HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Lương Hòa Cương

NGHIÊN CỨU GIẢI PHÁP BGP FLOWSPEC ĐỀ XUẤT ÁP DỤNG CHO HỆ THỐNG MẠNG

CHUYÊN NGÀNH: HỆ THỐNG THÔNG TIN
MÃ SỐ : 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

(Theo định hướng ứng dụng)

Hà Nội - 2019

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **PGS.TS. TRẦN QUANG ANH**

(Ghi rõ học hàm, học vị)

Phản biện 1: ……

Phản biện 2: ……

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

1. Lý do chọn đề tài

Trong những năm gần đây, hình thức tấn công DDoS thường được các hacker sử dụng để tấn công, gây tê liệt, gián đoạn các hệ thống mạng, dịch vụ. Theo khảo sát năm 2016, có những cuộc tấn công dai dẳng và kéo dài lên đến 48.5 giờ và đạt tới tần suất lớn nhất là hơn 200 Gbit trên giây. Tấn công từ chối dịch vụ là kiểu tấn công gây cạn kiệt tài nguyên hệ thống hoặc gây nghẽn đường truyền, làm ngắt quãng quá trình cung cấp dịch vụ, tệ hơn làm toàn bộ hệ thống ngừng hoạt động.

Hiện tại, các hệ thống mạng của các đơn vị đều đang sử dụng giao thức BGP để định tuyến, kết nối Internet trong nước, quốc tế. Do đó, việc nghiên cứu, áp dụng kỹ thuật BGP FlowSpec để đối phó, hạn chế nguy cơ tấn công DDos nhằm vào hệ thống mạng là hết sức đúng đắn, cần thiết.

2. Mục đích nghiên cứu

Mục đích của đề tài nghiên cứu giải pháp BGP FLOWSPEC nhằm ngăn chặn các cuộc tấn công DdoS giúp cho hệ thống mạng của đơn vị hoạt động an toàn và ổn định

3. Đối tượng và phạm vi nghiên cứu

Đối tượng: Các đơn vị cung cấp dịch vụ

Phạm vi: Áp dụng giải pháp BGP FLOWSPEC nhằm ngăn chặn các cuộc tấn công Ddos

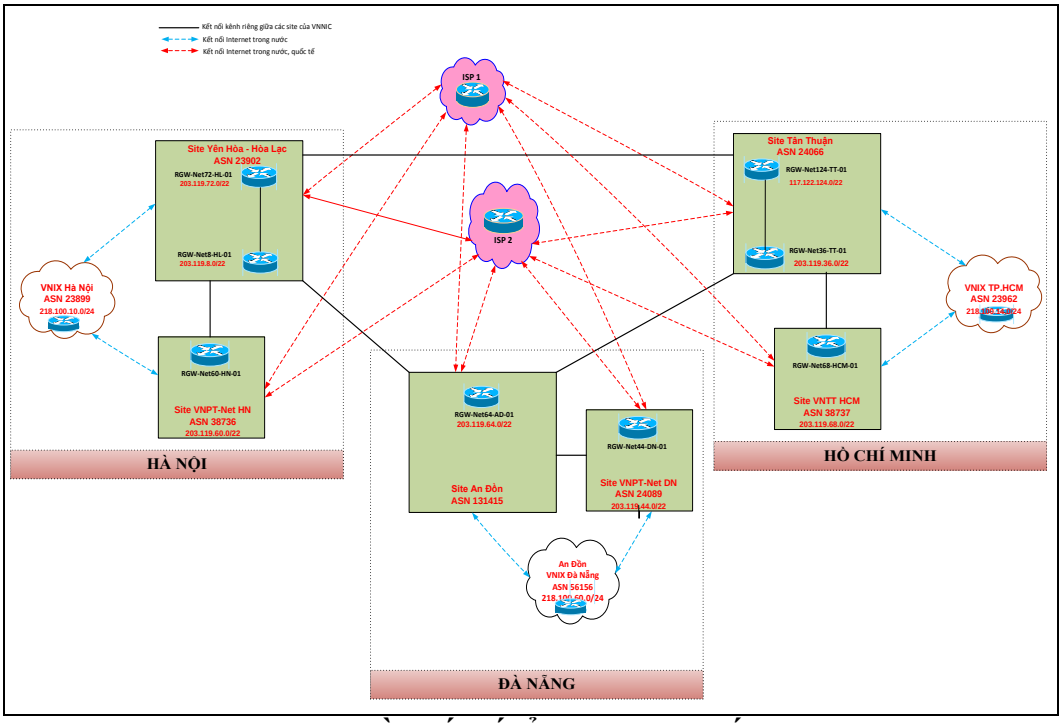
4. Phương pháp nghiên cứu

Nghiên cứu lý thuyết, hiện trạng các đơn vị và đề xuất áp dụng cho mô hình mạng các đơn vị

CHƯƠNG 1: PHÂN TÍCH HIỆN TRẠNG NHU CẦU PHÒNG CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ MẠNG

1.1. Hiện trạng hệ thống mạng

1.1.1 Tổng quan mạng



Hình 1.1: Sơ đồ thiết kế tổng quan hệ thống mạng VNNIC

1.1.2. Hiện trạng các hệ thống an toàn an ninh mạng VNNIC

Hiện tại, các phân mạng của VNNIC chủ yếu được bảo vệ bởi các hệ thống kiểm soát an toàn an ninh như sau:

- Các hệ thống tường lửa: kiểm soát các luồng lưu lượng vào/ra từng phân mạng.
- Các hệ thống phát hiện và ngăn chặn bất hợp pháp:
  - Tính năng IDP trên các firewall Juniper SRX: phát hiện và ngăn chặn bất hợp pháp.
  - Hệ thống Firepower/FightSight trên các firewall Cisco ASA 5525: phát hiện và ngăn chặn xâm nhập bất hợp pháp.

  Tính năng Botnet Traffic Fitering: phát hiện và ngăn chặn malware (mã độc).
- Hệ thống FireEye: phát hiện và ngăn chặn mã độc cho mạng OFFICE.
- Hệ thống TrendMicro: phát hiện và ngăn chặn Virus cho mạng OFFICE.

1.1.3. Hiện trạng phòng chống tấn công DDoS mạng VNNIC

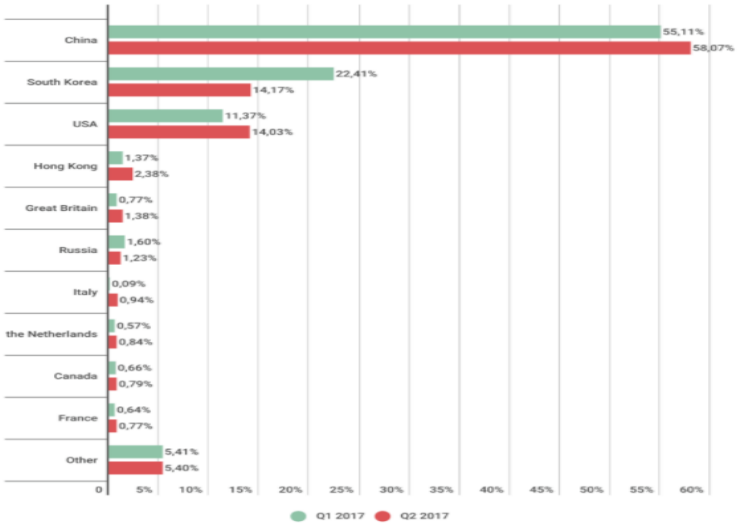
Kết luận:

Hiện hệ thống mạng VNNIC đã được trang bị nhiều hệ thống, công cụ an toàn an ninh tương đối toàn diện nhưng vẫn thiếu 1 giải pháp phòng chống các nguy cơ tấn công từ chối dịch vụ DDoS:

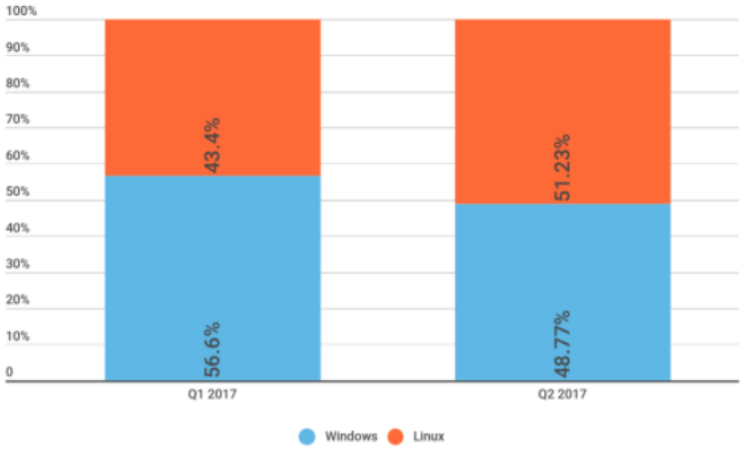
- Chưa có phương án rõ ràng nhằm phát hiện sớm các cuộc tấn công DDoS.
- Thiếu các giải pháp nhằm phân tích, xác định đặc điểm của luồng lưu lượng tấn công DDoS.
- Năng lực thiết bị tại lớp biên mạng, thiết bị mạng lõi mặc dù đã được nâng cấp nhưng chưa đồng đều, mới chủ yếu tập trung tại các phân mạng dịch vụ.

