SOPHOS
Cybersecurity evolved.

トラフィックの暗号化が進んだことでファイアウォールは効果を失ったのか？

今後導入するファイアウォールで求められるTLS インスペクションの 5 つの機能

ソフォスホワイトペーパー 2021 年 6 月

今後導入するファイアウォールで求められる TLS インスペクションの 5 つの機能

暗号化されたネットワークトラフィックが急増する中で、多くの次世代ファイアウォールが暗号化トラフィックを検査できないために、セキュリティで壊滅的な状況が発生し、悲惨な結果が生じています。

多くのネットワークでトラフィックの 90% 以上が暗号化されており、一般的なファイアウォールでフィルタリングされることなく通過しています。暗号化されているトラフィックを検査することの重要性を知りつつも、多くのファイアウォールがこの役割を果たすための機能を実装していないために対応できない状況にあります。ファイアウォールが暗号化トラフィックを検査できたとしても、TLS インスペクション機能の実装が不十分なケースが多く、多くの Web サイトが適切に動作しなくなり、ユーザーエクスペリエンスが低下する場合もあります。

ハッカーは、当然のように、組織が抱えているセキュリティ上のこの大きな盲点を狙っており、この弱点を悪用し、ネットワークに侵入し、攻撃拠点を維持しようとしています。

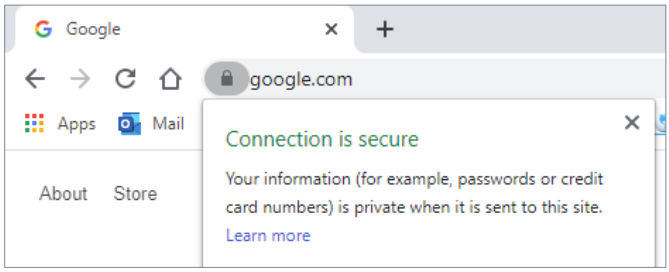
このホワイトペーパーでは、暗号化トラフィックによって多くの次世代ファイアウォールが本来の機能を果たすことができなくなっている状況、TSL インスペクションの課題、そしてこのセキュリティギャップを解消するために必要な 5 つの TSL インスペクション機能について説明します。

暗号化で守られるのはセキュリティではなくプライバシー

多くの人は、インターネット接続が暗号化されていれば「安全」だと考えています。しかし、この「安全」とは具体的には何を意味するのでしょうか？

SSL と TLS という用語は、同じ意味で使用されることが多くあります。実際、SSL は古い規格であり、TLS に置き換わっているのですが、現在でも TLS よりも SSL が一般的に使用されています。SSL という用語が使用されている場合でも、通常は TLS が使用されています。

TLS は、一対の機器間でやりとりされる通信を暗号化し、サーバー側のユーザーを、証明書とその発行者に基づいて検証し、機密性を確保し、なりすましを防止するように設計されています。



ブラウザに表示されている鍵のマークは、接続が暗号化されており、プライバシーが保護されていることを示します。

TLS で暗号化されているからといって、Web ページのコンテンツの安全性が保証されるわけではありません。マルウェアのペイロードをホストしているサイトであっても、完全に正当な暗号化されたセキュア接続を確立することができます。

Web サーバーへの接続が安全であるという主張は、実際には、接続の内容が盗聴されないことを意味します (実際、確実に盗聴を防ぐことはできない場合もあります)。暗号化されたトラフィックを検査することが非常に重要なのはこのためです。

TLS インスペクションは簡単ではない

TLS インスペクションの課題は、TLS が非常に複雑なプロトコルであることに由来します。接続を暗号化する方法を決定するためには、いくつもの証明書を交換し、使用している暗号スイートとネゴシエートする必要があります。さらに、TLS にはいくつかのバージョンがあり、アプリケーションや Web サービスによって異なる方法が採用されていることも問題を複雑にしている原因となっています。

そのため、厳しい規格であるにも関わらず、互換性が確保されない場合も多くあります。これは、やりとりされるコンテンツを検査して保護するために、プロセスに自身をインジェクトするセキュリティソリューションにとって、非常に大きな問題となります。

