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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2019

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS. TRẦN QUANG ANH

HÀ NỘI 2019

LỜI CAM ĐOAN

Tôi xin cam đoan các kết quả nghiên cứu trong luận văn này là sản phẩm của các nhân tôi dưới sự hướng dẫn của thầy giáo PGS.TS Trần Quang Anh. Các số liệu, kết quả được công bố là hoàn toàn trung thực. Những điều được trình bày trong toàn bộ luận văn này là những gì do tôi nghiên cứu hoặc là được tổng hợp từ nhiều nguồn tài liệu khác nhau. Các tài liệu tham khảo có xuất xứ rõ ràng và được trích dẫn đầy đủ, hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm trước lời cam đoan của mình.

Hà Nội, ngày 20 tháng 11 năm 2019

Người cam đoan

Lương Hòa Cương

LỜI CẢM ƠN

Đầu tiên, tôi gửi lời cảm ơn chân thành và biết ơn sâu sắc tới thầy giáo PGS.TS Trần Quang Anh – Học viện Bưu chính Viễn Thông, người thầy đã luôn tận tình chỉ bảo, giúp đỡ và hướng dẫn tôi trong suốt quá trình nghiên cứu luận văn này.

Tôi xin chân thành cám ơn các thầy, cô giáo trong Khoa Công nghệ thông tin- Học viện Bưu chính Viễn thông đã luôn tận tâm truyền dạy cho tôi những kiến thức bổ ích trong thời gian tôi tham gia học tập và nghiên cứu tại trường.

Tôi cũng xin gửi lời cảm ơn tới Ban lãnh đạo, các anh chị và các bạn trong lớp Hệ thống thông tin đã ủng hộ và khuyến khích tôi trong quá trình nghiên cứu và thực hiện khóa luận này.

Học viên

Lương Hòa Cương

MỤC LỤC

LỜI CAM ĐOAN ..... **i**

LỜI CẢM ƠN ..... **ii**

MỤC LỤC ..... **iii**

DANH MỤC HÌNH VẼ ..... **v**

DANH MỤC BẢNG ..... **vii**

THUẬT NGỮ VÀ VIẾT TẮT ..... **viii**

MỞ ĐẦU **1**

CHƯƠNG 1: PHÂN TÍCH HIỆN TRẠNG NHU CẦU PHÒNG CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ MẠNG VNNIC **2**

1.1. Hiện trạng hệ thống mạng **2**

1.1.1 Tổng quan mạng 2

1.1.2. Hiện trạng các hệ thống an toàn an ninh mạng VNNIC 3

1.1.3. Hiện trạng phòng chống tấn công DDoS mạng VNNIC 5

1.2. Nhu cầu triển khai phòng chống tấn công DDoS cho mạng VNNIC **6**

1.2.1. Tình hình tấn công DDoS trên thế giới 6

1.2.2. Tình hình tấn công DDoS tại Việt Nam 9

1.2.3. Phân tích nhu cầu 10

CHƯƠNG 2: NGHIÊN CỨU TỔNG QUAN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ VÀ KỸ THUẬT BGP FLOWSPEC **12**

2.1. Tấn công từ chối dịch vụ **12**

2.1.1. Khái niệm 12

2.1.2. Cơ chế hoạt động 13

2.1.3. Kiến trúc, mô hình tấn công DDoS 14

2.1.4. Phân loại tấn công DDoS 16

2.1.5. Các biện pháp phòng chống tấn công DDoS 17

2.2. Tấn công từ chối dịch vụ mạng **21**

2.2.1. Quá trình diễn ra một cuộc tấn công DDoS mạng 21

2.2.2. Các phương pháp phòng chống DDoS mạng truyền thống 22
2.3. Kỹ thuật BGP Flowspec 25
2.3.1. Khái niệm mở đầu 25
2.3.2. Mô hình, nguyên lý hoạt động của BGP Flowspec 27
2.3.3. Quá trình mã hóa Flowspec Rule trong bản tin BGP Update 30
2.3.4. Kỹ thuật điều hướng lưu lượng trong BGP Flowspec 35
2.4. Một số giải pháp áp dụng kỹ thuật BGP Flowspec phòng chống DDoS .38
2.4.1. Giải pháp áp dụng mã nguồn mở ExaBGP 38
2.4.2. Giải pháp thương mại của Arbor, Cisco kết hợp 41
2.4.3. So sánh và lựa chọn giải pháp 45
CHƯƠNG 3: TRIỂN KHAI THỬ NGHIỆM, ĐỀ XUẤT ÁP DỤNG KỸ THUẬT BGP FLOWSPEC CHO HỆ THỐNG MẠNG 47
3.1. Triển khai thử nghiệm 47
3.1.1. Mục tiêu thử nghiệm 47
3.1.2. Mô hình thử nghiệm 47
3.1.3. Triển khai thử nghiệm: 49
3.1.4. Kịch bản thử nghiệm 51
3.1.5. Kết quả thử nghiệm 52
3.2. Đề xuất áp dụng kỹ thuật BGP Flowspec cho hệ thống mạng VNNIC ...53
3.2.1. Giải pháp đề xuất 53
3.2.2. Mô hình đề xuất 56
3.2.3. Kế hoạch triển khai 58
KẾT LUẬN VÀ KIẾN NGHỊ 59
TÀI LIỆU THAM KHẢO 60
PHỤ LỤC 62

DANH MỤC HÌNH VẼ

Hình 1.1: Sơ đồ thiết kế tổng quan hệ thống mạng VNNIC 3
Hình 1.2: Phân bố diễn ra các cuộc tấn công DDoS theo quôc gia 7
Hình 1.3: Thống kê số lượng cuộc tấn công DDoS theo ngày 7
Hình 1.4: Thống kê tỉ lệ các cuộc tấn công DDoS theo chu kì 8
Hình 1.5: Tỉ lệ các máy bị nhiễm botnet theo hđh Window & Linux 8
Hình 1.6: Tỉ lệ các cuộc tấn công DDoS theo cường độ tấn công 8
Hình 1.7: Tỉ lệ các cuộc tấn công DDoS theo loại hình tấn công 9
Hình 1.8: Thống kê tỉ lệ các cuộc tấn công DDoS theo quốc gia năm 2016 10
Hình 1.9: Tấn công SYN attack mạng VNNIC 10
Hình 2.1: Kiến trúc tấn công DDoS trực tiếp 14
Hình 2.2: Kiến trúc tấn công DDoS gián tiếp 15
Hình 2.3: Quá trình diễn ra 1 cuộc tấn công DDoS 21
Hình 2.4: Kỹ thuật D/RTBH 23
Hình 2.5: Kỹ thuật S/RTBH 24
Hình 2.6: Mô hình hoạt động của BGP Flowspec 27
Hình 2.7: Mô hình hoạt động của BGP Flowspec Client 28
Hình 2.8: Mô hình hoạt động của BGP Flowsec Server 28
Hình 2.9: Mô hình nguyên lý hoạt động của BGP Flowspec 29
Hình 2.10: Định dạng bản tin BGP Update 31
Hình 2.11: flowspec NLRI 31
Hình 2.12: Kỹ thuật điều hướng lưu lượng trong BGP Flowspec 36
Hình 2.13: ExaBGP hoạt động theo mô hình inter-domain 39
Hình 2.14: ExaBGP hoạt động theo mô hình intra-domain 39
Hình 2.15: Đánh giá Gartner về giải pháp phòng chống DDoS 41
Hình 2.16: Nguyên lý hoạt động của giải pháp Arbor 42
Hình 2.17: Các thành phần của giải pháp Arbor Peakflow 43
Hình 2.18: Giao diện GUI của Peakflow 44
Hình 2.19: So sánh các giải pháp BGP Flowspec 45