1.2. Nhu cầu triển khai phòng chống tấn công DDoS cho mạng VNNIC

1.2.1. Tình hình tấn công DDoS trên thế giới



Hình 1.2: Phân bố diễn ra các cuộc tấn công DDoS theo quốc gia

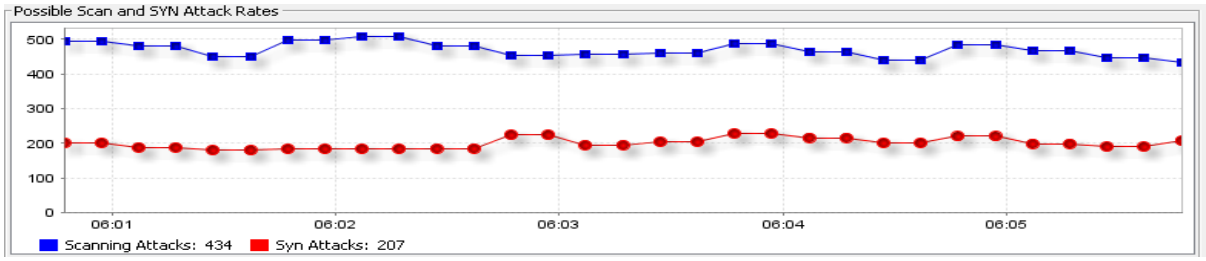


Hình 1.5: Tỉ lệ các máy bị nhiễm botnet theo hđh Window & Linux

1.2.2.Tình hình tấn công DDoS tại Việt Nam

Hình 1.8: Thống kê tỉ lệ các cuộc tấn công DDoS theo quốc gia năm 2016

1.2.3.Phân tích nhu cầu



Hình 1.9: Tấn công SYN attack mạng VNNIC

Kết luận:

Qua các phân tích nêu trên nguy cơ xảy ra các cuộc tấn công DDoS nhằm vào hệ thống mạng VNNIC là hết sức rõ ràng. Do đó, nhu cầu nghiên cứu, triển khai các giải pháp kỹ thuật nhằm phát hiện, phòng chống các cuộc tấn công DDoS phù hợp cho hệ thống mạng của Trung Tâm là hết sức cấp bách và cần thiết. Giải pháp phòng chống DDoS cho hệ thống mạng VNNIC cần đáp ứng các tiêu chí sau đây:

- Triển khai đồng bộ giải pháp phòng chống tấn công DDoS tại tất cả các site thuộc mạng VNNIC.
- Thời gian xử lý (phát hiện, cảnh báo, ngăn chặn) nhanh.
- Giải pháp phải đồng bộ, tổng thể, từ phát hiện đến ngăn chặn, giảm nhẹ khi tấn công xảy ra.

CHƯƠNG 2: NGHIÊN CỨU TỔNG QUAN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ VÀ KỸ THUẬT BGP FLOWSPEC

2.1. Tấn công từ chối dịch vụ

2.1.1. Khái niệm

Tấn công từ chối dịch vụ (Denial of Service - DoS) hay tấn công từ chối dịch vụ phân tán (Distributed Denial Of Service – DDoS): Tấn công từ chối dịch vụ là hình thức tấn công mà kẻ tấn công (hacker) cố gắng nhằm ngăn cản người dùng sử dụng thông tin hoặc dịch vụ bằng cách làm quá tải tài nguyên hệ thống (máy tính, máy chủ, hệ thống mạng, đường truyền, thiết bị mạng, DNS, Web, mail…).

2.1.2. Cơ chế hoạt động

Các cuộc tấn công DDoS thường diễn ra theo cơ chế gồm 3 giai đoạn như sau:

a) Giai đoạn 1: Chuẩn bị.

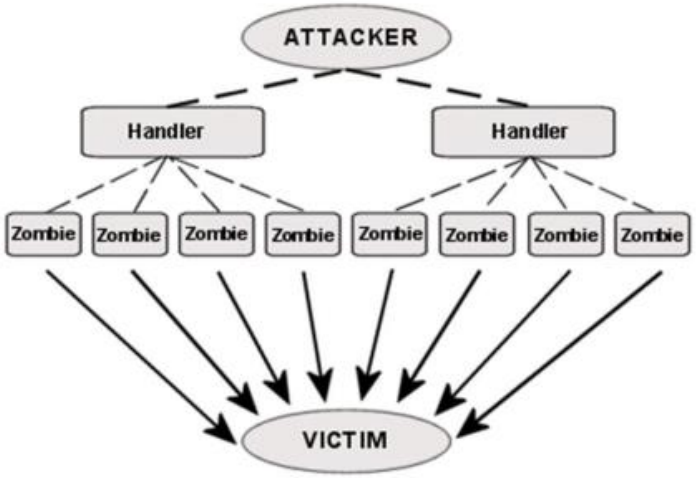
b) Giai đoạn 2: Xác định mục tiêu và thời điểm.

c) Giai đoạn 3: Phát động tấn công và xóa dấu vết.

2.1.3. Kiến trúc, mô hình tấn công DDoS

Mặc dù có nhiều dạng tấn công DDoS được ghi nhận, nhưng tựu trung có thể chia kiến trúc tấn công DdoS thành 2 loại chính:

- Kiến trúc tấn công DDoS trực tiếp.
- Kiến trúc tấn công DDoS gián tiếp hay phản chiếu.

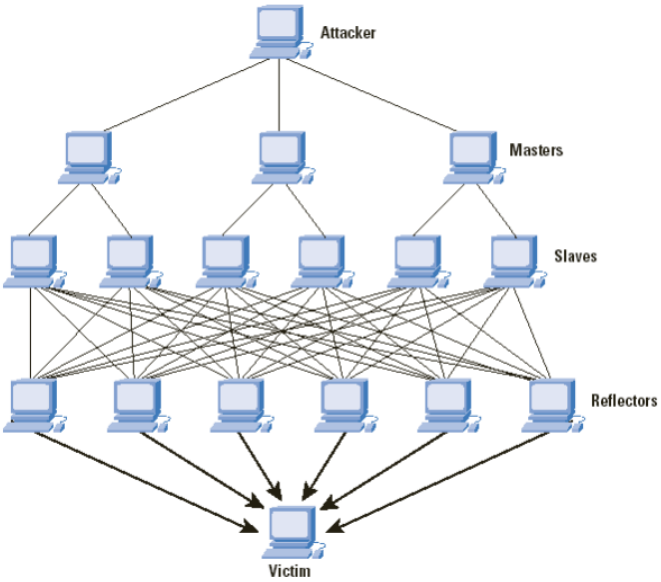


Hình 2.1: Kiến trúc tấn công DDoS trực tiếp

Các vai trò trong kiến trúc tấn công DDoS trực tiếp:

- Attacker.

- Handler.
- Zoombie.
- Victim.



Hình 2.2: Kiến trúc tấn công DDoS gián tiếp

Các vai trò trong tấn công DdoS gián tiếp:

- Attacker.
- Master.
- Slave.
- Reflector.
- Victim.

2.1.4. Phân loại tấn công DDoS

STT	Tiêu chí	Phân loại
1	Phân loại theo phương pháp tấn công	Tấn công gây ngập lụt: SYN flood…
		Tấn công Logic: TCP SYN…
2	Phân loại theo mức độ tự động	Tấn công thủ công
		Tấn công bán tự động
		Tấn công tự động
3	Phân loại theo mô hình OSI	Tấn công tầng mạng: ICMP flood, ICMP Fragmentation flood, IP Null…
		Tấn công tầng vận chuyển: SYN-ACK flood, UDP Flood, UDP Fragmentation, TCP Null…
		Tấn công tầng ứng dụng: DNS Flood, DNS Amplified, HTTP Fragmentation….
4	Phân loại theo phương thức giao tiếp giữa Master và Bot	DDoS dựa trên agent-handler
		DDoS dựa trên IRC
		DDoS dựa trên Web
		DDoS dựa trên P2P

5	Phân loại dựa trên cường độ tấn công	Tấn công cường độ cao
		Tấn công cường độ thấp
		Tấn công cường độ thay đổi
		Tấn công cường độ hỗn hợp
		Tấn công cường độ hỗn hợp
6	Phân loại dựa trên việc khai thác các lỗ hổng an ninh	Tấn công gây cạn kiệt băng thông: volumetric attack
		Tấn công gây cạn kiệt tài nguyên: ping of death...

Bảng 2.1: Phân loại các hình thức tấn công DDoS

2.1.5. Các biện pháp phòng chống tấn công DDoS

a) Triển khai các biện pháp phòng chống tấn công DDoS theo trên vị trí

b) Triển khai các biện pháp phòng chống DDoS theo mô hình OSI

c)Triển khai các biện pháp phòng chống DDoS theo thời điểm hành động

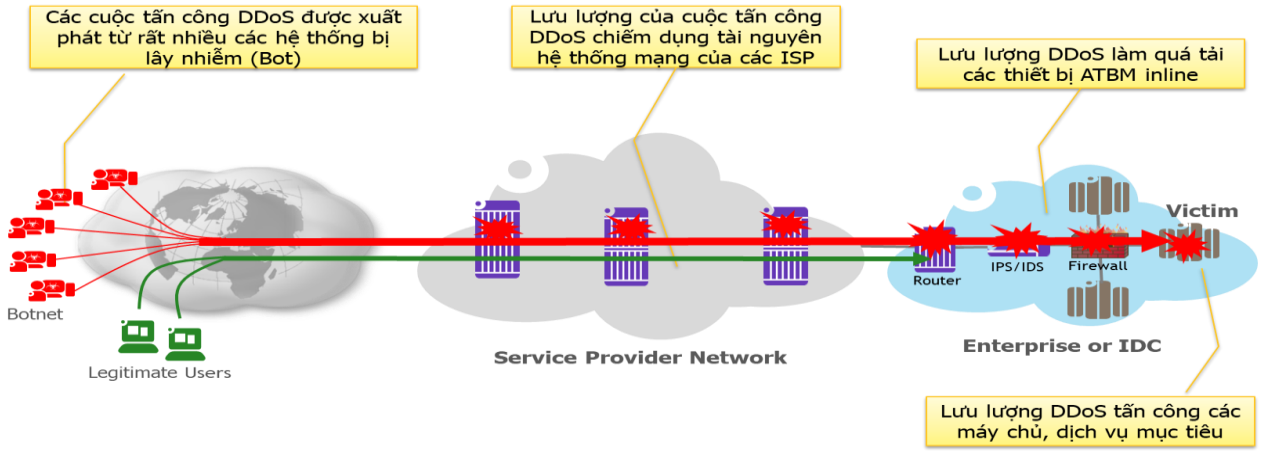
Kết luận:

Qua nghiên cứu các giải pháp ngăn chặn, giảm nhẹ tấn công DDoS nhóm đề tài nhận thấy để phòng chống DDoS hiệu quả cho hệ thống mạng VNNIC cũng như các hệ thống KTDV liên quan cần:

- Triển khai kết hợp đồng thời nhiều biện pháp kỹ thuật khác nhau.
- Triển khai toàn diện theo chiến lược cụ thể.
- Tự triển khai các giải pháp ngăn chặn, giảm nhẹ.
- Tự triển khai phân tán các dịch vụ cho phép.

2.2. Tấn công từ chối dịch vụ mạng

2.2.1. Quá trình diễn ra một cuộc tấn công DDoS mạng



Hình 2.3: Quá trình diễn ra 1 cuộc tấn công DDoS

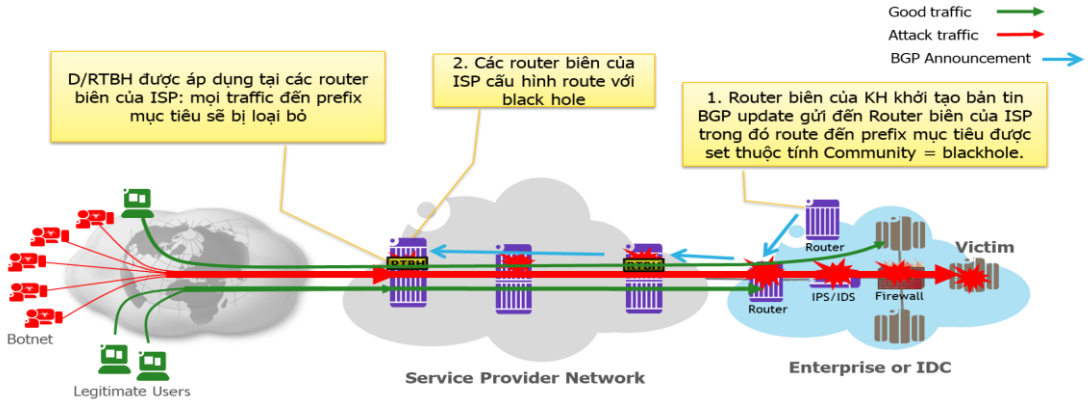
2.2.2. Các phương pháp phòng chống DDoS mạng truyền thống

a) Kỹ thuật ACL:

Kỹ thuật ACL đơn giản chỉ sử dụng các access list tại các router biên của các ISP hoặc mạng doanh nghiệp để chặn các lưu lượng DDoS theo nguồn hoặc đích. Kỹ thuật này có nhiều hạn chế như sau:

- Thời gian đáp ứng thấp do phải triển khai lần lượt trên các Router biên.
- Không linh hoạt.
- Router biên đã phải xử lý chặn các lưu lượng DDoS bằng ACL → gây ảnh hưởng đến hiệu năng của các router biên.

b) Kỹ thuật D/RTBH (Destination Remotely Triggered Black Hole):

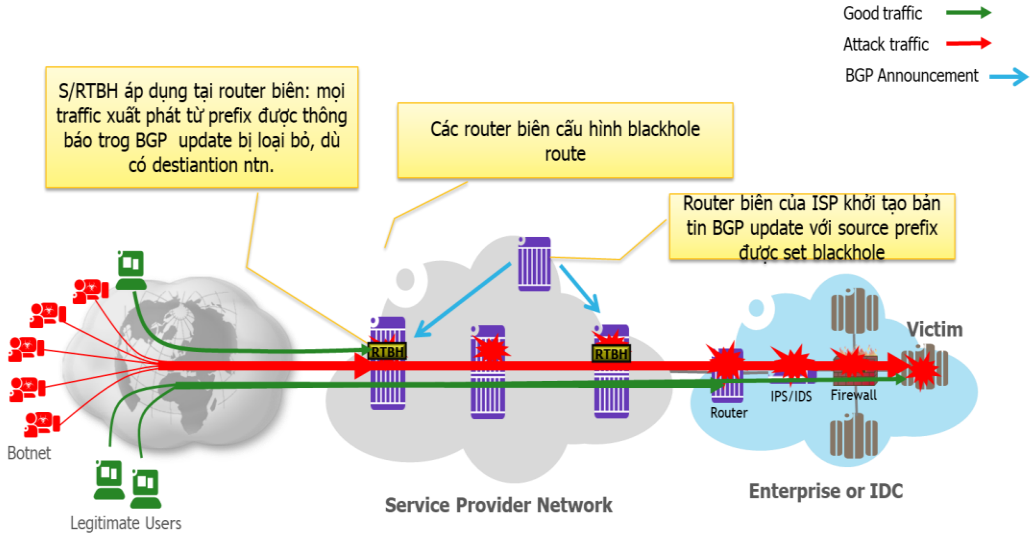


Hình 2.4: Kỹ thuật D/RTBH

Ưu điểm: Triển khai nhanh chóng, đồng thời, tự động đến các router biên. Thời gian đáp ứng nhanh (trong 1 chu kỳ gửi của bản tin BGP update).

Nhược điểm: Mọi traffic hướng đến mục tiêu đều bị loại bỏ, bao gồm cả các traffic hợp lệ.

c) Kỹ thuật S/RTBH (Source Remotely Triggered Black Hole):



Hình 2.5: Kỹ thuật S/RTBH

<u>Kết luận:</u>

Qua các nghiên cứu trình bày ở trên, có thể nhận thấy các phương pháp giảm nhẹ các cuộc tấn công DDoS mạng truyền thống sau khi đã phát hiện, xác định được cuộc tấn công vẫn còn rất nhiều hạn chế. Do đó, nhu cầu đặt ra là cần phải nghiên cứu, đề xuất các phương pháp kỹ thuật mới, nhằm ngăn chặn, giảm nhẹ hiệu quả các cuộc tấn công DDoS nhằm vào hệ thống mạng. Trên cơ sở đó, nhóm đề tài sẽ đề xuất giải pháp thích hợp áp dụng cho hệ thống mạng VNNIC. Đây cũng là nội dung chính của đề tài.

