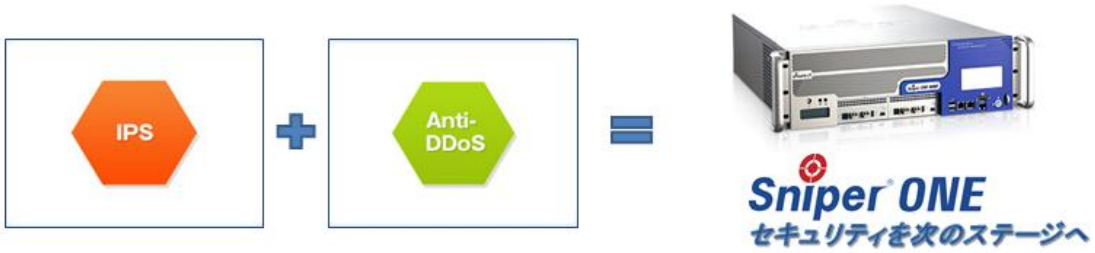
2015 年 8 月 21 日

株式会社セキュアソフト

SecureSoft Sniper ONE による DoS/DDoS 攻撃対策例

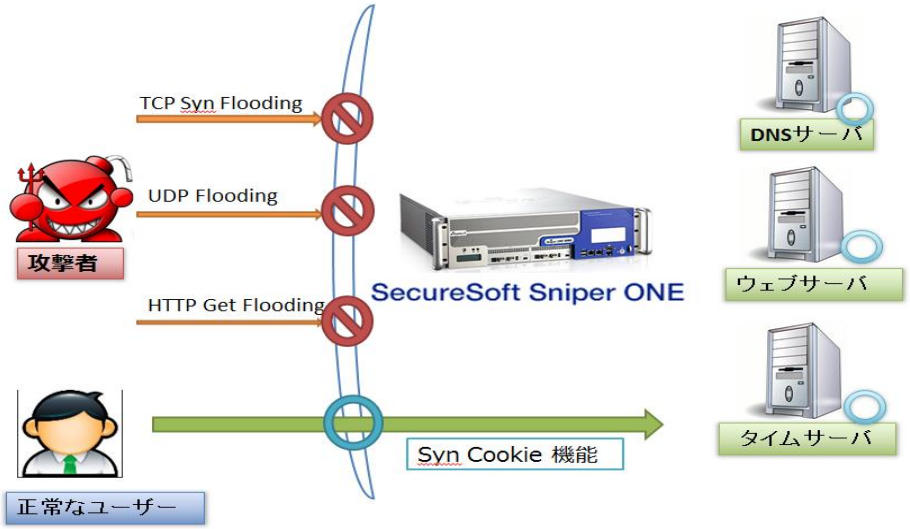
1. 概要

「JPCERT/CC インシデント報告対応レポート」（7 月 14 日発表）では、「DoS/DDoS 攻撃」は前四半期から倍増していることが確認されました。増加している「DoS/DDoS 攻撃」に対し、Sniper ONE の Anti-DDoS 機能を利用した「DoS/DDoS 攻撃」対策について説明いたします。



2. Sniper ONE による対策

「DoS/DDoS 攻撃」のなかで、特徴的な①「TCP Syn Flooding」、②「UDP Flooding」、③「HTTP GET Flooding」の対策について説明いたします。

