Arbor Networks® TMS

高度な脅威解析、サージカル・ミティゲーション、サービス・イネーブルメント

主な特長と利点

サージカル・ミティゲーション
正規の業務トラフィックの流れを妨げることなく、自動的に攻撃トラフィックだけを排除します。

8 Tbps に及ぶミティゲーションの統一されたコマンドとコントロール
DDoS 防御機能をかつてないレベルへ拡張。最大 8 テラビットの集約された中央管理型のミティゲーション能力を展開できます。

マネージド・サービスを可能にするもの
DDoS 防御サービスへのニーズは急速に高まっています。TMS は、高収益のクラウド内 DDoS 防御サービスを提供します。

攻撃に対する防御策の包括的なリスト
最大規模かつ最も複雑なボリューム型攻撃や、TCP ステートを枯渇させる攻撃、アプリケーション・レイヤ DDoS 攻撃から、インフラストラクチャと顧客を保護します。

導入方法の柔軟性
ネットワーク上のさまざまな範囲に対し、アプリケーション層の情報収集機能、脅威検知機能、サージカル・ミティゲーションを展開して、インフラ保護と高収益のマネージド DDoS 保護サービスを実現できます。

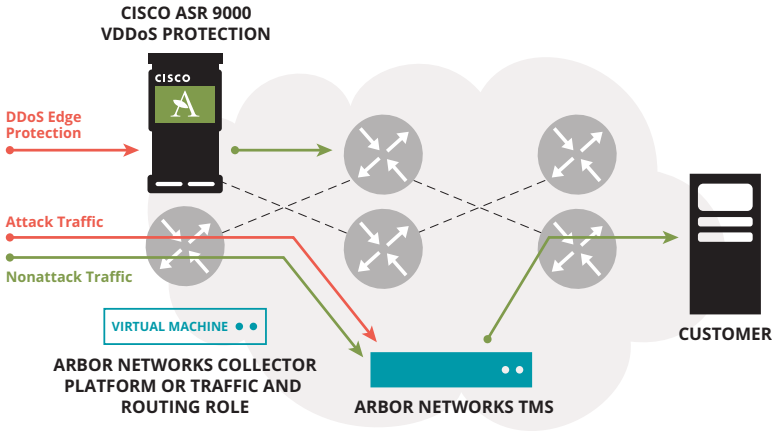
インターネット・サービス・プロバイダ（ISP）、クラウド・プロバイダ、および企業はみな共通の問題に直面しています。分散型サービス拒否（DDoS）攻撃は、サービスの可用性に多大なリスクを及ぼします。DDoS 攻撃の影響力、洗練度、および頻度はますます高まっており、データ・センターの運用者やネットワーク・プロバイダは、効果的で費用対効果が高く管理の容易な防御策を求めています。Arbor Networks® TMS は、DDoS 攻撃対策のリーダーとして実績を認められています。TMS は、業界をリードする DDoS 防御ミティゲーション・ソリューションとしてさまざまなサービス・プロバイダ、クラウド・プロバイダ、大企業のお客様に選ばれています。

Arbor Networks の DDoS 防御ソリューション

ネットワークワイドなインテリジェンスと異常検知能力にキャリア・クラスの脅威管理を統合した Arbor Networks のソリューションは、ネットワークトラフィックおよびアプリケーション・レイヤ DDoS 攻撃をの識別し、攻撃を阻止をサポートします。

TMS のネットワーク・アプライアンスは、Arbor Networks ソリューションに不可欠なトラフィック・スクラビング・コンポーネントを提供します。TMS をインラインで展開することで、「常にオン」状態の保護を実現できます。TMS は他の製品と異なり、「ダイバージョン分散／リインジェクション再注入」というミティゲーション・アーキテクチャもサポートしています。このモードでは DDoS 攻撃を含む運ぶトラフィック・ストリームのみが、Arbor Networks ソリューションによってアップデートされた発行されるルーティング情報更新を通して TMS にリダイレクトされます。次に TMS により悪意のあるトラフィックのみがストリームから排除され、正規のトラフィックが目的の宛先へと送信されます。

