ゼットスケーラーによる不正侵入防止システム（IPS）

zscaler™

IPSインスペクションは、綿密な防御戦略の重要なコンポーネントではありますが、組織内での実装の方法と場所を理解することも同様に重要です。本資料では、IDS/IPSデバイスがどのような目的で設計され、主要となるさまざまな機能によってどのような相違があり、それらの機能をどこに導入するのが最適であるかを考察します。また、ゼットスケーラーが提供するソリューションについても紹介するとともに、ゼットスケーラーのAPT（高度な標的型攻撃）保護戦略の重要な部分であるIPSやそれを補完する手法についても解説します。

IDSとIPSの機能

IDS（不正侵入検知）システムは、トラフィックを監視し、許可されないネットワークアクティビティを検知する目的で設計されました。IDSシステムは、ヘッダとペイロードを含むパケット全体を分析し、既知のマルウェアのシグネチャと比較します。IDSアプライアンスは通常、ダイレクトなデータストリームから外れた場所に置かれ、次のような不正パケットについて報告します。

- 不正コード
- ボットネット
- ウィルス
- 標的型攻撃とエクスプロイト
- スパイウェア
- クロスサイトスクリプティング（XSS）攻撃
- SQLインジェクション

...その他

正しくチューニングした不正侵入検知システムにメリットはありますが、覚えておくべきなのは、IDSテクノロジによってITチームが問題のアラートを受け取ることはできるものの、問題を防ぐことはできないということです。これに対し、IPS（不正侵入防止システム）は、不正パケットを検知してアクションを実行できます。IPSはネットワークトラフィックに対してインラインで展開されるため、これが可能になります。IPSテクノロジは、接続をリセットしてブロックするか、パケットをドロップすることで、不正トラフィックをブロックできます。パケットが転送されてIPSによって処理されるため、標的であるユーザに届く前に攻撃をブロックするには、リアルタイムで検知する必要があります。IPSは、管理者向けにログやアラートを生成することもできます。

IDSとIPSでの処理は通常、ファイアウォールの後に実行されます。ファイアウォールがパケットのヘッダを分析し、プロトコル、送信元 /送信先アドレス、ソート /送信先ポートなどの5組の情報に基づいてポリシーを適用します。ファイアウォールスキャンに基づいて許可されたトラフィックはIDS/IPSに送信され、パケットとペイロード全体がスキャンされます。

高度な脅威の検知方法

シグニチャベースの検知 (IPS)

IPSは主としてシグニチャに基づいて不正トラフィックを検知します。シグニチャは、きっかけとなる脆弱性、または使用されるエクスプロイトを識別する一連のパターンで、これによって脆弱性の要素や、ネットワークで確認された攻撃に必ず存在するマルウェアを把握できます。誤検知 (正規のトラフィックが不正であると誤って識別されること) のトリガーを回避するために、シグニチャは固有のものであること、また既知の攻撃の亜種をブロックし実際の攻撃をブロックするために、十分に幅広いものでことが必要となります。

シグネチャベースの検知をより有効で正確なものにするため、ネットワークトラフィックの解析と前処理が実行されます。たとえば、HTTPトラフィックの場合は、シグネチャを特定のヘッダ、デコードしたコンテンツ、要求、またはサーバの応答に適用できます。IPSベンダは、既知の脆弱性やエクスプロイトを監視し、調査することで、新しいシグネチャを記述する必要があります。多くのIPSベンダが、シグニチャデータベースを日々更新しています。

異常の検知 (IPS)

不正侵入防止システムの普及に伴い、攻撃者側もシグネチャベースの検知を回避する方法を構築しています。IPSの誤りを誘い、標的に処理されてしまうようなトラフィックを生成することで、トラフィックの前処理を攻撃者が突破できれば、シグニチャがネットワークトラフィックの誤った部分に適用されて、IPSによるアクションがトリガーされない可能性があります。一般的な回避手法としては、URLの複数エンコーディングを使用する、非標準の空白を使ってHTTPヘッダを区切る、または非標準のエンコーディング手法 (7 ビット ASCII) を使用するなどの方法があります。IPSテクノロジによって、異常を検知し、異常なトラフィックにフラグを設定、インラインでブロックすることで、このような回避手法を防止することが可能となります。

行動分析 (サンドボックス)

IPSシステムはインバウンドの脅威に対する強力な防御を提供できますが、攻撃者側もその検知を回避する方法を発見しています。ファイルを武器化し、ファイルを少しずつ変えていくことで、ハッカーは、シグネチャベースと異常ベースの両方のIPS検知を回避できてしまうのです。不正なペイロードの送付に使われるファイルが少しずつ変わるため、ファイルのハッシュも変わります。ファイルのハッシュは、ファイルが以前に見つかったものであるかどうかを確認するためにIPSが使用する、既知のファイルに対する数学的な計算です。サンドボックステクノロジにおいて一般的である行動分析は、ファイルの行動に関する詳細分析を実行することで、標的システムでのそのファイルの実行に関連する動作が不正であるかどうかを確認します。サンドボックスは、既存のセキュリティギャップを解消するためのレイヤを防衛戦略に組み込むテクノロジです。

機能の統合

IDS/IPSの機能の基本は広く使用されてはいるものの、その機能をどのように有効にし、どこに展開し、その情報がどのように使用されるかについては、大きく異なる場合があります。「専業の」IDS/IPSベンダは今も存在し、一般的にはデータセンタに導入されて、サーバの保護やアグリゲーションされてインターネットに送信されるユーザトラフィックの保護に利用されますが、多くの場合、IDS/IPSテクノロジは他の製品に吸収されています。

統合脅威管理アプライアンス

IDS/IPS機能が組み込まれた最初の製品カテゴリの1つであるUTM(統合脅威管理)は、ファイアウォール、IDS/IDP機能、ゲートウェイアンチウイルスを1つのアプライアンスに統合したものです。ガートナーは、UTM市場を、中小規模企業で使用される多機能ネットワークセキュリティ製品だと定義しています[1]。

企業がリモートオフィスやブランチオフィスを保護する方法を検討する場合、単一アプライアンスは非常に安価な印象のため、UTMが最初の選択肢となるケースが多くあります。しかし実際は必ずしもそうではなく、複数のブランチオフィスにUTMデバイスを購入するためにコストが非常に高くなるケースもあります。アプライアンスのインストールと導入に必要なコストを考慮する場合は、ポリシーがアップストリームとダウンストリームのデバイスとやり取りすること、また、ポリシーがすべてのブランチで一貫性のあるものであること、アップデートやメンテナンスが処理されることを確認し、ログを相関付けて組織の全体像を把握できるようにする必要があるため、最低価格の単一のUTMであっても、実は膨大なコストが必要になります。

「次世代」アプライアンス

IDS/IPS機能は多くの場合に、次世代ファイアウォール(NGFW)の1つのコンポーネントとして議論されます。この考え方は今でも健在ですが、NGFWはポリシーを一方的に適用するデバイスであり、そのインスペクションには「従来の」ファイアウォールのネットワークパケットヘッダ情報だけにとどまるものではないと多くの人が考えています。NGFWを企業のサーバの前面にセットアップすることで、企業の資産を不正アクセスから保護できます。これは、インバウンドや内部の攻撃の可能性があるデータセンタにおいては特に有効です。NGFWアプライアンスをLANの内側にセットアップすることで、クライアントとサーバを内部の攻撃から保護することもでき、エグレスポイントに置いてインターネットにアクセスするユーザを保護することができます。しかし、NGFWアプライアンスはすべてのポートとプロトコルに対応する必要があるため、ブランチオフィスへの導入は見送られるケースが多いほか、ブランチオフィスのトラフィックの大半がHTTP/HTTPSであることから、高額なコストを要することになります。

[1] ガートナーの「Unified Threat Management Devices」マジック・クアドラント

ゼットスケーラークラウドベースのATP（Advanced Threat Protection）

データセンタは今も中心的な存在であり、十分な防御が必要ではありますが、リモートオフィスやブランチオフィスなどの他の場所ではいくつもの課題が発生する可能性があります。リモート /ブランチオフィスのトラフィックの大半は多くの場合にWebトラフィックのみであり、費用対効果の確実に高い唯一の防御方法はおそらくUTMシステムです。単一のデバイスであれば安価ですが、ブランチ全体にこれらのデバイスを複製することはできません。結果として、多くのブランチオフィスに、標準以下あるいは一貫性のない不正侵入検知と防止が残されることになります。さらには、レイテンシが発生するVPNトンネルやコストのかかるMPLSリンクでデータセンタのIPSを経由させない限り、リモートユーザのトラフィックがインスペクションから完全に除外されてしまうのが一般的です。ハッカーはこの事実を熟知しています。

