HTTPS通信の可視化と高精度なWebフィルタリングによる検査

ALSI InterSafe WebFilterとA10のSSLインサイトソリューションの連携

課題：

- 増大するHTTPS通信に対する適切なアクセス制御
- HTTPS通信を悪用した脅威を検知するための高速なHTTPS通信の可視化とセキュリティの強化

解決策：

A10 ThunderのSSLインサイトソリューションによりHTTPS通信を高速に可視化（復号）し、アルプス システム インテグレーションのWebフィルタリングソフトウェアInterSafe WebFilterと連携することで、HTTPS通信の高速・高精度なWebフィルタリングを実現

メリット：

- 148カテゴリへの分類が可能で網羅率98%の国内最高水準の高精度URLデータベースを持つInterSafe WebFilterをHTTPS通信のWebフィルタリングに適用することでHTTPS通信に隠れた脅威を検知
- 大規模なセッションを処理可能なA10 ThunderによるHTTPS通信の高速な復号/再暗号化により高い通信パフォーマンスを維持
- 多様なセキュリティ機器との連携

常時HTTPS化の流れとHTTPS通信に潜む脅威

近年、多様化するサイバー犯罪への対処や情報機関からの盗聴、スヌーピングや改ざん、データの窃盗を防ぐために、主にWebサイトへのアクセスを中心に通信データの常時HTTPS化の流れが進んでいます。当初はクレジットカードでの取引やユーザーログイン情報など、機密性の高いデータ通信のみを暗号化していましたが、サーバー証明書の発行が容易になり、Webサイトの HTTPS化への対応度合いが検索サイトでのランキングに影響したり、ブラウザの表示にWebサイトの暗号化への対応状況が表示されるようになっていたり、多くのクラウドサービスがHTTPSでの接続を前提としていることから、今後通信プラットフォームを流れるほぼ全てのWebリクエストとレスポンスがHTTPS化されてくると考えられています。

その一方で、悪意のあるWebサイトがHTTPS化されていたり、HTTPSのポータルサイトに表示される広告にマルウェアが仕込まれたり、HTTPS通信を利用するSNSやクラウドストレージ経由でボット化したクライアントへの指令を行ったりするなど、HTTPS通信が情報漏えいの抜け道やサイバー攻撃の隠れ蓑として悪用されることも増えてきています。日々継続して新しくなるサイバー攻撃の手法に追従し、企業のセキュリティを担保するにはHTTPS通信に隠れた脅威の対策が必須となっています。

しかし、これまで導入されている多くのセキュリティ機器は暗号化トラフィックを検査できず、HTTPS通信を復号し検査できる数少ないセキュリティ機器も、多くの場合急増するHTTPS通信量のペースに追いつく性能を持っていません。Ponemon Institute社による2016年のレポート[*1]では、36%の組織しか暗号化通信の検査を行っておらず、暗号化通信の検査が行えない主な理由として、「暗号化通信を検査可能なセキュリティ機器がない」「リソースが不十分」「通信パフォーマンスの低下」の3点が挙げられています。

HTTPS通信の可視化：SSLインサイトソリューション

A10ネットワークスのA10 Thunderシリーズで利用できるSSLインサイトソリューションを利用することにより、HTTPS通信に隠れた脅威を可視化し、通信プラットフォームのパフォーマンスを落とすことなく、これまでに導入されているセキュリティ機器での脅威検知と防御を実現することができます。SSLインサイトソリューションはクライアントとインターネット間のHTTPS通信をはじめとするTLS/SSL通信をインターセプトし高速に復号します。復号したトラフィックをセキュリティ機器に送ることで、通信データに含まれる脅威の検査と分析をハイパフォーマンスで実現できます。トラフィックの分析が終了した通信データは再暗号化され、目的のアドレスに転送されます。

A10 ThunderによるSSLインサイトを導入する際には、Thunderアプライアンスを自組織の内部にあるクライアントとインターネットの間に設置する必要があります。平文化した通信データはインライン型・パッシブ型のセキュリティ機器に転送して検査することが出来るとともに、ICAPを通じて外部のICAPサーバーとの連携を行うことができます。

HTTPS通信の高精度なWebフィルタリング

A10ネットワークスのSSLインサイトとALSI InterSafe WebFilterとの連携

A10 ネットワークスは、HTTPS通信の高精度なWebフィルタリングを実現するために、アルプス システム インテグレーション株式会社（以下ALSI）と提携しました。A10 Thunderシリーズの提供するSSLインサイトソリューションにより復号したHTTPS通信をALSIの提供するWebフィルタリング製品であるInterSafe WebFilterで検査することで、HTTPS通信に対する高速・高精度なWebフィルタリングを実現できます。

