

# Deflector Shield

## ディフレクタ・シールド (攻撃をそらす楯)

シスコはDDoS攻撃に対抗するため、Riverhead Networksを買収した  
ゲール・メレディス・オッテソン(Gail Meredith Otteson)による報告

DDoS(Distributed Denial-Of-Service:分散型サービス拒否)攻撃は、“大量破壊兵器(weapons of mass disruption)”である。これはデータを危険に晒したり、情報を盗んだりする攻撃とは異なり、数日間あるいは数週間にわたってビジネスを停止させることがあるのだ。大企業やサービスプロバイダの防衛戦術は最近までやや粗いものであったことから頻りに防御用のソースコードを要することになり、結果として、攻撃者がDoSを成功させるという結果をたびたび招いていたのである。

「いずれにしても、ビジネスを停止させられたという点では攻撃者の勝ちです。実は攻撃を察知することはそれほど難しいことではありません。重要なのはビジネスを止めることなくその攻撃をかわすことなのです」とシスコのセキュリティ・テクノロジー・グループのマーケティング担当ディレクターであるスティーブ・ウー(Steve Woo)は語る。

崩壊に直面した時にビジネスを継続できるか否かは、ビジネスの生き残りにとって基本的な課題である。DDoSの妨害による損害は収益と生産性に破壊的な影響を与える。攻撃はIT経費を上昇させ、組織を訴訟の危険に晒すことにもなる。企業がそれまで築いてきた顧客の信用が損なわれ、時には永遠に失われてしまうことにもなりかねないのだ。ヤンキー・グループは2000年2月にAmazon、eBay、Yahooおよびその他の主要なWebサイトを襲った一連のDDoS攻撃がもたらした累積損失は12億米ドルに達するだろうと報告している。その潜在的な損失は、現在さらに大きな額になるはずである。

DDoS攻撃は規模の拡大にしたがって顕在化しにく

くなり、それを検知し緩和することが一層難しくなっている。典型的なDDoS攻撃では数百台あるいは数千台の“ゾンビ”のホストを取り込み、1つのターゲットに向けて攻撃を開始する。

ゾンビは、保護されないまま広帯域で常時接続でインターネットにつながっている数百万台のコンピュータから取り込まれる。攻撃者は悪質なソフトウェアをこれらのマシンに移植し、1つのコマンドで攻撃を開始するのである。攻撃の踏み台にされたPCの所有者は、自分のPCが検知できない量のDDoSトラフィックを送信していることに気がつかない。数千台以上に増殖したゾンビが標的に投げつけるトラフィックの累積量は、そのリソースを圧倒し正当なユーザーの利用を阻害するのである。

攻撃のターゲットにはプロバイダのネットワークインフラやデータセンターのリソースが含まれる可能性もある。Eコマース、データベース、アプリケーションサーバ、Web、DNS(Domain Name System)、およびEメールシステムなどのネットワークサービス、ネットワークルータ、ファイアウォールや侵入検知システム(IDS: Intrusion Detection Systems)そしてネットワークのアクセスリンクもターゲットになり得るのだ。

進行中の攻撃を検知するには多くの方法があり、シスコはそれらを遮断する多くのツールや手法を開発してきた。しかし、Riverhead Networksが悪質なトラフィックを遮断し、合法的なトラフィックを継続して、本来のビジネスの継続を保障するソリューションが発表される2002年までは、アプリケーションごとにきめ細かな緩和対策をとることが大きな課題となっていたのである。

## 自己防衛型ネットワーク

2004年3月、シスコはRiverheadの買収を完了し、同社のユニークなDDoS検知・緩和のテクノロジーを自らのセキュリティポートフォリオに加えた。

「これと類似したものなど、この地球上には存在していないのです」とシスコのITインターネット・サービス・グループのネットワーク・エンジニアであるローランド・ドビンス(Roland Dobbins)は言う。

「これは、シスコのセキュリティツールキットの中でも重要なツールなのです」

このDDoSソリューションには、自動的に脅威を検知すると同時に状況に適した方法で対抗、攻撃中もサービスの継続性を確保してシスコの自己防衛型ネットワーク(『PACKET』2004年夏号の『自己防衛型ネットワーク』を参照)に極めて重要な機能を加えるCisco Guard XTおよびCisco Traffic Anomaly Detector XTが含まれている。

