



人任せにしない IT 管理者のための Fireware®XTM とその実用的な利点

2009 年 7 月

はじめに: その真偽は?

「ファイアウォールは日用品、様々なモデルがあるが、どれも似通ったものである。」

IT の世界では、そんな意見が社会通念として受け入れられている。そして、もっとも一般的な意味においてファイアウォールというものは、どのトラフィックを許可したり拒否するか取り決めているリストに受信および送信するデータ・パケットを照らし合わせ確認するという、基本的なタスクをする点では同じであると言える。しかし、ファイアウォールの中には他よりも優れているものもあり、設定しやすいもの、デザインの良いものなど色々ある。

「その作用はほぼ同じだからファイアウォールは全部同じ」という考えは、実社会における経験の上ではあてはまらない。同じ論理を使えば、自動車は運転手を移動させるものという点でほぼ同じであるから、1988 年製のジオ・プリズムと 2010 年製のメルセデス E クラス・セダンには大した違いがないとすることができる。しかし、そうした自動車を実際に運転したことがあれば、その操作から人間工学さらには外観など、どの面においても 2 つの車種には雲泥の差があることを知っているはずだ。

このホワイトペーパーは、様々なネットワーク・セキュリティ・アプライアンスのメリットを比較中の IT プロに向けたものだ。過去にファイアウォールが単なる日用品であったとしても、現在においては決してそうではない。統合脅威管理(UTM)デバイスの時代において、ファイアウォールを取り入れるということは、いくつものサイドを持つネットワーク境界線に施す防衛アプライアンスの 1 つであるだけだ。ここでは WatchGuard® Fireware®XTM アプライアンスを実際に使った場合の比較に焦点をあてる。

比較の上で、リスク管理や各種規格など漠然とした問題や自社が好むブランドに関わる政治的な意味合いはとりあえず視野から外すことにし、ファイアウォールはすべて基本的なレベルのセキュリティを提供するという事実を受け入れることにする。ここでは人任せにせず、自分で実際に設定しデバイスを使用しているプロの IT の視点から、ネットワーク・ファイアウォールを見てみることにする。WatchGuard Firebox®X や Fireware XTM 1050 アプライアンスは、管理者に対して単なる日用品という点から抜け出ることができるのだろうか？

WatchGuard ではそれを実現している。そこで、このホワイトペーパーでは Fireware XTM オペレーティング・システムを実行する WatchGuard のセキュリティ・アプライアンスが、いかにして単なる日用品の粋を超えたセキュリティを提供できるのか見てみることにしよう：

- ・ 特に注意せずに許可している暗号化トラフィックを検査しネットワークを強化
- ・ 他社が提供していないボイス・オーバー・インターネット・プロトコル (VoIP) にセキュリティを追加
- ・ 強力なレポートと柔軟性、使いやすい管理ツールを通じて、ネットワークに優れた可視性を提供

セキュリティ・アプライアンスの中にはエンジニアリング色の強いものもあり、不可解なユーザ・インターフェイスを理解するには自分自身もエンジニアでなければ分からないようなものもある。その一方で、WatchGuard は先駆的な考えを持つエンジニア達により、IT 管理者達が本当に何が必要なのかを注意深く考慮するところから始まった。ファイアウォールはすべて似たようなものなのか、それとも Fireware XTM を実行するセキュリティ・アプライアンスは、もしかするとネットワーク・セキュリティのメルセデス E クラスなのかもしれないと思うようになるのか……先を読み進めてほしい。

不透明だったものを見抜く力： HTTPS 検査

大方のネットワーク管理者は HTTPS のような暗号化されたウェブ・トラフィックを許可し、ネットワーク境界線にある防衛を通過できるようにしている。暗号化とは、そうしたストリームを読み取り不可能なテキストにして寄せ集めた状態にしているため、その HTTPS 接続が必要な情報を携えているのか、それとも悪質なコードを含んでいるのか管理者はすぐに知ることができない。そうした内密な面を持ちながら許可されているアクセスと組み合わせられている点が、攻撃者にとって暗号化されたウェブ・トラフィックを魅力的なものにしている理由なのである。

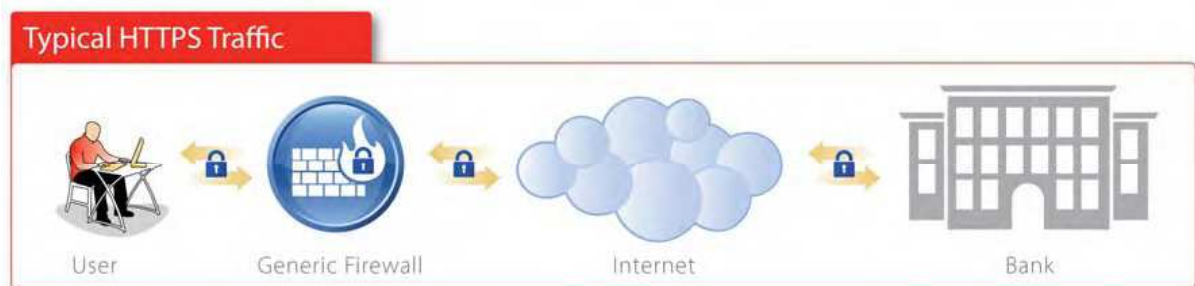


図 1： 普通のファイアウォールの内側にいるユーザが、HTTPS ウェブサイトから暗号化されたデータをリクエストする。その安全性にかかわらず、データは完全に暗号化された状態で戻される。普通のファイアウォールはこのトラフィックを解読しないため、データはそのペイロードにかかわらずネットワークに入ることができる。

4 年前においては、HTTPS に内在する証明書システムを操作するような高度のプログラミング技術を備えた攻撃者はあまりいなかったが、最近の攻撃者はそのハードルを越えている。HTTPS の乱用率は急速に上昇し、ウェブ暗号を利用した詐欺、侵害、犯罪行為に関するニュースは毎週のごとく報告されているほどになった。

犯罪者によって HTTPS が利用されたケースとしては、次のようなものがある：

- ・ 2008 年の後半に見られたフィッシング詐欺行為をまとめた Anti-Phishing Work Group (APWG) の報告によると、フィッシング詐欺者が最初から設定したフィッシング詐欺用サイトはそれほどなく、その代わりに 81% のフィッシング詐欺サイトは詐欺者によって侵害を受けた正当なウェブサイトだったという。