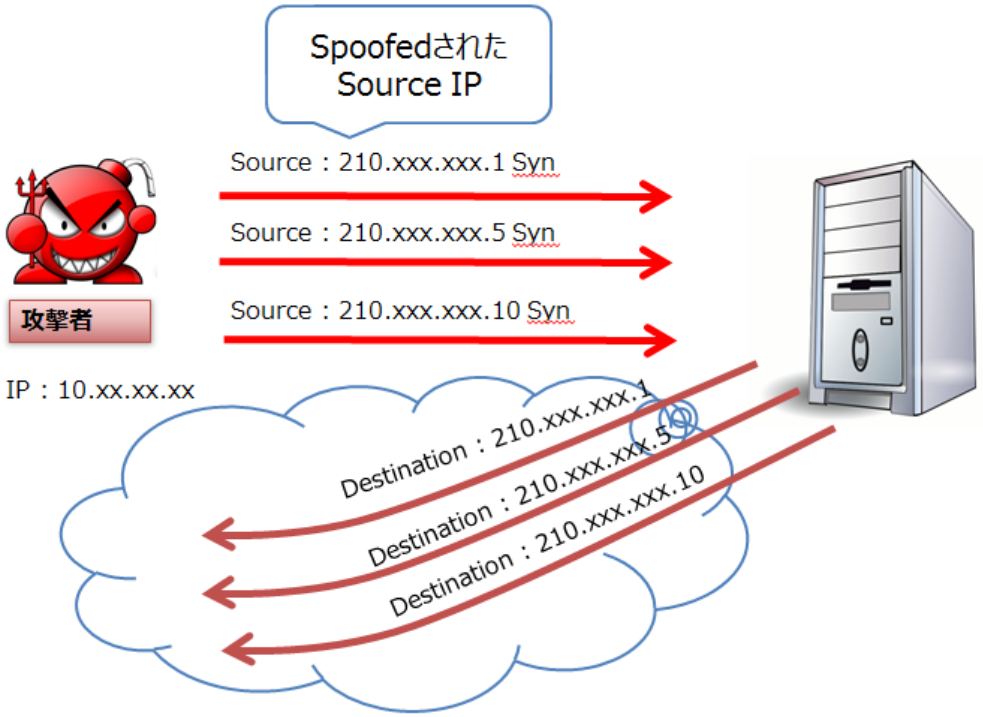


【図 1】Sniper ONE による多様な DDoS 攻撃の対策イメージ

①Spoofed TCP Syn Flooding

(1) 攻撃説明

偽装した IP アドレスから大量の Syn パケットを対象サーバに送りつける攻撃です。対象サーバでは Syn パケットに対し、Syn/Ack パケットを偽装された IP への送信と Ack パケットの受信待ちとなり、サーバの負荷の増加を招き、サービス不能状態となります。



【図 2】Spoofed Syn Flooding 攻撃

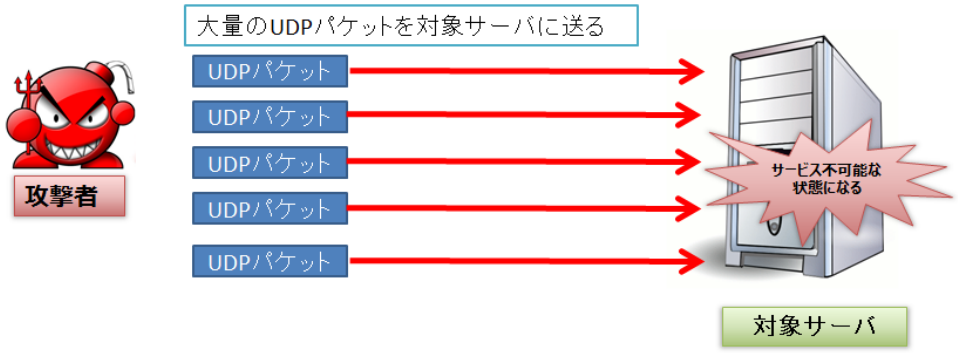
(2) Sniper ONE による対策

Sniper ONE の Anti-DDoS 機能は、このような TCP Syn Flooding 攻撃に対し、独自のシグネチャによる対策と TCP SSS エンジンにより正規の通信を保護しながら「DoS/DDoS 攻撃」のみを検知/遮断する機能を提供しています。

②UDP Flooding

(1) 攻撃説明

大量の不正な UDP パケットを送ることで対象サーバをサービス不能な状態にさせる「DoS/DDoS 攻撃」となります。この攻撃の対象としては、DNS サーバや NTP サーバがあります。



【図 3】UDP Flooding 攻撃

(2) Sniper ONE による対策

様々な UDP の「DoS/DDoS 攻撃」に対して Sniper ONE の Anti-DDoS 機能は下記のシグネチャと UDP SSS エンジンによりサーバを守る事が可能です。

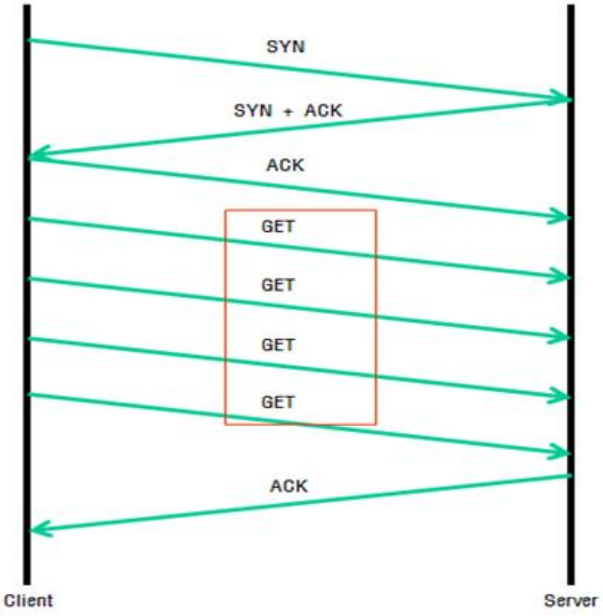
【表 1】Sniper ONE の UDP Flooding 系のシグネチャ

シグネチャ	説明
UDP Flooding	ある IP アドレスに対して同一のデータが閾値以上送信される場合に検知/遮断します。
UDP Source IP Flooding	特定の Source IP アドレスから UDP パケットが閾値以上になる場合に検知/遮断します。
UDP Destination IP Flooding	特定の Destination IP アドレスで UDP パケットが閾値以上になる場合に検知/遮断します。
UDP Packet Flooding	Source IP - Destination IP に対して UDP パケットが閾値以上になる場合に検知/遮断します。
UDP Tear Drop	UDP packet が fragment された場合に検知/遮断します。
UDP Invalid Data size	UDP Payload データが存在しない場合に検知/遮断します。
UDP Invalid Port	Src Port 又は Dst Port が 0 である場合に検知/遮断します。

③HTTP Get Flooding

(1) 攻撃説明

HTTP Get Flooding は TCP セッションが確立した後に Web サーバへ大量の Get リクエストを発生させることで、Web サーバの処理負荷量を増加する攻撃です。



【図 4】HTTP Get Flooding の攻撃 flow

(2) Sniper ONE による対策

Sniper ONE の Anti-DDoS 機能は HTTP Get Flooding に対するシグネチャを提供しています。シグネチャの検知ポリシーは下記の通りです。

【表 2】Sniper ONE の HTTP Get Flooding に関係するシグネチャ

シグネチャ	説明
HTTP Transaction Flooding(GET)	HTTP Get リクエストが閾値以上になる場合に検知/遮断します。

Sniper ONE の Anti-DDoS 機能で上記のシグネチャを利用して HTTP Get Flooding 系の攻撃を検知/遮断するができます。

また、HTTP Cookie 機能を利用して、正常なユーザのリクエストと不正なリクエストを区分する事が出来ます。

3. まとめ

今回は「DoS/DDoS 攻撃」に対する Sniper ONE の Anti-DDoS 機能をご説明しました。Sniper ONE の Anti-DDoS 機能はご紹介した対策以外にも様々な「DoS/DDoS 攻撃」対策機能やシグネチャを備えています。今後、ますます増加する可能性が高い「DoS/DDoS 攻撃」に対して、有効性の高いアプライアンスとして Sniper ONE をおすすめいたします。

以上