Cisco ASR 9000 vDDoS 攻撃対策ソリューション

メリット

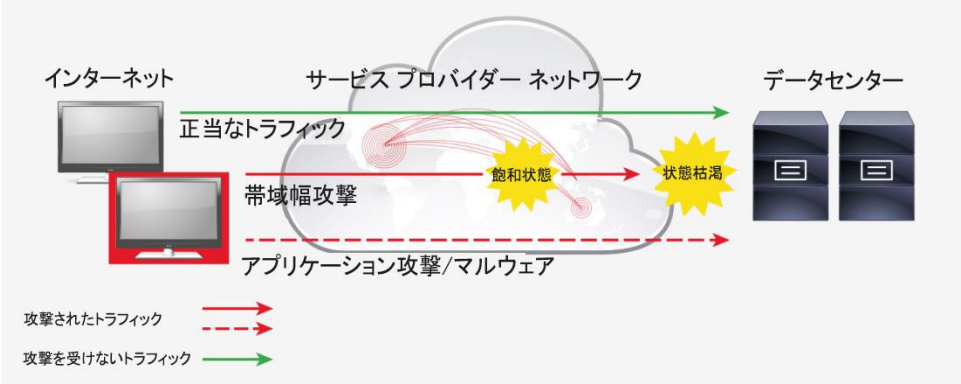
- **攻撃対策ソリューションの組み込み**：Cisco ASR 9000 シリーズ ルータおよび Cisco ASR 9000 シリーズ Virtualized Services Module（VSM）への投資を最大限活用して、ルータに DDoS 攻撃対策ソリューションを組み込みます。ソリューションの追加やサポートに関する複雑性を軽減しながら、ネットワークの可用性を保護します。
- **仮想化**：ラック スペース、電源、冷却装置、ケーブル、ポートを追加することなく、DDoS 攻撃軽減技術を Cisco ASR 9000 シリーズの導入に追加し、輸入にかかる費用や煩雑性を軽減します。Arbor Networks Peakflow を導入することで、仮想化環境における DDoS 攻撃の検出・分析もできます。
- **ネットワーク エッジ保護**：DDoS 攻撃をネットワーク エッジで阻止し、地域のスクラブ センターに対するバックホーリングを回避するための追加対策を実行します。
- **新たな収益**：顧客へ新しい仮想 DDoS 攻撃対策ソリューション サービスを迅速に提供できるようになります。
- **クラス最高レベルのソリューション**：Arbor Networks の Threat Management System（TMS）と Cisco ASR 9000 vDDoS 攻撃対策ソリューションを組み合わせることで、Arbor Networks Peakflow での包括的な DDoS 攻撃防御が実現します。

ネットワークが分散型サービス妨害（DDoS）攻撃を検出し、自動でブロックできるとしたらどうでしょうか。帯域幅攻撃や状態枯渇攻撃、アプリケーション層攻撃といった DDoS 攻撃からネットワークを保護できるよう、機能を強化しましょう。

ネットワークはビジネスにとって不可欠なものであり、これが利用できなければ、ビジネスに悪影響がおよびます。世界中のボットネットが WAN や LAN に対する DDoS 攻撃を始めると、トランジット プロバイダー、同僚、顧客、ネットワークに問題が生じます。リンク上のトラフィックが飽和状態になる可能性があります。ルータやドメイン ネーム システム（DNS）といったサービスなど、ネットワーク デバイスに障害が発生する場合もあります。また、お客様の接続が切断されることにより、コール センターへの問い合わせが急増することも考えられます。ビジネス実行を維持するには、ネットワークの可用性を維持する、つまりネットワークを DDoS 攻撃から効果的に保護する必要があります。

Cisco® ASR 9000 virtual DDoS（vDDoS）攻撃対策ソリューションでは、Arbor Networks の DDoS 攻撃検知および軽減技術をシスコのネットワークに組み込むことで、お使いのネットワークを DDoS 攻撃から保護します。その結果として、お客様のネットワークに対するあらゆる DDoS 攻撃を自動的に軽減できます。このソリューションでは、帯域幅攻撃、状態枯渇攻撃、アプリケーション層攻撃（図 1）などのさまざまな DDoS 攻撃からネットワークを保護し、継続的な可用性を確保します。Cisco ASR 9000 vDDoS は完全に仮想化され、軽減技術が ASR 9000 シリーズ ルータに組み込まれます。これにより、通常のフローやトラフィックを妨げることなく、DDoS 攻撃を受けたトラフィックを自動的に検出してブロックできます。このマルチテナント ソリューションにより、サービス プロバイダーは顧客に DDoS 攻撃対策ソリューションをサービスとして提供できるようになります。

図 1. Cisco ASR 9000 vDDoS により、さまざまな DDoS 攻撃から防御する



DDoS 攻撃の規模、頻度、複雑性の増大

Arbor Networks の『第 10 版年次ワールドワイド・インフラストラクチャ・セキュリティ・レポート』(2014 年)によれば、サービス プロバイダーのうち、73 % が DDoS 攻撃を経験し、55 % が自らのインフラストラクチャに対する DDoS 攻撃を経験しています。

