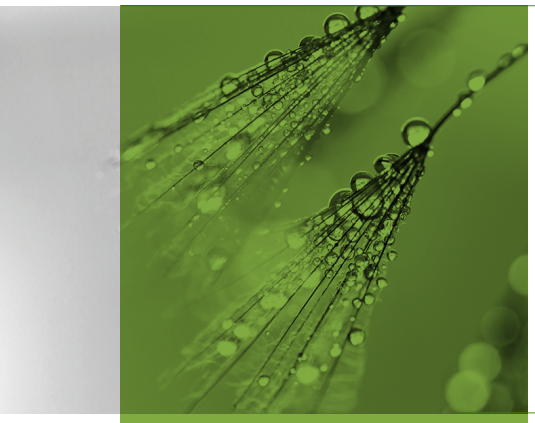

corero

ジュニパーネットワークスと Corero：大規模な DDoS 攻撃防御に向けた最新のアプローチ

コストを抑えつつ、高ボリューム型 DDoS 攻撃をリアルタイムで検知・緩和

課題

DDoS 攻撃は今日の重大な脅威の 1 つであり、規模、頻度、巧妙さのすべての点で進化し続けています。状況は深刻さを増しており、従来のアウトオブバンドのスクラビング センターや人的介入ではもはや対応が追いつかなくなっています。

ソリューション

ジュニパーネットワークスと Corero は、ネットワークのエッジ全体においてパケットレベルでの常時の監視、自動機械分析、インフラストラクチャベースのエンフォースメントを実施することにより、リアルタイムでラインレートを検出して攻撃を緩和する、革新的な DDoS 攻撃防御ソリューションを開発しました。

メリット

- *悪質なトラフィックをネットワーク エッジで排除することで、DDoS 攻撃の対策にかかるコストを削減します。*
- *自動対応により、DDoS 攻撃を数秒で阻止します。*
- *パケットレベルの常時モニタリングにより可視性が向上し、攻撃前、攻撃中、攻撃後のそれぞれにおいて詳細で実用的な情報が得られます。*
- *防御容量を毎秒数十テラビットにまで拡張できます。*

インターネットの登場以来、分散型サービス拒否（DDoS）攻撃は、誰かに損害を与えたり競合他社を妨害するといった悪事に対する報復手段として、悪意のある攻撃者に用いられてきました。DDoS 攻撃は、膨大な量のトラフィックを送りつけることにより Web サイト、ネットワーク、クラウドでオーバー フローを発生させるものです。攻撃を受けると、サービスの中断やダウンタイムが発生し、日常生活のあらゆる場面において、サービス プロバイダや企業のネットワークに頼っている正規ユーザーのアクセスが阻害されてしまいます。2017 年に DDoS 攻撃によって企業が被ることになる損失額は、平均 250 万ドルを超えると推定されています。[1]

課題

現在では、たとえコーディングの経験がない人であっても、100 ドルもあれば壊滅的な分散型サービス拒否（DDoS）攻撃を簡単に仕掛けることができます。

またその請負サービスによって、技術とコストの両面で、DDoS 攻撃を実行するためのハードルが下がってきています。また Internet of Things（IoT）の登場に伴い、コネクテッド デバイスもハッカーの恰好の標的となっています。原因として考えられるのは、IoT デバイスは大規模なネットワークを構成しているものの、基本的なセキュリティが組み込まれていないためです。2016 年、全世界で 10 万台近くのコネクテッド デバイスが「Mirai」という IoT ボットネットに感染し、ドメイン名システム（DNS）サービス プロバイダの Dyn 社を標的とした DDoS 攻撃に利用されました。ピーク容量は 1.2 テラビット毎秒（Tbps）にも達し、4 時間以上サービスの停止と遅延を招く結果となりました。しかし、Mirai は始まりにすぎませんでした。それ以降、JenX、Hajime、Satori、Reaper といった変種のプログラムが次々に現れ、攻撃はますます巧妙化し、検出が困難になっていったのです。

DDoS 請負サービスの普及と、安全対策の取られていない多数の IoT デバイスの拡散によって、DDoS 攻撃が大幅に増加する結果となっています。Corero の最新の『DDoS Trends and Analysis』レポートによると、2017 年第 3 四半期に組織に仕掛けられた DDoS 攻撃の 1 月あたりの平均件数は前期比 35% 増の 237 件であり、毎日 8 件の攻撃が試みられた計算になります。5G モバイル ネットワークへの移行が進めば、実効帯域が増え、攻撃トラフィックを生み出す感染コネクテッド デバイスのパイプラインが増強されることから、問題はさらに深刻化することになります。

[1] https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

DDoS 攻撃の頻度、規模、巧妙さが増すにつれ、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、多額のコストがかさむようになってきています。高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、データ トラフィックの量が対策コストに直接影響することから、経済的負担が増す結果となります。また、こういっ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、さらなる遅延や修復にかかるコストが発生することになります。こうした従来の方法では攻撃の検知から緩和まで最長で 30 分を要しますが、DDoS 攻撃によってわずか数分で Web サイトがダウンしてしまうことを鑑みると、このような事態はとても許容されるものではありません。

常時オン（Always-on）が当たり前の世界では、ダウンタイムはあらゆる企業やサービス プロバイダにとって重大な問題です。サービスプロバイダーや企業では、DDoS 攻撃対策における既存の戦略を見直し、高速で効果的な防御をはるかに低コストで提供する新たな手法を検討する必要があります。IP ネットワークは、高ボリューム型攻撃防御の最前線として、ソリューションの根幹となるべきです。そこにテレメトリ、機械分析、ネットワーク プログラマビリティを活用することで、よりインテリジェントで、適応性に優れ、自動化された検知・緩和プロセスを可能にします。

ジュニパーネットワークスと Corero による DDoS 攻撃防御ソリューション

ジュニパーネットワークスと Corero Network Security は、ネットワーク上の重要な場所を継続的にモニタリングし、速やかな検出、正確な意思決定、および自動緩和によって自己修復を行う DDoS 防御ソリューションを共同で開発しました（図 1）。

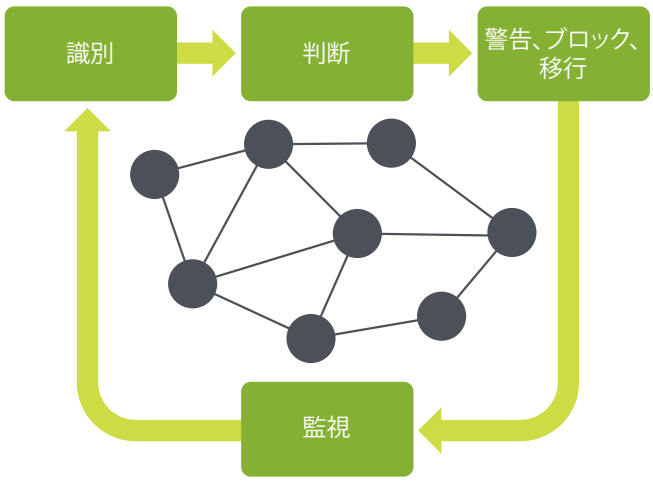

図 1 自己修復型ネットワーク

効果的な DDoS 攻撃防御のベスト プラクティスとは、できるだけ発信元に近い場所、一般的にはネットワークのエッジで攻撃を食い止めることです。したがって、DDoS 攻撃に向けた対策を実施する一般的な場所は、サービス プロバイダのピアリング ポイント、データ センター エッジ、サブスクライバ エッジの 3 カ所になります。

ジュニパーネットワークスと Corero Network Security による DDoS 攻撃防御ソリューションは高度に自動化されており、高い効果を発揮します。さらには、現在販売されているどの DDoS ソリューションよりも低いコストで、マルチテラビットへの容量拡張が可能になっています。同ソリューションは、ネットワークのエッジにおいて、以下の技法を用いて DDoS 攻撃を検知・緩和します（図 2 参照）。

- ジュニパーネットワークスの MX シリーズ 5G ユニバーサル ルーティング プラットフォームをネットワーク エッジに導入し、ヘッダーとペイロードの両方を含むサンプル ミラーを通して入力トラフィックを監視します。脅威の規模に合わせて動的に拡張でき、攻撃に柔軟に対応することが可能です。
- MX シリーズがサンプル ミラーを Corero SmartWall Threat Defense Director（TDD）に転送します。ここで、ルールベースの分析と機械分析を利用して、フィード内のすべてのパケットを検査し、DDoS 攻撃をすばやく正確に検知します。
- TDD は数秒で攻撃を検知し、柔軟性の高いファイアウォール マッチ フィルターを自動生成することで、MX シリーズを通して攻撃を緩和します。
- TDD はネットワーク設定プロトコル（NETCONF）を介して MX シリーズを自動で設定し、フィルターを使って攻撃トラフィックの発信源にもっとも近い入力ポイントで DDoS パケットをブロックする一時設定をインストールします。また同時に、フォワーディング性能を低下させることなく、正規トラフィックは意図した宛先に届けられます。
- MX シリーズのストリーミング 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が Corero SmartWall TDD に転送されます。
- SmartWall TDD SecureWatch Analytics は、攻撃前、攻撃中、攻撃後のネットワーク トラフィックを包括的に監視します。同アプリケーションでは Splunk を採用しており、攻撃の概要のほか、緩和プロセスの有効性に関する実用的な詳細情報をオペレーション チームに提示します。

このプロセスは、入力ポイントが攻撃にさらされていないことがミラーリングされたサンプルによりわかるまで続きます。攻撃の心配がなくなった時点で、SmartWall TDD によって MX シリーズのフィルターが削除され、通常のオペレーションが再開されます。その後も、MX シリーズから Corero の TDD へのミラーリングされたサンプルとストリーミング テレメトリの転送は続き、次の攻撃を監視しつつ、トラフィック フローが通常の状態に戻っていることを確認できるようになっています。

この運用モデルはすべてが自動化されており、事業活動を完全に保護し、オペレーション チームが常に監視できるようになっています。

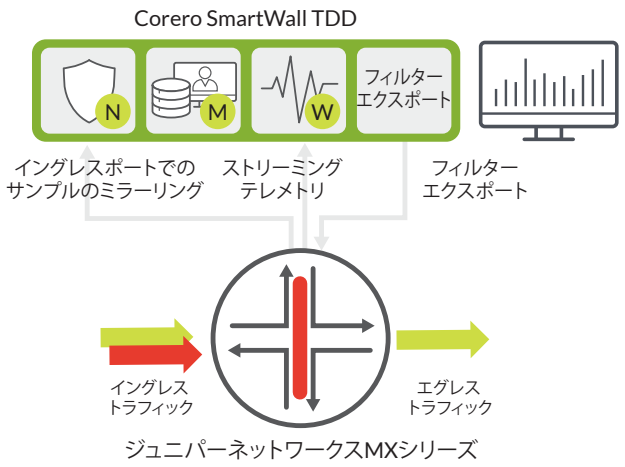

図 2 ジュニパーネットワークスと Corero による DDoS 攻撃防御ソリューション

特長とメリット

ジュニパーネットワークスと Corero による DDoS 攻撃防御ソリューションは、パケットレベルでのトラフィック検査のメリットと、インフラストラクチャベースの強力なエンフォースメントを組み合わせることで、コストを大きく抑えつつ、数十テラビット級という前代未聞の DDoS 攻撃をリルタイムで自動緩和します。

DDoS 攻撃対策コストの削減

MX シリーズ 5G ユニバーサル ルーティング プラットフォームの既存のフィルタリング機能を利用することで、悪質なトラフィックをネットワーク エッジで分散的に排除します。攻撃にさらされているすべてのトラフィックをアウトオブバンドの集中スクラビングセンターにリダイレクトした場合、遅延とコストの増大を招く結果となりますが、ジュニパーネットワークスと Corero のアプローチでは、こうした大量トラフィックに対処する DDoS 攻撃対策サービスのコストを大幅に節減できるだけでなく、高額なコストにつながる容量のアップグレードも不要です。加えて、防御機能の 95% 以上が完全に自動化されており、オペレータやアナリストの介入も必要ありません。これによって、人的介入による従来のアプローチを用いたソリューションに比べて、TCO がはるかに低く抑えられます。

即応性の向上とカスタマー エクスペリエンスの改善

自動化とは、DDoS 攻撃の検知 / ブロックを数秒でできることを意味しています。人手に大きく依存した従来のアプローチが 30 分以上の時間を要することを考えると、大変な進歩です。スピードは非常に重要な要素です。また、ジュニパーネットワークスと Corero によるソリューションは、正規トラフィックの流れを止めることなく、攻撃パケットのみを選択的にブロックすることで、攻撃のピーク時にもお客様のビジネスに影響が及ぶことがないようにします。

可視性、リソースの効率性、緩和効果の向上

ジュニパーネットワークスと Corero によるソリューションは、パケットレベルでの常時モニタリングを可能にします。従来のフローベースの検知アプローチに比べると、パケットベースの検査はより効果的で、ヘッダー情報だけでなく、ペイロード データまで細かく監視できます。また、サンプル ミラーリングではルーターで大量のデータを集約・処理する必要がないため、IP フロー情報エクスポート（IPFIX）プロトコルと比べて、ルーター リソースへの負荷が軽くてすみます。最後に、この連携ソリューションは環境の大幅な入れ替えを必要としません。ネットワークの境界部分に置かれた IP エッジ ルーターが防御の最前線として機能する階層型 DDoS 防御モデルの既存のソリューションとシームレスに連動することで、高ボリューム型攻撃のトラフィックをオフロードし、集中型のスクラビング リソースを利用して、巧妙なアプリケーション層攻撃にも確実に対処します。

数十テラビットへの拡張が可能

Corero SmartWall TDD は、攻撃防御のラインレート容量を最大 40 Tbps まで拡張でき、ネットワークの DDoS トラフィックをバックホールする必要がありません。また、MX シリーズ 5G ユニバーサル ルーティング プラットフォームはパケット転送容量を最大 80 Tbps まで拡張可能です。このように、同ソリューションは、現在市場で提供されている DDoS 攻撃防御システムのなかで最高の拡張性を備えた製品となっています。

ソリューション コンポーネント

Corero SmartWall Threat Defense Director

Corero SmartWall TDD は、高ボリューム型 DDoS 攻撃のリアルタイムの防御を可能にする画期的な製品であり、以下のような特長を備えています。

- 高ボリューム型攻撃の監視・緩和のための容量を数十テラビットまで拡張可能
- パケットレベルの検査により、高ボリューム型 DDoS 攻撃を正確に検知
- 機械分析による自動フィルタリングにより、インテリジェントな攻撃防御を提供
- 緩和に要する時間を数秒で測定し、リアルタイムに対応
- 閉ループのフィードバックにより、誤検知の問題を解消
- 年 / 月 / 週 / 日 / 分 / 秒のすべてを記録するフル ログ機能
- 許可 / ブロックの両方のトラフィックのパケット サンプルについてフォレンジック調査を実施
- Splunk を使った分析、レポーティング、アラーティング、自動化
- オープン インテグレーション API により、自動レスポンスと SecOps に対応
- BGP、NETCONF、Representational State Transfer（REST）、JavaScript Object Notation（JSON）、クラウドを介した攻撃防御シグナリング

ジュニパーネットワークスの MX シリーズ 5G ユニバーサル ルーティング プラットフォーム

MX シリーズは、以下のような特長を備えた強力な SDN 対応ルーター群を提供します。

- 比類のないシステム容量、密度、セキュリティ、パフォーマンス
- スループット性能を損なわない、業界初のインライン型データ プレーン セキュリティ
- 無制限のプログラマビリティにより、将来のイノベーションにも対応
- 自動化によるサービス提供の高速化
- マルチサービス ネットワークとノード スライシングの機能により、TCO を最大で 40% 削減
- Junos® Continuity によるダウンタイムのリスクを低減と稼動中のソフトウェア アップグレードが可能な統合型 ISSU(In-Service Software Upgrade)
- 多様な耐障害性機能により、ネットワークとサービスの比類のない可用性を提供
- ディープ パケット インスペクション（DPI）により、アプリケーションごとにトラフィックを検査
- Junos Telemetry Interface（JTI）経由で、監視 / 分析ツールにコンポーネントレベルのデータをストリーミング
- 比類のない省スペースと省電力

まとめ —コストを抑えつつ、リアルタイムに実行可能な大規模な DDoS 攻撃防御の最新アプローチ

マルチクラウド、IoT、5G の時代において、サイバーセキュリティの脅威は絶えず進化しています。なかでも DDoS 攻撃は、頻度、規模、巧妙さのすべての点で拡大を続けており、サービス プロバイダと企業の両方が、スピーディで効果的な防御を低コストで提供するソリューションにより既存のセキュリティ対策を増強する方法を探る必要があります。

IP ネットワークは、高ボリューム型攻撃に向けた防御の最前線として、最新のセキュリティ ソリューションの根幹となります。また、テレメトリ、機械学習分析、ネットワーク プログラマビリティによって、よりインテリジェントで、適応性に優れ、自動化された検出・緩和プロセスが可能になります。

ジュニパーネットワークスと Corero による DDoS 攻撃防御ソリューションは、パケットレベルでのトラフィック検査のメリットと、インフラストラクチャベースの強力なエンフォースメントを活用し、数十テラビット級という前代未聞の規模の DDoS 攻撃防御を、コストを大きく抑えつつ、リルタイムで自動実行します。

次なるステップ

ジュニパーネットワークスと Corero は、企業のネットワークを悪質な DDoS 攻撃から守るお手伝いをします。詳しくは、ジュニパーネットワークスまたは Corero のセールス担当者までお問い合せください。

Corero について

Corero Network Security は、リアルタイム型の高性能な DDoS 攻撃防御ソリューションを提供するリーディング カンパニーです。サービス プロバイダ、ホスティング プロバイダ、およびオンラインでビジネスを行う企業などが、輝かしい受賞歴を持つ Corero のテクノロジを利用して、攻撃を自動で検出・緩和する機能、ならびにネットワークの完全な可視化、分析、レポーティングにより、自社環境に対する DDoS 攻撃の脅威を解消しています。この業界屈指のテクノロジによって、極めて複雑な環境において DDoS 攻撃を阻止するための費用対効果に優れた拡張可能な機能がもたらされるだけでなく、費用対効果に優れたかつてない経済モデルが実現します。詳しくは www.corero.com をご覧ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、私たちのつながり方、働き方、生活に変革をもたらすクラウド時代において、製品、ソリューション、サービスにより、複雑なネットワークの簡素化を実現します。弊社は、顧客とパートナー企業に向けて、世界をつなぐ、自動化、拡張性を備えたセキュアなネットワークを提供するため、ネットワークをそれまでの制約から解放します。

ジュニパーネットワークス株式会社

東京本社
〒163-1445 東京都新宿区西新宿3-20-2
東京オペラシティタワー45階
電話: 03-5333-7400
FAX: 03-5333-7401

西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー18階

www.juniper.net

JUNIPER NETWORKS | Engineering Simplicity

EXPLORE JUNIPER
Get the App.
JUNIPER 1ON1
Available on the App Store
ANDROID APP ON Google Play