Cisco ASR 9000 vDDoS 攻撃対策ソリューション

製品概要

お客様のネットワークは DDoS 攻撃から保護されていますか。被害の可能性はかつてなく高まっています。これらの攻撃の強度、頻度、規模は驚くべき速さで増大しています。DDoS 攻撃を受けると、ダウンタイムや収益損失、ネットワークの可用性低下が発生し、メディアの注目に過度にさらされる可能性もあります。これらの攻撃からネットワークを保護することが非常に重要になっています。

この問題に対処するために、シスコは Arbor Networks 社と共同で、業界をリードする DDoS 攻撃ソリューションを開発しました。Cisco ASR 9000 Virtual DDoS 攻撃対策ソリューションにより、お客様のネットワークに安全な防御線を張ることができます。またこのソリューションでは、大規模で成長を続けるサービス プロバイダーや一般企業の要件にあう拡張が可能です。

このソリューションはピアリング ポイント、データセンター、クラウド エッジ、およびエンタープライズ WAN エッジでの導入を対象としており、ネットワークの周囲に安全な防御線を効果的に構築します。vDDoS 攻撃対策ソリューションは Cisco ASR 9000 シリーズ仮想サービス モジュール（VSM）で稼働し、VSM あたり最大 40 Gbps まで利用帯域を拡張することができます。

ASR 9000 vDDoS 攻撃対策ソリューションは通常、「オンデマンド」ソリューションとして導入されますが、固定モードで動作するように設定することもできます。「オンデマンド」モードでは、宛先が攻撃のターゲットになっているトラフィックだけが、VSM の vDDoS 攻撃対策ソリューションに転送されます。正常なトラフィックには影響しません。VSM モジュールの vDDoS 攻撃対策ソリューションでは、悪意のある攻撃トラフィックだけが特定されてブロックされます。正規のトラフィックはそのまま元の宛先へと送信されます。DDoS 攻撃の最中でもサービスや業務が中断されることはありません。

ASR 9000 vDDoS 攻撃対策ソリューションは、1 つのライセンスだけで段階的に拡張できる拡張性の高いソリューションです。また複数の VSM[1] を単一のシャーシに設置することで、単一の Cisco ASR 9000 シリーズ VSM の何倍もの容量に段階的に拡張できます。よって、大規模で成長を続けるサービス プロバイダーと一般企業の要件に応じたサービスの拡張が可能です。

DDoS 攻撃の進化

DDoS 攻撃は、感染させたデバイスの処理能力を利用して、ネットワークや Web サーバの正常な運用を妨害することを目的とした、サービス妨害攻撃です。DDoS 攻撃によって年間何十億ドルもの損失が発生しています。その影響は、取引や顧客の喪失、企業の信用低下、法的責任の発生にまで及びます。今日の DDoS 攻撃は強固な悪意を持った破壊的なものになっており、集中化も進んでいます。不満を持つユーザ、悪意のあるビジネス、恐喝者などが特定のサイトや競合他社をターゲットとするこのような攻撃は、一般的な防御を簡単に回避し圧倒してしまいます。ASR 9000 vDDoS 攻撃対策ソリューションはさまざまなタイプの DDoS 攻撃を防御するため、企業は収益をもたらすミッションクリティカルな業務を犠牲にすることなく、悪意のあるトラフィックを特定しブロックできます。Cisco ASR 9000 vDDoS 攻撃対策ソリューションでは、高度な異常検出機能を使用して、インテリジェンス フィルタリングと合わせて、統合化された送信元検証とスプーフィング対策技術を動的に適用し、正規のトランザクションを通しながら、個々の攻撃フローを特定してブロックします。

