

SSL インサイト機能搭載セキュア Web ゲートウェイ

Web アクセスの保護と SSL の盲点の排除

課題：

悪質なユーザーが SSL 暗号化を使用して攻撃を隠匿するため、組織には SSL トラフィックを復号化するための強力なハイパフォーマンスなプラットフォームが必要です。これにより、悪意ある Web サイトへのアクセスを制限できます。

ソリューション：

A10 Networks のセキュア Web ゲートウェイ機能は、SSL インサイト技術を搭載しています。組織は、SSL 通信をインターセプトして、ファイアウォールや脅威阻止プラットフォームなどのサードパーティー製セキュリティデバイスに転送し、検査することにより、望ましくないサイトへのアクセスをブロックしたり、暗号化されたデータを分析することが可能です。

利点：

- SSL トラフィックの高速な復号化により、企業防衛における盲点を排除
- 悪意ある Web サイトのブロックにより、マルウェア感染とフィッシング攻撃を防止
- 高度な脅威の検出により、大きな損失をもたらすデータ漏えいや知的財産の喪失を阻止
- 複数のサードパーティーセキュリティアプライアンスの負荷分散により、アップタイムを最大化

攻撃や侵入、マルウェアへの感染を防止するために、企業は送受信するトラフィックに脅威が含まれているかどうかを検査する必要があります。残念なことに、攻撃者が検知を逃れるために SSL 暗号を利用するケースが増加しています。SSL をサポートするアプリケーションがますます増加する中で（2016 年までに SSL 通信はインターネットトラフィックの 67% を占めると予測されています¹）、SSL 暗号は単に企業の防御壁でよく知られた抜け穴であるというより、悪質な攻撃者に悪用される巨大な穴を意味しています。

課題

セキュリティデバイスによる検知を回避するために SSL が多用されつつある状況は、企業防御のすきを露呈させます。組織では、トラフィックの検査、侵入のブロック、マルウェアの阻止、ユーザーがアクセスするアプリケーションの制御のために、非常に多くのセキュリティ製品群を活用しています。組織内のユーザーを保護するために、これらの製品はプレーンテキストのトラフィックだけでなく、すべての通信を検査しなければなりません。残念ながら、多くのファイアウォールや侵入防止製品、脅威阻止プラットフォームは、増大する SSL 暗号化の要求に追従できていません。

NSS Labs は、発行したレポート『SSL Performance Problems』で、次世代ファイアウォールベンダーの主要 8 社が 2048 ビット暗号化トラフィックの復号化の際に大幅なパフォーマンス低下を経験したことを発表しました。そのため NSS Labs は、「専用 SSL 復号化デバイスを使用しない企業ネットワークの SSL 検査の実行可能性を懸念する」と論じています。²

企業では、電子メール、CRM、ビジネスインテリジェンス、ファイルストレージなどの重要なアプリケーションをクラウドに移行していますが、社内でも運用しているアプリケーションと同様にこれらのアプリケーションを監視して保護する必要があります。このようなクラウドベースアプリケーションの多くは SSL を使用しており、その結果として組織の防御の大きな穴が露呈されています。エンドツーエンドのセキュリティを確保するために、組織では内部ユーザーからの送信 SSL トラフィックと、外部ユーザーから企業所有のアプリケーションサーバーへの受信 SSL トラフィックを検査し、企業防御の盲点を排除しなければなりません。

¹ 「Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report」、2015 年 5 月

² NSS Labs、「SSL Performance Problems」、<https://www.nsslabs.com/reports/ssl-performance-problems>

A10 NetworksのSSLインサイト機能付きセキュアWebゲートウェイソリューション

高速なSSL復号化

A10 Networks®のSSLインサイト機能を包含したセキュアWebゲートウェイは、SSL暗号化によって生じる盲点を排除して、CPUを集中的に使用するSSL復号化機能を代わりに実行します。この機能によって、セキュリティデバイスはプレーンテキストだけでなく、暗号化されたトラフィックも検査することが可能になります。A10 Networks Thunder® CFW製品ラインに標準装備されているセキュアWebゲートウェイ機能は、SSL暗号化トラフィックを復号化して、ファイアウォールなどのサードパーティー製セキュリティデバイスにDPI(ディープパケットインスペクション)のために転送します。トラフィックの分析とクリーンアップが終了すると、セキュアWebゲートウェイはそのトラフィックを再び暗号化して目的の宛先に転送します。

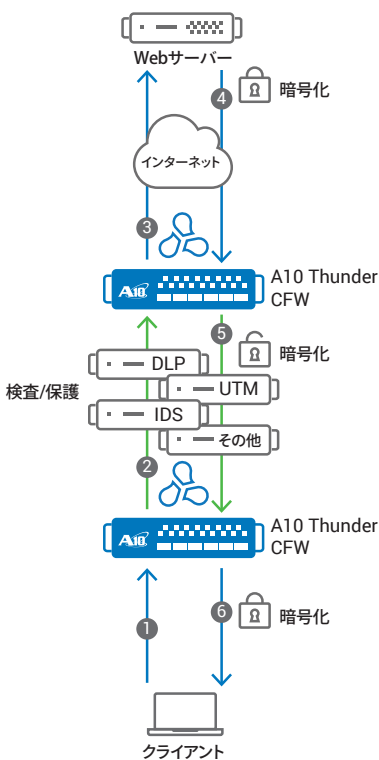


図1: Thunder CFWを利用したWebからの脅威に対する内部ユーザーの保護。

SSLインサイトのトラフィックフロー

- 1 クライアントから送信された暗号化トラフィックが、内部のクライアント側Thunder CFWによって復号化される。
- 2 Thunder CFWが暗号化されていないデータをセキュリティアプライアンスに送信し、アプライアンスがプレーンテキスト形式のデータを検査する。
- 3 外部のThunder CFWがデータを再度暗号化し、サーバーに送信する。
- 4 サーバーが暗号化された応答を外部のThunder CFWに送信する。
- 5 Thunder CFWが応答を復号化し、検査のためセキュリティデバイスへ転送する。
- 6 内部のThunder CFWがセキュリティデバイスからトラフィックを受信し、再度暗号化してクライアントに送信する。

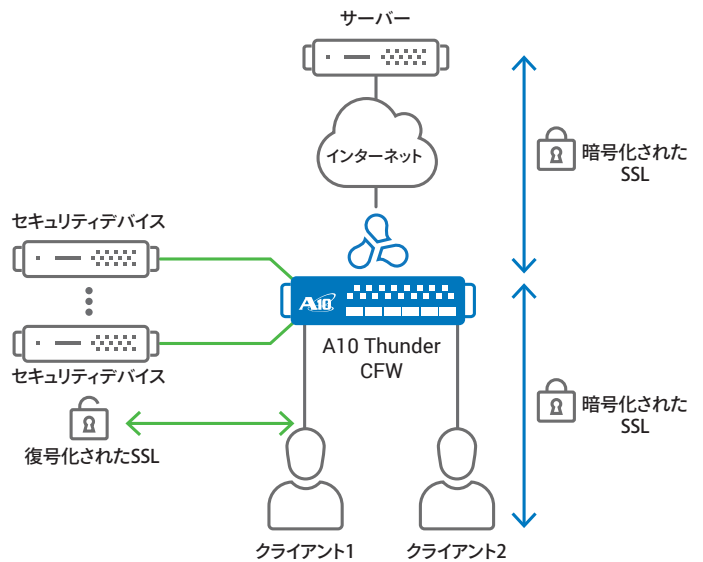


図2: Thunder CFWは、トラフィックを復号化し、非インラインにパッシブモードで導入されているセキュリティデバイスに転送可能。

組織では、インラインへの導入に加え、侵入検知システムやフォレンジックツールなどのセキュリティデバイスをパッシブモードで導入できます。セキュアWebゲートウェイとSSLインサイトの組み合わせは、SSLトラフィックを復号化し、暗号化されていないトラフィックのコピーを非インラインのセキュリティデバイスに転送して検査します。パッシブモードでは、ネットワークに変更を加えたりネットワークにSPOF(Single Point of Failure: 単一障害点)を生じさせたりすることなく、セキュリティデバイスを本番環境に簡単に統合できます。攻撃をアクティブにブロックするのではなく、イベントの検査、アラート、レポート作成を行うセキュリティデバイスについては、非インラインの導入が理想的です。