大規模な組織を標的にする犯罪集団は常に存在し、彼らは、そのような組織の防御は極めて堅牢であることを知っています。しかし、そのような大規模の組織には防御が十分とは言えないブランチオフィスやリモートオフィスが存在し、そのいずれかの場所で働くユーザがフィッシングメールをクリックしたり、ゼロフレームエクスプロイトによってマルウェアをデバイスにダウンロードしてしまうと、大規模な組織であってもハッカーの標的になり得ます。

そこで有益となるのがゼットスケーラーの活用です。 ゼットスケーラーのクラウドベースのATPエンジンは、トップクラスのIPS保護、アンチウイルス /アンチマルウェア、ブラックリスト、サンドボックスを始めとする多くの機能を組み合わせて提供します。ブランチオフィスやリモートのユーザは、アウトバウンドのHTTP/HTTPSトラフィックの送信先をZscaler Enforcement Node（ZEN）にするだけで、ゼットスケーラーの数百あるデータセンタのいずれかに置かれた最も近いZENに接続され、トラフィックのすべてのバイトとすべての応答がゼットスケーラーによってインスペクションされます。ハードウェアを購入したり、ソフトウェアをアップデートしたり、バージョンを管理/調整したりする必要はありません。ゼットスケーラーは、境界ベースのアプライアンスに固有の処理、パフォーマンス、スケーラビリティに関する問題を排除するために、ゼロから構築されています。

IPSアプライアンスの課題

境界ベースのアプライアンスでのIPS機能の提供では、ハードウェアやソフトウェアデバイスの導入とメンテナンスのコストをはるかに上回る、さまざまな問題が発生します。これらの課題は、境界ベースのセキュリティデバイス、特にデータセンタの境界の外に置かれたセキュリティデバイスに共通するもので、具体的には、次のような問題が存在します。

テクノロジの制限

IPSのパフォーマンスは、アプライアンスが処理するプロトコルデコードの量や実行する必要があるパターンマッチングの量に比例します。IPSテクノロジは、大量のURLやIPアドレスが含まれるブラックリストの処理を考慮して設計されていません。さらには、アンチウイルスや前述のファイルサンドボックスなどの高度なファイル分析テクノロジをサポートしていません。IPSは現在、より完全なUTMシステムとの統合によって、より広範なセキュリティを提供するようになりましたが、前述のとおり、UTMシステムは、リモートユーザやブランチオフィスにとっての妥当なオプションではありません。

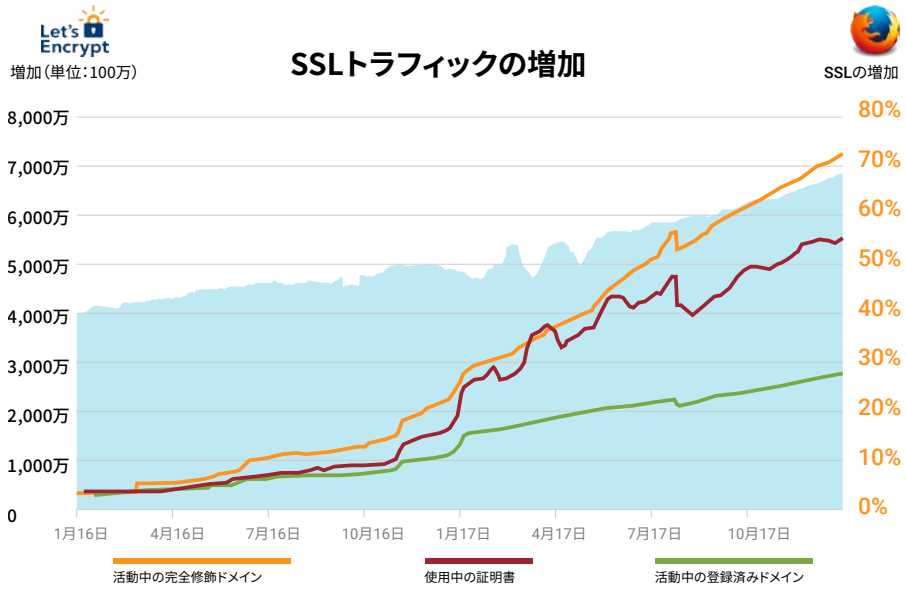
パフォーマンス

IPSアプライアンスのパフォーマンスは、有効にするシグニチャの数やコンテンツのインスペクションのスループットに左右されます。HTTPの場合は、多くの場合に応答が要求よりはるかに大きくなるため、サーバからクライアントへのHTTPシグネチャを有効にすると、IPSアプライアンスのパフォーマンスが大幅に低下します。事実、ほとんどのIPSアプライアンスで応答スキャンがデフォルトでオフになっており、それを最高のスループットとして発表しています。

その結果、セキュリティが大幅に低下してしまいます。ブラウザエクスプロイトやエクスプロイトキットを始めとするさまざまなタイプの攻撃を検知するには、HTTP応答の完全スキャンが必要です。さらに、ボットネットトラフィックの大部分は常に変動し、関係するIPアドレスやドメインが常に変化します。そのような状況であっても、要求ではなく応答をインスペクションすることで、構成のダウンロード、接続先のIPSやドメインのリストなどの要素を視覚化できるため、不正トラフィックのより効率的なブロックが可能になります。

SSL復号化の欠如

透過デバイスであるIPSの多くにとって、中間者 (MiTM) SSL復号化の実行は容易なことではありません。HTTPS復号化はプロセッサを大量に使用するため、IPSハードウェアアプライアンスが提供できるパフォーマンススループットが大幅に制限されることになります。この問題は、SSLトラフィックの増加と共にさらに深刻になります。Googleの透明度レポートによると、Googleを通過するトラフィックの90%以上が暗号化されるようになり[2]、さらには、LetsEncryptなどの無料のSSL証明書サイトを利用することで、ハッカーによる不正 Webサイトからの SSL配信も可能になりました。SSLに移行する脅威やハッカーが増加している今、企業の防衛戦略にすべてのSSLをインスペクションできる強力な機能を組み込む必要があります。



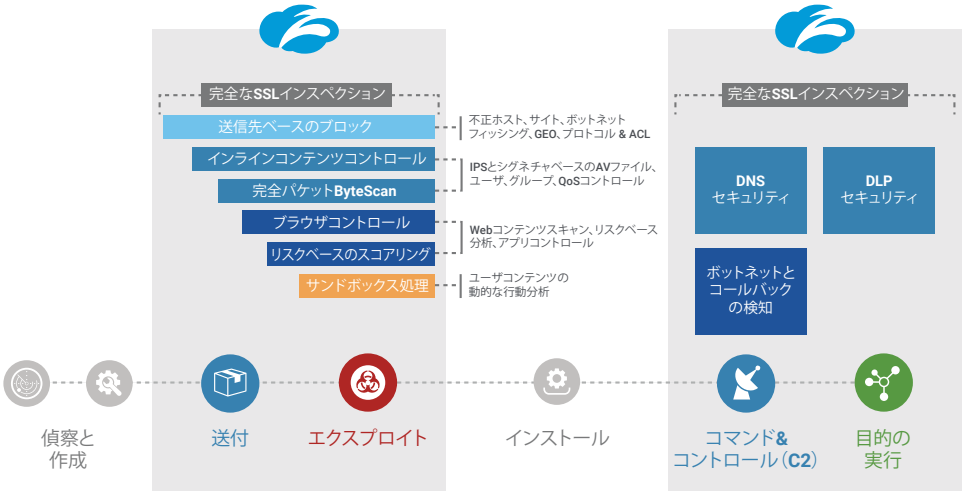
[2] Google透明性レポート:https://transparencyreport.google.com/https/overview?hl=en

非同期トラフィック

多くのネットワークにおいて、ユーザからのトラフィックの大半は、ネットワークの異なるゲートウェイロケーションから流入出します。非同期トラフィックと呼ばれるこのようなルーティングでは、IPSやその他のインスペクションデバイスで脅威が見逃されてしまうことがよくあります。脅威を正しく検知するには、ユーザ通信パターンのクライアント側とサーバ側の両方をIPSやその他のインスペクションアプライアンスが相関付けることで、シグニチャ検知が正しく実行されるようにする必要があります。単一のIPSアプライアンスを複数のゲートウェイロケーションに置くことは多くの場合に不可能であるため、インバウンドとアウトバウンドのユーザトラフィックが関連付けられていない状態では、アプライアンスが正しくトラフィックを追跡し、インスペクションできないため、攻撃が見逃されてしまいます。

パケットドロップの不利益

IPSはレイヤ 4でトラフィックをブロックしますが、Webブラウザなどのアプリケーションはレイヤ 5以上で動作します。一部のIPSプラットフォームは、パケットがドロップした場合のグレースフル TCPリセットが提供されません。そのため、多くのアプリケーションは、リセットされた接続の再試行を繰り返し、結果として、ネットワークのトラフィックが増加します。



ゼットスケーラーのクラウドプラットフォームは、IPS保護のセキュリティスタックへの統合を可能にします。ハードウェアパフォーマンスの制限なく、SSLを含むすべての脅威からの完全な保護を提供します。複雑な統合作業は必要ありません。

シグネチャベースのカテゴリをZscaler Cloud IPSで保護

ボットネットからの保護
- コマンド&コントロールサーバ
- コマンド&コントロールトラフィック

悪意のあるアクティブコンテンツからの保護
- 悪意のあるコンテンツ／サイト
- 脆弱性のあるActiveXコントロール
- ブラウザエクスプロイト
- ファイルフォーマットの脆弱性
- ブロックされた悪意のあるURL

なりすましからの保護
- 既知のフィッシングサイト
- 疑わしいフィッシングサイト
- スパイウェア／アドウェア
- Webスパム

不正な通信からの保護
- IRCトンネル
- SSHトンネリング
- アノニマイザー

クロスサイトスクリプト(XSS)プロテクション
- Cookieスティーリング
- 潜在的な悪意のあるリクエスト

疑わしい宛先からの保護

P2Pファイル共有からの保護

P2Pアノニマイザーからの保護

P2P VoIPからの保護

クリプトマイニング

ゼットスケーラーのクラウド IPS

ゼットスケーラーでは、IPSテクノロジが高度脅威検知の一部として統合されており、IPSも、ブラックリスト、ヒューリスティック(ページリスク)、アンチウイルス、ファイルサンドボックスなどと並行して、インスペクションの1つとして実行されます。ゼットスケーラーは、サーバではなくユーザを保護するため、データセンタでの発生が予想される、SQLインジェクション、サービス拒否、リモートコードの実行などのサーバ攻撃をIPSが検知するわけではありません。HTTP/HTTPS経由のユーザに対する脅威の検知に重点を置いているゼットスケーラーのIPSは、ブランチ /リモートオフィスやモバイルユーザに最適なソリューションです。優れたパフォーマンスとスケーラビリティを提供する統合セキュリティサービスであるゼットスケーラーなら、あらゆる環境に簡単にセキュリティレイヤを追加できます。

ゼットスケーラーは独自のByteScanテクノロジを活用し、クライアントとサーバの間の双方向のトラフィックをスキャンします。要求と応答の両方を解析し、すべてのWebトラフィックで脆弱性とエクスプロイトのシグニチャをマッチングします。ゼットスケーラーは、要求とそれをはるかに上回る大きさの応答の両方を考慮することで、脅威の全体像を提供します。すべてのシグネチャが、すべてのトランザクションの要求と応答にリアルタイムで適用されます。Webブラウザあるいはクライアントデバイスで動作するアプリケーションのどちらを起点にするかに関係なく、すべてのWebトラフィックがゼットスケーラーのIPSに渡されます。

シグニチャベースの検知

インバウンドとアウトバウンドのすべてのHTTP/HTTPSトラフィックが解析され、URL、ヘッダ、POSTデータ、応答の本文などが抽出されます。ゼットスケーラーのセキュリティチームは、毎年2,000以上の新しいシグネチャを公開しており、これらのシグネチャによって、Microsoft Active Protections Program (MAPP) や他のベンダが公開しているプログラムを始めとする、ブラウザとアプリケーションの脆弱性に対応します。さらには、エクスプロイトキット、コマンド &コントロールのトラフィック、クロスサイトスクリプティングなどに対応するシグネチャも公開しています。