ALSIのInterSafe WebFilterは、URLデータベースに基づいてWebアクセスをコントロールし、不正サイトへのアクセスや書き込みをブロックする法人向け国産Webフィルタリングソフトです。国内最大クラスの148カテゴリ、網羅率98%を有する高精度URLデータベースは大手携帯キャリア3社での採用をはじめ、日本国内での高いマーケットシェアを持ちます。さらに、未知のURLをクラウド上で判定する「高度分類クラウド」や国・地域別にアクセスを可視化する「Geoスコープ」により最新の脅威に対応し、安全なWebアクセス環境を実現します。

A10のSSLインサイトソリューションとALSI InterSafe WebFilterとの連携ソリューションを図1に示します。Thunderアプライアンスは企業の内部にあるクライアントとインターネットの間に設置し、クライアントからはプロキシサーバーとして指定する形になります。A10 ThunderはHTTP/HTTPS通信のフォワードプロキシとして動作しHTTP/HTTPS通信をインターセプトします。InterSafe WebFilterはICAP

*1 Hidden Threats in Encrypted Traffic: A Study of North America & EMEA, Ponemon Institute

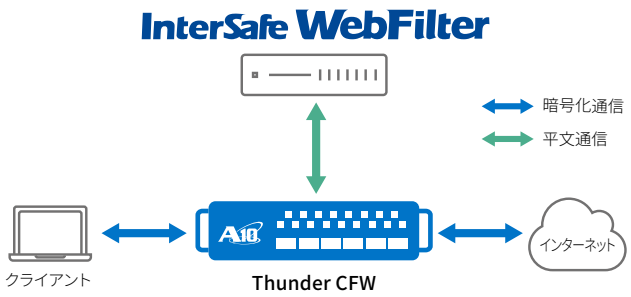

図1：A10 Thunderによる SSL インサイトソリューションと ALSI InterSafe WebFilter との連携

サーバーとして動作し、Thunder アプライアンスが ICAP クライアントとして動作することで、InterSafe WebFilter との通信を行います。この時の通信の流れは以下のようになります。

1. Thunder がクライアントから Web サーバーに向けた HTTP/HTTPS トラフィックをインターセプトし、HTTP の場合はそのまま、HTTPS の場合はトラフィックを復号して平文化したトラフィックを ICAP により InterSafe WebFilter に送信し、InterSafe WebFilter で HTTP/HTTPS 通信の Web フィルタリングを実施
2. InterSafe WebFilter から HTTP/HTTPS リクエストの送信可否を ICAP で Thunder に通知。アクセスをブロックする場合は InterSafe WebFilter の規制画面をクライアントに転送。
3. HTTP/HTTPS リクエストの送信が InterSafe WebFilter に許可された場合、平文化された HTTPS トラフィックを Thunder が再暗号化し Web サーバーにフォワード。HTTP トラフィックはそのままフォワード
4. Web サーバーはリクエストを受信し、レスポンスをクライアントに送信
5. HTTPS 通信の場合は Thunder が暗号化されたサーバーからのレスポンスをインターセプトし、一旦復号した後再暗号化しクライアントに送信

SSL/TLS 通信の特性上、リクエストの復号とレスポンスの再暗号化のためにはクライアントが Thunder を信頼できる必要があるため、Thunder にはクライアントが信頼できる証明書がインストールされている必要があります。Thunder には自組織の持つ任意の証明書をインストールして利用することが可能です。

HTTPS トラフィックに含まれるリクエスト内容を平文で InterSafe WebFilter に渡すことで、HTTP だけでなく HTTPS 通信に対しても専用のデータベースを利用し高度な Web フィルタリングを実現できます。クライアントと Thunder の間、および Thunder と Web サーバーとの間のコネクションは暗号化したまま保持されるため、なりすましやデータ窃盗は防止されます。

この構成でユーザー認証が必要な場合は、Thunder アプライアンスがプロキシサーバーとして動作しているため、ユーザー認証を Thunder 上で行う形を取ります。Thunder アプライアンスは認証サーバーと連携した各種認証方式に対応しています。認証したユーザー情報やクライアント IP の情報は InterSafe WebFilter に送信でき、ユーザーに応じた Web フィルタリングのルールを適用できます。