復号化と分析の一元管理ポイント

組織の多くは、アプリケーションの分析とフィルタリングを行うために複数のセキュリティソリューションを導入しています。セキュアWebゲートウェイとSSLインサイトの組み合わせは、SSLトラフィックを復号化してプレーンテキストで複数のデバイスに送信する一元管理ポイントを提供するため、トラフィックを何度も復号化する必要がなくなります。セキュアWebゲートウェイは以下のセキュリティデバイスと連携して動作可能です。

- ファイアウォール
- 侵入防止システム(IPS)
- 統合脅威管理(UTM)プラットフォーム
- データ損失防止(DLP)製品
- 脅威阻止プラットフォーム
- ネットワークフォレンジックおよびWeb監視ツール

多くのセキュリティデバイスは、インラインでの導入や高速なSSL復号化を考慮して設計されていません。Thunder CFWのセキュアWebゲートウェイとSSLインサイトの組み合わせを導入することによって、これらのデバイスは、多大なコンピューティング能力を消費するSSL処理を負担することなく、SSL暗号化データを検査できるようになります。トラフィックは、Thunder CFWで一度復号化されたあと、多くのインラインおよび非インラインのセキュリティデバイスに転送することができます。

包括的で拡張性の高い管理

管理を効率化および自動化するために、Thunder CFWは、業界標準のCLI、Webユーザーインターフェイス、およびサードパーティー製またはカスタムの管理コンソールと統合できるA10 Networks aXAPI® RESTベースAPIを備えています。大規模な導入の場合はA10 NetworksのaGalaxy®集中管理システムを使用して、物理的な場所にかかわらず、複数のThunder CFWアプライアンスで日常的なタスクを広範囲にわたって実行できます。

ロギングおよびレポート作成

Thunder CFWは、トラフィック分析のための高速syslogロギングに加えて、電子メールによるアラートや、トラフィック分析のためのNetFlowとsFlowの統計情報をサポートしています。Thunder CFWのWebユーザーインターフェイス上のダッシュボードには、システム情報、メモリーとCPUの使用率、ネットワークステータスがリアルタイムに表示されます。

機能と利点

利点

Thunder CFWのセキュアWebゲートウェイを使用すると、組織では以下のことが可能になります。

- **SSL高速化ハードウェアによるハイパフォーマンスの実現**
– A10 Thunder CFWに搭載されている強力な専用SSLセキュリティプロセッサは、1秒あたり数十万件のSSLハンドシェイクを処理できる拡張性を備えています。Thunder CFWはSSL高速化ハードウェアを搭載しており、1024ビットと2048ビットの鍵長でほぼ同等のパフォーマンスを発揮し、本番環境レベルで4096ビット鍵を高性能に処理できる非常に強力なパワーを有しています。
- **悪質なWebサイトのブロックと機密性の高いアプリケーションのバイパス** – コンプライアンス要件の遵守やデータプライバシーの確保のため、金融アプリケーションや医療アプリケーションなどに送信されるトラフィックなど信頼できる通信はSSL通信可視化の対象外とすることができます。オプションのURL分類サブスクリプションを利用することで、Thunder CFWは4億6000万ドメインのトラフィックを分類できるようになり、機密データを確実に暗号化した状態に維持することができます。このURL分類サブスクリプションにより、従業員の生産性を最大限に高めることができるとともに、マルウェアサイト、スパムサイト、フィッシングサイトなどの悪質なWebサイトへのアクセスをブロックしてセキュリティリスクを低減することができます。³
- **負荷分散によるセキュリティ機能の拡張** – SSL暗号処理のオフロードに加え、Thunder CFWは複数のファイアウォールやその他のセキュリティデバイスの負荷を分散できます。Thunder CFWを高可用性(HA)構成で導入すると、複数のセキュリティデバイスの負荷を分散できるほか、各接続を追跡して、要求と応答を確実に同一のデバイスに送信できます。
- **どの種類のトラフィックを復号化するかを制御してセキュリティインフラストラクチャーへの負荷を低減** – Thunder CFWは、アプリケーションの種類に基づくきめ細かいポリシーに従い、トラフィックを選択的にセキュリティデバイスとセキュリティサービスチェーンにリダイレクトできます。たとえば、Thunder CFWは電子メールトラフィックとWebトラフィックを復号化して脅威阻止プラットフォームに転送する一方で、他のタイプのトラフィックの負荷がこのデバイスにかかることを防止できます。