これはサービス・プロバイダ、大企業、および大規模なホスティング / クラウド・プロバイダにとって大きな利点となります。中央に配置された単一の TMS で、複数のリンクや複数のデータ・センターを保護できます。この結果、ミティゲーション機能の利用を大幅に効率化し、完全に疑いようのない非侵襲的なセキュリティを実現できます。インライン装置は、監視先のリンクにおけるすべてのトラフィックを常に検査する必要があります。TMS なら、特定のターゲットに対する攻撃の結果としてリダイレクトされたトラフィックを検査するだけですみます。



ARBOR NETWORKS
The Security Division of NETSCOUT

各種の脅威検知とミティゲーション処方

既知の悪意あるホストをブロック。ホワイトリストとブラックリストを利用します。ホワイトリストには承認を得たホストが、一方ブラックリストにはゾンビ（感染ホスト）がリストされ、ブラックリストのホストのトラフィックをブロックします。

アプリケーション層への攻撃をブロック。高度なフィルターを利用します。TMS が提供するペイロードの視認性と高度のフィルター機能が、隠れた攻撃によってクリティカルなサービスがダウンする事態を確実に防止します。

Web ベースの脅威からの防衛。HTTP を標的とした攻撃の検知とミティゲーション。これらの機能はフラッシュ・クラウドへの対応にも有効に作用します。

クリティカルな DNS サービスの防御。キャッシュ・ポイズニング、リソースを消耗させる攻撃、および増幅攻撃から保護します。DNS サービスの視認性を高めます。

VoIP サービスの防御。VoIP/SIP に特化した攻撃の検知とミティゲーション機能の採用により、pps を悪用して大量の異常なリクエストを実行する自動スクリプトやボットネットの攻撃から保護します。

大規模なリフレクション／増幅攻撃を阻止。単一の TMS シャーシ内で最大 80 Gbps の攻撃ミティゲーションを利用することで、NTP、DNS、SNMP、SSDP、SQL RS、Chargen といった攻撃を阻止します。

SSL パケットに隠れた攻撃を暴いて阻止。オプションの TMS 2300 ハードウェア・セキュリティ・モジュール（HSM）が SSL パケットを復号化して攻撃トラフィックを検知、ドロップし、さらに正規トラフィックを再度暗号化してネットワークに戻します。

ATLAS® インテリジェンス・フィード

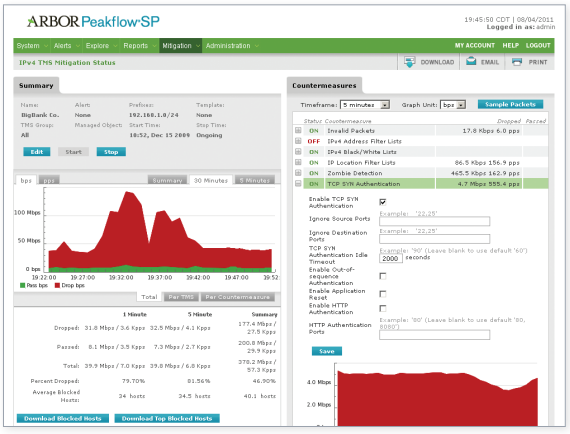
Arbor の研究者は、トラフィック監視とセンサーのグローバル・ネットワークを活用して、大半のボットネット・ベース攻撃に対する自動的な保護機能を提供する、的を絞った防御機能のライブラリである ATLAS インテリジェンス・フィードを開発しました。ATLAS インテリジェンス・フィードは Arbor の研究者が新たな脅威を発見し無効化するたびに、TMS を自動的にアップデートして新しい保護機能を追加します。

総合的な脅威検知機能

データ・センターや公衆網は DDoS 攻撃の標的になりやすく、これにはインフラ機器（ルーター、スイッチ、ロード・バランサーなど）、ドメイン・ネーム・システム（DNS）、帯域幅の容量、また Web、E コマース、音声、ビデオなどの主要なアプリケーションが含まれます。ファイアウォールや侵入防止システム（IPS）などのセキュリティ・デバイスも例外ではありません。Arbor Networks のソリューションは業界で最も包括的で適応力のある脅威検知能力を備えた製品で、複雑な混合攻撃から多様なリソースを保護するように設計されています。これらの機能には、統計異常検知、プロトコル異常検知、フィンガープリント照合、プロファイルを使用した異常検知などがあります。Arbor Networks のソリューションは常にリアルタイムで学習と適応を繰り返し、攻撃だけでなく、需要やサービス・レベルの異常な変化についても運用者に警告します。

わずか 4 秒間の高速サージカル・ミティゲーション

効果的なミティゲーションのポイントは、正規トラフィックを目的の宛先まで配信する一方で、攻撃トラフィックのみを識別してブロックする能力です。大規模な DDoS 攻撃の被害は、狙われた被害者ばかりではなく、同じネットワーク・サービスを共有しているその他の顧客にも及びます。サービス・プロバイダやホスティング・プロバイダは、このような付随的な損害を軽減するために、しばしば被害者のサイトへ向かう全トラフィックをシャットダウンし、これにより DDoS 攻撃者の狙いが達成されてしまいます。帯域幅の容量消耗を意図した大量のフラッド攻撃や、Web サイトをダウンさせる標的型攻撃など、攻撃の種類に関わらず、TMS は他のユーザーに影響を与えることなくわずか 4 秒間の高速ミティゲーションにより攻撃トラフィックを隔離して排除することができます。この手法としては、悪意あるホストの識別とブラックリストへの追加、IP ロケーション・ベースのミティゲーション、プロトコル異常ベースのフィルタリング、異常なパケットの削除、転送レート制限（実際に需要のあるスパイクは適切に管理）などが採用されています。ミティゲーションは自動あるいは運用者によって開始でき、防御手法を組み合わせて混合攻撃に対応することもできます。



リアルタイムの警告およびミティゲーション・ダッシュボード

リアルタイムのミティゲーション・ダッシュボード

TMS のリアルタイムのミティゲーション・ダッシュボードは、具体的に何が DDoS 警告の原因となっているのか、および攻撃に対して防御策がどのような効果を上げているかを表示する単一の画面です。ここで防御策を修正することも可能で、完全なパケット・キャプチャや復号を行い、正常なパケット・ストリームと攻撃のパケット・ストリーム両方の詳細を表示することができます。この情報は将来の参照および管理レポート用に保存され、運用者やマネージャーは自社のビジネス運用に対する攻撃についての完全な視認性とレポート機能を得ることができます。

拡張性の高い DDoS 攻撃検知およびミティゲーション

Arbor Networks® SP は、物理および仮想インスタンス上で拡張し、顧客側エッジからピアリング・エッジ、データ・センター（またはクラウド・エッジ）、モバイル・エッジに至るまでのサービス・プロバイダ・ネットワーク全体（各間のバックボーン・ネットワークを含む）にわたり、包括的な DDoS 検知機能を提供します。比類の無い視認性を備えた SP のワークフローにより、あらゆる TMS または Cisco ASR 9000 vDDoS 防御を介した迅速かつ効果的なミティゲーションを実現します。防御策ベースのミティゲーションは、TMS 5000 につき最大 100 Gbps、展開においては最大 4 Tbps まで増強できます。さらにブラックリストが防御ミティゲーションの前にさらなる予防線を追加します。Cisco ASR 9000 vDDoS 防御は、OpenFlow を使ってネットワークのあらゆる角度から数十 Tbps にもほのる大規模なブラックリスト手法を施し、重要な上流工程とコア・リンクを攻撃から保護します。

包括的な管理とレポート

TMS は、単独の制御ポイントを通じて最大 8 テラビットのミティゲーション能力の表示・管理能力を提供するため、運用操作を簡易化・合理化できます。これにより複数の大規模な攻撃を防止でき、ミティゲーション・プロセスを要約した包括的なレポートを作成して顧客や経営陣向けに提供することができます。

マネージド DDoS サービス用プラットフォーム

サービス・プロバイダやホスティング / クラウド・プロバイダは、Arbor Networks のソリューションを利用して顧客に DDoS 防御サービスを提供できます。カスタマイズされたポータル・アクセス、API、および管理の委任により、マネージド・サービス・プロバイダは自社のサービスを顧客のニーズに合わせて自由にカスタマイズできます。Arbor Networks のソリューションは、マネージド DDoS 防御の紛れもないリーダーとしての地位を確立しており、主要な DDoS マネージド・サービス・プロバイダの大多数がこのソリューションを選択しています。

TMS DDoS 防御の仕様

同時セッション数	セッション数制限なし
導入モード	インライン―アクティブ、インライン―監視中、SPAN ポート、大バージョン分散／リインジェクション再注入
ブロック処理	ソース・ブロッキング／ソース保留、パケットごとのブロック、およびソース、ヘッダー、転送レートをベースとしたブロック
攻撃に対する防御	フラッド攻撃（TCP、UDP、ICMP、DNS、SSDP、NTP、SNMP、SQL RS、Chargen アンプリフィケーション増幅、DNS アンプリフィケーション 増幅、Microsoft SQL Resolution Service アンプリフィケーション増幅、NTP アンプリフィケーション 増幅、SNMP アンプリフィケーション 増幅、SSDP アンプリフィケーション 増幅）、フラグメンテーション攻撃（Teardrop、Targa3、Jolt2、Nestea）、TCP スタック攻撃（SYN、FIN、RST、SYN ACK、URG-PSH、TCP フラグ）、アプリケーション攻撃（HTTP GET フラッド、SIP Invite フラッド、DNS 攻撃、HTTPS プロトコル攻撃）、DNS キャッシュ・ポイズニング、脆弱性攻撃、リソースを消耗させる攻撃（Slowloris、Pyloris、LOIC など）。フラッシュ・クラウドに対する防御。SSL 暗号化パケットに隠された IPv4 および IPv6 攻撃
DDoS 対策	ブラックリスト／ホワイトリスト、ジオ・ロケーションのレポートとブロック、ゾンビのブロック、パケット・コンテンツのフィルタリング、パケット・ヘッダーのフィルタリング、ボットネット排除（AIF フィード）、異常なパケットの排除（TCP、UDP、DNS、DNSSEC、HTTP、HTTPS、SIP）、さまざまなスプーフィング防止策、混合攻撃に対する防御、CDN ／プロキシを意識した対策、転送レート制限

第 10 版ワールドワイド・インフラストラクチャ・セキュリティ・レポート

Arbor Networks の『第 10 版ワールドワイド・インフラストラクチャ・セキュリティ・レポート』は、2013 年 11 月から 2014 年 10 月までの 12 か月間を網羅しています。Arbor ではこのレポート作成のため、全世界のティア 1 およびティア 2/3 サービス・プロバイダ、企業、その他のタイプのネットワーク運用者から 287 件の回答を収集しました。このレポートは、運用に関するセキュリティ・コミュニティの経験、所見、および懸念事項を収集することを目的としています。例年と同様、この調査ではインフラと顧客に対する脅威、インフラの保護に使用している技術、セキュリティ・インシデントの管理、検知、対処のために使用しているメカニズムといったトピックを扱っています。

10 年間にわたる DDoS レポート：

- 分散サービス拒否（DDoS）攻撃は、10 年前にはそのほとんどが単発的な迷惑行為に過ぎませんでしたが、今ではビジネスの継続性と最終利益に対する重大な脅威となっています。今日、DDoS 攻撃は、複雑で多くは長期にわたる高度な脅威キャンペーンの構成要素です。

- 2014 年の調査では、90% の回答者がアプリケーション・レイヤ攻撃を経験していました。これに対し、10 年前の調査では最も一般的な攻撃ベクトルとして、90% の回答者が単純な「ブルート・フォース型」のフラッド攻撃を挙げていました。