そして、もっとも重要なのは、ゼットスケーラーのクラウド全体で、1日あたり数回のシグネチャのアップデートと追加が透過的に実行されているということです。これは、シグニチャのアップデートが最大でも1日に1回程度であるアプライアンスベースのIPS機能と大きく異なる点です。さらには、ゼットスケーラーで何らかの脅威が検知されると、すべてのユーザがその脅威から保護されるというメリットもあります。すなわち、初めて検知された脅威から、すべてのユーザをすぐに保護できるようになります。

異常の検知 - プロキシ IPS

Zscaler Enforcement Node (ZEN) は、プロキシであり、透過デバイスではありません。クライアントからの要求をZENが受け取り、送信先サーバへの新しい要求を作成します。その機能を実行するには、ZENが要求全体を正しく解析できる必要があります。セキュリティデバイスを騙して要求を誤解させる回避手法は、ゼットスケーラーのようなプロキシアーキテクチャには通用しません。ZENが要求を解析できなければ、要求が送信先に転送されないため、ゼットスケーラーのプロトコルデコーダを回避しようとした場合も不正要求が転送されることはありません。

攻撃のブロック

Zscaler Encforcement Node（ZEN）は、不正トラフィックがブロックされたことを、ユーザやアプリケーションにわかりやすいHTMLページで通知します。 そのため、ユーザは、要求がブロックされたという事実とその理由を理解した上で、その後のアクションを実行できます。すべての攻撃がブロックされ、ログに記録され、リアルタイムで報告されます。管理者は、攻撃を相関付けたり、攻撃の前のユーザのアクティビティを確認できるため、フォレンジックがはるかに容易になります。

SSLインスペクション

ゼットスケーラーは、プロキシとしてSSLを復号化し、HTTPSトラフィックの完全スキャンによって、シグネチャをマッチングします。暗号化の有無に関係なく、すべてのWebトラフィックに同じレベルのセキュリティ保護が提供されるため、SSLの「死角」という重大な問題が解消されるだけでなく、ゼットスケーラーであれば、アプライアンスによるパフォーマンスへの影響なく、それを実現します。URLカテゴリまたはクラウドアプリケーションや場所に基づき、SSLインスペクションをオンまたはオフにできます。

すべてのトラフィックで高パフォーマンス、低レイテンシを実現

ゼットスケーラーは、独自のIPSエンジンを開発することで、スケーラビリティを実現しています。要求と応答の両方でのシグニチャベースの検知が常に有効になり、高度脅威ポリシーが脅威をブロックするように設定されている場合もレイテンシが追加されることはありません。 さらには、ゼットスケーラーのクラウドは、ユーザがインターネットにアクセスできるあらゆる接続ルートに容易に対応できるため、非同期トラフィックのインスペクションが問題になることはありません。ゼットスケーラーのお客様は、速度やインスペクション、またカバレッジといった必要な要素を、一部に限定せず、常にすべてを手に入れることができます。

まとめ

IPSは、特定のタイプの脅威からユーザを保護する役割を果たします。ゼットスケーラーは、 ByteScanとシグネチャベースの検知に加えて、サンドボックスとSSLインスペクションを含む完全統合されたセキュリティスタックを活用することで、ユーザを標的にする攻撃や不正トラフィックをブロックします。SSL復号化を有効にすることで、すべてのトラフィックに対する同じレベルのセキュリティインスペクションが可能になります。ハードウェアの制限が存在しない、組織のトラフィックの需要に合わせた柔軟な拡張が可能なゼットスケーラーのAPT（Advanced Threat Protection）スイートは、市場の他のIPSソリューションをはるかに上回る高いレベルの保護を提供します。

Zscaler Cloud IPS、**Zscaler Cloud Sandboxing**、
または**Zscaler ATP（Advanced Threat Protection）**の詳細については、
ゼットスケーラーのWebサイトをご覧いただくか、**デモをご依頼ください**。

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp