

Cisco FirePOWER / Cisco ASA と SSL インサイトの連携

SSL トラフィックに隠れたサイバー攻撃を検知

課題：

SSL 通信に隠れた攻撃を防御するため、Cisco FirePOWER や Cisco ASA は暗号化通信の完全な可視化が必要

ソリューション：

A10 Thunder CFW/SSLi は、SSL 通信をインターセプトし、復号化処理後のトラフィックを Cisco FirePOWER や Cisco ASA に送信して脅威検知・防御を行うことで、Cisco の顧客の防御における SSL の盲点を排除

利点：

- 暗号化通信内の脅威を検知するための SSL 通信の高速な復号化処理
- リアルタイムでのコンテキストアウェアネスとフルスタック可視化の統合によるデータ漏えいの防止
- コンピューター・モバイルデバイス・仮想化環境のマルウェアからの防御
- クラス最良の負荷分散とクラスターリングによる稼働時間とスケーラビリティの最大化



A10 Networks と Cisco は、暗号化トラフィックに隠れた悪意のある攻撃をパフォーマンス影響なく検出・抑止するための連携を共に進めています。A10 Thunder CFW/SSLi シリーズは SSL トラフィックをインターセプトし、復号化処理されたデータを Cisco FirePOWER や Cisco ASA に送ることで、それらの脅威を検出しブロックします。これにより暗号化トラフィックも含めた完全なネットワーク活動の可視化、攻撃と侵入の検知、コンピューター・モバイルデバイス・仮想化環境のマルウェアからの防御が実現され、安全でセキュアな環境をユーザーに提供することができます。

課題

暗号化により生じる防御の盲点

セキュリティとプライバシーの懸念により SSL 暗号化の適用が進んでいます。ほんの数年前は、ほとんどの Web アプリケーションはクレジットカード番号やユーザーログイン情報などの重要なコミュニケーションのみを暗号化していました。今日では、多くの有名な Web サイトは全ての Web リクエストとレスポンスを暗号化しています。実際、2016 年中にはインターネットトラフィックの 3 分の 2 が暗号化されると予測されています¹。

アプリケーションとデータを守るために、暗号化されたトラフィックも含め、組織は全てのトラフィックを検査しなくてはなりません。残念ながら、多くのセキュリティデバイスは暗号化されたトラフィックを検査することができず、また SSL 通信およびその後継である TLS 通信を復号化処理できるいくつかのデバイスも、急増する帯域幅に対応できていません。これにより、企業の防御において、危険なギャップと盲点が生じています。

A10 Networks の SSL インサイトソリューション

暗号化トラフィックに隠れた脅威を暴く

A10 Networks は Cisco のパートナーとして、暗号化トラフィックに隠れた攻撃を効果的に阻止します。Cisco のネットワークセキュリティソリューションはリアルタイムでのコンテキストアウェアネス、フルスタックでの可視化、インテリジェントなセキュリティの自動化を統合的に提供しています。次世代 IPS (侵入防御システム) の Cisco FirePOWER と Cisco ASA ファイアウォールは共に、様々な規模の企業のネットワークとデータセンターを防御します。

A10 Thunder CFW または SSLi との接続により、Cisco のネットワークセキュリティソリューションは洗練化された脅威や高度化したマルウェアを可視化し、阻止できるようになります。A10 Thunder CFW/SSLi が SSL/TLS 通信を復号化処理することで、Cisco のネットワークセキュリティソリューションにより全てのコミュニケーション、ユーザー、アプリケーション、デバイスを検査し脅威を検知できるようになります。

¹ 「Global Internet Phenomena Spotlight, Sandvine」2015 年

A10 Thunder CFW/SSLiは先進的で高性能なSSLインサイトテクノロジーを提供し、SSLトラフィックを復号化処理し、復号化処理されたトラフィックをCisco FirePOWERやCisco ASAに送信し検査します。その後、再度トラフィックを暗号化し意図した送信先に送信します。A10のSSLインサイトテクノロジーにより、計算量のかかるSSL暗号化・復号化処理の必要なく、Ciscoの機器のキャパシティをネットワークトラフィックの防御のために100%利用することができます。

Thunder CFW/SSLiはSSLトラフィックをインターセプトするために、透過型のSSLプロキシとして機能します。クライアントやサーバーからは、クライアントのネットワーク内のみで復号化処理された、エンドツーエンドの暗号化されたセッションが存在するよう見えます。SSLアクセラレーションハードウェアにより、Thunder CFW/SSLiは2048ビットや4096ビットの暗号化キーであっても高性能な処理を実現します。

セキュリティキャパシティのスケールと統合化された負荷分散

負荷分散機能により、Thunder CFW/SSLiは高可用性とスケーラビリティを提供し、複数のCisco FirePOWERやCisco ASAの導入を可能にします。加えて、セキュリティ機器の追加によるトラフィック増加への対応など、容易なセキュリティキャパシティの増強を可能にします。

Thunder CFW/SSLiはラウンドロビン・重み付きラウンドロビン・最少コネクション数や最短応答速度などに基づく多様な負荷分散アルゴリズムをサポートし、Ciscoのセキュリティ機器の導入におけるスケーラビリティを確保し、帯域幅の増加への対応を容易にします。

先進的なヘルスチェックによりCiscoのセキュリティ機器が予期した通りの応答をしているかを検知し、利用可能なセキュリティ機器に対してトラフィックを送信します。スクリプティング可能なヘルスチェックにより、Thunder CFW/SSLiは、幅広い基準に基づき複数セキュリティ機器の応答を評価し、パフォーマンスに見合った最適のセキュリティ機器にトラフィックを送信することで、低レイテンシーでの処理を実現できます。

境界の防御とデータセンターでのシナリオ

Ciscoのセキュリティ機器とA10 Thunder CFW/SSLiは様々なユースケースやセキュリティの要望に応じた様々な形態で導入できます。最大の効果を得るために、CiscoとA10 Networksの機器により、企業の所有するサーバーへのインバウンドのトラフィックとユーザーからのアウトバウンドトラフィックの双方をセキュアにすることができます。

典型的なシナリオでは、高可用性の設定がされた一組のThunder CFW/SSLiアプライアンスがSSLトラフィックを復号化処理し、多層防御のためにCisco FirePOWERやCisco ASAに転送し、検査後のトラフィックをThunder CFW/SSLiで再暗号化して宛先に送信します。図1に示すように、各SSLセッションに対し以下の処理を行います。

1. A10 Thunder CFW/SSLiアプライアンスがSSLトラフィックを復号化処理し1台もしくは複数のCiscoのセキュリティ機器に送信
2. Ciscoのセキュリティ機器が悪意のある活動を検知するためにトラフィックを検査し、トラフィックがセキュリティポリシーを侵害していないければA10 Thunder CFW/SSLiに送信
3. A10 Thunder CFW/SSLiがデータを暗号化し目的のサーバー/クライアントに送信