フィッシング詐欺者は、偽装したサイトに SSL 証明書を定期的に追加している。詐欺者が偽装したサイトを立ち上

げ、そのサイトに訪れるユーザが主流ブランドのサイトに来ていると思わせるような昔の方法は、今ではもうあまり使われていないと APWG は報告している。最近の詐欺者は分りやすく、極めて価値がありそうな(例: 安価な薬など)物を提供し、あまり知られてはいないが正当なビジネスを営んでいるように見えるフィッシング・サイトにユーザを誘導するようになっているという。HTTPS を介したコミュニケーションは、消費者の安全性を考慮しているように見えるため、悪質なサイトが正当な E コマース業者であるように見せかけている。その場合、攻撃者はソーシャル・エンジニアリングのテクニックとして、まず HTTPS を使い消費者の信頼を築く。そして騙されやすいユーザがクリックし支払いに必要な情報を提供した時点では、使える情報をすでに収穫している。そして、そこでやめる必要はどこにもなく、最近の攻撃者はそのユーザとのネットワーク接続を確立し、HTTPS が攻撃者の次の行動をすべて隠してしまうようになる。そして、安全で暗号化済みの接続を介し、攻撃者は Java 悪用のドライブバイ・ダウンロードを被害者に送信することができるようになる。

- ・ **Gheg という名のポットネット**(ゲグはアルバニア語の方言)は、主にスパムポットとして機能する。テンプレートベースのエンジンは、1 時間/1 ポットにあたり 7,000 件のメールを生成し送信することができる。通常、スパムポットがユーザのネットワークを感染させた場合、イグレス・フィルタを使ってポート 25 アウトバウンドをブロックすればスパミングを止めることができる(LAN にあるクライアントの大方はポート 25 なので、すべての IP アドレスにトラフィックを送信する必要はなく、メール・サーバにアクセスできればよしとするクライアントが大方だ)。とはいえ、Gheg がネットワークにあるクライアントを感染させた場合は、被害者のメール・サーバを使ってスパムを送信し、イグレス・フィルタリングを回避できる。Gheg ポットは暗号化されたポート 443(HTTPS)を使ってクライアントのコマンドやコントロール・サーバとコミュニケーションを取るようになる。

- ・ Cimbot もまた、密かに動くポットネット分野に踏み出しているスパムポットだ。スパムポット自体はユーザのディスク・ドライブで暗号化されたファイルとして保管される。大方のポット・クライアントのように自己実行をする代わりに、この種のポットは、ポットマスターからの指示が出た場合にのみ、自身を解読するようになっている。そして、よくある Windows プロセスとして実行するのではなく、システム・メモリにおいてのみ実行するためコンピュータでそれを検知することが難しい。Cimbot はポート 80(HTTP)と暗号化されたポート 443(HTTPS)でコマンドを受信することができる。

つまり、ネットワーク管理者であるならば、ネットワークに接続する HTTPS には害がないと信じることはもうできなくなっているのである。最近のネットワーク防衛は暗号化の中で何が起きているのかを見抜けなければならない。

WatchGuard HTTPS の検査が使えない理由

急成長している脅威に対応するため、WatchGuard は Fireware XTM オペレーティング・システムが HTTPS トラフィックを検査できるように構築した。Fireware XTM HTTPS 検査は受信トラフィックと送信トラフィックの両方で作用し、パケット・ヘッダーだけでなくペイロード(本文の内容)も検査することができる。

Fireware XTM は、これまで不透明だった脅威をなぜ見ることができるのだろうか?と疑問に思うかもしれない。しかし、それを説明するには、まず暗号化されたウェブ・トラフィックを使用している 2 つの状況について見てみることにしよう。

- ・ ファイアウォールの内側のトラステッド・ネットワークにいるユーザが、インターネット上の任意選択による HTTPS ウェブサイトに接続しようとする動きを Outbound(アウトバウンド/送信)トラフィックという。

- ・ インターネットに繋がっている誰かがユーザの HTTPS サーバに接続(およびランダムなデータをインプット)したいとする動きを Inbound(インバウンド/受信)トラフィックという。

状況 1: トラステッド・ユーザのアウトバウンド接続

XTM HTTPS 検査は、WatchGuard の定評あるセキュリティ・プロキシ技術を拡張させたものである。従って、WatchGuard XTM アプライアンスは送受信の接続を確立し、暗号化する両者の間に立っている(プロキシ)。これはどちらの方向においてもコミュニケーションを傍受、解釈、検査し、セキュリティやネットワーキングの理論に基づいて反応するようになっている。このためユーザのマシンの視点から見ると WatchGuard XTM アプライアンスは、ウェブ・サーバのようであり、ウェブ・サーバの視点からすれば WatchGuard XTM アプライアンスは、リクエストを送信するクライアントのように見えるのである。

通常であればネットワークの境界線デバイスが、暗号化された接続を読み取ることはできないはずなのに、なぜそれが可能なのか？と疑問に思うかもしれない。WatchGuard ソフトウェアは、ユーザの WatchGuard XTM アプライアンス独自に関する暗号化キー証明書を生成するようになっている(シリアル番号やユーザ・インプット、その他のパラメーターに基く)。アプライアンスはこのデジタル証明書をクライアントにエクスポートし、クライアントはそれをウェブ・ブラウザにインポートする。この証明書はユーザが自分で生成し、エクスポートしたものであるため、自分の証明機関(CA)として使うことができる。つまり、自分の身元を認証するのだから疑いを持つこともないわけだ。こういった点から、エクスポートされた証明書は通常のパブリック SSL 証明書よりも信用できるものになる。「trusted anchor」つまり、頼りになるものを意味するそのステータスは、HTTPS サイトに行く場合 XTM アプライアンスがユーザに代行して対応することを、ユーザが信頼できるようにしている。

