Say it your way

Hệ thống chống DDOS tự phát triển bởi Viettel

Hanoi - 2016

Nội dung chính

- Tình hình DDOS hiện tại: Trên thế giới và mạng ISP Viettel
- Giải pháp Anti DDOS Volume based tại Viettel
- So sánh sản phẩm thương mại
- The End

Giới thiệu về DDOS

- DDOS: Phương thức tấn công từ chối dịch vụ. Có 2 kiểu tấn công chính:
- Tấn công DDOS Volume Based: Làm nghẽn đường truyền hạ tầng mạng, ảnh hưởng dịch vụ diện rộng
- Tấn công DDOS layer 7: Tấn công dịch vụ tầng ứng dụng, làm nghẽn tài nguyên của 1 victim

Tình hình DDOS trên thế giới

- Thống kê Arbor: lưu lượng attack lớn nhất đã lên tới trên 300 Gbps (từ 2009-2013)

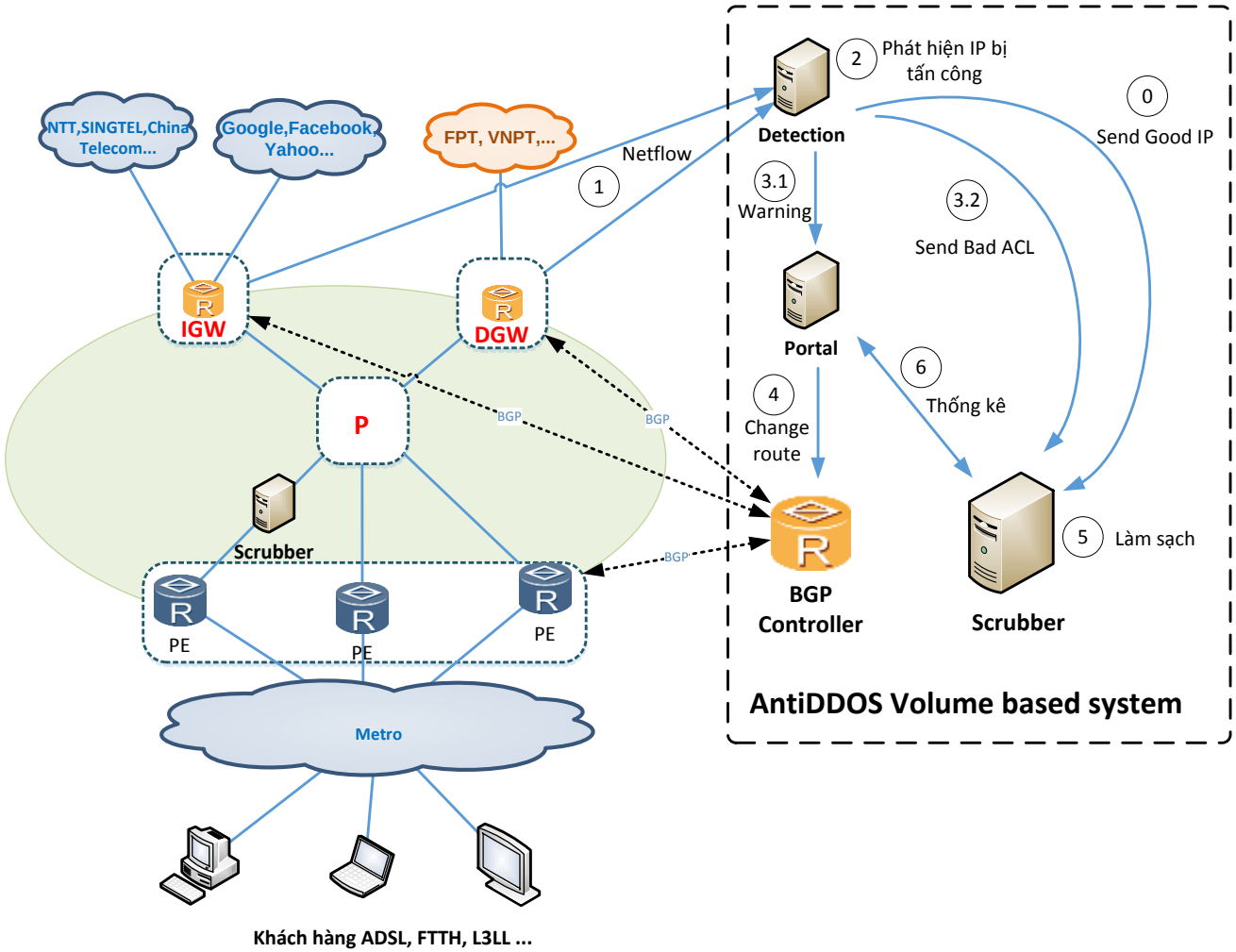
Tình hình DDOS tại Viettel

- Thống kê trong 1 tháng gần nhất, trên hệ thống phát hiện DDOS từ SIRC có 120 khách hàng dịch vụ cố định của Viettel và IDC bị tấn công DDOS
- Viettel IDC đã ghi nhận cuộc tấn công DDOS lớn nhất lên đến 20Gbps (ngày 25/7/2015 tại Bình Dương)
- Ngày 29/2/2016 VTNet tiếp nhận cuộc tấn công DDOS 1 khách hàng L3LL nhưng làm mất dịch vụ 28 khách hàng L3LL khác
- Gần đây nhất ngày 29/4/2016 Movitel bị tấn công DDOS làm nghẽn 4/5 uplink quốc tế

Việc xây dựng hệ thống Anti DDOS tại Viettel

- **Anti DDOS layer 7:**
  - Viettel đã hoàn thiện giải pháp, đã triển khai cho Văn phòng Chính phủ
  - Trong 1 tháng gần đây nhất, hệ thống phát hiện và tự động chặn 46 cuộc tấn công vào cổng thông tin điện tử chính phủ
- **Anti DDOS Volume Based:**

Giải pháp Anti DDOS Volume Based của Viettel



Các module thành phần

- Detection: Dùng để phát hiện cảnh báo IP bị tấn công DDOS
- BGP Controller: Là thiết bị Router, dùng để trigger thay đổi định tuyến tới lớp Edge (Gateway, PE)
- Scrubber: Dùng để lọc các traffic tấn công, trả về traffic sạch
- Portal: Xem thông tin cảnh báo, trạng thái cuộc tấn công, ra lệnh cho BGP Controller thay đổi định tuyến

Flow hoạt động chính

- (1): Các router IGW, DGW cấu hình đẩy Netflow về hệ thống Detection
- (2): Hệ thống Detection sẽ phát hiện ra:
  - (3.1): IP nào đang bị tấn công, gửi cảnh báo cho Portal
  - (3.2): Luồng traffic nào (UDP/TCP sync/SSDP,…) đang tấn công, gửi ACL cho Scubber để làm sạch
  - (0): Dựa vào netflow để lọc ra những good IP và định kỳ gửi cho hệ thống scrubber để tránh chặn nhầm.

Flow hoạt động chính

- (4): Sau khi Portal nhận được cảnh báo, sẽ gửi lệnh thay đổi route của địa chỉ bị tấn công đi qua hệ thống Scrubber.
- (5): Sau khi toàn bộ traffic tấn công đi qua hệ thống Scrubber, hệ thống Scrubber căn cứ vào thông tin gửi từ hệ thống Detection để làm sạch traffic.
- (6): Trong quá trình làm sạch, hệ thống Scrubber và Portal trao đổi dữ liệu về đợt tấn công để hiển thị rên Portal nhằm theo dõi hiệu quả của việc làm sạch traffic.

Module Detection

- Nhận traffic Netflow từ IGW, DGW
- Phân tích dữ liệu netflow để:
  - Đưa ra các good IP (DNS, NTP, Game server …), định kỳ gửi sang hệ thống Scrubber
  - Cảnh báo nếu 1 IP bị tấn công, gửi cảnh báo cho Portal
  - Đưa ra các flow đang tấn công IP đó, gửi ACL của các flow này sang hệ thống Scrubber để làm sạch.

Module Scrubber

- Cho phép các good IP gửi từ Detection đi qua
- Chặn các flow đang tấn công
- Phát hiện fake source IP
- Giới hạn rate limit theo IP client
- Giới hạn rate limit theo IP destination
- Trao đổi với Portal về các thống kê của đợt tấn công - realtime

Module Portal

- Nhận và hiển thị thông tin cảnh báo từ Detection
- Gọi lệnh thay đổi định tuyến của 1 IP đích thông qua BGP Controller
  - Gọi lệnh tự động khi nhận được thông tin cảnh báo từ Detection
  - Gọi lệnh bằng tay khi nhập IP trên Portal
- Trao đổi dữ liệu với Scrubber để hiển thị thông tin cuộc tấn công DDOS – real time
  - bps + pps vào/ra (tổng, per protocol tcp-udp-icmp-fragment)
  - Loại tấn công
  - Thống kê top N (10/20/..) các IP tấn công nhiều nhất
  - Top flow (ACL) tấn công nhiều nhất.

Module BGP Controller

- Can thiệp định tuyến BGP tới tất cả các phân lớp Gateway, PE:
  - Chặn tấn công theo IP source/destination, tùy chọn theo phân lớp IGW, DGW hoặc PE.
  - Lái lưu lượng tấn công cần làm sạch qua module Scrubber

So sánh triển khai của các ISP lớn trên thế giới

- 1 số ISP đang kinh doanh giải pháp Anti DDOS như 1 service như : China Telecom; AT&T; Shenzhen Telecom … đa số dùng giải pháp Abbor

- Sản phẩm Anti DDOS của Arbor bao gồm : CP + TMS+ APS báo giá 1 tỷ VNĐ/ 1Gbps băng thông tấn công cần xử lý

Say it your way

CẢM ƠN!