BCP38

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

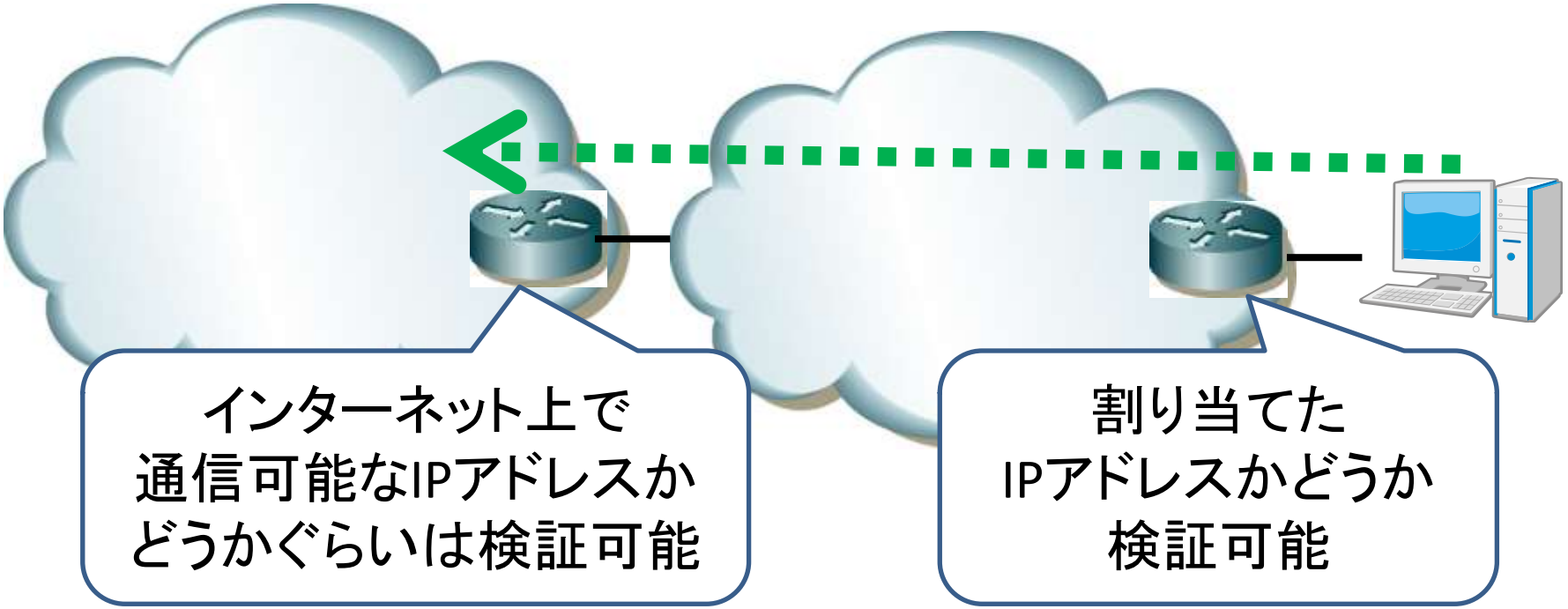
BCP38概要

- IETFのBest Current Practice, RFC2827
  - http://tools.ietf.org/html/bcp38
- 送信元IPアドレスの詐称を防ぐ
  - 詐称を利用した攻撃の影響を低減できる
  - 攻撃元を追跡できるようになる

BCP38実装

- パケットフィルタ
  - 許可する送信元IPアドレスであれば通過させる
  - それ以外のパケットを破棄
- uRPF strictモード
  - 経路情報を利用して送信元IPアドレスをチェック
  - そのインタフェースに向いている経路に対応する送信元IPアドレスであれば通過させる
  - 設定例とかは
    - http://www.janog.gr.jp/meeting/janog18/files/DNSamp_Maz.pdf