セキュリティの追加措置として、XTM アプライアンスにはリモート・サーバが見掛け通りのものであるかどうか確認するリモート証明書がある。例えば、あるユーザが当座預金口座の残額を見ようとしているとする。ユーザはブラウザを使って「bank.com」に行き、サイトのセキュア・サーバにログインする。すると、XTM アプライアンスはユーザとサイトの間に立つようになる。その際、「bank.com」の視点からは、XTM アプライアンスがリクエストを出しているクライアントに見え、「bank.com」のセキュア・ウェブ・サーバは、ユーザがリクエストした情報を送信すると、XTM アプライアンスは「bank.com」と独自の接続を確立して「bank.com」のトラフィックを解釈する。次に「trusted anchor」証明書からの暗号キーを使い、そのトラフィックを再び暗号化する。そしてユーザはそれを疑うことなく信頼し、ユーザのブラウザが XTM セキュリティ・アプライアンスの HTTPS レスポンスを解釈し検査する。

HTTP プロキシのセキュリティ・ロジックがデータをスキャンし、必要なセキュリティ機能を実行できるように、トラフィックはファイアウォール内で解釈化され、ボックスを出る前に再びデータは暗号化される。HTTPS がファイアウォールの内側で解釈された短時間において、それは HTTP になる。つまり、暗号化されたチャンネルは暗号化していないチャンネルと同じレベルのセキュリティを楽しめるといったように、それには様々な意味合いがある。Fireware XTM を設定し、その HTTPS をいくらでも掘り下げて検査することができ、セキュリティ・ニーズとパフォーマンスの要望におけるバランスを取ることが可能になる。様々な特徴をフィルターしたりブロックすることで、WatchGuard HTTP プロキシにトラフィックを渡すことさえできる(例:特徴とはつまり、プロトコル基準の厳密な解釈に基くもの、文字列に基くもの、正規表現に基くもの、.EXE を含む URL を拒否する、その他など)。

XTM は HTTPS トラフィックを検査した後、クリーン・トラフィックを再び暗号化し、そのデータをネットワーク上の最終目的宛先に送る。その質が劣る検査技術とは異なり、Fireware XTM は HTTPS パケットでフル・セキュリティ・スクリーニングとロジックを提供しているが、人の目には入らないようになっている。先の例では、ユーザの金融データはユーザと銀行の間の機密情報として維持されるが、フィルターを掛けているものは HTTPS ストリームには入っていなかったと自信を持つことができる。

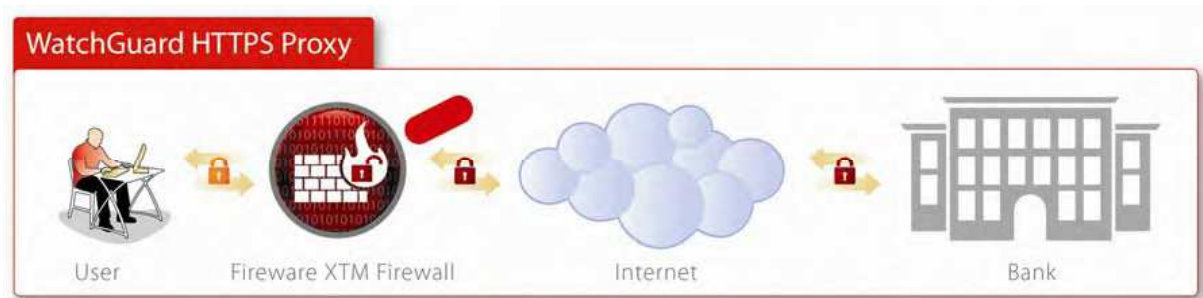


図 2: WatchGuard Firewall XTM ファイアウォールの内側にいるユーザが、暗号化されたデータを受取るために図 1 と同様のリクエストを出すと、ファイアウォールはその HTTPS トラフィックを解読し通常の HTTP にすることができます。その後、異常がないか調べデータを再び暗号化してからユーザに送る。ユーザのコミュニケーションは内密のままでありながら、ネットワークは暗号化されたセキュリティ脅威からネットワークを保護するレイヤーを追加することができる。

状況 2: 外部ユーザのインバウンド接続

自分のウェブ・サーバを暗号化し実行している場合、HTTPS 検査は不可欠なセキュリティ・レイヤーを提供することができます。E コマース用に自分の暗号化したウェブ・サーバを使用している場合、ウェブ・フォームでメール・アドレスや電話番号を記入するようにリクエストしていても、インターネットにいる攻撃者は様々な形で悪質なコードを送ってくる可能性がある。Verizon 社の侵入対応チームの報告によると、信頼しているビジネス・パートナーからの接続用に暗号化したサーバを維持している場合を見た場合、侵入されたパートナーを介してネットワークに入り込んでくる確率は全体の 3 分の 1 (32%) だという。

攻撃者は、そのサイトで登録し予期されている正当なトラフィックで埋められているチャンネルを介して接続を確立するため、どちらにせよ、このような攻撃は特定の毒々しさを持っている。そして、それは防衛策で対抗するチャンスもない間に行われてしまうのである。そうした点からも HTTPS トラフィックをより注意深く検査すべきであることがわかる。

「アウトバウンド」の状況と同様に「インバウンド」においても、WatchGuard XTM アプライアンスは接続する両者の間に立つようになっている。しかし、この状況において WatchGuard ソフトウェアは、トラフィックを解読するために使う暗号化キー証明書を生成しない。だが、このケースにおいては、内部のウェブ・サーバにすでにプライベート SSL 証明書があるので、ウェブ・サーバから証明書をエクスポートし WatchGuard XTM アプライアンスにインポートされる。次に、XTM デバイスはユーザのウェブ・サーバに代行してそれに応答し、解読、検査が済みクリーンであることが分っているトラフィックのみを送信することになる。

検査することが不可能な HTTPS を HTTP にすることは、非常に多くの面で報われると言えるだろう。ビジネス・パートナーから来たトラフィックが暗号化されていれば、それが予期していなかった、もしくは未認証の HTTP 方法で来た場合でも(例えばパートナーが OPTIONS/PUT/DELETE のようなコマンドを送信してくることはないと思っていった場合など)、それはネットワークに入って来ることができるだろう。しかし、それを暗号化されていないトラフィックとして自動的にブロックすることも可能だ。また、ユーザ・フォーラムなどでカスタマーがイメージを掲載できる場所を提供している場合に、攻撃者が実行可能なバイナリーをアップロードしようとすることもあるかもしれない。WatchGuard XTM HTTPS による検査なしには、そのような攻撃を阻止することはできないが HTTPS 検査ができれば許可していないトラフィックを阻止し、接続を切断させることが可能になる。