Hình 3.1: Mô hình thử nghiệm BGP Flowspec 48
Hình 3.2: Áp dụng công cụ Splunk thực hiện PTLL đi qua firewall.....55
Hình 3.3: Mô hình đề xuất triển khai giải pháp BGP Flowpsec cho mạng VNNIC.57

DANH MỤC BẢNG

Bảng 1.1:Tổng hợp các hệ thống ATAN mạng VNNIC.....4
Bảng 2.1: Phân loại các hình thức tấn công DDoS.....16
Bảng 2.2: Tổng hợp các hình thức tấn công DDoS phổ biến hiện nay.....17
Bảng 2.3:Các dòng sản phẩm hỗ trợ BGP Flowspec.....26
Bảng 2.4: Các loại thành phần con của mã hóa Flow specification NLRI.....34
Bảng 2.5: Mã hóa các hành động trong Flowspec Rule bằng thuộc tính Community35
Bảng 2.6: So sánh BGP flowspec với ACL, RTBH.....37
Bảng 3.1: Các thành phần của mô hình thử nghiệm BGP Flowspec.....49
Bảng 3.2: Ngưỡng cảnh báo thiết lập cho từng phân mạng.....54

THUẬT NGỮ VÀ VIẾT TẮT

Từ viết tắt	Tiếng Việt
ACL (Access control list)	Danh sách các câu lệnh điều khiển truy cập.
ASN (Autonomous System Number)	Số hiệu mạng.
ATBM	An toàn bảo mật
Attacker	Kẻ thực hiện các cuộc tấn công nhằm vào các hệ thống CNTT.
BGP (Border Gateway Protocol)	Giao thức định tuyến liên mạng.
Botnet	Các thiết bị đầu cuối bị lây nhiễm, lợi dụng bởi kẻ tấn công khi thực hiện các cuộc tấn công DDoS.
Client	Máy trạm.
DDoS (Distributed Deny of Service)	Tấn công từ chối dịch vụ phân tán.
DoS (Deny of Service)	Tấn công từ chối dịch vụ.
Firewall	Thiết bị tường lửa, có nhiệm vụ bảo vệ cho các hệ thống mạng.
Flow	Luồng lưu lượng.
Hacker	Kẻ tấn công.
IDC (Internet Data Center)	Trung tâm dữ liệu.
IDS (Intrusion detection system)	Phát hiện các xâm nhập bất hợp pháp.
IP (Internet Protocol)	Giao thức Internet.
IPS(Intrusion prevention system)	Ngăn chặn các xâm nhập bất hợp pháp.
ISP (Internet Service Provider)	Nhà cung cấp dịch vụ Internet.
KTDV	Các hệ thống kỹ thuạt dịch vụ.
KTV	Kỹ thuật viên.
Mạng OFFICE	Hệ thống mạng văn phòng cung cấp kết nối mạng cho cán bộ, nhân viên đơn vị.

NLRI (Network Layer Reachability Information)	Một trường trong bản tin BGP Update.
OSI (Open Systems Interconnection Reference Model)	Mô hình tham chiếu.
P2P (Point to Point)	Kết nối điểm – điểm.
PTLL	Phân tích lưu lượng.
RGW (Router Gateway)	Thiết bị định tuyến biên của hệ thống mạng .
Router	Thiết bị định tuyến.
Server	Máy chủ.
Victim	Hệ thống, máy chủ nạn nhân, mục tiêu của các cuộc tấn công.

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. Do đặc điểm cơ chế hoạt động, loại hình tấn công DDoS rất khó có thể phòng chống và ngăn chặn hoàn toàn. Tại Việt Nam, cùng với sự phát triển bùng nổ của các dịch vụ nội dung là sự gia tăng các hình thức tấn công mạng. Một trong những hình thức tấn công phổ biến, gây nhức nhối nhất cho các ISP, các nhà quản trị mạng là tấn công từ chối dịch vụ DDoS.

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

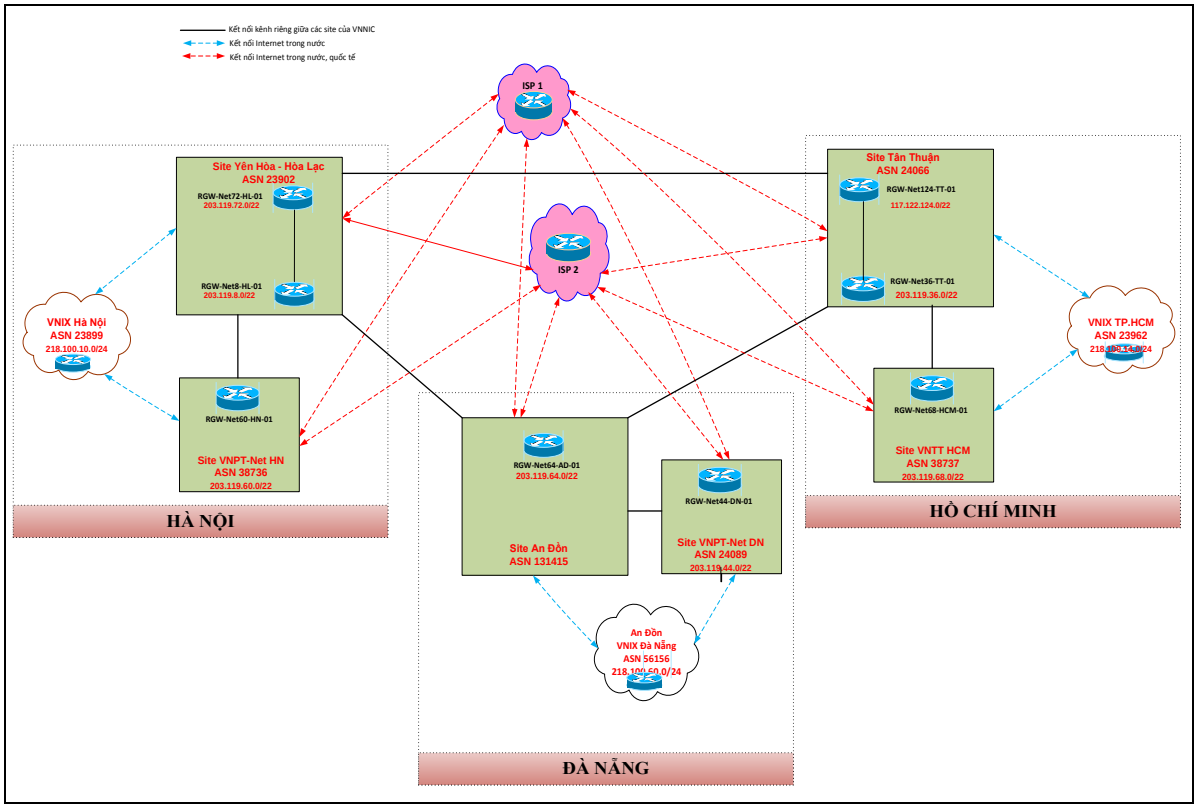
1.1.1 Tổng quan mạng

Hệ thống mạng VNNIC là hệ thống mạng của Trung Tâm Internet Việt Nam, với nhiệm vụ chính là cung cấp hạ tầng kết nối cho hệ thống máy chủ quốc gia tên miền .VN. Ngoài ra, hệ thống mạng VNNIC còn cung cấp kết nối cho các hệ thống kĩ thuật – dịch vụ khác của trung Tâm Internet Việt Nam như: hệ thống quản lí tài nguyên Internet, hệ thống máy chủ tên miền đệm, hệ thống thống kê tên miền, hệ thống mạng quản lí điều hành (TTHN: mail, voice, web …), hệ thống mạng quản lí giám sát, mạng văn phòng…Hiện tại, hệ thống mạng VNNIC bao gồm 6 site tại 3 miền (Hà Nội, Đà Nẵng, TP Hồ Chí Minh):

Tại mỗi site, hệ thống mạng VNNIC được thiết kế bao gồm các kết nối như sau:

- Internet trong nước: kết nối qua trạm trung chuyển Internet quốc gia VNIX, kết nối qua các ISP.
- Internet quốc tế: kêt nối qua các ISP, đảm bảo kết nối đa hướng dự phòng.
- Các site chính (Yên Hòa-Hòa Lạc, Tân Thuận, An Đồn) đươc kết nối trực tiếp với nhau bởi các đường thuê riêng đảm bảo an toàn bảo mật. Ngoài ra, các site có thể kết nối với nhau qua các ISP đảm bảo tính dự phòng.
- Các site chính và các site thuê địa điểm được kết nối trực tiếp với nhau bởi các đường thuê riêng.

lực xử lý lớn, trong khi 1 số phân mạng thiết bị định tuyến biên có năng lực xử lý còn hạn chế. Các phân mạng VNNIC kết nối ra bên ngoài (qua ISP, VNIX) đều đang sử dụng cổng kết nối tốc độ 1 Gbps.