[1] 単一シャーシに複数の VSM をインストールする機能は、今後のリリースでサポートされる予定です。

図 1 は Cisco ASR 9000 vDDoS 攻撃対策ソリューションの配置を示し、表 1 ではソリューションの特長と仕様をまとめています。

図 1. ASR 9000 vDDoS 攻撃対策ソリューションの配置

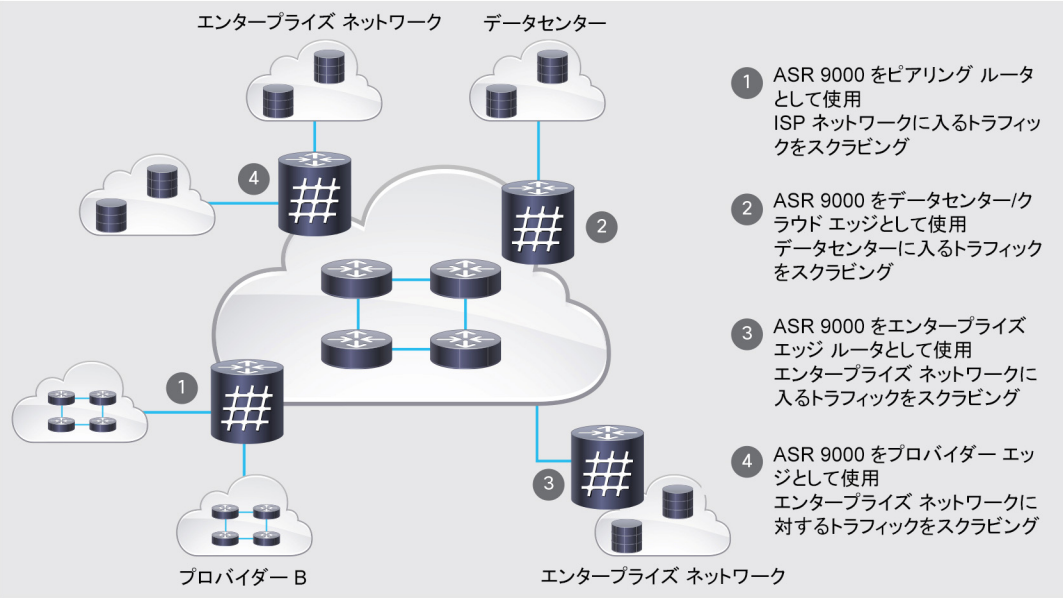

表 1. ASR 9000 vDDoS 攻撃対策ソリューションの特長および仕様

特長	利点
スループット	VSM あたり最大 40 Gbps
拡張性	1 つのシステムに複数の VSM[2]
サービスマネジメント	サービスのインスタンス化、アクティベーション、ファシリテーションは、「サービスイネーブルメント アーキテクチャ」で実行されます。
アーキテクチャ	分散型
段階的ライセンス	成長に応じて拡張可能なモデルには、10、20、40 Gbps のオプションがあります。
管理	ソリューション全体を 1 つのコンソールで一元的に管理します。
サポートされているモード	ソリューションは、「オンデマンド」モードまたは固定モードで導入できます。
ブロック アクション	ブロック アクションには、送信元のブロック/一時停止、パケット単位のブロック、そして送信元、ヘッダー、レート ベースのブロックの組み合わせがあります。
攻撃防御	Fast フラッド攻撃（TCP、User Datagram Protocol（UDP）、Internet Control Management Protocol（ICMP）、ドメイン ネーム システム（DNS）、Network Time Protocol（NTP）リフレクションおよびアンプ攻撃）、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、Session Initiation Protocol（SIP）Invite フラッド、DNS 攻撃、セキュア HTTP（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、リソース枯渇攻撃（Slowloris、Pyloris、LOIC など）、フラッシュ クラウド防御、セキュア ソケット レイヤ（SSL）暗号化パケットに潜む IPv4 および IPv6 攻撃
DDoS への対策	ブラックリストおよびホワイトリスト、位置情報のレポートおよびブロック、ゾンビ ブロック、パケット コンテンツ フィルタリング、パケット ヘッダー フィルタリング、ボットネット駆除（AIF）、異常パケットの駆除（TCP、UDP、DNS、DNSSEC、HTTP、HTTPS、SIP）、複数のスプーフィング対策、複合型攻撃防御、Cisco Discovery Network およびプロキシ認識対策、レート制限

[2] 単一シャーシに複数の VSM をインストールする機能は、今後のリリースでサポートされる予定です。

特長と利点

マルチギガビット パフォーマンス

各 VSM には高性能の処理機能が搭載され、攻撃トラフィック分析とトラフィックのクリーニングが可能になっており、大規模な DDoS 攻撃を防御できます。複数の VSM[3] を 1 つの ASR 9000 シリーズ ルータにインストールして、スループットの拡張性を高めることが可能です。

異なる攻撃ベクトルの軽減

ASR 9000 vDDoS 攻撃対策ソリューションの主な利点の 1 つは、ブラックリストとホワイトリストを維持できることにあります。ホワイトリストには承認されたホストが記録され、ブラックリストには、過去に攻撃を受けたために受信トラフィックをブロックする必要があるホストが記録されます。ブラックリストは ASR 9000 ルータのライン カードにロードされるため、ソリューションの拡張性を効率的に高められます。この機能によって、ASR 9000 の単一の VSM で 100 Gbps 以上にまで拡張できます。

このソリューションでは、いくつかの対策を複合してアプリケーション層のエクスプロイトをブロックします。HTTP 特有の攻撃が検出され軽減されます。DNS サービスは、キャッシュ ポイズニング、リソース枯渇、アンプ攻撃から保護されます。NTP、DNS、SNMP などの大規模なリフレクション攻撃も、このソリューションによって軽減されます。

動的転送

Cisco ASR 9000 vDDoS 攻撃対策ソリューションでは、「オンデマンド」スクラビング モデルが導入されます。一般的な導入では vDDoS 攻撃対策用の機器はトラフィックのデータ パス上に設置されませんが、必要に応じてデータ パス上に設置することもできます。動的転送によって、攻撃を受けている所を宛先とするトラフィックだけが自動的にリダイレクトされ、それ以外のトラフィックは通常のデータ パスを通過します。トラフィックのリダイレクトは、Border Gateway Protocol（BGP）または BGP Flow Spec などを使用して透過的に行われます。

トラフィックのスクラビング処理が実行されると、正常なトラフィックや正規のトラフィックはすべて最終的な宛先に転送されるため、これらの重要なトラフィックが失われることはありません。vDDoS 攻撃対策ソリューションでは、VMS に転送された DDoS 攻撃トラフィックだけを制御することで、最適なリソース使用率、透過性、信頼性が得られ、拡張性の高いソリューションが実現します。

サマリー

Cisco ASR 9000 vDDoS Protection ソリューションは、サービス プロバイダーと一般企業の両方のお客様を対象にしています。このソリューションにより、最も悪質な攻撃に直面しても業務が中断されることはありません。このソリューションをネットワーク エッジに導入すれば、ネットワークの周囲に安全な防御線を張ることができ、お客様のネットワーク インフラストラクチャとサービスが保護されます。

プラットフォーム サポート/互換性

Cisco ASR 9000 シリーズ vDDoS ソリューションは、以下の Cisco ASR 9000 シリーズ ルータでサポートされています。

- Cisco ASR 9904 ルータ
- Cisco ASR 9006 ルータ
- Cisco ASR 9010 ルータ
- Cisco ASR 9912 ルータ
- Cisco ASR 9922 ルータ

[3] 複数の VSM は将来のリリースでサポートされる予定です。

ハードウェアとソフトウェアの要件

このソリューションのハードウェアおよびソフトウェアの要件は次のとおりです。

ハードウェア:

- 固定およびモジュラ型のイーサネット ラインカード（第 2 世代以降）
- Route Switch Processor 440（RSP440）または Route Switch Processor 880（RSP880）
- Cisco ASR 9912 および ASR 9922 システム用 Cisco ASR 9000 シリーズ Route Processor 1（RP1）または Route Processor 2（RP2）
- 仮想サービス モジュール（VSM）

ソフトウェア:

- Cisco IOS® XR ソフトウェア リリース 5.3.0 以降
- Arbor TMS バージョン 7.0.1 以降

保証に関する情報

保証については、Cisco.com の製品保証 [英語] のページを参照してください。

発注情報

シスコ製品の購入方法については、購入案内のページの表 2 の情報を参照してください。

表 2. 発注情報

製品名	製品番号
最大 10 G のスクラビングが可能な DDoS ソフトウェア ライセンス	A9K-DDoS-LIC-10G
最大 10 G のスクラビングが可能な DDoS ソフトウェア ライセンス（スペア）	A9K-DDoS-LIC-10G=
最大 20 G のスクラビングが可能な DDoS ソフトウェア ライセンス	A9k-DDoS-LIC-20G
最大 20 G のスクラビングが可能な DDoS ソフトウェア ライセンス（スペア）	A9k-DDoS-LIC-20G=
最大 40 G のスクラビングが可能な DDoS ソフトウェア ライセンス	A9k-DDoS-LIC-40G
最大 40 G のスクラビングが可能な DDoS ソフトウェア ライセンス（スペア）	A9k-DDoS-LIC-40G=
10 ～ 20 G に対応する DDoS ソフトウェア アップグレード ライセンス	A9k-DDoS-10U20G=
10 ～ 40 G に対応する DDoS ソフトウェア アップグレード ライセンス	A9k-DDoS-10U40G=
20 ～ 40 G に対応する DDoS ソフトウェア アップグレード ライセンス	A9k-DDoS-20U40G=

シスコ サービス

シスコはライフサイクル サービス アプローチによって、サービス プロバイダー向けに包括的なサポートを提供しています。次世代 IP ネットワーク（IP NGN）の適切な導入、運用、最適化をサポートします。Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ向けのシスコ サービスは、効果的な導入に必要なサービスとアプローチを提供します。お客様のネットワーク投資が活かされるよう、最大限のパフォーマンスと可用性を実現します。シスコのサービスは、Cisco ASR 9000 シリーズの導入および実装後のサポート向けに特別に開発されたもので、ベスト プラクティスや、優れたツール、プロセス、ラボ環境を提供します。シスコ サービス チームは、お客様固有の要件に対応し、既存のサービスに対するリスクを軽減して、新しいネットワーク サービスの本稼働開始までの時間を短縮させます。

詳細情報

Cisco ASR 9000 シリーズの詳細情報については、http://www.cisco.com/jp/go/asr9000 をご覧ください。または、最寄りのシスコ代理店にお問い合わせください。また、http://www.arbornetworks.com/asr9000 [英語] もご覧ください。

シスコのサービスの詳細については、シスコの代理店にお問い合わせください。または、http://www.cisco.com/go/spservices [英語] をご覧ください。

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

C78-734529-00JA 15.08