HTTPS 検査: 重要点

WatchGuard の革新的な HTTPS 検査は、不透明で暗号化された接続を明白なものにすることで、長年の問題を解決している。現在出回っているセキュリティ・アプライアンスの中でも、それができるのはごく僅かである。現時点で我々の知るところでは、HTTPS 検査を提供する数少ないベンダーでさえ、WatchGuard Firewall XTM ができるような HTTPS パケット・ペイロード全体を完全に検査できる機能は提供していない。我々の競争相手である企業には HTTPS の解読ができるところもあるが、その検査の後にそれを再び暗号化することまではしていない。ユーザを念頭に置き構築された WatchGuard のセキュリティ・アプライアンスは良質なセキュリティを提供している。

「これで pwn を仕掛けられるか？」 VoIP セキュリティ

Telecommunications Industry Association(TIA)によると、2005年から2006年の間で住宅地域におけるIP電話の利用者数は三倍にもなったという。そして2006年から2007年においては、米国内の地域においてIP電話の採用率は2倍だったそうだ。2007年には米国家庭の10%がIP電話を所持しており、軌跡予測によると2009年にはそのユーザ数は1800万人を超えるだろうと予想されている。

急速に拡張しているように見えるが、米国以外におけるIP電話の利用率はそれよりも速い。米国の家庭においてIP電話の利用率が10%に達した時点で、フランスの家庭ではその数が40%だった。中国ではPublic Switched Telephone Network (PSTN - 公衆電話交換回線網)を使った電話数をIP電話の利用者数が上回っているという。

世界的に見て爆発的なIP電話の利用にもかかわらず、IP電話技術にかかわるセキュリティ問題はまだ的確に解決されていない。

IP電話のセキュリティが、いま必要な理由

「セキュリティと複雑性は反比例している」とは、以前からセキュリティ業界で言われている格言だ。つまりプロセスがより複雑になればなるほど、間違いや欠陥そして安全性が欠ける確率は上昇するというのだ。そしてVoIPの基本的操作には次の点が必要であるため、そういった原理はVoIPにとって利点にはならない。

- ・ アナログ・ボイスをデジタル・シグナルに変換する
- ・ デジタル・シグナルをインターネットが送信できるパケットに圧縮する
- ・ 受信側でそのパケットを聞き取れる声として再構築する
- ・ 電話番号をIPアドレスに変換する(その逆も同じ)
- ・ 電話システムにそのユーザがどこにいるのか知らせる

端的に言えば、VoIPを導入するということはネットワークで様々なコーデック、プロトコル、トランスポート方法などを取り入れることを意味する。複雑性がセキュリティを促進するものでなければ、VoIPが悪質なハッカー達に攻撃先を十分さらしてしまうことになるわけだ。

「VoIPは攻撃者が好む状態を提供してしまうがFireware XTMで対策を講じることができる」

VoIPとネットワーク・セキュリティは常に「反比例する」といった関係にあった。管理者がセッション・イニシエーション・プロトコル(SIP)やH.323を実施しようとした際、プロトコルは既知のスタンダード・ポートで接続を始めながら他のポートを必要に応じて動的に開こうとしていたため、ファイアウォールはVoIP接続を解除してしまっていた。そしてセキュリティ・ベンダーが、ダイナミック・ポートを一時的に開けるようにしたり、セッションが終了した場合その跡を残さずに閉じることができる特別なサービスを作成するには、しばらくかかった。今では多くのセキュリティ・ベンダーが「VoIPサポート!」と言っているが、高度な方法でVoIPを安全にしているからではなく、VoIP接続を解除しなくなったという意味だけで使っているわけで、それはVoIPセキュリティとは意味が違う。

2007年、Ciscoは統合IP電話でのリアルタイム・トランスポート・プロトコル(RTP)の実装にバグがあることを認め

セキュリティ・レスポンスを出し、大きくニュースで取り上げられたことがある。そのバグは、リモート攻撃者が IP 電話を傍聴できるようにするものだったが、その半年後にセキュリティ・ベンダーの VoIPShield は Cisco、Avaya、Nortel VoIP の製品において 100 件以上のセキュリティ問題を見つけたことを発表した。

2006 年以降、攻撃者がコーデック欠陥を悪用する確率が上昇している。その使用にあたり、コンピュータが解凍しなければならないファイルに悪質なコードを挿入することで、これまで害がないと思われてきたファイル形式 (QuickTime .MOV や Windows Media Player .WMP、.WAV など) を使って被害者のコンピュータでマルウェアを実行できることを攻撃者達が知った。

攻撃者はコーデック欠陥を悪用することを好む傾向があるため、VoIP は攻撃者が喜ぶ状況を提供していることになる。VoIP はオーディオ、ビデオ、ファックス、テキストを組み合わせ、様々なコーデック・オプションをそのような技術に提供するようになってきている。例えばオーディオについて見てみよう。ステレオ・サウンドや音質が必要なユーザなどは、大きめのパケットになるコーデックを好む場合もある。バンド幅を気にしているユーザであれば、ビットレートが平均して低い小さいパケットを作成するコーデックを好む者もいるが、処理にかかる負担は大きい。そうした理由から、一般的な利用状態において VoIP オーディオには少なくとも 8 つのコーデックがある。

このため VoIP 機能を楽しむには、VoIP を使用する上で実行しなければならない形式で、他人からの無規制 IP トラフィックを受け入れなければならないはず、LAN にある従来のデータ・パケットと混在することになる。明らかに VoIP 技術はネットワークへのリスクを拡大しているのだ。

WatchGuard の視点から見れば、攻撃者が電話や電話会議を傍聴できることはもちろんだが VoIP の問題はそれよりもひどいものである。なぜなら、VoIP はユーザの IP ネットワークと混ざり合い、そのもっとも深刻な脅威において、VoIP のセキュリティ問題はユーザのネットワーク・データすべてへの足掛かりとなるからだ。