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.

Khu vực	Phân mạng	Hệ thống tường lửa	Tính năng ATAN triển khai	Tác dụng
Hà Nội	203.119.8.0/22 (Mitec-Hòa Lạc)	ASA-5555 Pri/Sec	SourceFire Botnet Filtering	Phát hiện các xâm nhập trái phép, phát hiện các IP bị nhiễm malware trong mạng
	203.119.9.0/24 (OFFICE HN)	ASA-5525X Pri/Sec	Botnet Filtering	Phát hiện các IP bị nhiễm malware trong mạng
			FirePower	Phát hiện các xâm nhập trái phép
	203.119.72.0/22 (Mitec-Hòa Lạc)	SRX 3600	IDP	Phát hiên và ngăn chặn xâm nhập trái phép
	203.119.60.0/22 (Đinh Tiên Hoàng)	SRX 550 Pri/Sec	IDP	Phát hiên và ngăn chặn xâm nhập trái phép
Đà Nẵng	203.119.64.0/22 (An Đồn)	ASA-5555 Pri/Sec	Botnet Filtering	Phát hiện các IP bị nhiễm malware trong mạng
	203.119.65.0/24 (OFFICE ĐN)	ASA-5525X Pri/Sec	Botnet Filtering	Phát hiện các IP bị nhiễm malware trong mạng
			FirePower	Phát hiện các xâm nhập trái phép
	203.119.44.0/22 (VNPTNet-An Đồn)	ASA-5550 Pri/Sec	N/a	
Hồ Chí Minh	203.119.36.0/22 (Tân Thuận)	SRX 550 Pri/Sec	IDP	Phát hiên và ngăn chặn xâm nhập trái phép
	203.119.37.0/22 (OFFICE HCM)	ASA-5525X Pri/Sec	FirePower Botnet Filtering	Phát hiện các xâm nhập trái phép, phát hiện các IP bị nhiễm malware trong mạng
	117.122.124.0/22 (Tân Thuận)	SRX 3600 Pri/Sec	IDP	Phát hiên và ngăn chặn xâm nhập trái phép
	203.119.68.0/22 (VNTTTân Thuận)	SRX 550 Pri/Sec	IDP	Phát hiên và ngăn chặn xâm nhập trái phép

Bảng 1.1:Tổng hợp các hệ thống ATAN mạng VNNIC

1.1.3. Hiện trạng phòng chống tấn công DDoS mạng VNNIC

Hiện nay, các tấn công từ chối dịch vụ (DDoS) ngày càng gia tăng và phức tạp. Trước tình hình đó, trong những năm qua hệ thống mạng VNNIC đã triển khai 1 số biện pháp nhằm phát hiện, phòng chống và giảm nhẹ các cuộc tấn công DDoS, cụ thể:

- Giám sát lưu lượng mạng tại các NOC bằng các hệ thống giám sát hiện có (Cacti, Solarwind…). Tuy nhiên, chưa có 1 quy trình giám sát cụ thể nhằm phát hiện các cuộc tấn công DDoS.
- Đầu tư, nâng cấp các thiết bị mạng lõi có năng lực lớn (thiết bị định tuyến, thiết bị tường lửa).

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.
- Chưa có giải pháp kỹ thuật chuyên nghiệp để thực hiện ngăn chặn, giảm nhẹ khi tấn công DDoS xảy ra.
- Chưa có quy trình xử lý nhằm đối phó kịp thời khi các cuộc tấn công DDoS xảy ra. Việc đối phó, xử lý còn bị động, dựa chủ yếu trên kinh nghiệm của cán bộ quản trị mạng.
- Chưa có 1 đội ngũ cán bộ kĩ thuật chuyên trách nghiên cứu các nguy cơ tấn công; xử lý khi tấn công xảy ra, truy tìm dấu vết sau khi cuộc tấn công kết thúc.
- 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.

Trong khi đó, các cuộc tấn công DDoS đang ngày càng gia tăng, là 1 trong những nguy cơ chính gây gián đoạn các hệ thống mạng. Do đó, việc xác định nhu

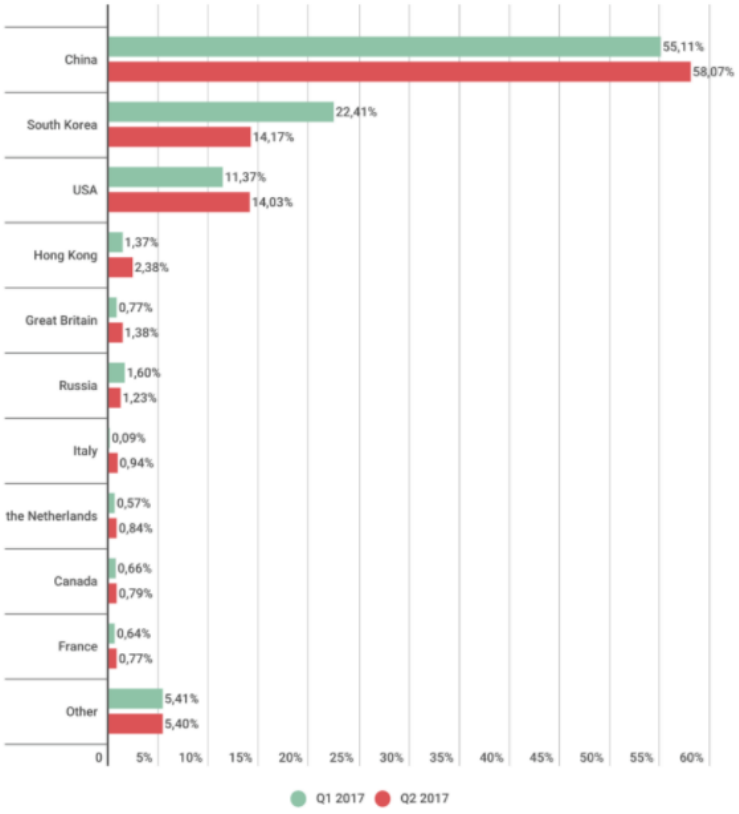
cầu, từ đó nghiên cứu các giải pháp nhằm phát hiện, xử lý hiệu quả các cuộc tấn công DDoS cho hệ thống mạng VNNIC là hết sức cần thiết.

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

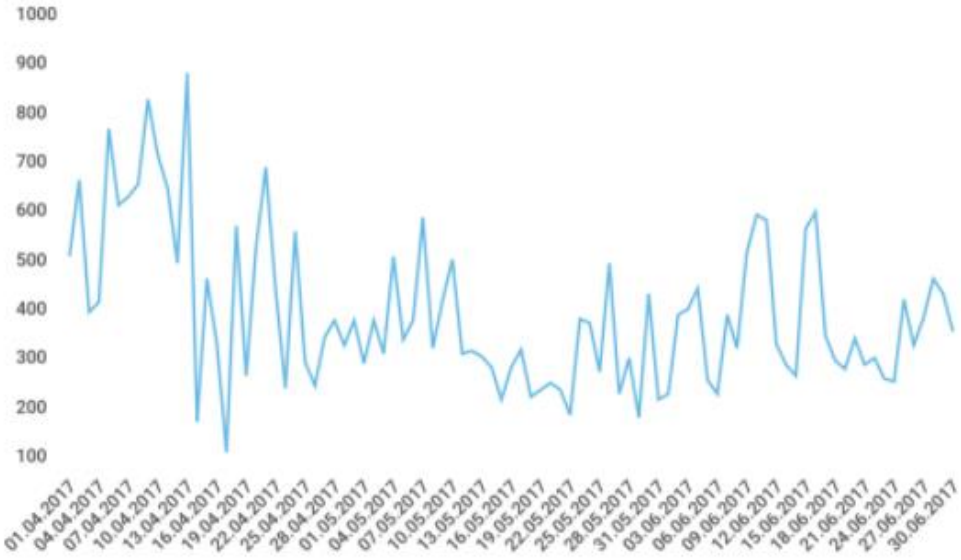
1.2.1. Tình hình tấn công DDoS trên thế giới

Trong những năm gần đây, tình hình các cuộc tấn công DDoS trên thế giới ngày càng diễn ra phức tạp. Tổng hợp báo cáo tình hình tấn công DDoS cập nhật mới nhất vào quý II năm 2017 do các tổ chức, các hãng bảo mật uy tín đưa ra có các thống kê đáng chú ý như sau:

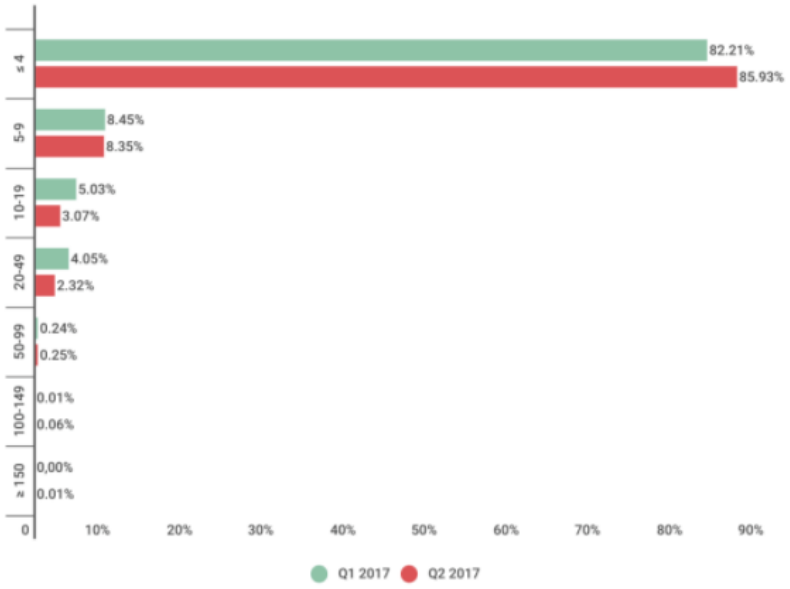
- 86 quốc gia bị tấn công trong Quý 2, 2017, tăng 14 quốc gia so với Quý 1 2017.
- Trung Quốc, Hàn Quốc và Mỹ tiếp tục là các quốc gia đứng đầu về số lượng cuộc tấn công và số lượng mục tiêu bị tấn công. Trong đó, Trung Quốc là quốc gia có số lượng cuộc tấn công cao nhất, chiếm 58,07%. Hàn Quốc chiếm 14,17% và Mỹ chiến 14,03%.
- Các cuộc tấn công DDoS dài hạn xuất hiện trở lại trong Quý 2, với thời gian được ghi nhận là 277 giờ, tăng 131% so với Quý 1. Cùng thời điểm đó, các cuộc tấn công kéo dài dưới 50 giờ không có sự thay đổi so với Quý 1 (99,7% trong Quý 2, 99,8% trong Quý 1).
- Tỉ lệ các cuộc tấn công trên TCP giảm xuống đáng kể (18,2% so với 26,6%) và ICPM (giảm từ 7,2% xuống 8,2%). Điều này làm tăng tỷ lệ SYN Flood và các cuộc tấn công trên UDP và HTTP.
- Các botnet của hệ điều hành Linux có dấu hiệu gia tăng. Các botnet này chịu trách nhiệm về 51,23% các cuộc tấn công trong Quý 2 so với 43,40% trong Quý 1. Các botnet trên Windows chiếm 48,77%.



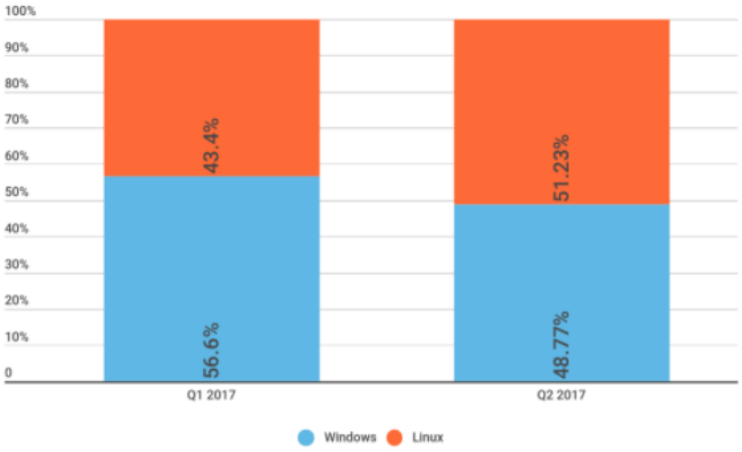
Hình 1.2: Phân bố diễn ra các cuộc tấn công DDoS theo quốc gia



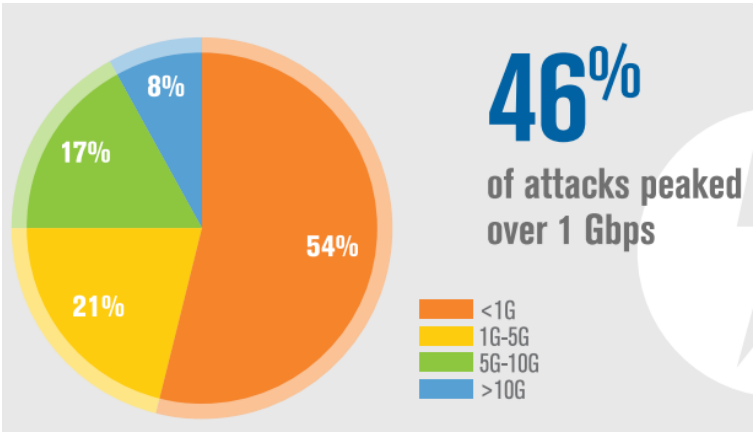
Hình 1.3: Thống kê số lượng cuộc tấn công DDoS theo ngày



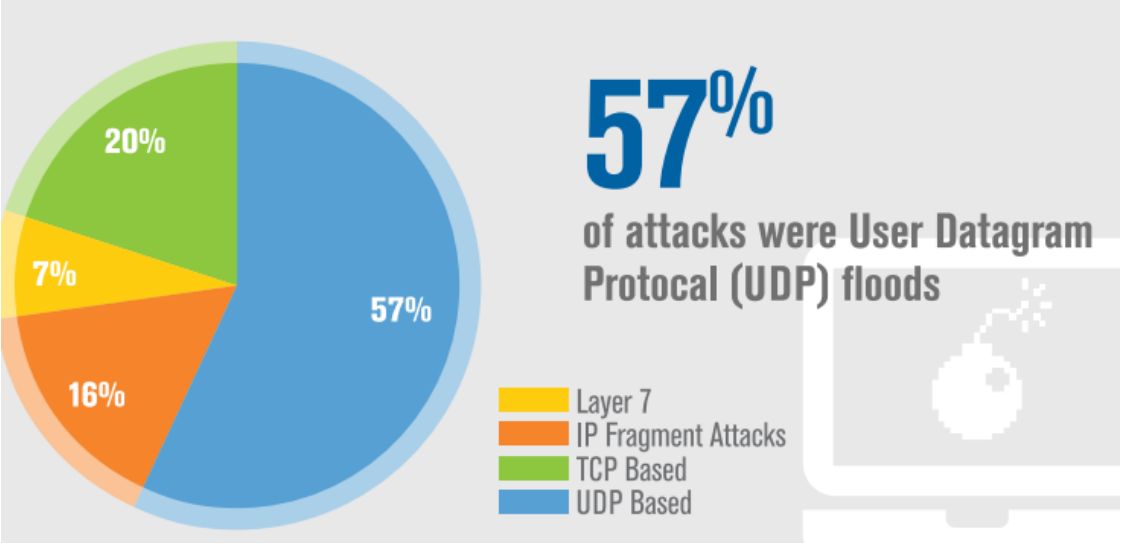
Hình 1.4: Thống kê tỉ lệ các cuộc tấn công DDoS theo chu kì



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



Hình 1.6: Tỉ lệ các cuộc tấn công DDoS theo cường độ tấn công



Hình 1.7: Tỉ lệ các cuộc tấn công DDoS theo loại hình tấn công

Có thể thấy trong những năm gần đây, các cuộc tấn công DDoS ngày càng diễn ra với tần suất, cường độ lớn hơn. Cuộc tấn công DDoS lớn nhất trên thế giới diễn ra tại Mỹ có quy mô lên tới 1000 Gbps. Các loại hình tấn công cũng ngày càng đa dạng, với chu kì tấn công khác nhau rất khó dự đoán. Đặc biệt, ngoài việc lợi dụng các máy tính bị lây nhiễm làm botnet như truyền thống đã xuất hiện các cuộc tấn công DDoS lợi dụng các thiết bị IoT (Internet of Thing). Tỉ lệ các cuộc tấn công DDoS đa hướng có chiều hướng gia tăng. Các cuộc tấn công DDoS diễn ra trên phạm vi khắp toàn cầu, tại nhiều quốc gia trên thế giới.

1.2.2.Tình hình tấn công DDoS tại Việt Nam

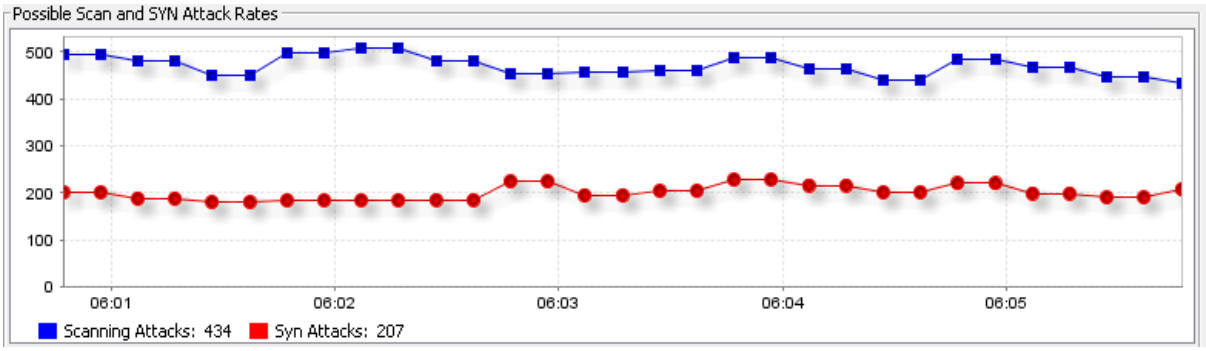
Trong những năm gần đây, cùng với sự phát triển bùng nổ của các dịch vụ nội dung tại Việt Nam là sự gia tăng các hình thức tấn công mạng. Theo thống kê của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, năm 2016 Trung tâm này đã ghi nhận tổng số 134.375 sự cố tấn công mạng. So với năm 2015, số lượng vụ tấn công mạng năm 2016 nhiều gấp hơn 4,2 lần (năm 2015 là 31.585)

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

1.2.3.Phân tích nhu cầu

Trung Tâm Internet Việt Nam được giao nhiệm vụ quản lí, vận hành và khai thác hệ thống máy chủ tên miền quốc gia .VN. Việc tăng cường, đảm bảo an toàn an ninh cho hệ thống mạng của Trung Tâm là một trong những nhiệm vụ ưu tiên hàng đầu. Trung Tâm Internet Việt Nam hiện đang cung cấp rất nhiều các dịch vụ khác nhau cho các NĐK, tổ chức, người dùng bên ngoài sử dụng như: đăng kí tên miền, truy vấn tên miền, Whois Service, Website...Khi hệ thống mạng bị gián đoạn sẽ gây ảnh hưởng đến các dịch vụ mà Trung Tâm cung cấp, ảnh hưởng đến công tác chuyên môn nghiệp vụ của cán bộ nhân viên Trung Tâm. Do đó, việc duy trì hệ thống mạng của Trung Tâm kết nối ổn định, liên tục là hết sức quan trọng. Đặc điểm của loại hình tấn công DDoS là nhằm gây gián đoạn, ngừng trệ hoạt động của các hệ thống mạng, máy chủ dịch vụ.

Ngoài ra, mặc dù chưa có các công cụ hệ thống giám sát phát hiện tấn công DDoS chuyên dụng nhưng trên hệ thống firewall mạng VNNIC cũng thường xuyên ghi nhận những cuộc tấn công SYN attack với cường độ khác nhau:



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.

Trong các chương tiếp theo, nhóm thực hiện đề tài sẽ nghiên cứu, đề xuất các giải pháp phòng chống tấn công DDoS phù hợp cho mạng VNNIC.

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…).

Tấn công từ chối dịch vụ (Denial of Service - DoS) hay tấn công từ chối dịch vụ phân tán (Distributed Denial Of Service – DDoS) chỉ khác nhau về phạm vi, mức độ tấn công, cụ thể:

- Tấn công từ chối dịch vụ (Denial of Service - DoS): Kẻ tấn công sử dụng 1 máy tính đơn để thực hiện cuộc tấn công. Hình thức tấn công từ chối dịch vụ là hình thức sơ khai ban đầu.
- Tấn công từ chối dịch vụ phân tán (Distributed Denial Of Service – DDoS): Kẻ tấn công sử dụng, huy động một số lượng lớn máy tính, bao gồm cả máy tính của các nạn nhân (victim) để thực hiện cuộc tấn công. Hình thức tấn công từ chối dịch vụ phân tán thường có quy mô lớn, diễn biến phức tạp và rất khó để ngăn chặn hoàn toàn.

Tấn công từ chối dịch vụ có các đặc điểm sau đây:

- Tấn công từ chối dịch vụ không làm thay đổi, giả mạo hay ăn cắp thông tin mà nhằm gây gián đoạn thông tin. Trong các đặc trưng của thông tin theo các tiêu chuẩn về an toàn thông tin (Confidentality, Integrity, Availability) thì tấn công DDoS nhằm vào đặc trưng Availability.
- Các cuộc tấn công DDoS dễ thực hiện, gây hậu quả lớn nhưng rất khó ngăn chặn, truy tìm thủ phạm. Hiện nay có rất nhiều các công cụ sẵn có trên Internet cho phép dễ dàng thực hiện các cuộc tấn công DDoS mạng mà không cần nhiều kỹ năng; ngay cả những attacker nghiệp dư cũng có thể thực hiện được. Các cuộc tấn công DDoS có cường độ lớn có thể gây tê liệt, gián đoạn kéo dài các hệ thống công

nghệ thông tin, khiến các dịch vụ bị ngừng trệ, gây thiệt hại lớn về kinh tế chính trị. Tuy vậy, rất khó có thể ngăn chặn hoàn toàn các cuộc tấn công DDoS nhằm vào các hệ thống mạng, các giải pháp hiện nay chủ yếu là nhằm giảm nhẹ các cuộc tấn công DDoS. Việc truy tìn thủ phạm cũng hết sức phức tạp, khó khăn do các attacker thường không tấn công 1 cách trực tiếp đến hệ thống nạn nhân, mà thông qua các máy tính, hệ thống trung gian bị chiếm quyền điều khiển.