上記に加え、負荷分散機能を利用することで、複数の InterSafe WebFilter サーバーの利用も可能です。ある InterSafe WebFilter サーバーに障害が発生した場合には、冗長化された別の InterSafe WebFilter サーバーに通信データを送信でき、高可用性とスケーラビリティをともに実現できます。

その他の拡張機能

A10 ネットワークスの SSL インサイトソリューションでは、一度復号した TLS 通信をパッシブ型・インライン型の複数のデバイスに送信して検査することが可能なため、復号し平文化された HTTPS 通信をサンドボックス機器などにミラーポートを経由して渡すことで、クライアントとサーバー間で送受信される HTTPS トラフィックをともに検査できるようになります。この結果、特定サイトからのダウンロードに含まれるマルウェアなどの脅威を検知することができます。サンドボックス製品が InterSafe WebFilter と連携できる場合、情報が動的に連携され、悪意のあるサイトへのアクセスを遮断することも出来ます。

SSL インサイトソリューションは L2/L3 の多様なネットワーク構成に対応でき、既存のネットワーク環境に合わせた導入が可能です。必要な性能に応じ単一アプライアンスおよび複数アプライアンスでの導入ができ、冗長構成をとることで可用性も担保できます。サンドボックス製品などのパッシブ型の機器だけでなく、インライン型で導入されている次世代ファイアウォール機器や IPS/IDS、SIEM 製品やフォレンジック製品と連携した動作が可能です。

また、詳細なポリシー設定により、利用者はトラフィックの種類、発信元/宛先 IP アドレスやその他の属性に応じてどの暗号化セッションを復号して検査対象とするか、どのセッションを暗号化されたままにして検査対象から除外しておくかを制御することもできます。

特長とメリット

A10 ネットワークスの Thunder シリーズによる SSL インサイトソリューションと ALSI InterSafe WebFiliter の連携ソリューションのメリットは以下になります。

- 格段に優れた HTTPS コネクション数の処理能力とスループット（1 台で最大 25Gbps、2 台で最大 50Gbps）
- 全てのポートに渡る HTTPS トラフィックの復号
- 148 カテゴリへの分類が可能で 45 億超のコンテンツ・98% の網羅率を有する業界最高水準の Web フィルタリング製品である InterSafe WebFilter のデータベースを利用した HTTP/HTTPS 通信に対する Web フィルタリングの実現
- サンドボックス機器やファイアウォール機器などの複数セキュリティ製品への復号データの送信と負荷分散
- サンドボックス機器が検知した脅威に基づく InterSafe WebFilter での動的な Web フィルタリング
- 多様なネットワーク構成への対応と詳細なポリシー設定

結論

Web サービス・Web アプリケーションの常時 TLS 化が進むにつれ、HTTPS 通信が企業の防御にとって危険な盲点となりつつあります。高速な HTTPS 通信の可視化を実現できる、A10 Thunder シリーズの提供する SSL インサイトソリューションを、カテゴリ数、網羅率、精度ともに業界最高水準の Web フィルタリング製品である ALSI InterSafe WebFilter と共に利用することで、HTTPS 通信の高速・高精度な Web フィルタリングを実現し、HTTPS 通信に隠れた脅威に対する有効な防御を提供できます。また、SSL インサイトで復号したデータをサンドボックス機器などの他のセキュリティ製品で検査することにより、HTTPS 通信に含まれた未知の脅威の検出と InterSafe WebFilter との連携による動的なアクセス制限を行うこともでき、より効果的なセキュリティ強化が可能です。

アルプス システム インテグレーション株式会社について

アルプス システム インテグレーション株式会社（ALSI〔アルシー〕）は、グローバルに事業を展開するアルプス電気グループの IT 戦略会社です。セキュリティソリューション、製造業・流通業向け業務支援システム開発、ファームウェア開発、IoT ソリューションを展開しています。セキュリティソリューションでは、国内の草分けとして 1996 年より事業を開始した Web フィルタリングを中心とするアクセスマネージメントと、情報の保護と活用を両立する情報漏洩対策を両輪に、お客様に安心・安全を提供します。

A10ネットワークス株式会社

www.a10networks.co.jp
a10networks.co.jp/contact

Part Number: A10-SB ALSI InterSafe and A10 Oct 2018

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションを提供することを使命としています。詳しくはホームページをご覧ください。 www.a10networks.co.jp