しかし、Fireware XTM で対策を講じることができる。

WatchGuard の VoIP セキュリティの仕組み

Fireware XTM にはスタンダードでアプリケーション・レイヤー・ゲートウェイが含まれている。これは H.323 やセッション・イニシエーション・プロトコル (SIP) といったような VoIP 関連のプロトコルを遮断し検査するようになっており、ゲートウェイ・セキュリティ・プロキシは VoIP にまつわるリスクを減少させている。

ファイアウォールは単なる日用品であると思っているならば、他のセキュリティ・ベンダーに VoIP セキュリティと呼ばれているサービスが次の機能を提供しているか、聞いてみるといいだろう。ちなみに、これらは WatchGuard XTM アプライアンスではスタンダード機能として取り入れられているものである。

セキュア・コール・セットアップ

H.323 プロトコル・スイートは 5 つのオーディオ・コーデックをサポートしている：

- ・ G.711
- ・ G.722
- ・ G.723.1
- ・ G.728
- ・ G.729

実際のところ、5 つすべてを使う管理者はあまりいない。現実的には G.711 や G.729 といった、もっとも一般的なコーデック 2 つだけを使うのが主だろう。XTM VoIP セキュリティは、使用していないコーデックで圧縮されている接続リクエストを拒否することができる。特定のコーデック接続を拒否することで、ネットワークはそうしたコーデック

にあるセキュリティ・ホールを悪用する攻撃や、まだ開発されていない攻撃に対しても脆弱ではなくなる。

アプリケーション・レイヤー・ゲートウェイは、ホワइटリストからのコールも許可できるようにする。おそらく使用している VoIP のインプリメンテーションは、ユーザとビジネス・パートナーの利用のためにあるもので、世界中の誰もが使えるようにしているわけではないだろう。その環境で利用者に制限を掛ければ、未認証の電話番号や認証していない IP アドレスからの電話を XTM VoIP が拒否するように設定することができる。

トポロジーを安全に

VoIP の機能やレスポンスの中には、ユーザがどの VoIP ギアを使っているのか、そしてどのバージョンのソフトを使っているのかなどを示すデータを表示するものもある(どのサーバ・ソフトウェアがそのウェブ・ページをホストしているのか、ウェブ・ページ・エラーで詳細情報を暴露してしまうケースと似ている)。Fireware XTM では、チェックボックスをマークするだけでユーザのネットワーク・トポロジーを隠せるようになっている。同様に SIP や H.323 置換がユーザ・エージェント・ヘッダーで明らかになってしまうこともあり、それはハッカーにとって有益な情報となる。WatchGuard の VoIP セキュリティ機能は、ユーザの任意でヘッダーに入れる文字列を決めることができ、攻撃者に情報を明らかにしない、または(そう望むのであれば)攻撃者を欺くこともできる。VoIP レスポンスがユーザのシステムを公開しなかったり、別のシステムのように見せかけることがなければ、チャンスに便乗しようとしているハッカーは真実を分析する気も起こらず、もっと狙いやすいターゲットに移ることだろう。

VoIP に関する攻撃はディレクトリ獲得に関与するものもあり、攻撃者はユーザの VoIP データベースやソフト・スイッチにある電話番号やアドレスをすべて掻き集めようとする。WatchGuard VoIP セキュリティは、何かが SIP REGISTER コマンドを送信すると開始するようになっている。そうすると、アプリケーション・レイヤー・ゲートウェイは追加検査を行い、ディレクトリ獲得を阻止する。そんなオプションを探してオンにする時間も惜しいという管理者のために、WatchGuard ではこのセキュリティ機能をデフォルト設定にしている。

バンド幅を確保

WatchGuard XTM VoIP セキュリティ機能では、スループットでアドバンテージを取り、効率的にリソースを使うこともできる。

特定のコーデックで圧縮されているコールを拒否できることから、ユーザはもっとも効率的なコーデックをスタンダードにすることができ、望むのであればバンド幅を取りすぎるコールを拒否することもできる。

XTM のアプリケーション・レイヤー・ゲートウェイは、アイドル・タイムアウトも強制することができる。既存のメディア接続の動きがない間に(ユーザが規定する期間)送信するデータがない場合、その接続を自動終了させることができ、その分ネットワーク・リソースを解放させることが可能になる。

電話関連の攻撃例としては、1 分間の料金が市外局番に電話をしたりするなど、ハッカーは被害者のシステムが意図していない電話を掛けるように強制させることがある。その他のケースでは VoIP 無料接続で大規模なボリュームを確立し、サービス拒否の状態を作ったりすることもある。WatchGuard XTM セキュリティは、許可できるセッションの最大数や1回の電話で許可するチャンネルの最大数をユーザが規定できるように支援しているため、強制電話や膨大なコネクション数など攻撃者によるダメージを最小限に抑えることができる。そのように制限をかけることで、普段では見えない量の電話問題をユーザが見つめる確率も高くなる。

VoIP セキュリティ、その要点

VoIP セキュリティが表に出てくるに伴って、2 つの主な問題に注意しなければならない。まずはデータ・セキュリティを軽視した LAN とテレフォニーを混ぜた統合インプリメンテーション、そして防衛手段を実際に追加していない

が、VoIP を「サポート」しているとベンダーが言っているものだ。統合メッセージングでは、普通のインターネット・トラフィックと VoIP 関連のコーデックやプロトコルをフィルターできる脅威管理が必要だ。先に説明したセキュリティ機能やその他様々な機能と共に、XTM は組織が必要とするテレコミュニケーション機能をサポートしながら、普通のファイアウォールを上回るレベルのセキュリティを維持することができる。

柔軟性を持つ管理方法

研究者やアナリストは印象的な「ゼロデイ」セキュリティ欠陥に多大な注意を払っているが、ネットワークの最大脅威はそれではなく、間違っただ設定と不注意この 2 つである。

ビジネス・ネットワークの最大脅威は間違っただ設定と不注意、この 2 つである。

セキュリティに影響する管理方法

世界でもっとも優れたセキュリティ・ソリューションを所有し導入しているからといっても、その製品が複雑でユーザが適切に使いこなせなければネットワーク・セキュリティを強化させることはできない。様々なニュースでもそうした点は報道されている。

