SSLインサイト

暗号化トラフィックに隠された脅威を発見

課題:

悪意ある利用者はSSL暗号化を使用して攻撃を隠匿。組織はSSLトラフィックを復号化することのできる強力でハイパフォーマンスなプラットフォームが必要。

解決策:

A10ネットワークスの製品により、SSL通信をインターセプトし、ファイアウォールなどの他社製セキュリティデバイスや脅威防御プラットフォーム、フォレンジックツールなどに送信して検査できるため、すべてのデータを分析可能

メリット:

- SSLトラフィックを高速に復号化することにより、企業防御の盲点を排除
- 高度な脅威を検知して、高額なコストがかかるデータ侵害と知的所有権の損失を防止
- 複数の他社製セキュリティアプライアンスの負荷を分散し、アップタイムを最大化
- パフォーマンスとスループットを向上し、サイバー攻撃からの防御を成功

SSL暗号化の課題

攻撃、侵入、マルウェアを阻止するために、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。残念ながら、攻撃者は検知を逃れるためにますます頻繁に暗号化を利用しています。SSLをサポートするアプリケーションは増加を続けていますが（実際、SSLはすべてのインターネットトラフィックの25～35%を占めています[1]）、SSLは企業の防御における些細な隙間としてよく知られているだけでなく、悪意ある攻撃者が悪用する可能性のある巨大な穴でもあるのです。

SSLの使用によって企業防御の盲点が明らかに

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可能な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、これらの製品は平文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。

残念なことに、多くのファイアウォール、侵入防止、脅威防止の各製品は増大するSSL暗号化の要求に追随できていません。NIST（米連邦情報技術局）のSpecial Publication 800-131Aによって拍車がかかった1024ビットから2048ビットのSSL暗号への移行により、セキュリティデバイスに負担がかかっています。2048ビットの証明書の復号化には、1024ビットの証明書の約6.3倍の処理能力が必要なのです[2]。SSL証明書の鍵長が長くなり続け、ある認証機関ではすべての証明書の20%が4096ビットの鍵長になっていますが[3]、多くのセキュリティデバイスはこうした復号化の要求に対応することができません。

NSS Labsは、発行したレポート『SSL Performance Problems（SSLパフォーマンスの問題）』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。[4]

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、社内でホストするアプリケーションと同様にこうしたアプリケーションを監視し、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、組織の防御の大きな欠陥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。

SSLインサイトを利用した高速なSSL復号化

A10 Networks® Thunder™ ADC製品ラインのSSLインサイト機能により、SSL暗号化によって生まれる盲点を排除できます。CPUを集中的に使用するSSL復号化がオフロードされるため、セキュリティデバイスは平文だけでなく、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。Thunder ADC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他社製セキュリティデバイスに転送しDPI（ディープパケットインスペクション）を行います。トラフィックの分析とクリーンアップが終了すると、Thunder ADCは再びトラフィックを暗号化して目的の宛先に転送します。

[1] NSS Labs、「SSL Performance Problems」、https://www.nsslabs.com/reports/ssl-performance-problems
[2] StackExchangeの分析によると、2048ビットRSA認定はコモディティハードウェア上で復号化に1024ビットRSAの6.3倍、暗号化に3.4倍多くの処理能力を必要とする。
[3] NetCraft SSL Survey、2013年5月、http://www.netcraft.com/internet-data-mining/ssl-survey/
[4] NSS Labs、「SSL Performance Problems」、https://www.nsslabs.com/reports/ssl-performance-problems

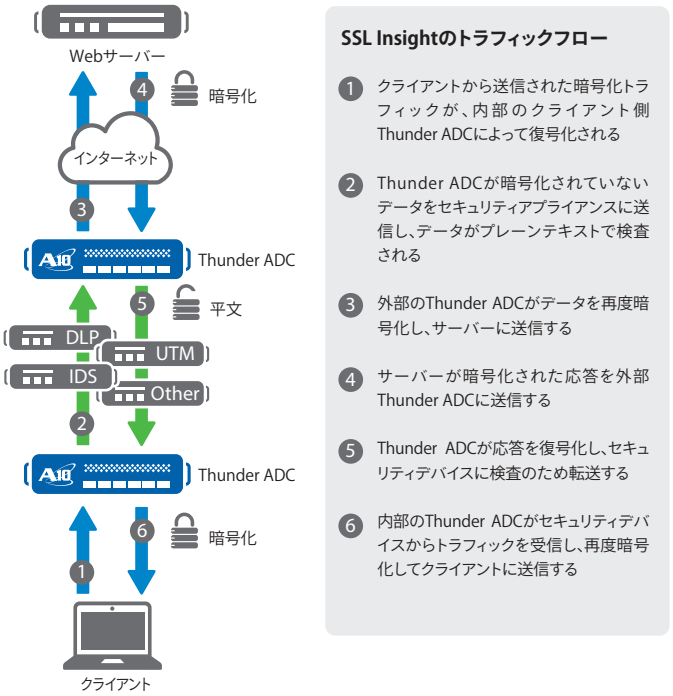

図1：Thunder ADCを利用したWebからの脅威に対する内部ユーザーの保護

SSLトラフィックを完全に可視化

専用セキュリティデバイスはネットワークトラフィックの詳細な検査および分析機能は提供しますが、そのほとんどは高速でSSLトラフィックを暗号化できるように設計されていません。実際、一部のセキュリティ製品はSSLトラフィックを一切復号化できません。A10 Thunder ADCに標準で装備されているSSLインサイト機能は、CPUを集中的に使用する暗号化および復号化タスクを専用セキュリティデバイスからオフロードし、アプリケーションのパフォーマンスを高めます。

Thunder ADCは、SSLトラフィックをインターセプトするSSLフォワードプロキシーとして機能します。組織はThunder ADCアプライアンスを導入するだけで、通信を効率的に保護できます。

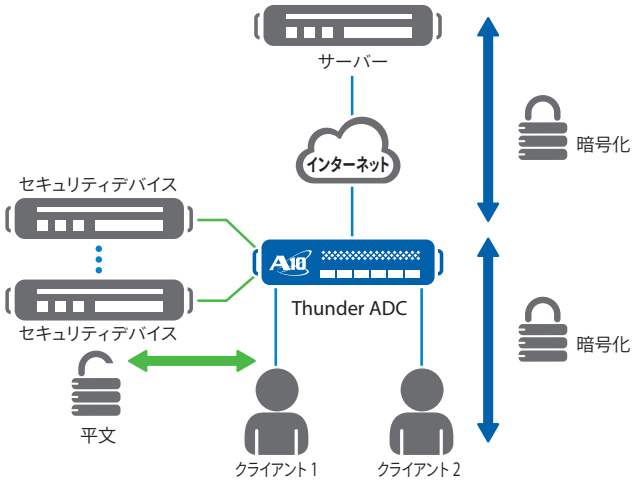

図2：Thunder ADCは、トラフィックを復号化し、非インラインにパッシブモードで導入されているセキュリティデバイスに転送可能

組織では、インラインでの導入に加え、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。Thunder ADC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検査のために非インラインのセキュリティデバイスに転送します。パッシブモードのセキュリティデバイスは、ネットワークへの変更やネットワークへの単一障害点の追加を伴わずに、本番環境に容易に統合できます。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は、非インラインへの導入が理想的です。

SSLインサイトを利用すると、次のことが可能になります。

- **SSL高速化ハードウェアを利用して高いハイパフォーマンスを実現**
  – A10 Thunder ADCは強力な専用SSLセキュリティプロセッサーを装備しており、1秒あたり最大174,000回の2048ビットSSLハンドシェイクを実行できるように拡張可能です。SSL高速化ハードウェアを備えたThunder ADCは、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提供し、ハイパフォーマンスの本番環境レベルで4096ビット鍵を処理できる非常に強力なパワーを有しています。

- **負荷分散によりセキュリティ機能を拡張**
  – SSL暗号化のオフロードに加え、Thunder ADC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 ADCをHA（高可用性）で導入することにより、複数のセキュリティデバイスの負荷を分散できます。また各接続を追跡して、要求と応答を確実に同一のデバイスに送信できます。

- **復号化するトラフィックの種類を制御することにより、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 ADCでは、きめ細かく調整できるポリシーを利用して、アプリケーションの種類に基づいて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 ADC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防止プラットフォームに転送し、他の種類のトラフィックの負荷をこのデバイスにかけないように設定できます。

- **aFleXポリシーによるきめ細かいトラフィック制御**
  – Thunder ADCのお客様は、A10 Networks aFleX®スクリプトを使用して要求を検査、更新、変更、破棄できます。aFleXスクリプトでは、インターセプトして他社製セキュリティデバイスに転送するトラフィックや、クリーンアップしてから目的の宛先に転送するトラフィックを完全に制御できます。aFleXはアプリケーショントラフィックの完全な制御を可能にするため、お客様は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。

- **重要なアプリケーションを選択的にバイパス**
  – コンプライアンス要件への対応やデータプライバシーを保証するため、SSLインサイトはバンキングアプリケーションや医療アプリケーションなどに向けた信頼できるトラフィックをバイパスできます。URL分類サブスクリプションを利用することで[5]、Thunder ADCは4億6000万ドメインのトラフィックを分類できるため、機密データを確実に暗号化した状態に維持できます。さらにThunder ADCのお客様は、手動でもバイパスリストを作成可能です。

[5] URL分類サブスクリプションはACOS (Advanced Core Operating System) 4.0より提供予定

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の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。SSLインサイトは、SSLトラフィックを復号化してプレーンテキストで多数のデバイスに送信する一元管理ポイントを提供するので、トラフィックを何度も復号化する必要がなくなります。Thunder ADCは、次の機能と相互運用できます。