TLS 1.3 の重要性と間違った認識

最新の TLS 規格である TLS 1.3 は、パフォーマンスの向上、プライバシー保護、過去に検出された脆弱性の解消など、以前のバージョンと比較して多くの利点があります。

サーバーでの TLS 1.3 の採用はまだ始まったばかりですが、主要なブラウザではすべて TLS 1.3 規格がサポートされています。しかし、TLS 1.3 の実装には複雑な作業と研究開発の労力が求められることから、TLS インスペクション機能を実装している市場にあるファイアウォールの多くは、TLS 1.3 を完全にサポートしておらず、TLS 1.2 へのダウングレードを強制する場合もあります。TLS 1.2 を使用する接続は、既知の脆弱性が悪用され攻撃を受ける恐れがあります。

新しい技術が登場するときに多くあることですが、TLS 1.3 のインスペクションについても多くの誤解が存在しています。これらの誤解には、TLS 1.3 は検査できないというものもあります。これは事実ではありません。完全に外部から実行するパッシブな TLS インスペクションは可能ではなくなりましたが、企業ネットワークなどでインスペクションに協力するエンドポイントがあれば、十分に検査することができます。

また、暗号化されたトラフィックフローを検査すれば、安全性が低下するという主張もあります。これは、現在の多くの TLS インスペクションソリューションで見られるように、TLS 1.3 の接続を TLS 1.2 にダウングレードしている場合に発生する問題です。TLS 1.2 には脆弱性があり、悪意のある中間者攻撃を受ける恐れがあります。TLS 1.3 ではこれらの脆弱性が解消されており、接続を TLS 1.2 にダウングレードしなければ、暗号化トラフィックを検査してもリスクは生じません。

最後に、証明書ピンニング (ピン留め) によって TLS を検査できなくなるという主張もあります。これは、ハードコードされた証明書を使用している一部のアプリケーションについては正しいのですが、多くのアプリケーションでは、無効化された証明書に対応する証明書ピンニングのアプローチを使用しており、問題なく TLS インスペクションを利用できます。

証明書検証の重要性

証明書の検証は、TLS の基本コンポーネントの 1 つであり、クライアントやファイアウォールなどのインスペクションデバイスが通信元のサーバーのアイデンティティを証明するための機能です。

しかし、証明書検証が機能するためには、適切な実装が必要となります。適切に実装されなければ、ファイアウォールやファイアウォールに接続するエンドポイントは、実在しないサーバーと通信していると誤って認識し、悪意のある中間者攻撃を受ける恐れがあります。

パフォーマンス、プライバシー、保護のバランスを確保する

TLS で暗号化されたトラフィックフローを扱う場合には、高度な技術も求められますが、一方で、ポリシーや法規制に関する制約についても検討し、尊重しなければなりません。さらに、企業の信頼できるアプリケーショントラフィックやストリーミングメディアも暗号化されており、暗号化されている TLS トラフィックの大部分を占めていますが、これらは必ずしも検査が必要ではありません。