BCP38実装個所



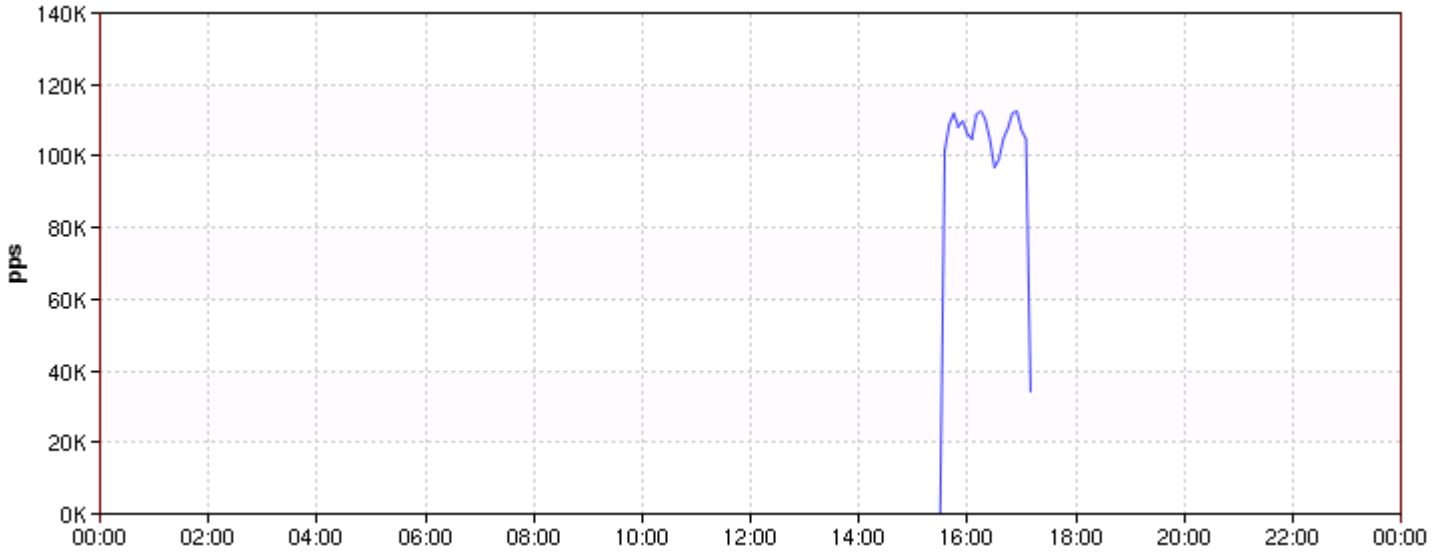
- ISPの顧客収容ルータ
  - パケットの送信元に近いところでやる必要がある

IIJでの実装

- 2006年から導入
  - 機器検証
  - カスタマサポート部門や営業部門からの協力
  - 顧客アナウンス
  - 1年がかりぐらいのプロジェクト
  - 実装ポリシも紹介しています
    - http://www.iij.ad.jp/company/development/tech/activities/sav/
- 動いてるよ！

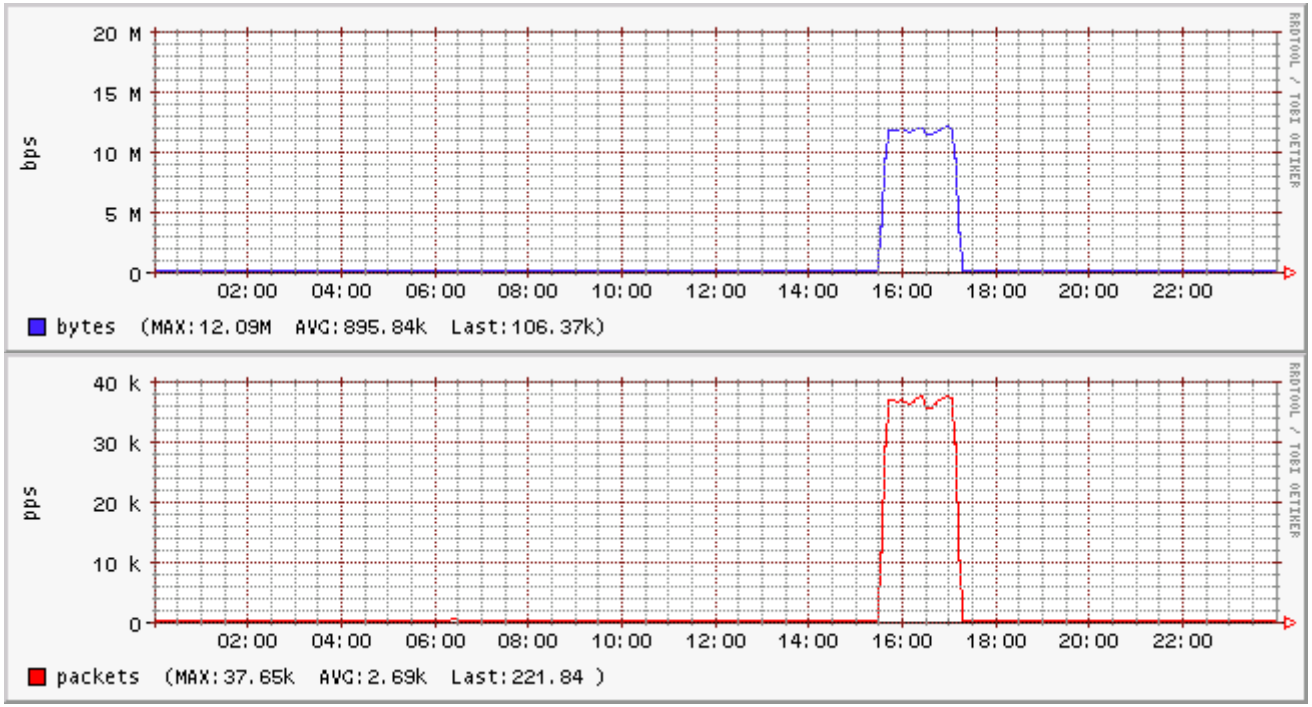
ある攻撃と思しきトラヒック

- 先週の話です
- 110Kpps程度のsyn floodと思われるトラヒック
- とあるIXから流入



uRPF looseモードで攻撃軽減

戻りの経路が無いので破棄したトラヒック



- 攻撃の発生元でBCP38していれば、影響をもっと軽減できたはず