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.

- Chuẩn bị công cụ quan trọng của cuộc tấn công, công cụ này thông thường hoạt động theo mô hình client-server. Hacker có thể viết phần mềm này hay download một cách dễ dàng, theo thống kê tạm thời có khoảng hơn 10 công cụ DDoS được cung cấp miễn phí trên mạng (các công cụ này sẽ phân tích chi tiết vào phần sau)

- Kế tiếp, dùng các kỹ thuật hack khác để nắm trọn quyền một số host trên mạng. tiến hành cài đặt các software cần thiết trên các host này, việc cấu hình và thử nghiệm toàn bộ attack-netword (bao gồm mạng lưới các máy đã bị lợi dụng cùng với các software đã được thiết lập trên đó, máy của hacker hoặc một số máy khác đã được thiết lập như điểm phát động tấn công) cũng sẽ được thực hiện trong giai đoạn này.

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

- Sau khi xác định mục tiêu lấn cuối, hacker sẽ có hoạt động điều chỉnh attack-netword chuyển hướng tấn công về phía mục tiêu.

- Yếu tố thời điểm sẽ quyết định mức độ thiệt hại và tốc độ đáp ứng của mục tiêu đối với cuộc tấn công.

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

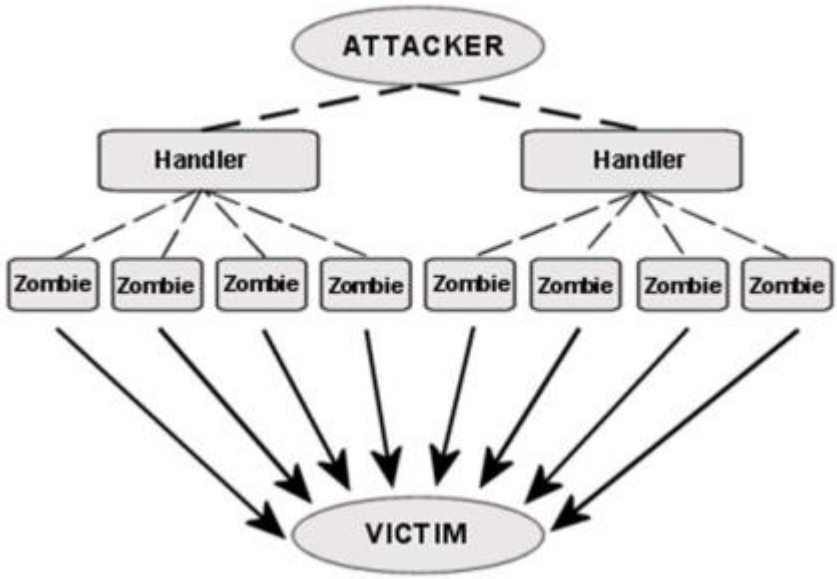
Đúng thời điểm đã định, hacker phát động tấn công từ máy của mình, lệnh tấn công này có thể đi qua nhiều cấp mói đến host thực sự tấn công. Toàn bộ attack-network (có thể lên đến hàng ngàn máy), sẽ vắt cạn năng lực của server mục tiêu liên tục, ngăn chặn không cho nó hoạt động như thiết kế.

- Sau một khoảng thời gian tấn công thích hợp, hacker tiến hành xóa mọi dấu vết có thể truy ngược đến mình, việc này đòi hỏi trình độ khác cao và không tuyệt đối cần thiết.

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.



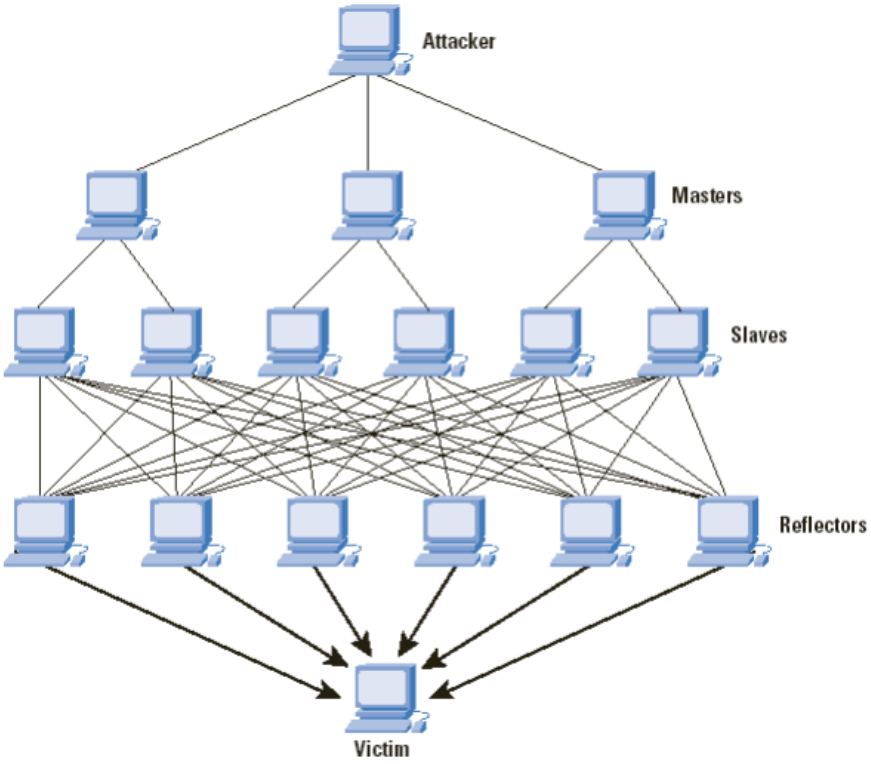
Hình 2.1: Kiến trúc tấn công DDoS trực tiếp

Kiến trúc tấn công DDoS trực tiếp được minh họa trong mình bên trên. trước hết, kẻ tấn công (Attacker) thực hiện chiếm quyền điều khiển hàng ngàn máy tính có kết nối Internet, biến các máy tính này thành các Zombie – những máy tính bị kiểm soát và điều khiển từ xa bởi Attacker. Attacker thường điều khiển các Zombie thông qua các máy trung gian (Handler). Hệ thống các Zombie chịu sự điều khiển của Attacker còn được gọi là mạng máy tính ma hay botnet. Theo lệnh gửi từ Attacker, các Zombie đồng loạt tạo và gửi các yêu cầu truy nhập giả mạo đến hệ thống nạn nhân (Victim), gây ngập lụt, quá tải đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy chủ, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng.

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

Hình trên minh họa kiến trúc tấn công DDoS gián tiếp hay còn gọi là kiến trúc tấn công DDoS phản chiếu. Tương tự như kiến trúc tấn công DDoS trực tiếp, kẻ tấn công (Attacker) trước hết thực hiện chiếm quyền điều khiển một lượng rất lớn máy tính có kết nối Internet, biến các máy tính này thành các Zombie, hay còn gọi la Slave. Attacker điều khiển các Slave thông qua các máy trung gian (Master). Theo lệnh gửi từ Attacker, các Slave đồng loạt tạo và gửi các yêu cầu truy nhập giả mạo với địa chỉ nguồn của các gói tin là địa chỉ của máy nạn nhân (Victim) đến đến một số lớn các máy khác (Reflectors) trên mạng Internet. Các Reflectors gửi phản hồi (Reply) đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào yêu cầu giả mạo. Khi các Reflectors có số lượng lớn, số phản hồi sẽ rất lớn và gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng. Các Reflectors bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất lớn trên mạng Internet và không chịu sự điều khiển của Attacker.

Các vai trò trong tấn công DdoS gián tiếp:

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

2.1.4. Phân loại tấn công DDoS

Hiện nay, các loại hình tấn công DDoS rất đa dạng, ta có thể phân loại các hình thức tấn công DDoS dựa trên nhiều tiêu chí khác nhau. Để có một cái nhìn tổng quát, nhóm đề tài đã thực hiện bảng tổng hợp sau đây (chi tiết xem trong phần phụ lục 03):

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

Bảng sau tổng hợp các hình thức tấn công DDoS phổ biến nhất hiện nay:

ACK Attack or ACK-PUSH Flood	Mirai Botnet	Slow Session Attack
DNS Amplified (Reflective)	Multiple Verb - Single Request	Slowloris Attack
DNS Flood	Non-Spoofed UDP Flood	Smurf Attack
Excessive Verb - Single Session	NTP Amplified (Reflective)	Specially Crafted Packet
Excessive Verb (HTTP GET Flood)	NTP Flood	SSDP Amplified (Refelctive)
Fake Session Attack	Other Amplified Attacks (Reflective)	SYN Flood
Fraggle Attack	Ping Flood	SYN-ACK Flood
Fragmented ACK Flood	Random Recursive GET	TCP Null
HTTP Fragmentation	Recursive GET	TOS Flood
ICMP Flood	RST/FIN Flood	UDP Flood
ICMP Fragmentation Flood	Same Source/Dest Flood (LAND Attack)	UDP Fragmentation
IP NULL	Slow Read Attack	Volumetric Attack

Bảng 2.2: Tổng hợp các hình thức tấn công DDoS phổ biến hiện nay

Trong các hình thức tấn công DDoS liệt kê trong bảng trên, các loại hình tấn công DDoS mà hệ thống mạng dịch vụ của VNNIC hay gặp bao gồm:

- Volumetric Attack.
- SYN Flood.
- ICMP Flood.
- DNS Amplified.
- DNS Flood.

Thông tin chi tiết về các hình thức tấn công này được trình bày trong phần phụ lục 04.

2.1.5. Các biện pháp phòng chống tấn công DDoS

Như đã trình bày ở trên, đặc điểm của tấn công DDoS là rất khó ngăn chặn hoàn toàn, các giải pháp chủ yếu đều nhằm giảm nhẹ các hình thức tấn công DDoS. Các hình thức tấn công DDoS cũng rất đa dạng; với mỗi hình thức tấn công DDoS cũng có một số các giải pháp tương ứng nhằm hạn chế, giảm nhẹ. Đối với các hình thức tấn công DDoS lớp mạng dạng volumetric attack, hiện có 1 số các giải pháp được trình bày chi tiết ở mục II. Đối với các hình thức tấn công dạng protocol; lợi dụng các đặc điểm của giao thức có thể thực hiện các cấu hình tinh chỉnh các tham số của giao thức; cập nhật phiên bản mới của giao thức…. Đối với các hình thức tấn

công DDoS lớp ứng dụng có thể áp dụng các kết hợp các biện pháp lọc gói tin bằng tường lửa, cập nhật các bản vá, tinh chỉnh các cấu hình của phần mềm, dịch vụ.

Tuy nhiên, để có thể thực sự phòng chống, giảm nhẹ hiệu quả các cuộc tấn công DDoS cần phải triển khai kết hợp toàn diện, đồng thời nhiều giải pháp kỹ thuật khác nhau. Các giải pháp này có thể triển khai đồng thời theo các chiến lược cụ thể, từ quá trình phát hiện tấn công, xác định đặc điểm, ngăn chặn khi tấn công xảy ra đến xử lý sau tấn công. Tổng quan, ta có thể xây dựng các giải pháp phòng chống tấn công DDoS theo các chiến lược như sau:

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

1) Triển khai ở nguồn tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở gần nguồn của tấn công. Phương pháp này nhằm hạn chế các mạng người dùng tham gia tấn công DDoS. Một số biện pháp cụ thể bao gồm:

- Thực hiện lọc các gói tin sử dụng địa chỉ giả mạo tại các cổng mạng.
- Sử dụng các tường lửa có khả năng nhận dạng và giảm tần suất chuyển các gói tin hoặc yêu cầu không được xác nhận.

2) Triển khai ở đích tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở gần đích của tấn công, tức là tại bộ định tuyến ở cổng mạng hoặc bộ định tuyến của hệ thống đích. Các biện pháp cụ thể có thể gồm:

- Truy tìm địa chỉ IP: Gồm các kỹ thuật nhận dạng địa chỉ và người dùng giả mạo.
- Lọc và đánh dấu các gói tin: Các gói tin hợp lệ được đánh dấu sao cho hệ thống nạn nhân có thể phân biệt các gói tin hợp lệ và gói tin tấn công. Một số kỹ thuật lọc và đánhdấu gói tin được đề xuất gồm: Lọc IP dựa trên lịch sử, Lọc dựa trên đếm hop, Nhận dạng đường dẫn,…

3) Triển khai ở mạng đích tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở các bộ định tuyến của mạng đích dựa trên lọc gói tin, phát hiện và lọc các gói tin độc hại.

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

Các biện pháp phòng chống tấn công DDoS được triển khai theo tầng mạng, tầng vận chuyển và tầng ứng dụng:

1) Phòng chống tấn công DDoS ở tầng mạng bao gồm một số biện pháp:

- Pushback: Là cơ chế phòng chống tấn công DDoS ở tầng Network cho phép một bộ định tuyến yêu cầu các bộ định tuyến liền kề phía trước giảm tần suất truyền các gói tin.
- SIP defender: Một kiến trúc an ninh mở cho phép giám sát luồng các gói tin giữa các máy chủ SIP và người dùng và proxy bên ngoài với mục đích phát hiện và ngăn chặn tấn công vào các máy chủ SIP.
- Các phương pháp dựa trên ô đố chữ: Gồm các phương pháp dựa trên ô đố chữ mật mã để chống lại tấn công DDoS ở mức IP.
- Sử dụng các kỹ thuật lọc gói tin dựa trên địa chỉ IP.

2) Phòng chống tấn công DDoS ở tầng vận chuyển bao gồm một số biện pháp:

- Tăng kích thước Backlogs giúp tăng khả năng chấp nhận kết nối mới của hệ thống đích.
- Giảm thời gian chờ xác nhận yêu cầu kết nối TCP-SYN giúp máy chủ hủy bỏ các yêu cầu kết nối không được xác nhận trong khoảng thời gian ngắn hơn, giải phóng tài nguyên các kết nối chờ chiếm giữ.
- Sử dụng tường lửa hoặc proxy để lọc các gói tin hoặc thực thi các chính sách an ninh đã xác lập trước.

3) Phòng chống tấn công DDoS ở tầng ứng dụng có thể bao gồm một số biện pháp:

- Tối thiểu hóa hành vi truy nhập trang để phòng chống tấn công gây ngập lụt HTTP.
- Sử dụng các phương pháp thống kê để phát hiện tấn công DDoS ở mức HTTP.
- Giám sát hành vi của người dùng trong các phiên làm việc để phát hiện tấn công.