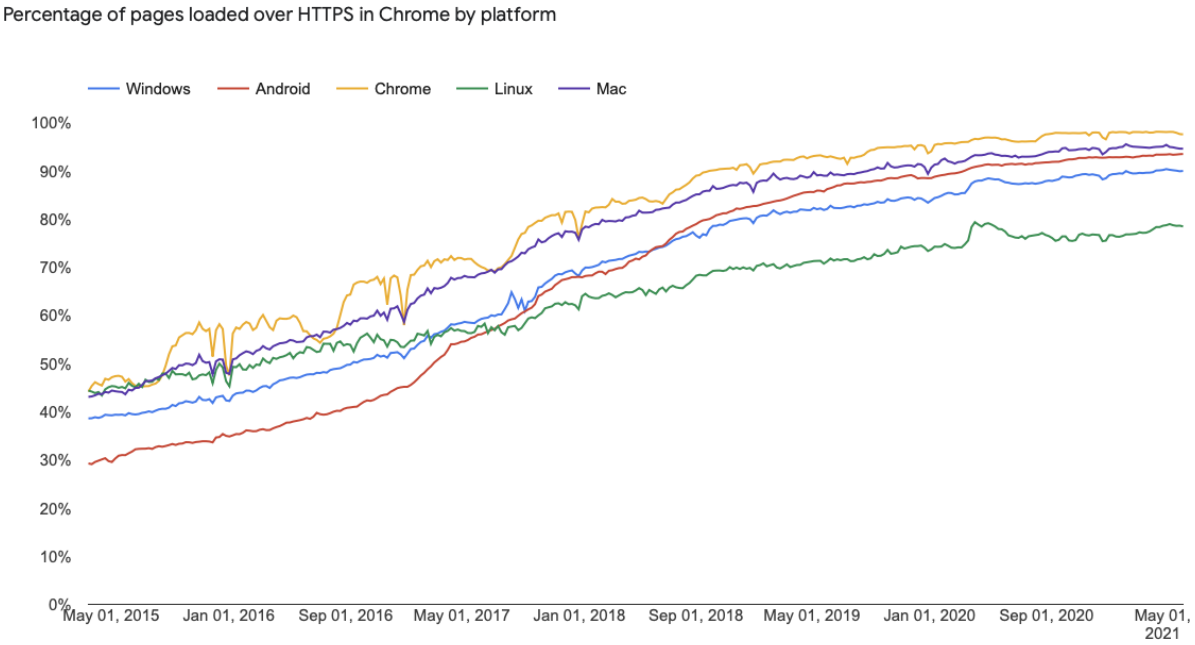
暗号化されたトラフィックはすべて同じように扱うことは不可能であり、また、そうするべきでもありません。プライバシー、セキュリティ、コンプライアンス、そしてパフォーマンスのバランスを確保しなければならりません。国や地域によっては、このバランスについての指針が示されている場合もあります。また、企業や組織は状況を踏まえて最適なバランスを独自に検討しなければならない場合もあります。

残念ながら、現在市場にあるほとんどのファイアウォールに搭載されている TLS インスペクションソリューションには制約があり、バランスを欠いたアプローチを採用せざるを得なくなっています。つまり、求められるパフォーマンスと相互運用性を実現するために、セキュリティとコンプライアンスが犠牲になっているのです。

暗号化されるトラフィックは 100% に近づいている

インターネット接続はほぼ 100% 暗号化されるようになっています。実際、Google 透明性レポートによると、ほぼすべてのプラットフォームにおける Web セッションの 90% 以上が暗号化されており、わずか約 60% であって 2 年前と比較して劇的に増加しています。

Google 透明性レポート



暗号化されるトラフィックは、この 2 年間で劇的に増加しており、100% に向かって推移しています。

暗号化によってファイアウォールは無用になったか？

Google 透明性レポートが示しているように、暗号化されるトラフィックが急増したことで、多くの組織にとってこのようなトラフィックがセキュリティの死角となりました。組織が現在使用しているファイアウォールでは、このような大量の暗号化されたセッションを検査することはできません。事実、TLS 暗号化によって、ネットワークでやりとりされるトラフィックの大部分を検査できなくなったため、ほとんどのファイアウォールは本来の機能を果たすことができなくなりました。

本当に危険なのは、暗号化されたトラフィックに潜む脅威

近年、TLS による暗号化が爆発的に普及していることから、ハッカーのような攻撃者も暗号化されたトラフィックを使用してマルウェアを組織のネットワークに送り付け、検知を回避しながら、ネットワークに身を潜めるようになりました。