- **aFleXポリシーによるきめ細かいトラフィック制御**
– A10 Networks aFleX® TCLスクリプティングテクノロジーにより、リクエストの検査、更新、変更、破棄が可能です。aFleXスクリプティングを使用すると、どのトラフィックをインターセプトしてサードパーティー製セキュリティデバイスに転送するのか、どのトラフィックをクリーンアップしてから目的の宛先に転送するのかを完全に制御できます。aFleX TCLスクリプティングによってアプリケーショントラフィックの完全な制御が可能になるため、ほぼすべての種類のアプリケーションの課題を解決できます。

機能³

SSLインサイト機能付きセキュアWebゲートウェイ:

- WebrootをベースにしたURL分類サービスにより、特定のWebサイトを監視、ブロック、または選択的にバイパス(URL分類サービスを使用するにはサブスクリプションライセンスが必要⁴)
- ホスト名によるSSLインサイトのバイパスにより、バイパスリストは最大100万のServer Name Indication(SNI)値まで拡張可能
- マルチバイパスリストのサポート
- HTTPS、SMTP、XMPPの復号化
- 幅広い暗号化方式とプロトコルのサポート(TLS 1.0、TLS 1.1、TLS 1.2、SSLv3)。Perfect Forward Secrecy(PFS)をサポートしたRSA、DHE、ECDHE暗号化方式。SHA、SHA-2、MD5ハッシュングアルゴリズム
- クライアント証明書の検知と迂回(オプション)
- 信頼されていない証明書をOnline Certificate Status Protocol(OCSP)で処理
- SSLインサイトイベントからのフロー情報を記録するTLSアラートロギング
- フォワードプロキシフェイルセーフにより、ハンドシェイクが失敗した場合にトラフィックを迂回
- TCPの上位層で動作しているプロトコルに関係なく、SSLまたはTLSのトラフィックを検知およびインターセプトする動的ポート復号化
- SSLセッションIDの再利用

アプリケーション配信:

- 高度なレイヤー4/レイヤー7サーバーロードバランシング
- aFleX TCLスクリプティング - カスタマイズ可能なアプリケーション対応スイッチングのためのディープパケットインスペクションと変換をサポート
- アクティブ-アクティブ構成とアクティブ-スタンバイ構成をサポートする高可用性
- ファイアウォールロードバランシング(FWLB)

導入:

- パッシブな非インラインサードパーティーデバイスとともにインラインの透過的プロキシまたは明示的プロキシとして導入
- アクティブなインラインサードパーティーデバイスとともにインラインの透過的プロキシまたは明示的プロキシとして導入
- ICAP接続デバイスとともに、インラインの透過的なプロキシまたは明示的なプロキシとして導入

³ 利用可能な機能はアプライアンスモデルによって異なります。機能と認定の完全なリストについては、Thunder CFWのデータシートを参照してください。

⁴ URL分類サブスクリプションによる機密性の高いWebサイトのバイパス機能は、Advance Core Operating System(ACOS®) 4.0.1で利用可能です。URLフィルタリングは、ACOS 4.1.0でサポートされています。

管理:

- 専用管理インターフェイス (コンソール、SSH、telnet、HTTPS)
- 日本語対応 Web ベース GUI
- 業界標準のコマンドラインインターフェイス (CLI)
- SNMP、システムロギング、電子メールアラート、NetFlow v9およびv10 (IPFIX)、sFlow
- ポートミラーリング
- REST スタイル XML API (aXAPI)
- LDAP、TACACS+、RADIUS のサポート

キャリアグレードハードウェア:

- ハイパフォーマンスを実現する専用 SSL セキュリティプロセッサ
- 40 GbE ポートと 100 GbE ポート
- 改ざん検知
- 非インラインの導入では、トラフィックフローをトラフィックタイプごとにセグメント化し、最大 4 つのネットワークインターフェイスにブロードキャストできるため、関連するトラフィックのフィルタリングやセキュリティ環境のスケールアウトが可能
- インライン導入では、A10 Thunder CFW は SSL 復号化機能をオフロードし、複数のセキュリティデバイスの負荷を分散可能
- セキュリティおよび機能の保証

認定:

- Common Criteria EAL 2+
- FIPS 140-2 Level 2
- 統合運用テストコマンド (JITC: Joint Interoperability Test Command)

ソリューションのコンポーネント

- SSL インサイト機能を含む Thunder CFW のセキュア Web ゲートウェイ機能
- aGalaxy® 集中管理システム
- aFlex TCL スクリプティングテクノロジー
- aXAPI® REST ベース API

まとめ - Web アクセスの保護と SSL の盲点の排除

Thunder CFW のセキュア Web ゲートウェイ機能は、SSL インサイト機能を包含し、強力なロードバランシング、URL フィルタリング、および SSL 復号化を実現するソリューションを提供します。SSL インサイト機能によって、次のことが可能です。

- 暗号化データを含むすべてのネットワークデータの分析と、徹底した脅威対策の実施
- 84 以上の URL 分類カテゴリーに基づく Web アクセスの監視および制御
- 業界最高レベルのコンテンツ検査ソリューションによる、サイバー攻撃の回避

Thunder CFW を使用すると、次のことが可能です。

- A10 の 64 ビット ACOS (Advanced Core Operating System) プラットフォーム、Flexible Traffic Acceleration (FTA) テクノロジー、専用セキュリティプロセッサを活用した、企業ネットワークのパフォーマンス、可用性、拡張性の最大化
- SSL 利用の拡大や 2048 ビットおよび 4096 ビット SSL 鍵を含むより高度な暗号化標準の利用を視野に入れた、将来を見据えた投資
- トラフィックを復号化して複数の検査デバイスに転送する、復号化とセキュリティの一元管理ポイントの提供

次のステップ

詳細については、A10 の営業窓口にお問い合わせいただくか、http://www.a10networks.co.jp/lp_thunder-cfw/ を参照してください。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE: ATEN) はアプリケーションネットワークングおよびセキュリティ分野におけるリーダーとして、高性能なアプリケーションネットワーク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クングソリューションをご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

Facebook: <http://www.facebook.com/A10networksjapan>

A10 ネットワークス株式会社

〒105-0001
東京都港区虎ノ門 4-3-20
神谷町 MTビル 16 階
TEL: 03-5777-1995
FAX: 03-5777-1997
jin@10networks.com
www.a10networks.co.jp

海外拠点

北米 (A10 Networks 本社)
sales@a10networks.com

ヨーロッパ
emea_sales@a10networks.com

南米
latam_sales@a10networks.com

中国
china_sales@a10networks.com

香港
HongKong@a10networks.com

台湾
taiwan@a10networks.com

韓国
korea@a10networks.com

南アジア
SouthAsia@a10networks.com

オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化する A10 のアプリケーションサービスゲートウェイ、Thunder の詳細は、A10 ネットワークスの Web サイト www.a10networks.co.jp をご覧ください。A10 の営業担当者にご連絡ください。

Part Number: A10-SB-19154-JA-01
June 2016

©2016 A10 Networks, Inc. All rights reserved. A10 Networks、A10 Networks ロゴ、ACOS、Thunder および SSL Insight は米国およびその他の各国における A10 Networks, Inc. の商標または登録商標です。その他の商標はそれぞれの所有者の資産です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標については詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks