を大幅に複雑にします。

パケットではなく、コンテンツを識別する

従業員が何の制約もなく好きなアプリケーションを使用し、Webアクセスしていれば、企業が脅威攻撃からネットワークを保護するのに苦労していたとしても不思議はありません。脅威攻撃に対する制御を取り戻すための最初の手順は、一般に攻撃経路として使用される望ましくない、または悪いアプリケーション活動を減らすためにアプリケーションを識別し制御することです。次に、アプリケーション使用の制御ポリシーを補完するために、コンテンツを制御するためのポリシーを実装できます。

NGFWのコンテンツ識別機能には、次のものがあります。

- **脅威防御:** 脅威の動向に対応しながら、アプリケーションの脆弱性、スパイウェア、およびウイルスがネットワークに侵入するのを防止するための革新的な機能を求めてください。このような機能の例には、リアセンブル（再構築）され、構文解析されたアプリケーション データのストリームを取得し、そのストリームを検査して特定の脅威識別子にあてはまらないかを調べるアプリケーション デコーダや、脅威の種類ごとに個別のスキャン エンジンとシグネチャを組み合わせて使用するのではなく、単一パスで広範のマルウェア (ウイルス、スパイウェア、脆弱性攻撃など) を検出しブロックするための一貫した脅威エンジンおよびシグネチャ形式が含まれます。
- **ストリーム ベースのウイルス スキャン:** この手法では、スキャンを開始するためにファイル全体がメモリにロードされるまで待つことなく、ファイルの最初のパケットを受信したらすぐにスキャンを開始します。ファイルをバッファに格納してからスキャンするのではなく、トラフィックが受信され、スキャンされて、直ちに目的の宛先に送信されるため、パフォーマンスや待ち時間の問題が最小限に抑えられます。
- **脆弱性攻撃からの保護:** 既知および未知のネットワーク層や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、サービス拒否 (DoS) 攻撃、およびポート スキャンが企業の情報リソースを危険にさらしたり、損害を与えたりするのをブロックするために複数の不正侵入防御システム (IPS) 機能を使用し、アプリケーション脆弱性の防御を有効にします。IPSのメカニズムには、次のものがあります。
    - プロトコル デコーダおよびアノマリ検知
    - ステートフル パターン マッチング
    - 統計アノマリ検知

- ヒューリスティック ベースの分析
- 無効または不正な形式のパケットのブロック
- IPデフラグメンテーションおよびTCP再構築
- カスタムの脆弱性およびスパイウェア シグネチャ

無効または不正な形式のパケットを排除するためにトラフィックが正常化される一方で、攻撃回避テクニックによらず最高の精度と保護を実現するためにTCP再構築およびIPデフラグメンテーションが実行されます。

- **URLフィルタリング:** ホストされたデータベースに関連した待ち時間の問題を削減するために、URLフィルタリング データベースは標準で装備されている必要があります。カスタマイズ機能には、カスタムURLカテゴリや、Webサイトへのアクセスを「許可」、「ブロック」、「警告してから許可」することが可能な特定のグループやユーザに対するきめ細かなポリシー作成を行う機能が含まれている必要があります。
- **ファイルおよびデータ フィルタリング:** データ フィルタリングにより、管理者は、許可されていないファイルやデータの転送に関連したリスクを軽減するポリシーを実施できるようになります。
  - **種別によるファイル ブロッキング:** ファイル種別を識別するために、ファイル拡張子のみを見るのではなくペイロード内を詳細に検査することによって、幅広い種類のファイルのやりとりを制御します。
  - **データ フィルタリング:** アプリケーション コンテンツまたは添付ファイル内のクレジット カードや社会保障番号などの機密のデータ パターンの転送を制御します。
  - **ファイル転送機能の制御:** 個々のアプリケーション内のファイル転送機能を制御することにより、アプリケーション使用を許可しながら、好ましくない受信または送信のファイル転送を防止します。

以上がすべてです。次に説明する6つの機能は、技術的な要素は少ないですが重要です。

可視化

次世代ファイアウォールにより、IT管理者は、効果的な方法で表示された実用的なデータを入手できます。特定アプリケーション、アプリケーション詳細、ユーザ、コンテンツ情報をすばやく、簡単に表示する機能はきわめて貴重です。

制御

次世代ファイアウォール ソリューションは、以下を組み合わせることで、きめ細かなアプリケーション使用の制御ポリシーを提供します。

- 許可または拒否する
- 特定のアプリケーション機能を許可し、トラフィック シェーピングを適用する
- 許可するが、スキャンする
- 暗号化解除して検査する
- 特定のユーザまたはグループを許可する

パフォーマンス

インラインのNGFWは、計算が集中する高度なネットワーク セキュリティ機能を、待ち時間をほとんどまたはまったく発生させることなく、リアルタイムに実行する必要があります。次世代ファイアウォールは、専用プラットフォーム上の機能に固有の高速プロセッサを使用して、マルチギガビットのトラフィック フローを処理できる必要があります。管理とパケット処理の可用性を実現するために、マネジメント プレーンとコントロール プレーンが分離されていることが理想です。

柔軟性

ネットワークの柔軟性は、ほとんどすべての組織のコンピューティング環境との互換性を保つのに役立ちます。再設計や再構成を行わなくても実装できるかどうかは、次に示すような、広範囲のネットワーク機能およびオプションをサポートしているかどうかに依存します。

- 802.1qおよびポート ベースのVLAN
- トランク ポート
- トランスペアレント モード
- ダイナミック ルーティング プロトコル (OSPFやBGPなど)
- IPv6のサポート

- IPSecおよびSSL VPNのサポート
- 数多くのインタフェースおよび複数の混合モード (タップ、レイヤ1、レイヤ2、レイヤ3など)

信頼性

サービス停止を伴わずに運用するために、次に示すような信頼性に関する機能が必要になります。

- アクティブ/パッシブまたはアクティブ/アクティブによる冗長化 (あるいはその両方)
- ステート情報および設定情報の同期
- ハードウェアパーツの冗長化 (電源冗長など)

拡張性

拡張性は主に、堅牢な管理機能 (デバイスとポリシーの集中管理およびデバイス間の同期を含む) と高性能なハードウェアを備えているかどうかに依存しますが、1つの物理的なファイアウォールを多数のファイアウォールとして機能するように設定できる仮想システムのサポートによっても促進されます。

管理性

管理性は、次世代ファイアウォールに求めるべき重要な特性です。管理や保守が難しすぎる複雑なソリューションは、結果的に効率を下げるだけでなく、間違った (かつ安全でない) 設定が行われる恐れさえあります。重要な管理機能には、次のものがあります。

- ローカルおよびリモート管理
- 集中管理
- 役割ベースでの管理権限の委譲
- シグネチャの自動更新
- デバイス ステータスやセキュリティ イベントのリアルタイムの監視
- 堅牢なロギングおよびカスタマイズ可能なレポート

用語集

Ares: Ares Galaxyは、Delphiで記述された、Microsoft Windows向けのオープン ソースのP2Pファイル共有プログラムです。このソフトウェアの支持者は、迅速なダウンロードが可能で、他のファイル共有プログラムより適切で完全な検索機能を備えているうえ、接続が速いと主張しています。

AV: Anti-Virus (アンチウイルス)。

BearShare: BearShareは、P2Pファイル共有アプリケーションです。

BGP: Border Gateway Protocol (境界ゲートウェイ プロトコル)。ルーティングプロトコルの一種です。

BitTorrent: BitTorrentは、配布者にハードウェア、ホスティング、および帯域幅リソースのコストを負わせることなく、大量のデータを広範に配布するP2Pファイル共有通信プロトコルです。代わりに、各ユーザがより新しい受信者にデータの各部分を提供するため、特定の個々の発信者にかかるコストと負荷が軽減されます。

Boface: Bofaceは、マルウェアをコンピュータにダウンロードおよびインストールした後、Facebookユーザをだまして偽のアンチウイルス プログラムを購入させるワームです。

CPE: Customer-Premises Equipment (顧客敷地内の装置) または Customer-Provided Equipment (顧客によって提供された装置)。

eMule: eMuleは、クライアント ノード間のソースの直接交換、ダウンロード失敗時の迅速な回復、および頻繁にアップロードするユーザへの優先システム等を特徴とするP2Pファイル共有アプリケーションです。帯域幅を節約するためにzlib圧縮形式でデータを転送します。

FastTrack: FastTrackはP2Pプロトコルです。

Fbaction: Fbactionは、Facebookユーザを狙ったフィッシング攻撃です。

FINRA: Financial Industry Regulatory Authority (金融取引業規制機構)。

FTP: File Transfer Protocol (ファイル転送プロトコル)。

Gbridge: Gbridgeは、Google Gtalkインスタント メッセージング セッションの内部にVPNトンネルを確立します (GbridgeはGoogleアプリケーションではありません)。それにより、Gbridgeユーザは、同じGtalkユーザ アカウントの下でログインしている複数のPCに接続できるようになります。

Gnutella: Gnutellaは、2005年12月の時点では世界で3番目に普及しているインターネット ファイル共有ネットワークでした。Gnutellaの一般的なクライアントには、Limewire、Morpheus、およびBearShareがあります。

Gpass: Gpassは、インターネットの検閲をくぐり抜けるために中国で広範に使用されているインターネット アンチジャミング製品です。セキュアなインターネット アクセス メカニズムを提供することによって、ユーザのプライバシーとオンラインの安全性を効果的に保護します。

HA: Highly Available (可用性が高い) またはHigh Availability (高可用性)。

HIPAA: Health Insurance Portability and Accountability Act (医療保険の相互運用性と説明責任に関する法律)。

HTTP: Hypertext Transfer Protocol (ハイパーテキスト転送プロトコル)。

HTTPS: Hypertext Transfer Protocol over SSL/TLS (SSL/TLS経由のハイパーテキスト転送プロトコル)。

IM: Instant Messenger (インスタント メッセンジャー)。

IPSec: IPSec (Internet Protocol Security: インターネット プロトコル セキュリティ) は、認証と暗号化を使用してIPネットワーク経由の通信を保護するためのプロトコル スイートです。

Kazaa: Kazaaは、FastTrackプロトコルを使用するP2Pファイル共有アプリケーションです。

Koobface: Koobfaceは、FacebookユーザをだましてAdobe Flash Playerの偽の更新をダウンロードおよびインストールさせるワームです。特に、Koobfaceは、感染したPCからクレジット カード番号などの機密情報を収集しようとします。

LDAP: Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル)。

Limewire: Limewireは、オープン ソースのP2Pアプリケーションです。

Mariposa: Mariposaは、「Butterfly Bot」と呼ばれるコンピュータ ウイルスで構築されたボットネットであり、全世界の800 ～ 1,200万のPCを感染させたと推測されています。Mariposaボットネットは、Webサイトや金融機関のパスワードを盗み、サービス拒否攻撃を仕掛け、さらにはウイルスを拡散させます。

Mediafire: Mediafireは、無料で、無制限のファイルおよびイメージ ホスティングWebサイトです。このサービスは無料で使用でき、ユーザは最大100MBのファイルをアップロードできます。

Morpheus: MorpheusはP2Pアプリケーションです。

MS-RPC: Microsoft Remote Procedure Callは、Microsoft Windowsネットワーク上で使用される通信プロトコルです。

Orkut: Googleが所有し、運営しているソーシャル ネットワーキング サイト。

OSI: Open Systems Interconnection (開放型システム間相互接続) モデル。ネットワークのための7層の参照モデル。各層は、物理、データリンク、ネットワーク、トランスポート、セッション、プレゼンテーション、およびアプリケーションです。

OSPF: Open Shortest Path First (オープン ショーテスト パス ファースト)。ルーティングプロトコルの一種です。

P2P: Peer-to-Peer (ピアツーピア)。

PCI DSS: Payment Card Industry Data Security Standard (クレジットカード業界のデータセキュリティに関する標準)。

QoS: Quality of Service (サービスの品質)。

RIP: Routing Information Protocol (ルーティング情報プロトコル)。

Skype: Skypeは、ユーザがインターネット経由で電話をかけることができるようにするアプリケーションです。追加機能に、インスタントメッセージング、ファイル転送、およびビデオ会議があります。

SMB: SMB (Server Message Block: サーバ メッセージ ブロック) は、CIFS (Common Internet File System: 共通インターネット ファイル システム) とも呼ばれるアプリケーション層プロトコルです。

SMTP: Simple Mail Transfer Protocol (簡易メール転送プロトコル)。

SSH: Secure Shellは、ローカル コンピュータとリモート コンピュータの間にセキュアなチャネルを確立できるようにするための一連の標準および関連するネットワーク プロトコルです。

SSL/TLS: Secure Sockets Layer/Transport Layer Security (セキュアソケット層/トランスポート層セキュリティ)。インターネット上のクライアントとサーバの間のセキュアな通信のためのセッションベースの暗号化および認証アルゴリズムを提供するトランスポート層プロトコル。

Stateful inspection: 動的パケット フィルタリングとも呼ばれます。送信接続への受信応答を動的に許可するために、ファイアウォールを通過するアクティブな接続のステータスを保持します。

TCP: Transmission Control Protocol (伝送制御プロトコル)。

Teamviewer: Teamviewerは、インターネットを経由したPCのリモート制御を可能にすることにより、ユーザがインターネット上の任意の場所にあるコンピュータを (ファイアウォールを通り抜けて) 制御できるようにします。

UDP: User Datagram Protocol (ユーザ データグラム プロトコル)。

UltraSurf: UltraSurfは、ユーザが任意のWebサイトを自由に参照できるようにする完全な透明性と高レベルの暗号化を備えたプロキシを実装します。インターネット検閲が行われている国でよく使用されています。

URL: Uniform Resource Locator (ユニフォーム リソース ロケータ)。

VLAN: Virtual Local Area Network (仮想ローカル エリア ネットワーク)。

VoIP: Voice over Internet Protocol (ボイス オーバー インターネット プロトコル)。

VPN: Virtual Private Network (仮想プライベート ネットワーク)。

zlib: zlibは、データ圧縮に使用されるソフトウェア ライブラリです。

paloalto NETWORKS

the network security company™

ガートナー
2010 マジック
クアドラントで
エンタープライズ
ファイアウォール
“ビジョナリー”
の格付けを獲得

たった1つのファイアウォールで ネットワーク セキュリティを作り変える

アプリケーションと脅威は劇的に進化

あなたのセキュリティ インフラは進化していますか？

あなたのネットワークに必要なものがここにある

Palo Alto Networksは、アプリケーションとおよびリスク分析レポート［AVRレポート］によって、これまでのファイアウォールを通り抜けていた通信を正確に示すことができます。AVRレポートは、各種のアプリケーションとそれらの使用方法、相対的なセキュリティ上のリスクを考慮に入れながら、ネットワークを通過するアプリケーション通信の分析とそれに基づくビジネス リスクの評価を提供する、分析レポートです。

あなたのネットワーク上での実際の分析ならびに無料のAVRレポート提供をご希望される場合はこちら
www.paloaltonetworks.jp/AVR

Network Security

www.paloaltonetworks.jp