- ・ 米国メイン州を拠点とした食料品チェーン店「Hannaford Bros.」のネットワークが 2008 年 8 月に侵入され、同社は大きな被害を被った。これにより顧客のクレジットカード・データは紛失され、少なくとも世界中で 2,000 件にもものぼる詐欺事件に繋がった。Hannaford の CIO ビル・ホーマ氏は、この被害からの回復に掛かる費用は「かなりの数字……何百万ドルだろう」と述べている。アナリスト達は、このネットワーク侵害はおそらく Hannaford が複雑なネットワーク・メッセージング・ツールを間違っただ設定したことで機密データを露呈してしまったのだろうと見ている。
- ・ Verizon の RISK チームによる 2008 年度の報告によると、4 年間に渡り実社会で発生したネットワーク侵害 500 件のうち 87%において、被害者である組織のポリシーやコントロールは適切に行われていたものの、そのポリシーに従っていなかったと報告している。
- ・ 調査会社の Gartner は 2009 年、ワイヤレス・ローカル・エリア・ネットワークにおける 70%のネットワーク侵害の原因は誤っただ設定によるものだろうと予測している。
- ・ ベンダーが 2001 年に Code Red ワームの悪用に対応するパッチを出していたにもかかわらず、Code Red ワームは 2008 年の時点でもまだ感染を拡げていた。さらに、少なくとも 4 年は経っている Rbot というボットは、マイクロソフトの Malicious Software Removal Tool が 2008 年にもっとも除去したマルウェアだった。どちらのケースにおいても、かなりの数のインターネット利用者がそうした悪用を阻止できるソフトウェア・パッチのインストールを軽視していることが分かる。

つまり、不適切に設定されているギアはセキュリティを台無しにしてしまうわけだ。そうした考えが、WatchGuard が使いやすいセキュリティ・アプライアンスを提供していくことを全面的に約束している理由となっている。そして他のベンダーが全費用を請求している管理ツールを WatchGuard XTM 製品ではスタンダードとして取り入れている理由も、そのような背景があるからだ。

昨今の不況において、多くの IT 部が人員削減を行った。それにより残ったスタッフの作業量が増加した場合もあるだろう。WatchGuard は、それぞれの状況下において最適な管理方法が必要であり、また直感的に使用できるギアが必要であることを理解している。購入前にセキュリティ製品を比較しているならば、他のベンダーが WatchGuard のように次の管理機能を備えており、それらをスタンダードとして提供しているかどうかチェックしてみるといいだろう。

管理インターフェイスの選択肢

WatchGuard 製品シリーズはいずれも 3 つの管理方法を提供している:

- Win32 ベース・クライアント GUI (WatchGuard System Manager)
- ウェブベースのクライアントレス GUI
- コマンドライン・インターフェイス(CLI)

Fortinet や Cisco, Sonicwall などは、どれもこのようなオプションいずれかを提供しているが、3 つすべてを提供しているところはない。そしてスタンダード製品でそれらを提供していることはもちろんない。しかし WatchGuard では、3 つの管理オプションが基本として備えられているほか、WatchGuard Firebox から XTM シリーズに渡り、まったく同じ方法で 3 つのオプションは作動することができ、安価なモデルからもっともパワフルなモデルでも対応できるようになっている。例えば、リモートから小規模のブランチ・オフィスを管理し、本社のセキュリティ・アプライアンスも管理している場合、各環境で使用する WatchGuard アプライアンス・モデルは違うものだろう。だが、同じ技術やメニューを使ってそれぞれ作業を行うことができるのである。

最善の CLI インプリメンテーション

コマンドライン・インターフェイス(CLI)を好むのであれば、WatchGuard のコマンドラインが気に入るだろう。Linux の bash シェルや Cisco OS で使えるショートカットとして学んだトリックは(例: "status" と入力するところを "st" と入力するなど)、WatchGuard CLI でも使うことができる。効率性を考慮しプログラムされているコマンドラインは、省略コマンドやオートコンプリート文字列("conf" を "configure" にするなど)を受け入れることができる。

WatchGuard のスクリプト可能な CLI は、アプライアンスを設定したり管理したりするための Unix Expect ツールなど、馴染みのコマンドを許可している。柔軟性を持つスクリプティング・サポートは、WatchGuard 製品とネットワークにあるその他のセキュリティ・デバイスとの間で優れた相互運用性を見せている。実際、ネットワークでほかのデバイスが検出した脅威に対し、WatchGuard アプライアンスが自動的に対応できるようにプログラムすることもできる。ルーターやスイッチ、外部のスキャナーが持つネットワークに対する観点は異なるが、Fireware を使えば全デバイスのインテリジェンスを収集しまとめることで、トラフィックの急増を知らせたり悪質なパターンを阻止したりすることができる。

コマンドライン・インターフェイス機能は、セキュリティをサポートする賢明な取り組みと言える。例えば、ネットワークに侵入することに成功した攻撃者は、すぐに防衛を中断させたり排除しようとしたりするが、WatchGuard のコマンドラインはシェルではなく Fireware のコンフィギュレーション・ファイルを削除するために、コマンドを提供しないようになっている。また、Cisco ユーザも Cisco の "enable" モードに似ている WatchGuard の 2 ティア・コマンド・モードを認識できる。つまり、認証されていても監視できるのは WatchGuard デバイスとそのステータスのみである。コマンドを出すには、追加のパスワードと共に Command Mode を入力しなければならない。つまり機密なコントロール・センターに、もう 1 つのレイヤーを付け加えることになる。

WatchGuard CLI の Help モードは、コンテキスト・センシティブ(状況依存)である。文字列の最後に "?" マークを挿入することで、その文字列の説明を呼び出したりコマンドに関係するリストを呼び出すことができる。下記は、 "?" の前に来た文字列により異なるそれぞれの反応だ。

```
WG(config)#?  
Configure commands:  
bridge  
local area network settings
```

cluster
Firecluster
ddns
dynamic DNS service
debug-cli
configure debugging options
default-packet-handling
default packet handling

WG(config)#ip ?
allowed-site
allowed IP address
blocked-port
blocked ports
blocked-site
blocked IP address
dns
IP Domain Name Service Resolver
dynamic-routing
dynamic routing configuration

