2015 年 12 月 25 日
株式会社セキュアソフト

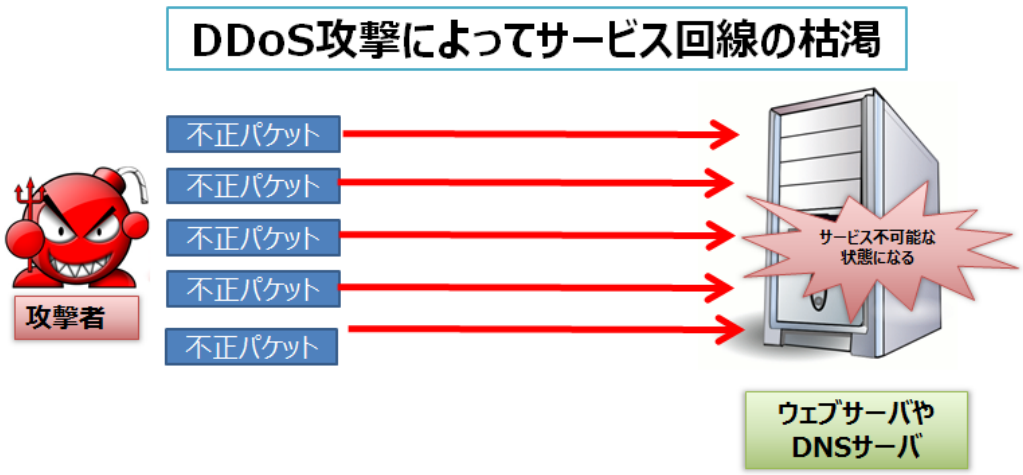
Securesoft Sniper ONE の特徴：Rate Limit 機能

Sniper ONE には 8 つの特徴的なオプション機能が搭載されています。「IPS 機能」、「DDoS 対応機能」、「DNS サーバ保護機能」、「RegEx 対応機能」、「Rate Limit 機能」、「DHCP サーバ保護機能」、「VoIP ネットワーク保護機能」、「HTTPS 対応機能」があります。Sniper ONE はこのオプションライセンス機能を利用して 1 台のアプライアンスで 8 つの機能を組み合わせて利用する事が可能です。

本レポートでは Sniper ONE の 8 つの機能の中で、「Rate Limit 機能」について説明いたします。

1. サービス回線の枯渇

サービス回線の枯渇事象は、ウェブサービスや DNS サービスのために用意した回線の処理範囲より多量の通信が発生し、サービス回線のリソースが一杯となり、ウェブページが正常に表示されるのに時間が掛かるか、もしくは、全く表示されない場合に発生しています。この現象は多量のトラフィックを送って攻撃する DDoS 攻撃によって被害が発生する場合が多く、また、最初にインフラを設計した時のサービス回線の最大処理能力を超えるユーザがサービスを利用する事によっても発生し、このようなケースは少なくありません。



【図 1】DDoS 攻撃によってサービス回線の枯渇が発生

DDoS 攻撃やユーザ数が増加される事によってサービス回線のリソースが枯渇される事を防ぐためには、多量のトラフィックを発生するユーザやサーバから発生する通信量を効果的に制限する Rate Limit 機能が大変有効です。 Sniper ONE では Rate Limit 機能をオプション機能として搭載しています。

2. Securesoft Sniper ONE の特徴：Rate Limit 機能

Sniper ONE のオプション機能としての Rate Limit 機能は外部から内部への大量のアクセスが発生する場合、正常通信であっても内部インフラ保護のためにアクセスを制限する事が可能です。特に Sniper ONE の Rate Limit 機能は大量のトラフィックを発生するサービスに対して制限(Rate Limit)が可能です。

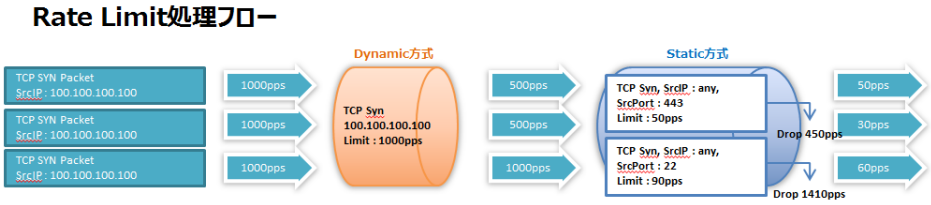
Sniper ONE の Rate Limit 機能は「Dynamic 方式」と「Static 方式」、2 つの方式をユーザに提供し、柔軟にサービストラフィックを制御する事をサポートします。

1） Dynamic 方式

- ヘビーユーザ(攻撃者含)もしくは大量のトラフィックを発生するサーバの通信を自動で検出します。
- Rate Limit 専用のシグネチャ(Flood 系)ごとに閾値ベースで制限します。
- リアルタイムに状況確認と迅速な対応が可能です。
- 閾値学習機能を利用することによって閾値を自動的に設定することが可能です。

2） Static 方式

- 保護しようとする対象(回線、サーバ)が明確に把握できていることを前提として、その特定通信を制限することを想定した方式です。
- 5-Tuple(Source IP address/port number, Destination IP address/port number and the protocol)ベース制限条件をかけてルール設定します。



【図 2】Rate Limit の処理フロー

また、Sniper ONE の管理画面からトラフィックが制限されることを簡単にチェックする事が可能です。

【図 3】多量のトラフィックが制限された通信量グラフ（Sniper ONE の管理画面から）

3. まとめ

DDoS 攻撃によって生じるサービス回線の枯渇は Anti-DDoS ソリューションを利用して対応する事が可能です。しかし、正常なユーザでも接続数が増加する事によって生じるサービス回線枯渇は Anti-DDoS ソリューションだけでは限界があります。また、ユーザ数が増加する事に対応する為にはサービス回線の施設をアップグレードする事が根本的な対策案となりますが、そのために発生する所要時間やコストは大きな負担となります。

Sniper ONE の Rate Limit 機能はヘビーユーザ(攻撃者を含む)もしくは大量のトラフィックを発生するサーバの通信量を制限して、他のライトユーザに安定的なサービス提供をする事が可能です。そして、Anti-DDoS 機能を同時に利用することで DDoS 攻撃によって生じるサービス回線枯渇に関しても有効な対策となります。

以上