- 人的要素は、防御能力を左右する要因の 1 つです。このことは現在だけでなく、WISR レポートの 10 年間を通じて一貫しています。昨年度だけでも、54% の回答者が、セキュリティ組織に熟練の人材を雇用し定着させることが困難であると答えました。

- 2014 年に報告された最大の DDoS 攻撃は 400 Gbps でしたが、これに対し 10 年前に報告された最大の攻撃はわずか 8 Gbps でした。

最新のレポートは次のアドレスからダウンロードできます。
www.arbornetworks.com/report

TMS 5000

25 Gbps、10 Mpps – 100 Gbps、40 Mpps

TMS 2x00

2301： 1.5 Gbps、3.5 Mpps
2302： 2.5 Gbps、5 Mpps
2305： 5 Gbps、7 Mpps
2310： 10 Gbps、10 Mpps
2800： 10～40 Gbps、30 Mpps

TMS 2x00 アプライアンスは、ソフトウェア・ライセンス・キーのアップグレードによりインプレースで簡単に拡張可能。

ARBOR NETWORKS
The Security Division of NETSCOUT

本社

76 Blanchard Road
Burlington, MA 01803 USA

米国内フリーダイヤル：+1 866 212 7267
TEL：+1 781 362 4300

北米販売担当者

フリーダイヤル：+1 855 773 9200

欧州

TEL：+44 207 127 8147

アジア太平洋

TEL：+65 6664 3140

日本

〒 101-0063
東京都千代田区神田淡路町 2-105
ワテラス アネックス 13 階
TEL：03 3525 8040
お問い合わせ japan@arbor.net

www.arbornetworks.com

DS/TMS/EN/0715-LETTER

TMS 2300、2800、5000 の仕様

	TMS 2300 シリーズ	TMS 2800	TMS 5000
スループットおよびミティゲーション 2300 および 2800 シリーズはソフトウェア・ライセンスのアップグレードが可能	**2301:** 1.5 Gbps、3.5 Mpps **2302:** 2.5 Gbps、5 Mpps **2305:** 5 Gbps、7 Mpps **2310:** 10 Gbps、10 Mpps	10 Gbps、20 Gbps、30 Gbps、40 Gbps のライセンス、すべて最大 30 Mpps	**APMe × 1：**最大 25 Gbps、10 Mpps **APMe × 2：**最大 50 Gbps、20 Mpps **APMe × 3：**最大 75 Gbps、30 Mpps **APMe × 4：**最大 100 Gbps、40 Mpps
電力要件	冗長対応二重化電源 **AC：**100～127V/200～240V、50～60 Hz、6/3A **DC：**-48～-72V、最大 13A	冗長対応電源 **AC：**100～127 VAC、200～240 VAC、12A @ 100 VAC、6A @ 200 VAC、50/60 Hz **DC：**-48～-72Vdc、30A @ -48Vdc	冗長対応四重化電源 **AC：**100～240V、50～60Hz **DC：**40.5～72 VDC
寸法	**筐体：**2U ラックサイズ **重量：**39 lbs (17.7 kg) **高さ：**3.45 インチ（8.76 cm） **幅：**17.14 インチ（43.53 cm） **奥行き：**20 インチ（50.8 cm）	**筐体：**2U ラックサイズ **重量：**39 lbs (17.7 kg) **高さ：**3.45 インチ（8.76 cm） **幅：**17.14 インチ（43.53 cm） **奥行き：**20 インチ（50.8 cm）	**筐体：**6U ラックサイズ **重量：**AC 使用時：77.15 lb (34.99 kg)、DC 使用時：58.52 lb (26.54 kg)、APM-E ブレード 1 点ごとに 6 lb (2.72 kg) を追加 **高さ：**10.463 インチ（265.76 mm） **幅：**19.00 インチ（482.6 mm） **奥行き：**18.19 インチ（462.00 mm）（ハンドルを含む）
ネットワーク・インターフェイス	12 × 1 GigE (銅線または GigE SX、GigE LX の SFP) または 6 × 10 GigE (SR または LR 用の SFP+)	8 × 10 GigE (SR または LR 用の SFP+、または混合繊維)	32 × 10 GigE (QSFP+ とブレイクアウト・ケーブル、SR4 または 4LR) 2016 年の予定： 8 × 40 GigE (QSFP+ SR4 または LR4) 4 × 100 GigE (QSFP28 SR4 または LR4)
ストレージ	デュアル RAID 1 SSD ドライブ	デュアル RAID 1、240 GB SSD ドライブ	デュアル・ハード・ドライブ RAID 1
環境	**動作温度：**41°～104°F (5°～40°C) **相対湿度：**73°～ 104°F (23°～ 40°C)で動作時 5～85%、非動作時 95%	**動作温度：**41°～131°F (5°～55°C) **相対湿度：**73°～104F (23°～40°C) で動作時 5～85%、非動作時 95%	**動作温度：**23° F～104° F (-5° C～40°C) **相対湿度：**動作時 5～85% (結露なし)
準拠規格	RoHS 2002/95/EC、IEC/EN/UL 60950-1 第 2 版、E2006/95/EC、2001/95/EC、FCC パート 15 サブパート B クラス A、EN 55022、EN 55024、EN 61000-3-2、EN 61000-3-3、EN 61000-4-2、EN 61000-4-3、EN 61000-4-4、EN 61000-4-5、EN 61000-4-6、EN 61000-4-8、EN 61000-4-11、IC ICES-003 クラス A、ETSI EN 300 386、ETS 300-019-2-1、ETS 300-019-2-2、ETS 300-019-2-3、ETS 753、CISPR 22 クラス A、CISPR 24、Gost、BSMI、VCCI クラス A、KCC クラス A、UL マーク、CE マーク、ETSI、NEBS-3 (DC)、NEBS-1 (AC)	UL 60950-1 第 2 版／CSA C22.2 No. 60950-1-07 第 2 版、低電圧指令 2006/95/EC、安全指令 2001/95/EC、IEC60950-1 および第 2 版、各国の偏差に対する CB 認証およびレポート、FCC 47CFR パート 15、クラス A 制限検証済み、ICES-003 クラス A 制限、EMC 指令、2004/108/EC、EN55022、EN55024、EN61000-4-2、EN61000-4-3、EN61000-4-4、EN61000-4-5、EN61000-4-6、EN61000-4-8、EN61000-4-11、EN61000-3-2、EN61000-3-3、VCCI クラス A ITE (CISPR 22、クラス A 制限)、BSMI 承認、CNS 13438、クラス A および CNS13436 安全性、KCC 承認、Gost 承認、CISPR 22 クラス A 制限、CISPR 24 イミュニティ、RoHS (recast) 指令 2011/65/EU	RoHS 6/6、IEC/EN/UL 60950-1、FCC パート 15 サブパート B クラス A、ETSI EN 300 386、UL マーク、CE マーク
ハードウェア・バイパス	外部		
SSL 復号化 / 再暗号化 オプションのハードウェア・セキュリティ・モジュール (HSM) を介して	**2301 & 2302：**750 Mbps **2305 & 2310：**5 Gbps **HTTPS 接続：**最大 45,000 **同時セッション：**最大 150,000	**確認済みスループット：**最大 5 Gbps **HTTPS 接続：**最大 45,000 **同時セッション：**最大 150,000	非対応
	サポートされる SSL：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2 **サポートされる FIPS サイファー・スイート：**RSA_WITH_AES_128_SHA、RSA_WITH_AES_256_SHA、RSA_WITH_AES_256_SHA256、SSL3_CK_RSA_DES_192_CBC3_SHA **サポートされる非 FIPS サイファー・スイート：**SSL3_CK_RSA_RC4_128_SHA、SSL3_CK_RSA_RC4_128_MD5、SSL3_CK_RSA_DES_64_CBC_SHA		