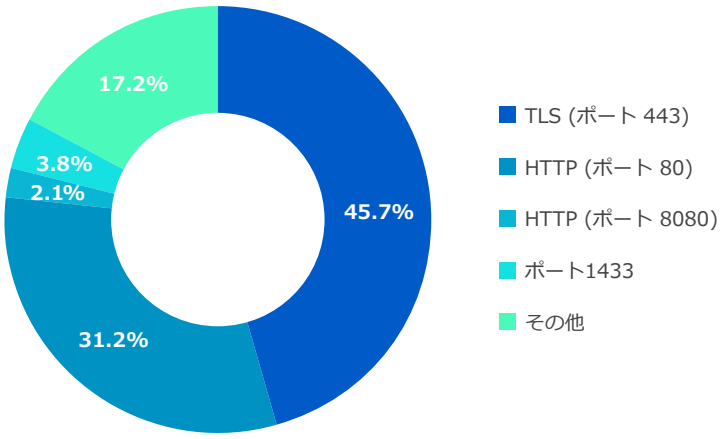
この 1 年間、ランサムウェア攻撃、特に手動で展開されるランサムウェアでは TLS が使用されるケースが増加していますが、これは攻撃者が HTTPS を利用したモジュール型のツールを使用していることが一因です。しかし、悪意のある TLS トラフィックの大半は、ローダー、ドロッパー、ドキュメントベースのインストーラーなど、保護されている Web ページにアクセスしてインストールパッケージを取得するための、攻撃の初期段階で使用されるマルウェアです。

ほぼすべての脅威が、暗号化された接続から ネットワークに侵入している。

攻撃者は、一度ネットワークに侵入すると、検出を回避するためにあらゆる手段を講じます。TLS を使用すれば、コントロールサーバーからクライアントに送信するコマンドが検知されなくなり、ネットワークから収集した情報を外部に送信することも、セキュリティを侵害したホストに別のペイロードを秘密裏にダウンロードすることもできます。

この 1 年間で、TLS を利用して通信を隠蔽するマルウェアは劇的に増加しています。2020 年にソフォスが検出したインターネット上のリモートシステムと通信するマルウェアのうち、TLS を使用していたのは 23% でしたが、現在では 46% 近くになっています。

マルウェアが C&C サーバーとの通信で使用するプロトコル (TLS など)、
2021 年第 1 四半期

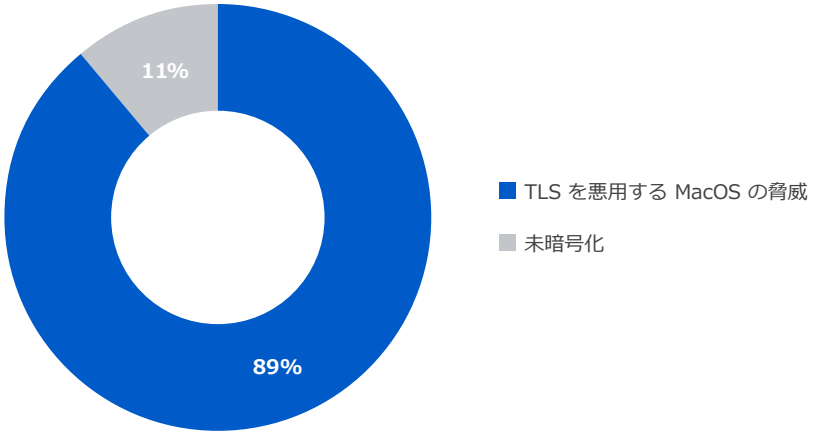


マルウェアが外部への通信に使用するプロトコルの内訳

また、TLS 通信の中には、443 以外のインターネットプロトコルポートを使用するものがかなりの割合で含まれています。たとえば、マルウェアが非標準のポート番号で Tor や SOCKS プロキシを使用している場合などです。

ハッカーは、Discord、Github、Google Cloud など、TLS 暗号化を利用してコンテンツのプライバシーを保護する正規のファイル共有サービスを使用して、悪意のあるコンテンツをホスティングするようになっています。これにより、マルウェアが完全に難読化され、ほとんどのネットワークで検知されずに侵入できるようになります。

検知を回避するために暗号化を利用するのはマルウェアだけではありません。スパイウェア、アドウェア、ブラウザのツールバーなどのリスクのあるアプリケーションや、ピアツーピアのファイル共有クライアント、プロキシ回避ツールなども、ファイアウォールでの検知を回避するために暗号化を利用しています。macOS プラットフォームで特にこの傾向が強く、C&C と通信する macOS の脅威の 89% 以上が、TLS を使用してコールホームを実行したり、追加の攻撃コードを取得したりしていることが判明しています。