2.3. Kỹ thuật BGP Flowspec

2.3.1. Khái niệm mở đầu

- **Phần Flow Specification**
  - Source / Destination Prefix
  - IP Protocol (UDP, TCP, ICMP, etc.)
  - Source and/or Destination Port
  - ICMP Type and Code
  - TCP Flags
  - Packet Length
  - DSCP (Diffserv Code Point)
  - Fragment (DF, IsF, FF, LF)
- **Phần Action**:

Ưu điểm của kỹ thuật này là:

➢ Các rule được phân phối 1 cách nhanh chóng, đồng thời đến toàn bộ các router biên mà không cần thay đổi cấu hình. Từ đó, cải tiến thời gian đáp ứng, xử lý sự cố tấn công DDoS (response time).

➢ Luồng lưu lượng tấn công DDoS được xác định chính xác dựa trên các đặc điểm, tiêu chí lớp 3, lớp 4 cụ thể. Do đó, việc ngăn chặn, xử lý các luồng tấn công DDoS không ảnh hưởng đến các luồng lưu lượng hợp lệ.

Kỹ thuật BGP flowspec đã được chuẩn hóa bởi IETF như sau:

➢ RFC 5575: "Dissemination of Flow Specification Rules" năm 2009 (công bố chính thức): BGP flowspec áp dụng cho IPv4.

➢ RFC 7674: "Clarification of the Flowspec Redirect Extended Community" năm 2015 (công bố chính thức): cập nhật định dạng thuộc tính Community cho hành động điều hướng lưu lượng.

➢ "Dissemination of Flow Specification Rules for IPv6" năm 2017 (đang ở dạng dự thảo): xây dựng tiêu chuẩn về BGP flowspec cho IPv6.

Thông tin về các dòng sản phẩm thiết bị hỗ trợ BGP Flowspec:

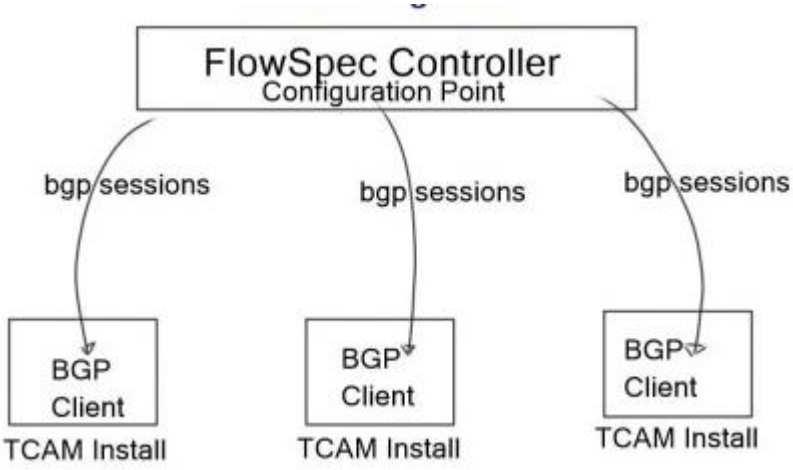
STT	Chức năng	Dòng sản phẩm hỗ trợ
1	Phát hiện tấn công DDoS	Arbor Peakflow SP 3.5

		Juniper DDoS Secure 5.14.2-0 Netflow
3	BGP Flowspec Client (router biên)	Alcatel-Lucent SR OS 9.0R1 Juniper JUNOS 7.3 Các dòng Cisco ASR và CSR có OS hỗ trợ (5.2.0 trở lên)
4	BGP Flowspec Controller	Arbor Peakflow SP 3.5 ExaBGP sFlow-RT Cisco ASR 9000

Bảng 2.3:Các dòng sản phẩm hỗ trợ BGP Flowspec

2.3.2. Mô hình, nguyên lý hoạt động của BGP Flowspec

2.3.2.1. Mô hình

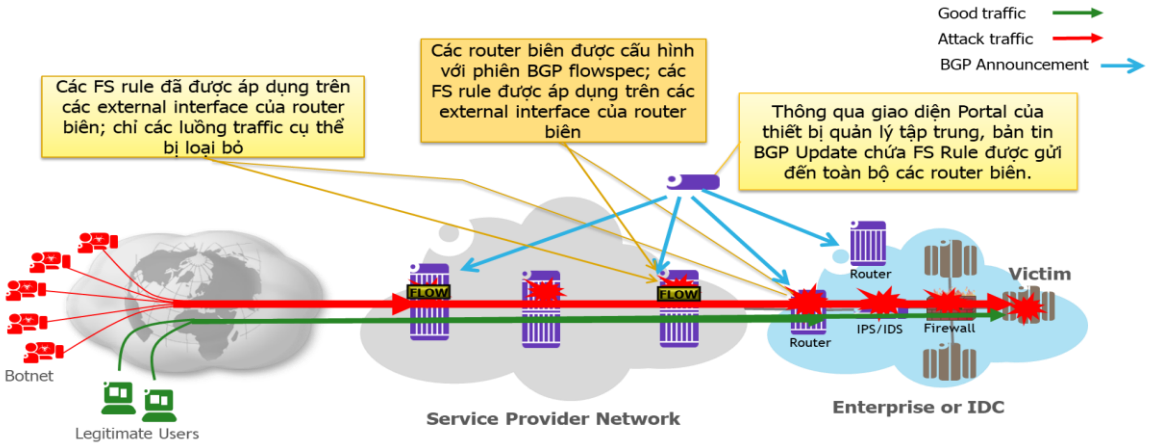


Hình 2.6: Mô hình hoạt động của BGP Flowspec

BGP Flowspec hoạt động theo mô hình Server – Client như hình vẽ bên trên. Theo đó, 1 thiết bị quản lý tập trung sẽ đóng vai trò làm BGP Flowspec Server. Các router biên của mạng doanh nghiệp, mạng ISP sẽ đóng vai trò làm BGP Flowspec Client. BGP Flowspec Server và BGP Flowspec Client được cấu hình flowspec peering với nhau và được xác định rõ vai trò.

Kỹ thuật BGP Flowspec có thể hoạt động với cả 2 mô hình intra-domain và inter-domain:

2.3.2.2. Nguyên lý hoạt động



Hình 2.9: Mô hình nguyên lý hoạt động của BGP Flowspec

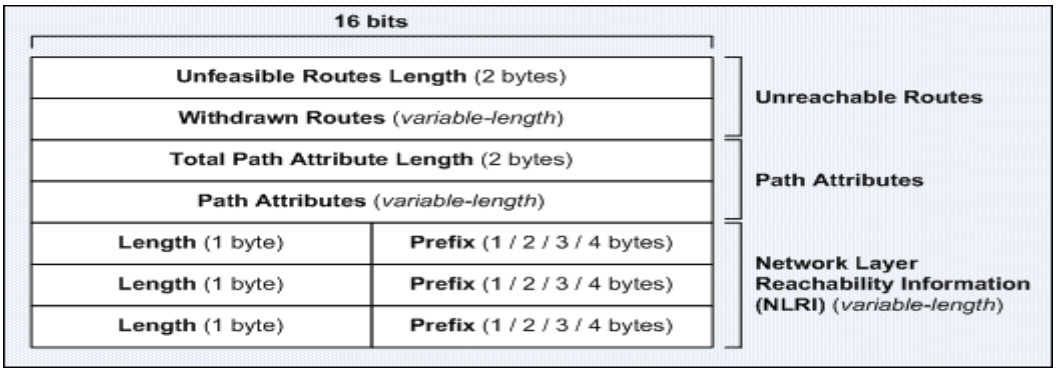
2.3.3. Quá trình mã hóa Flowspec Rule trong bản tin BGP Update

2.3.3.1. . Nhắc lại bản tin BGP Update

Như chúng ta biết, bản tin BGP Update được các BGP peer trao đổi với nhau khi có sự thay đổi về các tuyến đường (route) trong bảng định tuyến. Bản tin BGP Update chứa các thông tin chủ yếu sau đây:

- Unfeasible Routes Lenth (2byte): độ dài của trường Widrawn Routes ngay phía sau.
- Widrawn Routes (độ dài thay đổi): chứa thông tin các route không đến được mà 1 BGP speaker muốn thông báo cho BGP neighbor của mình. Khi nhận được, BGP neighbor sẽ loại bỏ các route này khỏi bảng định tuyến.
- Total Path Attribute Lenth (2 byte): độ dài của trường Path Attributes ngay phía sau.
- Path Attributes (độ dài thay đổi): chứa thông tin các thuộc tính của tuyến đường (path). Các thuộc tính này được sử dụng trong quá trình lựa chọn tuyến đường tốt nhất từ BGP table cập nhật vào bảng định tuyến.
- NLRI (Network Layer Reachability Information): Danh sách các IP prefix mới có thể đến được thông qua tuyến đường này.

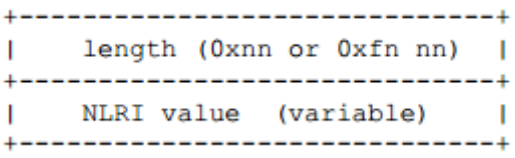
Định dạng cụ thể của bản tin BGP Update thông thường được quy định trong RFC 4760 như sau:



Hình 2.10: Định dạng bản tin BGP Update

2.3.3.2. Mã hóa flow specification trong trường NLRI

Theo RFC 4760, trường NLRI ở định dạng MP_REACH_NLRI và MP_UNREACH_NLRI bao gồm trường NLRI length có độ dài 1-2 octet; theo sau là trường NLRI value có độ dài thay đổi.



Hình 2.11: flowspec NLRI

Nếu độ dài của NLRI value < 240 bit thì trường NLRI length sẽ được mã hóa trong 1 octet tương ứng với 2 chữ số hexa (0xnn). Nếu độ dài của NLRI value >= 240 bit thì trường NLRI length sẽ được mã hóa sử dụng 3 chữ số hexa (0xfnnn).

Mã hóa Flow specification NLRI type có thể bao gồm các thành phần con sau đây, mỗi thành phần con tương ứng với 1 chỉ tiêu trong flow specification. Một gói tin chỉ được coi là khớp với flow specification nếu nó khớp với tất cả các thành phần con. Có tất cả 12 loại thành phần con được liệt kê trong bảng sau đây:

Các thành phần con phải tuân thủ nghiêm ngặt thứ tự của các type. Mã hóa sắp xếp các type theo thứ tự lần lượt từ type 1 → type 12.

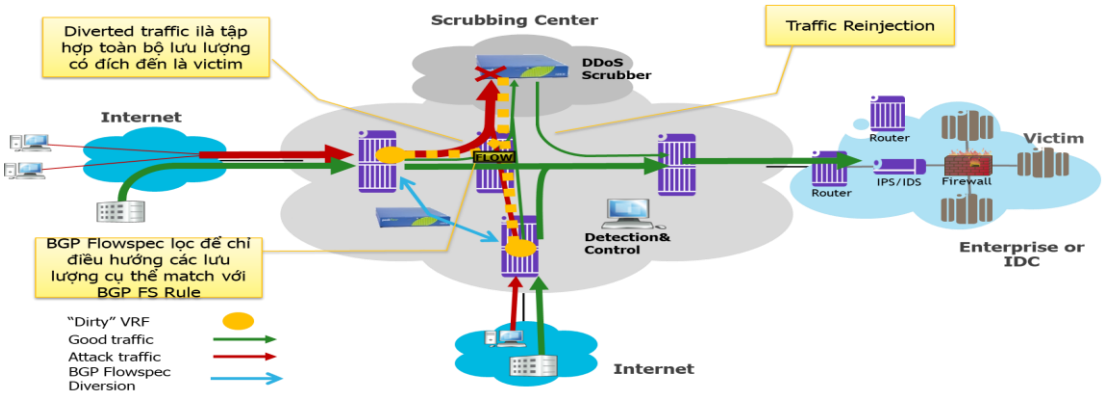
2.3.3.3. Mã hóa Action trong thuộc tính Community

Mặc định, hành động được áp dụng với các lưu lượng khớp với flow specification là cho phép. Các giá trị thuộc tính mở rộng Community sau đây được sử dụng để chỉ ra các hành động áp dụng với flow specifcation:

2.3.4. Kỹ thuật điều hướng lưu lượng trong BGP Flowspec

Kỹ thuật Diversion hay Offramping: định tuyến lại các lưu lượng, thay vì đến trực tiếp các máy chủ dịch vụ bị tấn công thì chuyển hướng đến Scrubbing Center. Kỹ thuật Diverson thường được thực hiện bằng cách quảng bá các BGP prefix (chưa địa chỉ máy chủ bị tấn công) cụ thể hơn trong bảng định tuyến toàn cầu hay sử dụng. Khi đó, mọi lưu lượng (cả hợp lệ, không hợp lệ) có đích đến là máy chủ, dịch vụ bị tấn công đều bị điều hướng đến Scrubbing Center.

Kỹ thuật Reinjection hay Onramping: điều hướng các lưu lượng sạch từ Scrubbing Center quay trở lại đích đến ban đầu. Kỹ thuật Reinjection thường sử dụng đường hầm hoặc VRF để chuyển hướng các lưu lượng sạch về lại đích dự kiến mà không bị loop.



Hình 2.12: Kỹ thuật điều hướng lưu lượng trong BGP Flowspec

. So sánh kỹ thuật BGP Flowspec và các kỹ thuật phòng chống DDoS mạng truyền thống

Sau khi đã nghiên cứu, tìm hiểu chuyên sâu về kỹ thuật BGP Flowspec; nhóm đề tài thực hiện so sánh, đánh giá các ưu điểm của kỹ thuật này so với các kỹ thuật phòng chống tấn công DDoS mạng truyền thống (ACL, S/RTBH, D/RTBH)

STT	Tiêu chí	ACL	RTBH	Flowspec
1	Hiệu quả	Cao	Thấp	Cao
2	Số bước thực hiện	Nhiều bước	3	3
3	Lưu lượng hợp lệ	Cho phép	Block	Cho phép
4	Lưu lượng tấn công	Block	Block	Block
5	Thời gian xử lý	Mất nhiều thời gian	Không	Không
6	Độ chi tiết	Cao	Thô	Cao
7	Hành động xử lý	Ít	Ít	Nhiều
8	Điều hướng lưu lượng	Không	Không	Có

Bảng 2.6: So sánh BGP flowspec với ACL, RTBH

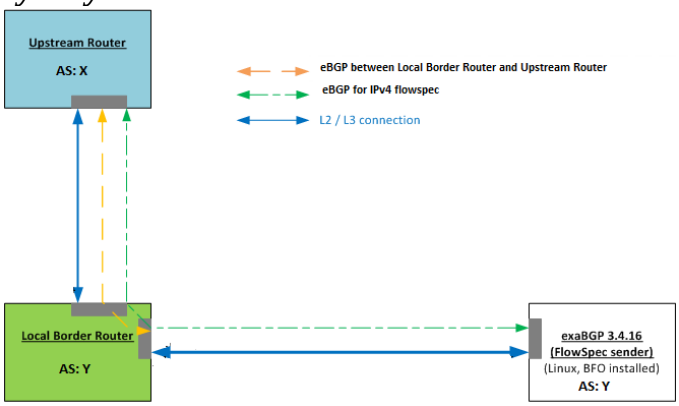
Như vậy, rõ ràng BGP Flowspec có những ưu điểm vượt trội so với các kỹ thuật phòng chống tấn công DDoS truyền thống.

2.4. Một số giải pháp áp dụng kỹ thuật BGP Flowspec phòng chống DDoS

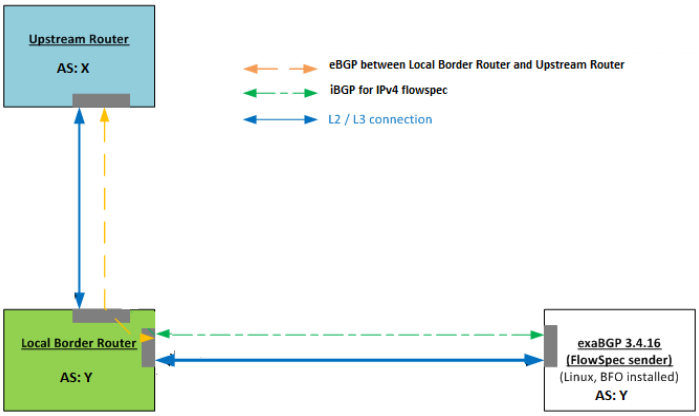
2.4.1. Giải pháp áp dụng mã nguồn mở ExaBGP

a) Giới thiệu

b) Mô hình nguyên lý



Hình 2.13: ExaBGP hoạt động theo mô hình inter-domain



Hình 2.14: ExaBGP hoạt động theo mô hình intra-domain

c) Cài đặt, cấu hình:

Để triển khai công cụ ExaBGP làm Flowspec Controller; đầu tiên cài đặt công cụ như sau:

```
• wget https://github.com/Exa-Networks/exabgp/archive/3.4.5.tar.gz
• tar zxvf 3.4.5.tar.gz
 • cd exabgp-3.4.5
• chmod +x setup.py
• ./setup.py install
```

Tiếp theo cần chỉnh sửa file config. File config bao gồm:

- Thiết lập mối quan hệ BGP flowspec peering với các router biên. Từ đó, ExaBGP Server có thể điều khiển các router biên này.

```
cd usr/local/data/exabgp/configs
sudo nano flowspec-conf.txt
neighbor 203.119.72.160 {                    ##  Địa chỉ của flowspec neighbor router.
router-id 203.119.72.159;                   ## Địa chỉ của Exa BGP Server
local-address 203.119.72.159;
local-as 12346;
peer-as 12346;
```

- Cấu hình các Flowspec rule dưới dạng static hoặc dynamic. Trong trường hợp cấu hinh tĩnh các Flowspec rule trong file config, mỗi lần thay đổi các rule này sẽ thiết lập lại mối quan hệ Flowspec peering. Ngược lại, trong trương hợp sử dụng script động dynamic.sh; có thể thay đổi và inject các Flowspec rule mà không ảnh hưởng đến Flowspec peering.

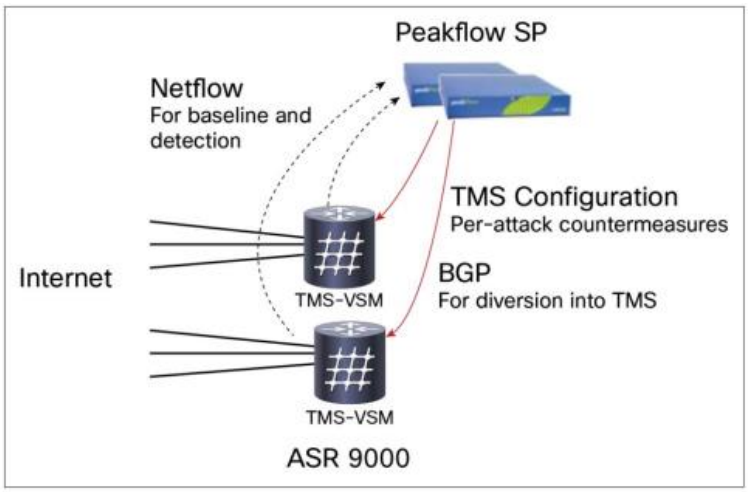
(Tham khảo phần hướng dẫn cấu hình chi tiết ở phụ lục).

2.4.2. Giải pháp thương mại của Arbor, Cisco kết hợp

a) Lý do lựa chọn giải pháp

Hình 2.15: Đánh giá Gartner về giải pháp phòng chống DDoS

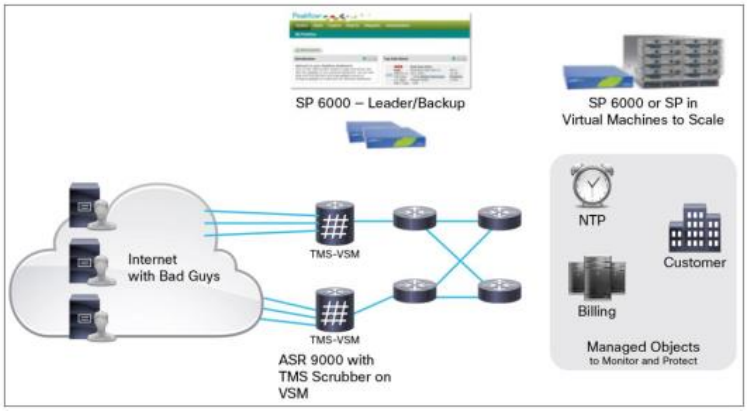
b) Nguyên lý hoạt động



Hình 2.16: Nguyên lý hoạt động của giải pháp Arbor

c) Các thành phần của giải pháp

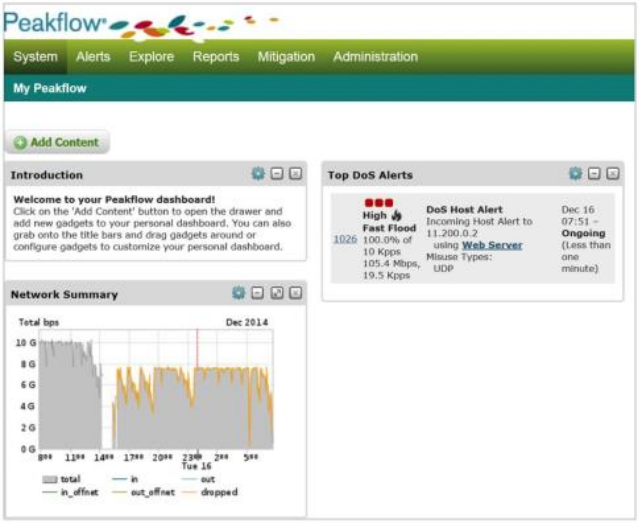
Peakflow là 1 giải pháp tổng thể của Arbor nhằm phân tích mạng, đồng thời phát hiện và giảm nhẹ các cuộc tấn công DDoS. Do đó, giải pháp này bao gồm nhiều chức năng cũng như nhiều các thiết bị phần cứng để thực hiện các chức năng này.



Hình 2.17: Các thành phần của giải pháp Arbor Peakflow

Peakflow SP:

- Chức năng của BGP Flowspec Controller.
- Điều khiển toàn bộ hệ thống và quản lý giao tiếp giữa chúng.
- Hiển thị giao diện GUI.
- Nhận các thông tin về Netflow và định tuyến từ router.
- Phân tích dữ liệu để phát hiện bất thường và đưa ra cảnh báo.
- Tạo các tuyến Diversion và Reinjection thông qua BGP/BGP Flowspec.
- Xác định các biện pháp đối phó thích hợp (Flowspec Rule) và lập trình các biện pháp này vào trong card TMS.
- Nhận các thống kê, các mẫu lưu lượng từ TMS và hiển thị nó ra GUI.
- Quản lý các license của hệ thống.



Hình 2.18: Giao diện GUI của Peakflow

Peakflow Threat Management System (TMS):

- Chức năng của 1 Scrubber Device.
- Nhận các biện pháp đối phó được lập trình sẵn từ SP.
- Triển khai các biện pháp đối phó để loại bỏ các traffic tấn công.
- Chuyển tiếp các traffic hợp lệ đến các đích thông thường.
- Gửi các thống kê về Peakflow SP.
- Capture các mẫu gói tin và gửi nó về Peakflow SP.

Peakflow TMS được cài đặt trên card VMS của Cisco ASR 9K, đồng thời có thể kết hợp với các thiết bị TMS phần cứng của Arbor. Vì đóng vai trò là 1 scrubber device, TMS phải có hiệu năng lớn tương ứng với dung lượng của cuộc tấn công DDoS (volume). Theo đó, hiệu năng phần cứng phải đáp ứng được cuộc tấn công lớn nhất có thể dự đoán.

Router Cisco ASR 9K:

2.4.3. So sánh và lựa chọn giải pháp

Sau khi đã nghiên cứu kỹ 2 giải pháp nêu trên, nhóm đề tài thực hiện so sánh 2 giải pháp theo các tiêu chí cụ thể:

STT	Tiêu chí	Giải pháp ExaBGP	Giải pháp Arbor
1	Chi phí	Mã nguồn mở, miễn phí	Thương mại, mất phí
2	Tuân thủ RFC 5575	Có	Có
3	Tự động phát hiện và cảnh báo tấn công DDoS	Không	Có (thiết lập ngưỡng baseline tự động gửi cảnh báo)
4	Phân tích lưu lượng để tìm nguồn tấn công	Không	Có (tích hợp sẵn Netflow)
5	Thiết lập các hành động xử lý, ngăn chặn lưu lượng DDoS	Có	Có
6	Thực hiện điều hướng lưu lượng	Thủ công	Tự động
7	Thực hiện làm sạch lưu lượng	Không	Có (phần mềm TMS trên card VMS)
8	Giao diện	Dòng lệnh	GUI
9	Phù hợp với mạng VNNIC	Có (phần mềm ExaBGP có thể tương tác với các router mạng VNNIC hiện tại ASR 100; ASR 1001-X)	Không (giải pháp Arbor Peakflow muốn triển khai đầy đủ phải nâng cấp lên các router Cisco ASR 9000)

Hình 2.19: So sánh các giải pháp BGP Flowspec

Kết luận:

Qua nghiên cứu, so sánh 2 giải pháp bên trên nhóm đề tài nhận thấy cả 2 giải pháp đều hỗ trợ, hoạt động theo kỹ thuật BGP flowspec được mô tả trong RFC 5575. Trong đó, giải pháp Arbor tổng thể, toàn diện hơn; bao gồm quá trình từ phát hiện, phân tích, xử lý đến làm sạch lưu lượng tấn công DDoS. Tuy nhiên hạn chế của giải pháp này là chưa phù hợp với hệ thống mạng VNNIC hiện tại (sử dụng các dòng Cisco ASR 1001; 1001-X làm router biên); muốn triển khai phải nâng cấp các router biên lên dòng Cisco ASR 9000; mất chi phí đầu tư, cần tiếp tục thử nghiệm thực tế để đánh giá hiệu quả so với chi phí cần đầu tư. Trong khi đó, công cụ ExaBGP vẫn đáp ứng được quá trình xử lý tấn công DDoS bằng kỹ thuật Flowspec sau khi phát hiện tấn công xảy ra. Công cụ ExaBGP cũng miễn phí và có thể tiến hành triển khai ngay được. Do đó, nhóm đề tài đề xuất trước mắt sẽ triển khai giải pháp sử dụng công cụ ExaBGP nhằm ngăn chặn, xử lý tấn công DDoS cho mạng VNNIC; giải pháp Arbor cần tiếp tục nghiên cứu thử nghiệm thêm.

CHƯƠNG 3: TRIỂN KHAI THỬ NGHIỆM, ĐỀ XUẤT ÁP DỤNG KỸ THUẬT BGP FLOWSPEC CHO HỆ THỐNG MẠNG

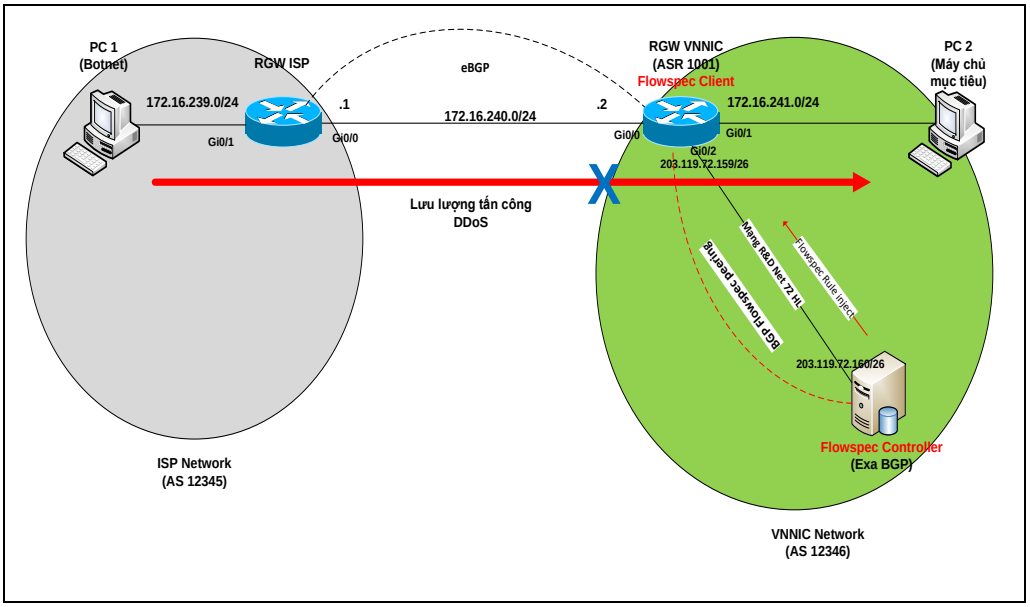
3.1. Triển khai thử nghiệm

3.1.1. Mục tiêu thử nghiệm

- Thử nghiệm áp dụng kỹ thuật BGP Flowspec nhằm ngăn chặn các luồng lưu lượng tấn công DDoS sau khi phát hiện ra. Hệ thống thử nghiệm mô phỏng theo đúng mô hình của hệ thống mạng VNNIC.
- Thử nghiệm hoạt động của công cụ mã nguồn mở ExaBGP với vai trò làm BGP Flowspec Controller.
- Đánh giá kết quả thử nghiệm làm căn cứ đề xuất giải pháp áp dụng cho mạng VNNIC.

3.1.2. Mô hình thử nghiệm

- ASN 12345: đại diện cho mạng phía ISP.
- ASN 12346: đại diện cho mạng VNNIC.



Hình 3.1: Mô hình thử nghiệm BGP Flowspec

Hệ thống thử nghiệm bao gồm các thành phần được liệt kê chi tiết trong bảng bên trên.

- Máy tính PC-02 phải kết nối được Internet (Ở đây mô phỏng bằng cách PC-02 phải ping được PC-01).

- Các client trên Internet có thể sử dụng dịch vụ do PC-02 cung cấp (Ở đây mô phỏng bằng cách PC-01 có thể ping được PC-02).

3.1.3. Triển khai thử nghiệm:

Bước 1: Cấu hình trên RGW VNNIC: (*tham khảo chi tiết trong phụ lục 02).*

- Cấu hình các interface.
- Cấu hình eBGP peering với RGW ISP & quảng bá prefix 172.16.241.0/24
- Cấu hình BGP flowspec peering với máy chủ ExaBGP:

```
configure terminal
router bgp 12346
neighbor 203.119.72.160 remote-as 12346
address-family ipv4 flowspec
neighbor 203.119.72.160 activate
exit
```

Bước 2: Cấu hình trên RGW ISP: (*tham khảo chi tiết trong phụ lục 02).*

- Cấu hình các interface.
- Cấu hình eBGP peering với RGW VNNIC & quảng bá prefix 172.16.239.0/24

Bước 3: Cài đặt PC-01; PC-02:

- Cài đặt hệ điều hành Window 10.
- Cấu hình địa chỉ IP, Default Gateway tương ứng.

Bước 4: Cài đặt, cấu hình máy chủ ExaBGP: tham khảo phụ lục 01.

- Cài đặt hệ điều hành Ubuntu mới nhất.
- Cấu hình địa chỉ IP cho cổng kết nối.
- Cài đặt công cụ ExaBGP 3.4.5.
- Cấu hình BGP flowspec peering với RGW VNNIC bằng cách chỉnh sửa file config.txt

```
cd usr/local/data/exabgp/configs
sudo nano flowspec-conf.txt
neighbor 203.119.72.160 {                    ## Địa chỉ của flowspec neighbor router.
router-id 203.119.72.159;                    ## Địa chỉ của Exa BGP Server
local-address 203.119.72.159;
local-as 12346;
peer-as 12346;
```

- Cấu hình sẵn script dynamic.sh cho phép cập nhật động flowspec rule.

```
#!/bin/sh
# ignore Control C
# if the user ^C exabgp we will get that signal too, ignore it and let exabgp send us a SIGTERM
trap '' SIGINT
```

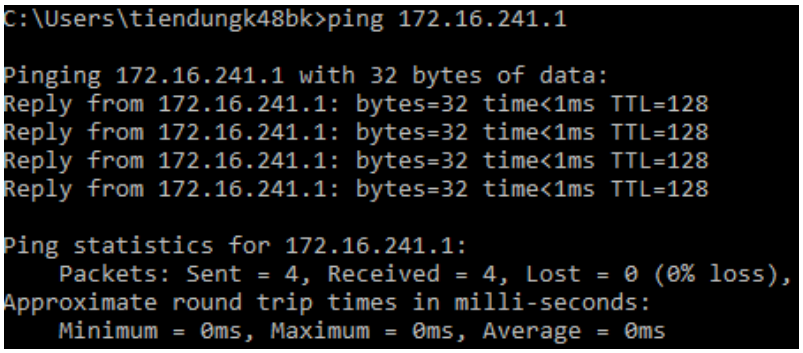
```
# command and watchdog name are case sensitive
while `true`;
do
echo "announce flow route {\\n match {\\n source 40.40.40.1/32;\\n destination 40.40.50.1/32;\\n }\\n then {\\n discard;\\n }\\n }\\n"
sleep 10
echo "announce flow route {\\n match {\\n source 80.80.80.1/32;\\n destination 80.80.80.1/32;\\n }\\n then {\\n discard;\\n }\\n }\\n"
Done
```

Kết quả:

- Các phiên BGP peering UP; các RGW nhận được prefix do peer quảng bá.
- PC-01 & PC-02 ping được nhau.

3.1.4. Kịch bản thử nghiệm

Sau khi hệ thống thử nghiệm được xây dựng xong; bình thường PC-01 kết nối được tới PC-02:



Tiến hành cấu hình trên exaBGP điều khiển RGW VNNIC bằng Flowpsec rule: thực hiện drop các lưu lượng đến từ vùng địa chỉ của PC-01 *(tham khảo chi tiết phụ lục 01).*

```
echo "announce flow route {\\n match {\\n source 172.16.239.2/32;\\n destination 172.16.241.2/32;\\n }\\n then {\\n discard;\\n }\\n }\\n"
```

Kiểm tra trên RGW-VNNIC thấy đã nhận được flowspec rule thông qua bản tin BGP Update từ ExaBGP:

```
RGW-VNNIC#show flowspec ipv4
AFI: IPv4
Flow :Dest:172.16.241.2/32,Source:172.16.239.2/32
Actions :Traffic-rate: 0 bps (bgp.1)
RGW-VNNIC#show bgp ipv4 flowspec sum | begin Neighbor
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
172.16.240.1 0 1 200 161 49 0 0 00:20:52 3
```

Thử lại từ PC-01 không gửi được lưu lượng đến PC-02 nữa; luồng lưu lượng tấn công DDoS từ PC-01 đã bị chặn ngay tại RGW VNNIC:

```
C:\Users\tiendungk48bk>ping 172.16.241.1

Pinging 172.16.241.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.241.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3.1.5. Kết quả thử nghiệm

a) Kết quả:

b) Đánh giá:

c) Đề xuất:

3.2. Đề xuất áp dụng kỹ thuật BGP Flowspec cho hệ thống mạng VNNIC

3.2.1. Giải pháp đề xuất

Để có thể phòng chống các cuộc tấn công DDoS một cách hiệu quả cho hệ thống mạng VNNIC sau quá trình nghiên cứu, thử nghiệm; nhóm thực hiện đề tài đề xuất giải pháp tổng thể như sau:

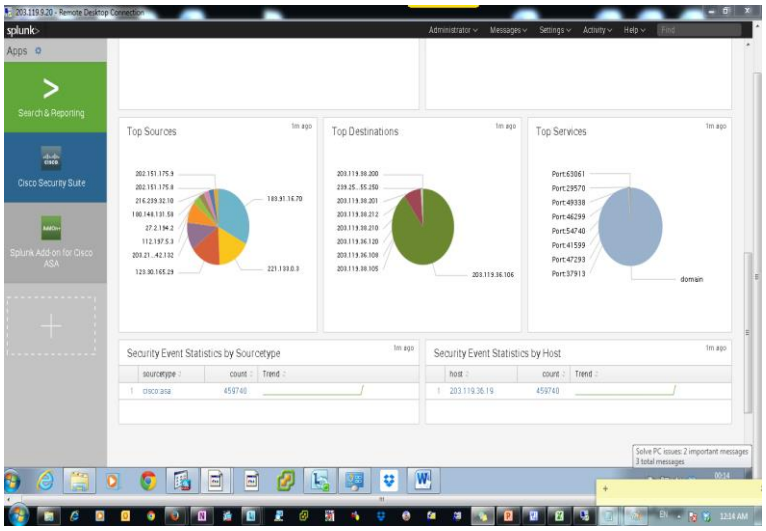
a) Triển khai các biện pháp phòng ngừa

b) Triển khai hệ thống giám sát, phát hiện tấn công DDoS cho mạng VNNIC

STT	RGW	Interface	Lưu lượng max	Ngưỡng cảnh báo
1	RGW-Net8-HL-01	Gi0/1	28.53 Mbps	100 Mbps
2	RGW-Net72-HL-01	Te0/0/0	94 Mbps	150 Mbps
3	RGW-Net64-AD-01	Gi0/0/0	8.14 Mbps	50 Mbps
4	RGW-Net36-TT-01	Gi0/0/0	39.55 Mbps	100 Mbps
5	RGW-Net117-TT-01	Te0/0/0	14 Mbps	100 Mbps

Bảng 3.2: Ngưỡng cảnh báo thiết lập cho từng phân mạng

c) Triển khai các hệ thống phân tích lưu lượng, truy tìm nguồn tấn công



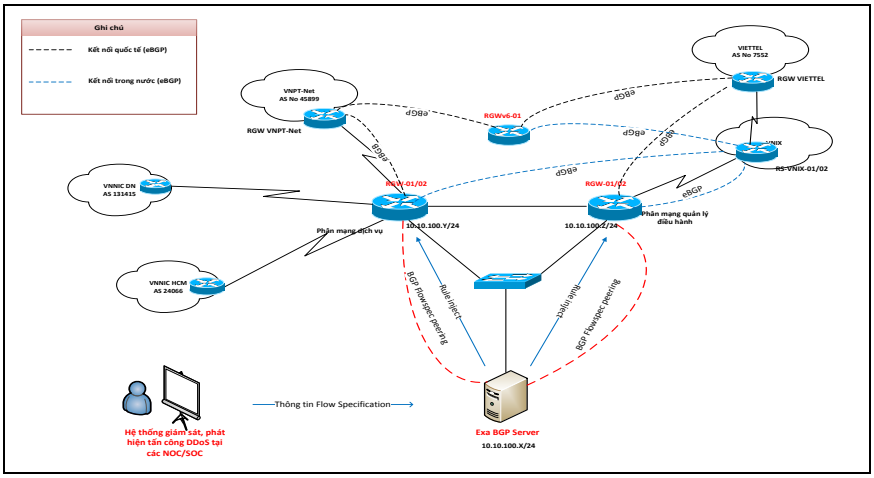
Hình 3.2: Áp dụng công cụ Splunk thực hiện PTLL đi qua firewall

d) Triển khai các quy trình, hệ thống xử lý, ngăn chặn khi tấn công xảy ra

e) Triển khai xử lý sau tấn công

3.2.2. Mô hình đề xuất

- Exa BGP Server: máy chủ cài đặt công cụ ExaBGP, đóng vai trò làm BGP Flowspec Controller.
- Các RGW tại các phân mạng: sử dụng các dòng thiết bị hỗ trợ, đóng vai trò làm BGP Flowspec Client.
- BGP Flowpsec peering can thiệp vào chính sách định tuyến nên cần được triển khai trong cùng 1 ASN (nội vùng).
- Nếu Exa BGP triển khai tập trung, trong trường hợp bị tấn công DDoS có thể bị mất kết nối, không thể tác động đến các RGW từ xa được.



Hình 3.3: Mô hình đề xuất triển khai giải pháp BGP Flowpsec cho mạng VNNIC

- Không cần thiết phải kết nối Internet để đảm bảo an toàn an ninh.
- Cho phép truy cập ssh từ phân mạng OFFICE, phân mạng quản trị.

- Có thể triển khai BGP flowspec peering trực tiếp với các RGW.

Máy chủ cài đặt BGP Exa BGP có yêu cầu tối thiểu như sau:

- Phần cứng: RAM: 4GB; CPU: 2 GHz, HDD: 50 Gbps.
- Hệ điều hành: Linux (Ubuntu, Redhat….)
- Phần mềm: ExaBGP 3.4.5.

3.2.3. Kế hoạch triển khai

Để có thể triển khai giải pháp nêu trên, nhóm thực hiện đề tài đề xuất kế hoạch triển khai gồm các công việc như sau:

- Triển khai các biện pháp nhằm phát hiện sớm tấn công DDoS tại NOC/SOC.
- Triển khai các hệ thống phân tích lưu lượng cho hệ thống mạng VNNIC.
- Quy hoạch các thiết bị router có năng lực lớn, hỗ trợ BGP Flowspec client làm RGW mạng VNNIC. Làm việc với các ISP nâng cấp tốc độ các đường kết nối uplink mạng VNNIC.
- Cài đặt, cấu hình các máy chủ Exa BGP và tích hợp với các RGW theo mô hình.
- Xây dựng quy trình VHKT giải pháp BGP Flowspec phòng chống DDoS.
- Hướng dẫn, phổ biến tại các NOC/SOC/nhóm ATBM.

KẾT LUẬN VÀ KIẾN NGHỊ

Bám theo các nội dung đăng ký của đề cương đề tài, nhóm chủ trì đề tài đã thực hiện nghiên cứu, xây dựng và triển khai hoàn chỉnh đề tài theo các nội dung:

- Phân tích hiện trạng nhu cầu phòng chống tấn công từ chối dịch vụ mạng VNNIC.
- Nghiên cứu tổng quan hình thức tấn công từ chối dịch vụ.
- Nghiên cứu kỹ thuật BGP Flowspec.
- Triển khai thử nghiệm, đề xuất áp dụng kỹ thuật BGP Flowspec cho hệ thống mạng VNNIC.

Nhóm thực hiện đề tài mong muốn được tiếp tục nghiên cứu, triển khai áp dụng kỹ thuật BGP Flowpsec cũng như các giải pháp phát hiện, phòng chống tấn công DDoS cho hệ thống mạng VNNIC; nhằm góp phần tăng cường an toàn ổn định kết nối cho các hệ thống KTDV của Trung Tâm. Ngoài ra, một trong những hướng phát triển tiếp theo của đề tài là nghiên cứu áp dụng kỹ thuật BGP Flowspec cho hệ thống VNIX. Về mặt kỹ thuật, điều này hoàn toàn khả thi, hiện trên thế giới đã có AMS-IX triển khai.

Trong nội dung nghiên cứu không tránh khỏi những thiếu sót mong nhận được sự góp ý của hội đồng.