近年の DDoS 攻撃は規模、頻度ともに増大を続けており、常に 400 Gbps 規模に到達している状況です。これらの攻撃は、もはや単純なシングルベクトル攻撃にとどまりません。より複雑なマルチベクトル型の攻撃が一般的となり、一層大きな脅威にさらされているのが現状です。事態をより複雑にする要因は、各種の DDoS 攻撃を動的に組み合わせたハッカーの新しいツールです。

- 帯域幅攻撃:特定のトラフィックまたはプロトコル メッセージを大量に送り込むことで、リソースの機能を停止させます。この攻撃では、Web サイト(特にオンラインのギャンブル サイトやゲーム サイト)、企業のインターネット接続、ホスティング プロバイダー、クラウド プロバイダーを主な標的としています。
- 状態枯渇攻撃:標的とするリソースのプロトコル状態がオーバーフローまたはエラーとなる攻撃です。ファイアウォール、侵入防御システム、Web アプリケーション ファイアウォール、ロード バランサ、データベースを主なターゲットとします。
- アプリケーション層攻撃:検出が困難なため、「低速・低空飛行型」の攻撃と揶揄されることもあります。政府/自治体、企業、およびあらゆるタイプのサービス プロバイダーで動作する重要なアプリケーションを標的とします。

DDoS 攻撃検知および軽減のしくみ

ネットワーク ルータから、Cisco Unified Computing System™(Cisco UCS®)で仮想マシンとして動作する Arbor Networks の Peakflow SP コレクタに NetFlow を送信します。DDoS 攻撃が検知されると、自動的に軽減されるか、または分析して手動で軽減できます。DDoS 攻撃軽減技術(Arbor Networks TMS および vDDoS 攻撃対策ソリューション)の分析と管理は、すべて Arbor Networks の Peakflow SP で行います。

手動および自動による軽減は、Arbor Networks の Peakflow SP で設定します。実際の軽減は、ASR 9000 シリーズ VSM および Cisco ASR 9000 シリーズ ルータ(Cisco ASR 9006 ルータ以上)内部にあるラインカード スロットで動作する vDDoS 攻撃対策ソフトウェアによって実行されます。Peakflow および vDDoS 攻撃対策ソリューションでは、Arbor Networks の ATLAS インテリジェンス フィード(AIF)から定期的に更新を受信して、ボットネットなどのソースの中から最も新しく関連性の高い DDoS 脅威に関して端末に通知を行います。

何を導入すべきか

- Cisco ASR 9000 シリーズ ルータ(モデル:ASR 9006 ルータ、ASR 9010 ルータ、ASR 9912 ルータ、ASR 9922 ルータ)
- Cisco ASR 9000 シリーズ VSM

- Cisco ASR 9000 vDDoS 攻撃対策ソリューション
- Arbor Networks Peakflow
- すべてのコンポーネントに対するサポート
- インストレーション
- Arbor Networks AIF のサブスクリプション

主な機能

- 1 秒以内の DDoS 攻撃検知
- ASR 9000 シリーズ VSM による最大 40 Gbps の軽減
- 1 秒あたり最大数十テラバイトのブラックリスト登録
- Tier 1 サービス プロバイダー ネットワークに対する導入拡大
- マルチテナント型の顧客ポータル

「Arbor で実証されている DDoS 攻撃軽減技術を ASR 9000 ルータと統合することで、シスコのお客様は、増大する DDoS 攻撃へ積極的に対処できるようになっています。最善の組み合わせのソリューションです。」
- Chris Rodriguez、Frost & Sullivan シニア業界アナリスト

使用可能なモデルとオプション

Cisco ASR 9000 vDDoS 攻撃対策ソリューション：ソフトウェアは 10、20、40 Gbps の軽減に対応しています。

Arbor Networks Peakflow：あらゆる規模のネットワークをサポートするためのスケール、NetFlow データの収集、DDoS 攻撃のトラフィック分析、およびお客様のログインに必要なポータルの提供を行います。

使用例

サービス プロバイダー	• ネットワーク、サービス、接続に影響を与える DDoS 攻撃の検知。 • ネットワーク エッジ ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、Web アプリケーション ファイアウォール（WAF）、侵入防御システム（IPS）など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • お客様への DDoS 攻撃防御サービス提供による収益の創出。
インターネット サービス プロバイダー	• ネットワーク、サービス、接続に影響を与える DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてクラウド DDoS 攻撃対策ソリューション サービスへ信号を送信。
ホスティング プロバイダーまたはクラウド プロバイダー	• ネットワーク、サービス、接続に影響を与える入出力に対する DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてサービス プロバイダーまたはクラウド DDoS 攻撃対策ソリューション サービスへアップストリームの信号を送信。
モバイル ネットワーク オペレータ	• ネットワーク インフラストラクチャ、サービス、端末への入力に対する DDoS 攻撃の検知と軽減。 • モバイル デバイスからの出力に対する DDoS 攻撃の検知と軽減。 • 誤設定された端末や不正動作を行うモバイル アプリケーションからの破壊的なトラフィックの検知、分析、軽減。

オーバー ザ トップ プロバイダー	• ネットワーク、サービス、接続に影響を与える入出力に対する DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてサービス プロバイダーまたはクラウド DDoS 攻撃対策ソリューション サービスへアップストリームの信号を送信。
企業	• ネットワーク、サービス、接続に影響を与える DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてサービス プロバイダーまたはクラウド DDoS 攻撃対策ソリューション サービスへアップストリームの信号を送信。
エンタープライズ データセンター	• ネットワーク、サービス、接続に影響を与える入出力に対する DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてサービス プロバイダーまたはクラウド DDoS 攻撃対策ソリューション サービスへアップストリームの信号を送信。
政府/自治体	• ネットワーク、サービス、接続に影響を与える DDoS 攻撃の検知。 • ISP Edge ASR 9000 シリーズ ルータでの DDoS 攻撃の軽減。 • ファイアウォール、WAF、IPS など、ネットワーク、サービス、ステートフル デバイスの可用性を保護。 • 必要に応じてサービス プロバイダーまたはクラウド DDoS 攻撃対策ソリューション サービスへアップストリームの信号を送信。

Cisco Capital

目標の達成に役立つファイナンス

シスコ キャピタル®では、目標を達成し、競争力を維持するために必要なテクノロジーの取得を支援します。シスコは設備投資（CapEx）の削減をサポートします。成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムは、お客様がハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に取得できるようにします。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら

データセンター オペレータによる Arbor Networks およびシスコのさまざまな機能を使用したインフラストラクチャとお客様の保護

課題

冗長接続によって、データセンター オペレータに対する小規模でシンプルな DDoS 攻撃には対処できていました。しかし、攻撃はより大規模で複雑になり、損害も大きくなっていきました。帯域幅攻撃によってデータセンターの接続が飽和し、状態枯渇攻撃によってステートフル ファイアウォールと IPS のオーバーランが発生しました。

予算の調達は困難でしたが、サービス プロバイダーは Cisco ASR 9000 vDDoS 攻撃対策ソリューションを導入することにしました。これにより、DDoS 攻撃対策ソリューション サービスからお客様に対する新たな収益が創出されました。

Arbor Networks Peakflow は 1 秒程度のほんのわずかな時間で DDoS 攻撃をすばやく検知し、軽減します。また、Cisco ASR 9000 vDDoS 攻撃対策ソリューションと Arbor Networks TMS を仮想化し、Cisco ASR 9000 シリーズ ルータに組み込むことで、お客様のネットワークを標的とした DDoS 攻撃を軽減します。Arbor Networks の Arbor Cloud により、さらに手厚い保護が実現します。インターネット接続が飽和状態になってしまう前にクラウドでこれらの攻撃をブロックすることで、プロバイダーは大規模な帯域幅攻撃からインフラストラクチャ、サービスや顧客を保護できます。

シスコが選ばれる理由

ネットワーキング業界のリーダーであるシスコは、高い拡張性と可用性を持つネットワークを構築し、それらを攻撃から防御するための知識を持つ理想的なパートナーです。DDoS 攻撃はいまや、お客様のネットワークの可用性に対する最も大きなセキュリティ脅威です。シスコは、業界トップクラスを誇る Arbor Networks の DDoS 攻撃検知（Peakflow）および軽減技術を Cisco ASR 9000 シリーズ ルータに組み込むことで、入力エッジでのネットワーク保護を実現しています。

「市場をリードする Arbor の DDoS 攻撃軽減技術を追加した ASR 9000 ルータは、ネットワーク エッジで DDoS 攻撃を軽減するというニーズを満たします。これは両社にとって賢明な選択だと言えます。」
- Jeff Wilson（Infonetics Research 社主席アナリスト）

次のステップ

このソリューションに関する一般情報の詳細については、Cisco ASR 9000 vDDoS 攻撃対策ソリューション [英語] の「At-a-Glance（概要）」を参照してください。このソリューションに関する詳細については、Cisco ASR 9000 vDDoS 攻撃対策ソリューションのデータシート [英語] を参照してください。Peakflow ソリューションの技術的な実装、拡張、運用の詳細については、Cisco ASR 9000 vDDoS 攻撃対策ソリューションのホワイト ペーパー [英語] を参照してください。

追加情報については、arbornetworks.com/asr9000 [英語] を参照してください。

DDoS 攻撃に対するネットワークの保護、およびお客様への DDoS 攻撃対策ソリューション サービスを提供するには、シスコのセールス担当者またはシスコ認定チャネル パートナーにお問い合わせください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C22-736143-00JA 17.08