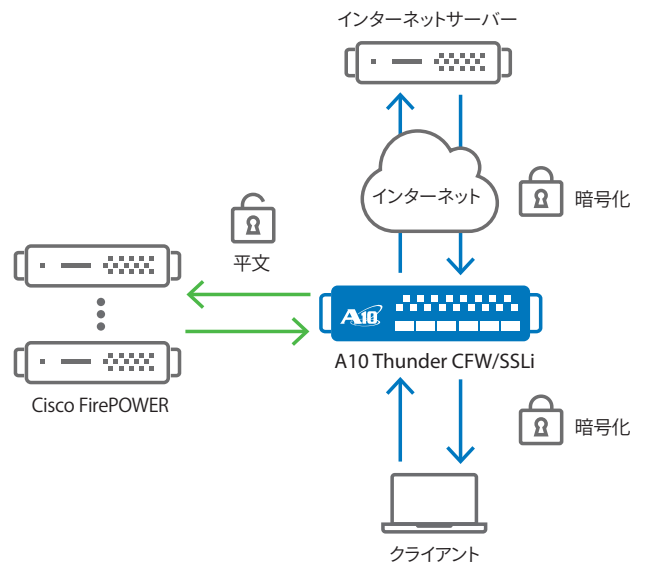


図1: Ciscoセキュリティ機器とA10 Thunder CFW/SSLiの連携

強力なSSLセキュリティプロセッサによる高性能処理

SSLハンドシェイク処理はSSL暗号化において最も計算量を要する部分になります。また、セッションにおけるデータの暗号化と復号化もCPUでの処理を要します。A10 Thunder CFW/SSLiは多数のセキュアコネクションを同時に処理できるよう設計されています。アプリケーションデリバリーコントローラーに初めてSSLインサイトテクノロジーを導入したA10 Networksは、並外れたSSLコネクション数とスループットを提供します。

A10 Networksの64ビットのAdvanced Core Operating System (ACOS)により、Thunder CFW/SSLiは汎用CPUと専用セキュリティプロセッサから得られる最大のパフォーマンスと線形のスケーラビリティを提供します。専用の高性能セキュリティプロセッサにより、多数のSSLセッションを同時に処理することができます。

特長とメリット

Cisco FirePOWERおよびCisco ASAとSSLインサイトテクノロジーの連携には、以下の特長とメリットがあります。

- 暗号化トラフィックに隠れた脅威を検知するための高性能なSSL復号化処理
- リアルタイムでのコンテキストアウェアネスとフルスタック可視化の統合によるデータ漏えいの防止
- マルウェアからのコンピューター・モバイルデバイス・仮想化環境の防御
- クラス最良の負荷分散とクラスターリングによる稼働時間とスケーラビリティの最大化

A10 Thunder CFW/SSLiに標準で含まれる強力なSSLインサイト機能により、以下が実現されます。

- 暗号化通信も含めたネットワーク通信の完全な可視化、攻撃や侵入の検知、安全でセキュアなユーザー経験
- Thunder CFW/SSLiを負荷分散と復号化処理の集約ポイントとして利用することによる、インターセプトしたSSL通信のセキュリティ分析・情報漏えい防止 (Data Loss Prevention: DLP) ・脅威防御や侵入検知機器などの複数のセキュリティ機器での検査
- 銀行や健康に関するデータなどの機微なトラフィックに対して復号化処理をせずバイパスすることも可能
- 暗号化キー長の増大やSSL通信の利用拡大に対する投資の保護

結論

データを暗号化するアプリケーションの数が増えるにつれ、SSLが企業の防御における危険な盲点となってきます。A10 Thunder CFW/SSLiとCisco FirePOWERおよびCisco ASAの連携により、暗号化通信をインターセプトし安全性を確保するための、理想的で容易に導入できる、スケーラブルなソリューションが提供されます。A10 NetworksではA10 Thunder CFW/SSLiとCiscoのネットワークセキュリティソリューションの相互接続性について動作検証を済ませています。

A10のSSLインサイトを利用することで、以下が実現できます。

- A10の64ビットACOSと専用セキュリティプロセッサによるパフォーマンス・可用性・スケーラビリティの最大化
- サイバー攻撃とマルウェアを検知し防御するためのCisco FirePOWERやCisco ASAなどの先進的ネットワークプラットフォームとThunder CFW/SSLiの統合
- 先進的な脅威からネットワークを防御するための統合されたリアルタイムの Awareness とインテリジェントなセキュリティの自動化

次のステップ

詳細については、A10の営業窓口にお問合せいただくか、
<http://www.a10networks.co.jp/products/thunderseries/thunder-SSLi.html>
をご覧ください。

シスコシステムズ合同会社について

シスコシステムズ合同会社は、米国シスコ (NASDAQ: CSCO) の日本法人です。シスコは、ビジネスの基盤となるインテリジェントなネットワークングソリューションから、音声、映像、データ、ストレージ、セキュリティ、エンターテインメントをはじめとする新しい分野、そして、人々の仕事や生活、娯楽、学習のあり方を一変させることのできるネットワーク プラットフォームの提案を目指しています。シスコの会社概要・詳細は以下のWebサイトでご参照頂けます。

<http://www.cisco.com/jp>

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
jinfo@a10networks.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-19149-JA-02
May 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。商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks