JUNIPER NETWORKS | Engineering Simplicity

"Your Best Partner" NISSHO ELECTRONICS

Juniper TDD
Threat Defense Director

最速でスケーラブルな DDoS 攻撃からの保護ソリューション

SmartWall Threat Defense Director (TDD) は、
最大規模のプロバイダーネットワークでも完全なエッジ保護を提供します。
MXシリーズルーターの高性能パケットフィルタリング機能と組み合わせることにより、
TDDは、エッジに専用のアプライアンスを配置したり、
スクラビングセンターに大量の攻撃トラフィックをバックホールしたりする必要なく、
毎秒数十テラビットのトラフィック保護にもスケーラブルに対応可能です。

特徴

包括的な可視性
TDDは、ビッグデータ分析を活用して、ネットワーク全体で発生するDDoS攻撃アクティビティに関する明確で有用なインテリジェンスに加え包括的な可視性、レポート、アラート機能を提供します。

あらゆる規模のDDoS攻撃を迅速に検出
DDoS攻撃で一般的な大きなボリューム攻撃をブロックするだけでなく、レガシーソリューションでは対応が困難であった規模が非常に小さく短時間で終了するような攻撃をも検出し、取り除くことができます。

運用コストの削減
DDoS攻撃への応答を秒単位で自動化することにより、人間の介入と誤検知を大幅に削減して、運用コストとTCOを最小化します。

自動保護
オペレータの介入なしに広範なDDoS攻撃を自動的に緩和し、接続を完全に維持するとともに正規トラフィックの配信中断を回避し、攻撃を迅速に停止します。

大規模ネットワークへ対応
数十テラビット級のトラフィックにまで常時オンの保護能力を拡張可能ですので、最大規模のプロバイダーネットワークにも対応します。

既存のMXエッジルーターを活用
専用のデバイスを導入したりトラフィックをバックホールしたりすることなく、既設のネットワークエッジデバイスにより攻撃トラフィックをローカルでブロックできます。

マネージサービスイネーブラー
サービスプロバイダーは、ブラックホール ルーティングしたり正規トラフィックを中断することなく、リアルタイムのDDoS防御によりセキュリティサービスを強化できます。

セキュリティポリシーの適用
プロアクティブなトラフィック検査による検出とリアルタイムでのセキュリティポリシー適用により、IPv4とIPv6の両方のトラフィックに対するレイヤー3〜7 ボリュームDDoS攻撃を防ぎます。

最新の脅威状況

DDoS攻撃は、サーバー、PC、ラップトップ、およびウェブカメラなどのコンシューマー向けIoTデバイスを含む、安全性の低いエンドポイントをハイジャックすることによって構成された大規模なボットネットから開始されることが多いです。そして攻撃の75%以上は、インターネットサービスおよびホストシステム脆弱性をつき、一連の単純なリクエストを送信するだけでターゲットに対しデータのフラッドを生成する手法を用いていると言われています。

飽和攻撃未満の小ボリューム攻撃は引き続き攻撃の大勢を占め、2019年に観測されたすべてのイベントの92%が5Gbps未満でしたが、10Gbps以上の攻撃は前年比35%以上増加したと報告されています。

DDoS 攻撃の頻度、規模、巧妙さが増しマルチベクター化が進むにつれ、アウトオブバンドのスクラビング センターや人的介入といった従来のアプローチでは対応が追いつかず、コストがかさむようになってきています。大ボリューム型攻撃の場合、疑わしいトラフィックをスクラビング センターにリダイレクトすることで遅延が生じるだけでなく、経済的負担が増す結果となります。スクラビング容量は配備に費用がかかるため、一般的にはプロバイダーのエッジ容量の一部、多くの場合20%以下の利用に絞っており、これは大ボリューム攻撃に対処するには不十分であることを意味します。

また、従来のアプローチでは、手動での分析や人的介入が必要なことから、攻撃が上手く緩和される場合であっても対処まで数分から数十分を要します。これでは攻撃がブロックされる前にダメージを被りかねません。最新の調査結果では攻撃継続時間も短くなる傾向にあり、観測された攻撃の85%は10分以内に終了している事実からも裏付けられます。被害者がリピート攻撃を受け、より多くのサービス停止を引き起こす可能性が高いことも指摘されています。

13% マルチベクター攻撃の増加率 *

35% 10Gbps を超える攻撃の増加 *

85% 10 分以内に終了する攻撃数 *

23% 24 時間以内に同じ犠牲者が繰り返し攻撃される確率 *

* 出展 : Corero 社 2019 Full Year DDoS Trends Report

ジュニパーの DDoS 防衛アプローチ

ネットワークベースのソリューション

SmartWall Threat Defense Director(TDD)は、DDoS対策製品を開発するCorero Network SecurityとJuniper Networksにより共同開発され、最新世代のMXルーターの強力な機能を活用するネットワークベースのDDoS防御ソリューションです。ピアリングポイント、データセンターエッジ、加入者エッジなどに導入済みのルーターを活用することにより、ネットワークエッジで効果的なDDoS攻撃防御を実現します。

強力なシリコンとSDNの活用

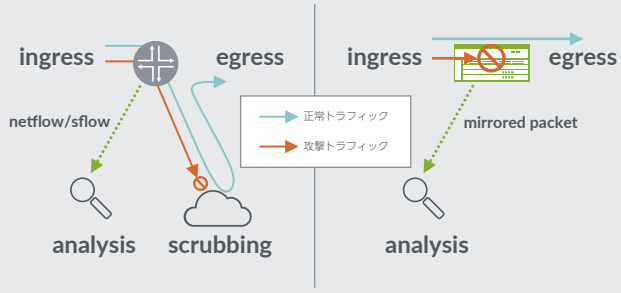
MXルーターに搭載されているパケット処理用カスタムASICは、パケットのヘッダおよびペイロード内のフィールドにマッチするフレキシブル・フィルタリング・ルールを生成することができます。このフィルタは、全てのパケットに適用され、不正なトラフィックフローをシリコンレイヤーでブロックします。また、NETFONFなどのSDNプロトコルを使用して、CoreroのSmartWallソフトウェアによって定義されたフィルタルールをMXルーターに配布します。新しい攻撃ベクトルを検出すると攻撃緩和ルールを動的に生成し、対応するフィルタリングルールが即座に適用されます。

精度とリアルタイム性の両立

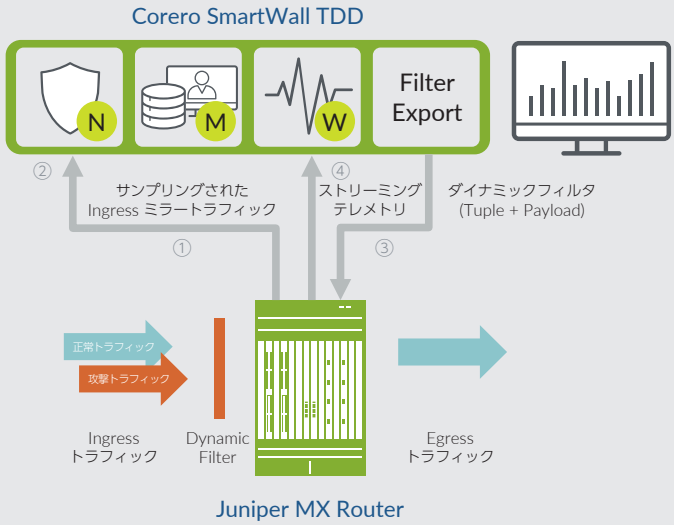
パケットレベルで常時モニタリングを可能にします。ヘッダ情報だけでなくペイロードデータも検査対象としますので、従来のフローベースの検出アプローチと比べ有効性が高まります。そして、自動化されたネットワークベースのDDoS防御は、攻撃検出から緩和までのプロセスを、数分や数十分ではなく、数秒以内に完了します。

DDoS 対策における従来手法と TDD の比較

従来の DDoS 対策	Juniper TDD
Netflow ● 集約の遅延 ● ヘッダーのみの検査 ● 処理負担が高い	**Sampled Mirror** ● 即座に転送 ● ヘッダーとペイロードを検査 ● 処理負担が低い
Flowspec ● BGP による伝搬 ● ヘッダーのみ ● 可視化の限界	**NETCONF** ● 一時的な設定 ● ヘッダーとペイロード ● ストリーミングテレメトリ



連携ソリューション イメージ



① ヘッダーとペイロードの両方を含む入力トラフィックをサンプリング
② ルールベースの分析と機械分析を利用して、DDoS攻撃をすばやく検知
③ 柔軟性の高いファイアウォールフィルタを自動生成することで、MXルーターを通してDDoS攻撃をブロック
④ MXルーターのストリーミングテレメトリにより、許可/ブロックされたトラフィックの統計データを収集し監視

ソフトウェア コンポーネント

TDD は3つの仮想化されたアプリケーションから構成されます。

SmartWall Network Threat Defense (vNTD)
検出エンジンです。MXルーターから送信されたサンプル ミラーパケットをマルチステージ パイプラインにより解析し、DDoS攻撃トラフィックを検出します。ネットワークトポロジーに合わせて複数のvNTDを配置することができます。

SmartWall Central Management Server (vCMS)
検出エンジンを制御し、攻撃トラフィックを通常のネットワークトラフィックから区別するために使用される攻撃緩和ポリシーを設定することができます。管理、設定、モニタリングのための複数のオプションを提供し、これにはブラウザーベースのGUI、フルSSH CLI、そしてパワフルなREST APIが含まれます。

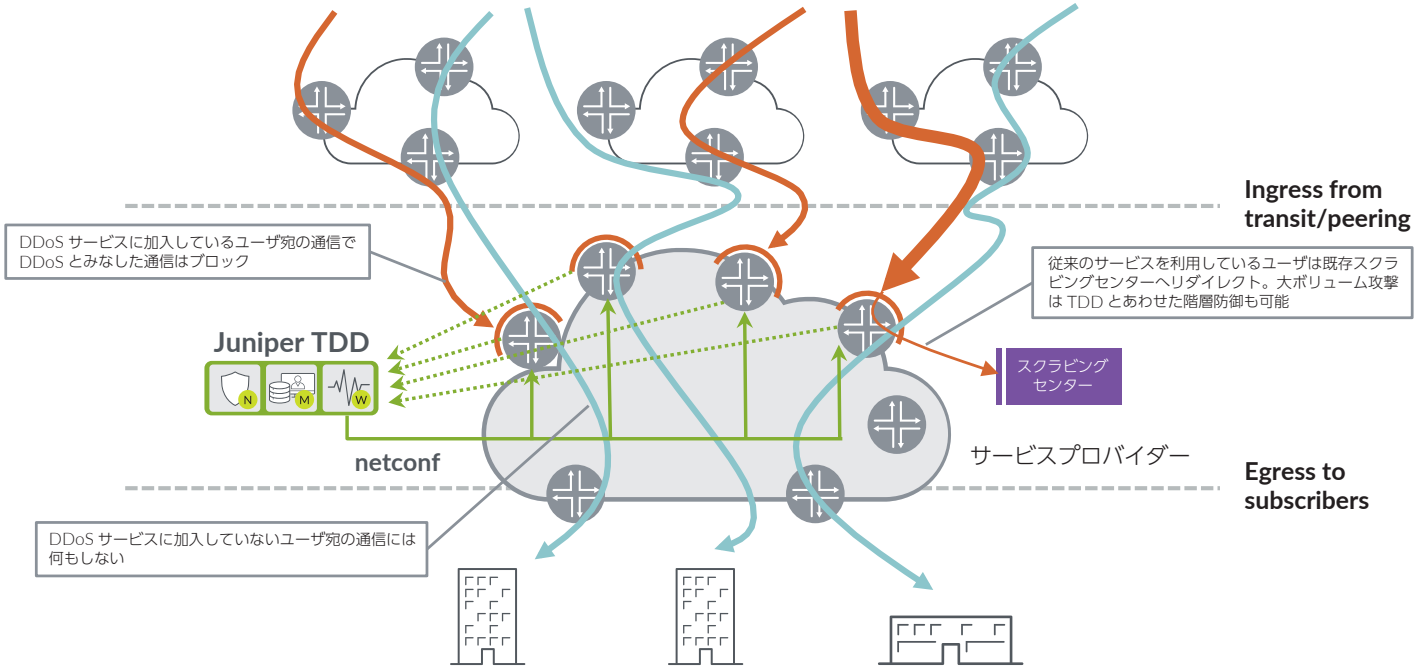
SmartWall SecureWatch Analytic (vSWA)
洗練されたDDoS攻撃フォレンジックを可能にするSplunkベースの分析エンジンです。検出エンジンから(vCMSを介して)情報を受信して、アクティブなDDoS攻撃を識別します。次に、vSWAはファイアウォールフィルタコマンドをルーターに送信し、ルーターに到着した攻撃トラフィックをフィルタ処理します。また、vSWAは、リアルタイムおよび履歴統計を表示します。これにより、ネットワークに対する攻撃を可視化し、vCMSポリシーを調整・最適化することができます。

プロバイダーエッジでの効果的な DDoS 検知と対策

トランジットやピアリングから届く DDoS 攻撃
エッジや顧客への正常トラフィック
MX ルーターからのサンプリングされたミラーパケット
フィルタルールを MX ルーターへ配信
一時的なフィルタ（tuple+payload）で攻撃を MX ルーターで防御

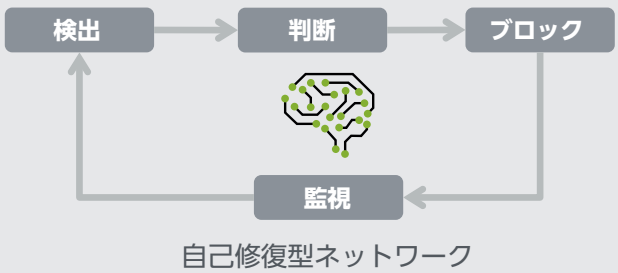
BGP Flow Spec の機能を利用して、MX ルーターだけでなく他社ルーターに対し TDD の下記機能を提供可能

- 識別・判断の速さを利用して最速数秒単位で BGP の Action を実行
- Rate Limit や Redirect などの BGP Action
- Action は即時実行とオペレーターによる手動実行が選択可能



プロバイダー向け DDoS ソリューション

Juniper NetworksとCoreroの連携により、ネットワーク境界自身がDDoS防御エンフォーサとなり、トラフィック経路に追加のアプライアンスを配置する必要がなくなります。SmartWall Threat Defense Director のDDoS検出・緩和技術の活用とMXルータの自動制御により、攻撃トラフィックは、ブラックホールしたりスクラビングセンターへバックホールすることなく、ネットワークのエッジでリアルタイムに除去することができます。
TDDは、ネットワークエッジを継続的にモニタリングし、迅速な検出、正確な判断、そして対処を通じてネットワークを自己修復するDDoS防御ソリューションです。



自己修復型ネットワーク

高検知率	パケットレベルでトラフィックを検査
リアルタイム性	手動介入なしに数秒でフィルタポリシーを適用
スケーラブル	最大 40Tbps まで柔軟に拡張可能な攻撃緩和能力
コスト効果	大容量スクラビングセンターが不要 既設 MX ルーターを活用した効果的なエッジ防御

TDD 製品ラインナップ

ベースライセンス

モデル	説明
J-COR-DOSDD-100G-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **100Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-100G-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **100Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-100G-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **100Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-200G-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **200Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-200G-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **200Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-200G-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **200Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-500G-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **500Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-500G-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **500Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOSDD-500G-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription. Includes 1 Detection Engine lic, **max 5**, for up to **500Gbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-1T-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription Includes 1 Detection Engine lic, **max 5**, for up to **1Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-1T-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription Includes 1 Detection Engine lic, **max 5**, for up to **1Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-1T-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription Includes 1 Detection Engine lic, **max 5**, for up to **1Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-10T-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription Includes 1 Detection Engine lic, **max 20**, for up to **10Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-10T-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription Includes 1 Detection Engine lic, **max 20**, for up to **10Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-10T-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription Includes 1 Detection Engine lic, **max 20**, for up to **10Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-40T-1	SmartWall Threat Defense Director Virtual Edition **1 Year** SW subscription Includes 1 Detection Engine lic, **max 40**, for up to **40Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-40T-3	SmartWall Threat Defense Director Virtual Edition **3 Year** SW subscription Includes 1 Detection Engine lic, **max 40**, for up to **40Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity
J-COR-DOS-DD-40T-5	SmartWall Threat Defense Director Virtual Edition **5 Year** SW subscription Includes 1 Detection Engine lic, **max 40**, for up to **40Tbps** agg monitoring and mitigation. Each DE with 10G processing capacity

オプションライセンス

モデル	説明
J-COR-DOS-DE-1P-1	SmartWall Threat Defense Director Detection Engine, **1 pack**, Virtual Edition **1 Year** SW subscription with 10 Gbps of processing capacity
J-COR-DOS-DE-1P-3	SmartWall Threat Defense Director Detection Engine, **1 pack**, Virtual Edition **3 Year** SW subscription with 10 Gbps of processing capacity
J-COR-DOS-DE-1P-5	SmartWall Threat Defense Director Detection Engine, **1 pack**, Virtual Edition **5 Year** SW subscription with 10 Gbps of processing capacity
J-COR-DOS-DE-10P-1	SmartWall Threat Defense Director Detection Engine , **10 pack**, Virtual Edition **1 Year** SW subscription with 10 Gbps of processing capacity per Detection Engine
J-COR-DOS-DE-10P-3	SmartWall Threat Defense Director Detection Engine , **10 pack**, Virtual Edition **3 Year** SW subscription with 10 Gbps of processing capacity per Detection Engine
J-COR-DOS-DE-10P-5	SmartWall Threat Defense Director Detection Engine , **10 pack**, Virtual Edition **5 Year** SW subscription with 10 Gbps of processing capacity per Detection Engine

日商エレクトロニクス株式会社

〒102-0084　東京都千代田区二番町 3-5 麹町三葉ビル
お問い合わせ：jg@nissho-ele.co.jp
URL：https://www.nissho-ele.co.jp

■本　社／東京 03(6272)5011
■支　社／関西 06(7506)9400　中部 052-265-6471
■支　店／中国 082(236)9750　九州 092(781)1886
■営業所／北海道 011(231)2770

2020-09-500-N