ほとんどの組織はなす術がない

これまで見てきたように、TLS インスペクションは複雑であり、その処理に膨大なリソースを必要とします。ネットワークトラフィックの 90% 以上が暗号化される中で、この処理に対応できるファイアウォールはほとんどありません。

現在、ほとんどのファイアウォールには、適切な TLS インスペクション機能が実装されていません。検査の対象とする必要があるトラフィックをインテリジェントに選別できず、すべての暗号化トラフィックを解読する場合の膨大な負荷にも対応できません。また、パケット処理エンジンや DPI (ディープパケットインスペクション) エンジンは、TLS インスペクションを効率的に処理するように設計されていません。さらに、最新の規格に対応していないインスペクション機能を実装すると、セキュリティを低下させる結果となり、脆弱性が攻撃される恐れがあるだけでなく、ユーザー環境も悪化させることになります。

暗号化されたネットワークトラフィックが急増する一方で、多くの次世代ファイアウォールが暗号化トラフィックを検査できないことから、ネットワークセキュリティでは壊滅的な状況が発生しています。

次回購入するファイアウォールで確認すべき 5 つの機能

暗号化されたネットワークトラフィックによるリスクを最小限に抑えるために、今後購入するファイアウォールに以下の 5 つの TLS インスペクション機能が実装されていることを確認してください。

1. TLS 1.3 などの最新規格に対応し、すべてのポート / プロトコルを効果的に処理する最新で高性能なストリーミングインスペクションエンジンを搭載し、リスクのあるトラフィックや脅威を特定できること。
2. 検査を除外するトラフィックのリストがあらかじめ準備されており、動的に更新されること。これにより、復号化が不要なサイトやサービスのユーザーエクスペリエンスが損なわれることを防ぎます。
3. 暗号化されたトラフィックフローや、互換性のないサイトやサービスで発生する可能性のある問題をダッシュボードで確認でき、問題が発生する前にオンザフライで例外処理を追加できること。
4. 強力な証明書認証により、無効な証明書、自己署名証明書、失効した証明書、または信頼できない証明書を処理して、悪意のある中間者攻撃 (MITM) を回避できること。
5. ユーザープライバシー、組織のセキュリティ、ネットワークパフォーマンスなど、お客様のニーズに合わせて最適なバランスを組み立てることができるポリシーツールを利用できること。

Sophos Firewall - 暗号化された現在のインターネット環境のために設計されたファイアウォール

Sophos Firewall の革新的な Xstream アーキテクチャと XGS シリーズアプライアンスは、最高の TLS インスペクション機能をファイアウォールで利用できるようにします。また、パフォーマンスを犠牲にすることなく、TLS で暗号化されたトラフィックというセキュリティの盲点を解消します。

Sophos Firewall の利点：

- 高いパフォーマンス – 再設計された接続能力の高い軽量なストリーミングエンジン
- 暗号化されたトラフィックフローやエラーをわかりやすく可視化してダッシュボードに表示でき、2 回クリックするだけで例外処理を追加可能
- 最高のセキュリティ – TLS 1.3 および堅牢な証明書検証を備えたすべての最新の暗号スイートをサポート
- すべてのトラフィックの検査、アプリケーションやポートに依存しない
- 広範な除外リストを組み込んでおり、最適なパフォーマンスと広範な相互運用性と共に優れたユーザーエクスペリエンスを確保して、Web トラフィックへの影響を回避する
- 強力なポリシーツールを利用でき、パフォーマンス、プライバシー、セキュリティのバランスを完璧に実現

詳細については、Sophos Firewall のソリューション概説を参照してください。www.sophos.com/firewall にアクセスしてオンラインデモを簡単にご覧いただくこともできます。

ソフォス株式会社営業部
sales@sophos.co.jp

21-06-17 EN (DD)