- 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
- 脅威防御プラットフォーム
- 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、インラインへの導入や高速SSL復号化を考慮して設計されていません。Thunder ADCを導入すれば、これらのデバイスはコンピューティング機能を多用するSSL処理の負荷なしで、SSL暗号化データを検査できるようになります。Thunder ADCは、トラフィックを一度復号化すると、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できます。

包括的で拡張性の高い管理

管理の合理化と自動化のために、Thunder ADCは業界標準のCLI、Webベースユーザーインターフェイス、そして他社製または独自開発の管理コンソールと統合できるRESTful API（aXAPI®）を備えています。大規模な導入では、aGalaxy®一元管理システムによって、物理的な場所にかかわらず、複数のThunderアプライアンスでルーチンタスクを大規模に実行できます。

機能

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 ADCデータシートを参照してください。

SSLインサイト

- Webrootの提供するURL分類サービス[6]により、特定のWebサイトを選択的に迂回（URL分類サービスにはサブスクリプションライセンスが必要）
- ホスト名をベースにしたSSLインサイトバイパスでは、バイパスリストは最大100万のServer Name Indication（SNI）値を格納可能[7]
- 複数のバイパスリストをサポート[6]
- HTTPS、SMTP6、XMPPの復号化[6]
- 暗号化とプロトコルを包括的にサポート
  - TLS 1.0、TLS 1.1、TLS 1.2、SSLv3
  - RSA、DHE、ECDHE暗号化によるPFS（Perfect Forward Secrecy）をサポート
  - SHA、SHA-2、MD5ハッシュアルゴリズム
- クライアント証明書の検知と選択的バイパス[6]
- 信頼性の低い証明書の処理[6] – クライアントをエラーページにリダイレクト、または信頼性の低い証明書を持つクライアントへのトラフィックを暗号化してデフォルトブラウザーエラーメッセージを保持可能
- 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サーバーの負荷分散
- aFleX機能 – ディープパケットインスペクション、カスタマイズ可能な変換機能、アプリケーションを認識したスイッチング
- 高可用性 – アクティブ-アクティブ、アクティブ-スタンバイの設定
- ファイアウォール負荷分散（FWLB）

SSLインサイトの導入

- パッシブな非インライン他社製デバイスとともにインライン導入
- アクティブなインライン他社製デバイスとともにインライン導入

管理機能

- 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
- 業界標準コマンドラインインターフェイス（CLI）対応
- SNMP、Syslog、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XMLyAPI（aXAPI）
- LDAP、TACACS+、RADIUSのサポート

キャリアグレードのハードウェア

- 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ー
- 40 Gbポート、100 Gbポート搭載
- ハードウェア改ざん検知
- 非インライン他社製デバイスとともにインライン導入する場合、トラフィックフローをポリシーによってセグメント化し、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
- インライン他社製デバイスとともにインライン導入する場合、Thunder ADC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に負荷を分散可能

認定

- セキュリティおよび機能の保証に関する認定
  - ICSA Labs のWebアプリケーションファイアウォール
  - Common Criteria EAL 2+
  - FIPS 140-2 Level 2
  - 総合運用テストコマンド（JITC：Joint Interoperability Test Command）

[6] 本機能はACOS 4.0で提供予定

[7] ACOS 4.0では、バイパスリストは以前のACOSバージョンの10,000 SNI値から、200,000～1,000,000 SNI値まで登録可能。バイパスリストのサイズは、Thunderアプライアンスモデルによって異なります。

ロギングおよびレポート作成

Thunder ADCは、トラフィック分析のために高速のsyslogロギングに加え、電子メールアラートやNetFlowとsFlowの統計情報をサポートしています。Thunder ADCのWebユーザーインターフェイスのリアルタイム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表示されます。

まとめ

Thunder ADCに標準機能として装備されているSSLインサイトは、強力な負荷分散、高可用性、およびSSL復号化ソリューションを提供します。SSLインサイトを利用すると、次のことが可能になります。

- 完全な脅威防御を実現する、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
- 最善のコンテンツ検査ソリューション導入による、サイバー攻撃の回避
- A10の64ビットACOS®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ーを活用した、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

A10が提供する非常に強力なSSLオフロードソリューションにより、企業は次のことを実現できます。

- さまざまな環境に適切なモデルを選択できるよう、パフォーマンスとハードウェア高速化のさまざまなオプションを提供するThunder ADCを使用して、企業防御の盲点を排除
- SSL利用の拡大や、2048ビットおよび4096ビットSSL暗号を含むより高度な暗号化標準の利用を視野に入れることで、投資の将来性を保証
- 追加のセキュリティアプライアンスを購入せずに高速SSL復号化機能を提供し、CAPEXを低減
- 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を提供

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キング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キングソリューション群を提供しています。世界中で数千社にのぼる大企業やサービスプロバイダー、大規模Webプロバイダーといったお客様のデータセンターに導入され、アプリケーションとネットワークを高速化し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**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB-19113-JA-04
Jan 2015