WG(config)#ip i?
icmp
Internet Control Message Protocol
ipsec
IP Security Protocol

集中管理とリモート管理

タイピングが得意でなかったり、マウス操作ができるインターフェイスがただ好きなのだという人もいるだろう。そこで WatchGuard ではリッチ Windows クライアント、そしてグラフィカル・ウェブ・インターフェイスといった 2 つの選択肢を提供している。

PC に Win32 クライアントをインストールすれば、それを WatchGuard Management Server にすることができる。このクライアント・ベースの UI は、ワンタッチ・コンフィギュレーション・アップデートなどの機能を有効にする。一度、集中管理先からアップデートをプッシュすれば、それに対応する WatchGuard セキュリティ・デバイスすべてが同じアップデートを受取るようになる。これにより、複数のデバイスで何度もコンフィギュレーション設定を入力する必要がなくなり、アップデートをインストールするために様々な場所に出向く必要もなくなる。ファームウェア・アップデートやライセンス・キーの同期化においても同様で、1 度の管理操作を集中管理している WatchGuard アプライアンス全体に適用することも可能になる。さらに、自動実行されるようにスケジュールを組むこともできるので、時間外のメンテナンス枠でのアップデートに最適だ。そんな Windows クライアントの Watchguard System Manager を非常に気に入るようになるのではないだろうか。ここ数年の間に改良され、毎日監視されているしっかりしたユーザー・コミュニティ・スワップでは実用的なアドバイスも提供されている。

Win32 管理クライアントを称賛するごとく、WatchGuard のウェブベースのクライアントレス・ユーザー・インターフェイスは、世界中どこにいても WatchGuard アプライアンスをコントロールできるようにする。WatchGuard XTM のウェブベース UI は、最新技術を使い極めて豊かでダイナミックな管理環境を提供し、その他多くのファイアウォールで見られる前世代のウェブベース GUI に比べて遥かに先を行くものになっている。

CLI やクライアント・ベースの GUI、クライアントレス・ウェブベースの GUI は何役もこなさなければならない役割にとって、いずれも利点がある。しかし 3 つとも使用できるならば、そのうち 1 つを選ばなければならない理由があるだろうか？

リッチ・レポートイング

WatchGuard では、セキュリティ・アプライアンスは様々な方法でネットワークを監視できるものであるべきだと信じている。実績があり信頼をうけている WatchGuard System Manager は、リアルタイムで一目で見ることができる優れた機能の HostWatch や Bandwidth Meter、Traffic Monitor などですでによく知られている。しかし、ネットワーク・セキュリティやビジネス・ヘルスは絡み合っているものである。つまり、ネットワークで何が起きているのを知るだけでは充分ではなく、ほかの部署やシニア・マネジメントに自分が知っている情報を知らせる必要がある。こうした点において、XTM はすでに設定されている 40 件以上のレポートを提供することができる。

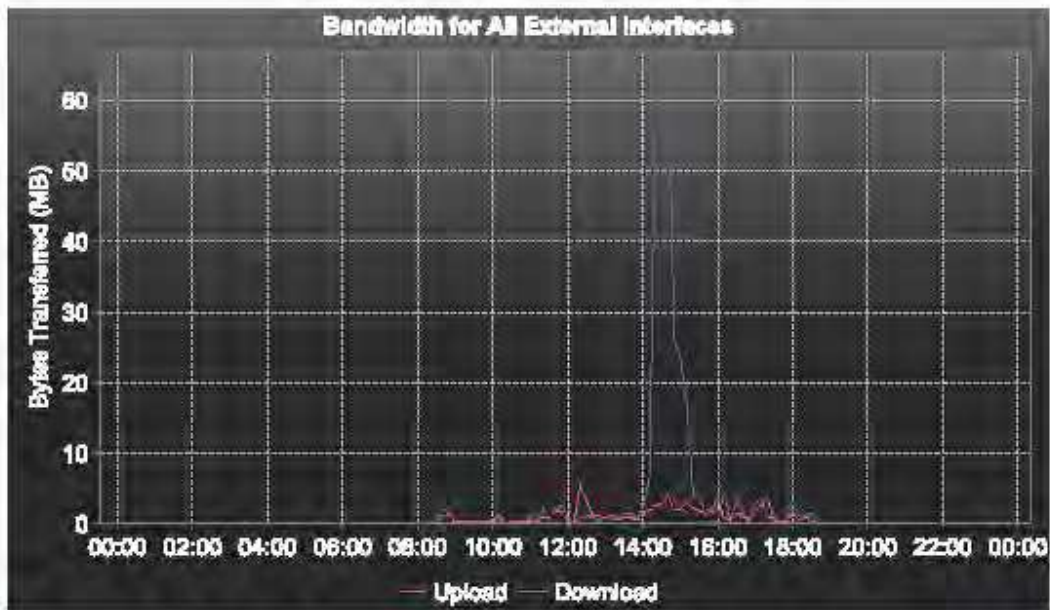


Bandwidth Usage for All External Interfaces

edge_00788 (203.215.153.106) 727300788245F



From	To	Number of Logs
6/16/08 12:00 AM	6/17/08 12:00 AM	130



Bandwidth Statistics for All External Interfaces

Time	Bytes Transferred			
	Upload	Bytes (%)	Download	Bytes (%)
6/16/08 12:00 AM	49481	0.06%	39949	0.01%
6/16/08 12:10 AM	40140	0.05%	38473	0.01%
6/16/08 12:20 AM	51102	0.06%	52287	0.02%
6/16/08 12:30 AM	37328	0.04%	36820	0.01%
6/16/08 12:40 AM	40721	0.05%	38864	0.01%
Total	.21 MB	0.26%	.20 MB	0.06%

図 3: Fireware XTM Reporting Options では、WatchGuard Server Center でデバイスのグループを作成することができる。そして、デバイス・グループ用に HTML や PDF 形式のレポートを作成することもできる。オプション・メニューではレポート保管先や HTML レポートで使われるロゴや URL をカスタマイズすることができる。

Fireware XTM ではスタンダードとしてレポートの一部には次が含まれている:

- ・ サービスや時間、セッションによるパケット・フィルターの概要
- ・ ウェブ・トレンドの概要
- ・ ウェブ・アクティビティ監査
- ・ もっとも頻繁に現れるドメイン
- ・ Time による URL の詳細
- ・ もっともアクティブなクライアント
- ・ 侵入防止の概要
- ・ VPNトンネルのバンド幅
- ・ アラーム(警告)
- ・ Virus によるウイルス対策サービスの概要
- ・ Virus による詳細
- ・ Proxy によるプロキシド・トラフィックの概要
- ・ Time によるプロキシド・トラフィックの概要
- ・ Session によるプロキシド・トラフィックの概要
- ・ spamBlocker 概要
- ・ SMTP プロキシ詳細

すでに設定済みのレポート評価を提供しているからといって、そこで気楽にしているというわけではない。むしろ、それをバネにして自分が望むレポートをカスタマイズするように使うことができる。デバイスをグループでまとめたり、各グループ用のカスタム・レポートを作成することもできる。またオンデマンドでレポートを出力したり、先にスケジュールを組んで実行することも可能だ。ユーザのニーズにより、レポート形式は HTML または PDF がありロゴや URL もカスタマイズできる。

柔軟な管理方法: 結論

WatchGuard では購入時に基本として含まれ提供している管理パッケージと、やっとなら比較できるような機能をライバルのセキュリティ・ベンダーは多額で出している。WatchGuard ではクライアントベース、ウェブ、コマンドライン・インターフェイスを個人の任意でいつでも制限なしに使えるようになっている。これはどの WatchGuard 製品においても同じである。スタンダード・レポート・パッケージで WatchGuard が提供している機能を上回るものはない。実際、現時点で Fortinet では高価なレポート・アップグレードを購入しない限り、提供しているレポート数は 2 つとなっている。

柔軟でわかりやすく、常にコントロールできるということは、単に便利であるという枠を超えている。このセクションでは悪名高いネットワーク侵入について触れ、実際の原因はネットワーク・ツールの管理的混乱が原因になっている点であることを説明した。誤った設定がデータ侵入に繋がる可能性がある、ほぼ全員と言えるセキュリティ専門家が同意している。先に述べた管理機能やレポート機能、その他機能と共に、XTM はセキュリティ・アプライアンスが単に便利な製品というレベルを超え、明らかに優れたセキュリティを提供しているのだ。

結論: ノーがイエスであるとき

ネットワーク管理者であれば、ネットワークで何が起きているのかをもっと知りたいと思っているだろうし、より使いやすくパワフルな方法でトラフィックをコントロールできたらと望んでいることだろう。Fireware XTM を実行している

WatchGuard アプライアンス・モデルはユーザを念頭にデザインされた機能を通じて、そのようなニーズに応えることができる。

これでファイアウォールはどれも同じではないということを理解していただけたでしょうか？判断するのは君だ。今使用しているファイアウォールやセキュリティ・アプライアンスに次の点は含まれているだろうか？

- ・ HTTPSトラフィックのフル・ペイロードを検査し、いくつかの方法でフィルターを掛け再構築し再び暗号化してから、安全をもって宛先に送信することができるだろうか？
- ・ VoIPトラフィックを許可するだけでなく、無用かつ要求していないコーデックをフィルターに掛けることでセキュリティを追加し、VoIPシステムが使う機密情報を暴露するようなサインを覆い隠すことができるだろうか？
- ・ 3つの異なる管理インターフェイスを提供することで、ユーザのスタイルやニーズに合わせることもできるだろうか？

どのファイアウォールも同じではないので、自分のネットワークに最適なものを使っていることを確かめよう。WatchGuard Fireware XTMを使用することで得られる利点の詳細については、WatchGuard リセラーまで問い合わせることをお勧めする。www.watchguard.com

住所: 505 Fifth Avenue South Suite 500 Seattle, WA 98104 U.S.
WEB: www.watchguard.com
米国・営業: 1.800.734.9905
国際・セールス: +1.206.613.0895

WatchGuard について:

1996年より、WatchGuard Technologiesは信頼でき容易に管理できるセキュリティ・アプライアンスを世界中の何百、何千という企業に提供してきました。弊社の拡張可能な脅威管理(XTM)ソリューション、Firebox X シリーズは、そのレベルでもっとも使いやすく、強力かつ信頼できるマルチレイヤーのセキュリティを連結させた優れた製品です。弊社最新のアプライアンス、WatchGuard XTM 1050は、高度なパフォーマンスと完全に拡張可能でありながらエンタープライズ・レベルのセキュリティを備え、お求めやすい価格でご提供しています。WatchGuardは民間企業であり、本社は米国ワシントン州シアトルに所在し北米、ヨーロッパ、アジアパシフィック、南米にオフィスを構えています。詳細につきましては www.watchguard.com をご参照ください。

同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向に基づき提供します。©2009 WatchGuard Technologies, Inc. 無断複製・転載を禁じます。WatchGuard および WatchGuard のロゴは WatchGuard Technologies, Inc. の米国およびそのほかの国における登録商標あるいは商標です。そのほかすべての登録商標および商標は、各所有者に権利があります。Part No.WGCE66633_072409

脚注:

Pg.2 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

Pg.5 『2009 Data Breach Investigations Report』 <http://www.verizonbusiness.com/products/security/risk/databreach/>

Pg.6 初の市販ファイアウォールを開発したチームのマネージャーを務めたフレッド・アヴォリオのセキュリティ格言：
<http://www.avolio.com/papers/axioms.html>.

Pg.6 コーデックは関係当局によって”compression” や”decompression”、”coder”や”decoder”などをブレンドしたり短くしたりする

Pg.8 2009年の攻撃例については『VoIP hackers strike Perth business 』を読むことを薦める

Pg.8 『Hannaford to spend ‘millions’ on IT security upgrades after breach』 Computerworld, April 22, 2008.

Pg.8 Hannaford Bros. のネットワーク侵害の詳細と WatchGuard 製品であればどのように対応できたかという点についてはホワイトペーパー『How WatchGuard Could Have Saved Hannaford and TJX Money 』を参照することをすすめる。
<http://www.watchguard.com/infocenter/whitepapers.asp>