GuardおよびDetectorは大企業や政府機関の一般に公開されているデータセンターとWebサービス、およびマネージドホスティングやWebコネクティビティサービスを提供しているサービスプロバイダの多層防衛戦略には欠くことのできないコンポーネントとなっている。このソリューションはフラディングおよびアプリケーションという2つの基本的なタイプの攻撃に対して防御する。

フラディング攻撃(flooding attack)は大量のTCP、UDP、またはInternet Control Message Protocol(ICMP)のパケットによってネットワークリンクを圧迫し、有効なトラフィックがネットワークのリソースを使えなくなり、その負荷によってインラインのセキュリティデバイスに障害が発生する原因となる。

アプリケーション攻撃(application attack)は、TCPやHTTPなどのプロトコルの予期されるふるまいを利用してコンピューティングリソースを枯渇させることによって、正当なトランザクションやリクエストの処理を不可能にしてしまう。その例として、HTTPハーフオープン(half-open)やHTTPエラー攻撃(error attacks)がある。

## その他のセキュリティツール

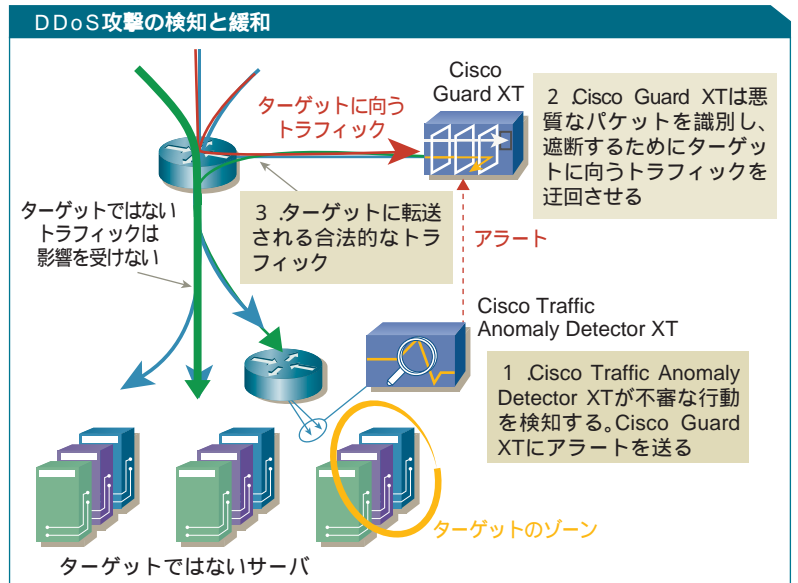
シスコは既存の技術を利用して、DoS攻撃を検知し緩和するために多くのツールやテクニックを創り出してきた。これらのデバイスは多層防衛(defense-in-depth)アーキテクチャの中で極めて重要なセキュリティ上の役割を果たし、シスコのセキュリティツールキットの中でも重要なツールである。ここには以下が含まれる。

ファイアウォール(Firewall)は、主に静的なセキュリティポリシーを実行するのに使われる。

侵入検知システム(Intrusion detection system)は、シグネチャが分かっている攻撃の検知に有効であるが、単体ではDoS攻撃に対する拡張可能で細かい対策は提供していない。

ルータ(Router)は、Cisco Guardの緩和プロセスで重要な役割を果たしている。アクセス制御リスト(ACL: Access Control Lists)およびRemotely Triggered Blackholes(RTBH)は非常に有益だが、一般には“付随的損害(collateral damage)”を限定するのに役立つふるまいに基づくフィードバックメカニズムが含まれていない。

ロードバランサー(Load balancers)はDDoSアプリケーション攻撃に対抗するために設計されたものではないが、非常に大きな負荷を分散させるのに役立つ。



**通常通りの業務:** 多くのデバイスがDDoS攻撃を検知し、Cisco Guardへアラートを送ることができる。Guardはルータにターゲットのデバイスへ向うトラフィックをすべて自分へ迂回させるよう伝える。トラフィックを分析し、“洗浄し(scrubs)”, 悪質なパケットを廃棄してから合法的なトラフィックをターゲットへ転送し、攻撃下でもビジネスの継続性を維持する

## 小さな者たちを守る：長距離迂回法

サービスプロバイダとしては、数ギガビットのアクセスリンクを持つ大企業の顧客にはそれぞれに1つのGuardを展開することが適切な処置かもしれない。しかし、もっと規模の小さい顧客の低速リンクのそばで多くのGuardを展開するのはコスト効果が薄い。サービスプロバイダは中央のネットワークのロケーションで1つのGuardを展開し、顧客の域内へのエッジリンクにDetectorを配置する長距離迂回法を使って、このような顧客を効率よく守ることができるのである。エッジのDetectorが識別した攻撃トラフィックは、複数のBGPピアリングルータから中央のGuardへど長距離迂回して洗浄され、多くはGRE(Generic Routing Encapsulation)トンネルを通じて、あるいはその他のトポロジー的に適切な再注入法で元の宛先へ転送される。

サービスプロバイダの中には、すでにCisco GuardとDetectorを使ってマネージドDDoS防御サービスを提供しているところがある。Guardを装備したこれらのプロバイダは、もうネットワーク上の全員を守るためにターゲットにされた顧客に対するサービスを中断する必要はない。彼らはむしろ自分自身とその顧客双方の収益およびビジネスの継続性を守り、Service-Level Agreements(SLA)を順守することができるのである。

Rackspace Managed Hostingはテキサス州サンアントニオに本社を置くマネージドホスティングプロバイダだ。「熱烈支援」を標榜する同社は、極めて重大なDDoS攻撃に晒されていることを顧客に伝えたくなかったのである。Guardに関するベータテスト協力者であり、シスコのレファレンスカスタマでもあるRackspaceはマネージドDDoSサービスを提供した最初の会社の1つだ。RackspaceはPreventTierサービスを通じて5600社の顧客のさまざまな要求に応え、専属契約あるいはアドホック的にDDoS緩和サービスを提供している。Guardは日常的なDDoS攻撃の約80%を自動的に緩和。Rackspaceの卓越した管理体制で、さらに新しいさまざまな襲撃も簡単に攻略しているのである。

「Guardの素晴らしい点はクリティカルパスに位置していないことです」とRackspaceのエンジニアリング担当副社長であるポール・フルータン(Paul Froutan)は言う。

「我々のシステムに障害発生ポイントを生むことがないのです。これは我々にとって極めて重要なことなのです」

### 効果的な緩和戦略

DDoS防御に専心するには、実行すべき4つのポイントがある。まず第一に攻撃を検知するだけでなく、それを緩和すること。第二に合法的な(正しい)トラフィックと悪質なトラフィックを正確に区別し、サービスを継続できるようにすること。第三に価値の高いセキュリティサービス資産(ファイアウォールやIDSなど他のセキュリティデバイスを含む)を最大限守ることができるように、トポロジー的に適切な方法で展開されていること。最後に、予測可能でコスト効果の高い方法で拡張できることである。

Cisco Guard XTとCisco Traffic Anomaly Detector XTはシスコのルータと対話しながら、この4つの要求をすべて満たす効果的なソリューションを創造する。

4つのステップのソリューションには検知 / 迂回 / 分析 / フィルタリング / フォワーディングが含まれている(37ページの図を参照)。

### 検知

Cisco Guardは正常なトラフィックパターンを見張り、それを学習してから、観察したふるまいに基づいて動的にポリシーとスレッショルド(閾値)を作成する。Detectorは新しいDay-Zero型の攻撃が識別できるように、異常に基づくアルゴリズムを使ってDDoSの活動を見張る。また、この活動が変化した場合には変則的なトラフィックとそのターゲットに関する詳細な情報とともにGuardにアラートを送るのである。

シスコの顧客の多くはすでにDDoS攻撃を検知できるIDSなどのデバイスを使っているが、これらのデバイスもCisco Guardにアラートを送るように構成することができる。デバイスにはCisco IDSアプライアンス、Cisco Catalyst 6500 IDSモジュール(IDSM-2)およびCisco NetFlowテクノロジーを基礎にしたArbor Networks Peakflowサービスプロバイダ向け異常検知システムが含まれている。これらの検知システムは、すべて攻撃中にはCisco Guardを通じた迂回を始動させるよう構成することができ、またネットワーク運用担当者が必要に応じてマニュアルによる始動を選ぶこともできる。

### 迂回

いったんGuardに潜在的な攻撃のアラートが届くと、`/**/=/* diversion phase`(迂回の段階)が開始される。Guardは隣接する上流のルータにBGP(Border Gateway Protocol)をアナウンスすることによって迂回を開始する。そのルータはDDoSターゲットに向うトラフィックをすべてGuardへ送る。他の宛先へ向かうトラフィックはそのままネットワークトポロジーを通じて引き続きターゲットではないゾーンへ向かうので、ターゲットに向うトラフィックの迂回による影響を受けない。

### 分析とフィルタリング

Guardは迂回してきたトラフィックを分析し、フィルタリングによって悪質なバケットを廃棄して合法的なものだけを転送する。Guardはそれを遂行するために、フローを“洗浄(scrub)”するMulti-Verification Process(MVP)と名付けた特許申請中のユニークな技術を使

っている。この浄化プロセスには5つのモジュールがある。

**パケットフィルタリング**( Packet filtering ): 静的および動的双方のDDoSフィルタが、重要ではないトラフィックがターゲットに到達する前に遮断する。静的フィルタはユーザーが構成できるが、出荷時にデフォルト値が設定されている。動的フィルタは観察したふるまいと詳細なフロー分析に基づいて別のモジュールによって挿入されるもので、リアルタイムのアップデートで検証レベルを上げたり、識別された悪質なソースやフローを遮断したりすることができる。

**アクティブ・ベリフィケーション**( Active verification ): システムに入るパケットの合法性を検証することで、有効なパケットを廃棄してしまうリスクを排除する。ところが、進化したDDoS攻撃は合法的なIPソースアドレスを使ってくるので、このステップで遮断できるのは旧型の攻撃だけとなる。その合法的なアドレスからのフローは保留状態にし、異常認知モジュールに転送してさらに分析を深める。

**異常認知**( Anomaly recognition ): 静的フィルタやアクティブ・ベリフィケーションで止められなかったトラフィックを監視し、基準のふるまいパターンと比較して、正常な運用時に見られる合法的なソースのパターンとの乖離を調べる。この段階で攻撃のソースとタイプを識別して悪質なトラフィックを遮断、あるいはさらに詳細な分析を行う動的フィルタをインストールするガイドラインをパケットフィルタリングモジュールに提供する。

**プロトコル分析**( Protocol analysis ): 異常認知モジュールが識別した不審なフローを処理し、アプリケーション別の攻撃を調べる。不完全なトランザクションやエラーを含め、変則的なふるまいをするプロトコルのトランザクションを検知する。

**レート制限**( Rate limiting ): これはオプション機能であり、変則的なふるまいをするフローがターゲットを圧倒するのを避けるために、フローごとのトラフィックシェーピングを行うと同時にさらに細かい監視をする。

## フォワーディング

合法的なフローはGuardが検証した後でターゲット

に転送され、攻撃中もサービスの継続性が維持されている。この最終ステップこそがCisco Guardが他のどのDDoS緩和の技術や製品とも異なる特長を築いている点である。

## スケーラビリティとクラスター化

DDoS攻撃の本質を考えれば、非常に大量のパケットをうまく処理する極めて拡張性に優れたソリューションが必要になってくる。

Cisco Traffic Anomaly Detector XTは、300万ppsで同時に最大90ゾーンまで、2Gbpsの監視を行うために2ギガビットイーサネットインタフェースを持っている。Cisco Guard XTにも2ギガビットイーサネットインタフェースがあり、最大100万ppsまで1Gbpsの緩和を行うことができる。Guardは最大150万のコネクションを同時に処理することができ、サーバのタイプやゾーンの大きさによって異なるが、平均して同時に攻撃された15ヵ所のゾーンを保護する。これは最大で10万台のゾンビに対する防御が可能だということであり、1ミリ秒以下のレイテンシで合法的なトラフィックをターゲットに送ることができる。

両デバイスとも即日展開が可能で、コマンドラインインタフェースまたはWebベースのユーザーコンソールを通じた管理ができる。

通常、中規模のサービスプロバイダや企業の非武装地帯( DMZ : demilitarized zone )のネットワークなら、1対のGuardで十分守ることができる( DMZは外部のインターネットユーザーにWebおよびFTPサーバを含む公共のサーバへのアクセスを許す一方、企業の私的なLANに対するセキュリティを維持している )。

さらに大きなキャパシティが必要な場合には1台のCisco Catalyst 6500シリーズ・スイッチの背後でGuardを最大8つまでクラスター化し、非常に大量の攻撃や複数のターゲットに対する攻撃で数ギガバイトの保護が可能である。

DDoS攻撃の攻略に関するホワイトペーパーは、[cisco.com/packet/163\\_5b1](http://cisco.com/packet/163_5b1)で見ることができる。