Phân loại

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

Ta có thể triển khai đồng bộ các biện pháp phòng chống DDoS theo 3 thời điểm như sau:

1) Trước khi xảy ra tấn công: Các biện pháp phòng chống tấn công DDoS thuộc dạng này được triển khai nhằm ngăn chặn tấn công xảy ra. Các biện pháp thuộc dạng này bao gồm việc cập nhật hệ thống, tăng cường năng lực hệ thống, đảm

bảo cấu hình an ninh phù hợp, sửa lỗi, vá các lỗ hổng để giảm thiểu khả năng bị tin tặc khai thác phục vụ tấn công.

2) Trong khi xảy ra tấn công: Các biện pháp phòng chống tấn công DDoS thuộc dạng này tập trung phát hiện và ngăn chặn khi cuộc tấn công xảy ra. Các biện pháp này được triển khai trên các hệ thống như firewall, IDS/IPS, router có tính năng an toàn an ninh.

3) Sau khi xảy ra tấn công: Gồm các biện pháp được triển khai để lần vết và truy tìm nguồn gốc của tấn công DDoS.

Hiện nay, các giải pháp giảm nhẹ các cuộc tấn công DDoS có các hướng tiếp cận sau:

- Thuê các dịch vụ phòng chống DDoS (các dịch vụ dựa trên cloud, các scrubbing center): toàn bộ lưu lượng in/out của mạng đích sẽ được định tuyến đến các thiết bị, hệ thống của nhà cung cấp dịch vụ bảo vệ. Các thiết bị, hệ thống này sẽ kiểm tra làm sạch các lưu lượng tấn công DDoS và chuyển tiếp các lưu lượng hợp lệ quay về mạng đích. Một số nhà cung cấp dịch vụ phòng chống DDoS như: CloudFlare, Coreno, Imperva Incapsula, F5 Network, Arbor, Nexusguard, Akamai, Radware, Kdatacenter…Tại Việt Nam có antiddos.vn cung cấp dịch vụ này.
- Triển khai dịch vụ phân tán sử dụng công nghệ CDN: tùy vào khả năng, hiện trạng có thể tự triển khai phân tán dịch vụ hoặc đi thuê các nhà cung cấp dịch vụ CDN.
- Tự triển khai các hệ thống, thiết bị tại chỗ (onsite) nhằm ngăn chặn, giảm nhẹ các cuộc tấn công DDoS. Hướng tiếp cận này phù hợp với các hệ thống mạng, hệ thống dịch vụ lớn, đủ khả năng tự đầu tư, xây dựng, vận hành các giải pháp, thiết bị cho riêng mình.

Kết luận:

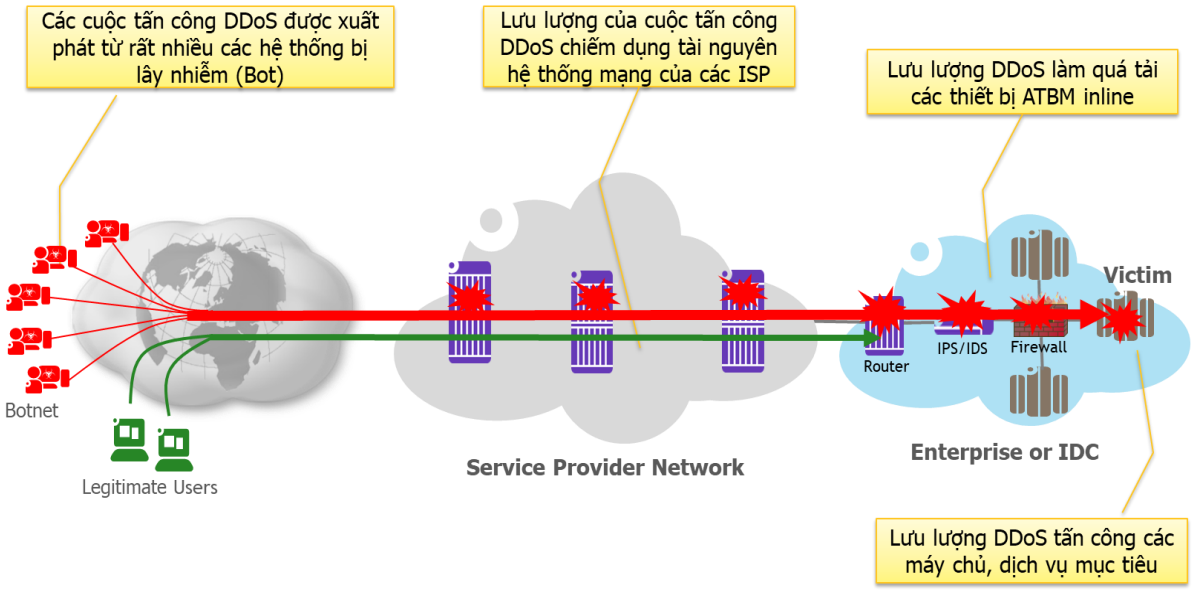
Qua nghiên cứu các giải pháp ngăn chặn, giảm nhẹ tấn công DDoS nhóm đề tài nhận thấy để phòng chống DDoS hiệu quả cho hệ thống mạng VNNIC cũng như các hệ thống KTDV liên quan cần:

- 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

Như đã trình bày bên trên về các hình thức tấn công DDoS nói chung, ngoài dạng tấn công tầng ứng dụng, trong mục này sẽ tập trung nghiên cứu về dạng tấn công DDoS tầng mạng và tầng vận chuyển – nội dung chính. Dạng tấn công này thường được gọi là volumetric attack, thực hiện huy động các lưu lượng không hợp lệ hướng đến máy chủ mục tiêu, nhằm chiếm dụng băng thông đường truyền, từ đó làm quá tải tê liệt các thiết bị mạng (router biên, firewall…) từ đó gây gián đoạn dịch vụ. Đây là loại hình tấn công DDoS chủ yếu hiện nay, ngay cả các cuộc tấn công DDoS tầng ứng dụng cũng hầu hết sẽ gây ra các hệ quả như các cuộc tấn công volumetric attack và phần nào cũng có thể áp dụng chung các phương pháp phòng chống, giảm nhẹ.

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

Quá trình 1 cuộc tấn công DDoS diễn ra được mô tả như hình vẽ bên trên:

- Đầu tiên, một số lượng lớn các hệ thống bị lây nhiễm, điều khiển (gọi là các bot) đồng loạt gửi các lưu lượng không hợp lệ nhằm đến 1 máy chủ, dịch vụ mục tiêu. Số lượng các bot càng lớn thì lưu lượng không hợp lệ này càng lớn. Lưu lượng không hợp lệ này được gọi là lưu lượng tấn công DDoS.
- Lưu lượng tấn công DDoS này đi qua các hệ thống mạng của các ISP, chiếm dụng tài nguyên (đường truyền, hiệu năng thiết bị) và gây ảnh hưởng đến hệ thống mạng của các ISP.

- Lưu lượng DDoS đến hệ thống mạng của doanh nghiệp hoặc trung tâm dữ liệu; gây quá tải thậm chí tê liệt các thiết bị mạng, thiết bị an toàn bảo mật nằm trên đường đi của nó (Router, IPS/IDS, Firewall). Cuối cùng, lưu lượng DDoS này tấn công các máy chủ mục tiêu, gây tê liệt máy chủ và gián đoạn dịch vụ. Các lưu lượng hợp lệ hầu như không thể đến được máy chủ, dịch vụ.

2.2.2. Các phương pháp phòng chống DDoS mạng truyền thống

Để có thể phòng chống DDoS một cách hiệu quả, các hệ thống mạng của các ISP, doanh nghiệp cần thiết kế mô hình bảo mật "Defense in Depth" (Phòng thủ theo chiều sâu). Theo đó, chức năng phòng chống DDoS được triển khai đồng thời tại nhiều lớp mạng khác nhau trong mô hình OSI, tại nhiều thiết bị mạng trong các phân mạng khác nhau (Routers, DDoS Scrubbers, IDS/IPS appliances, Load Balancers, Firewalls…).

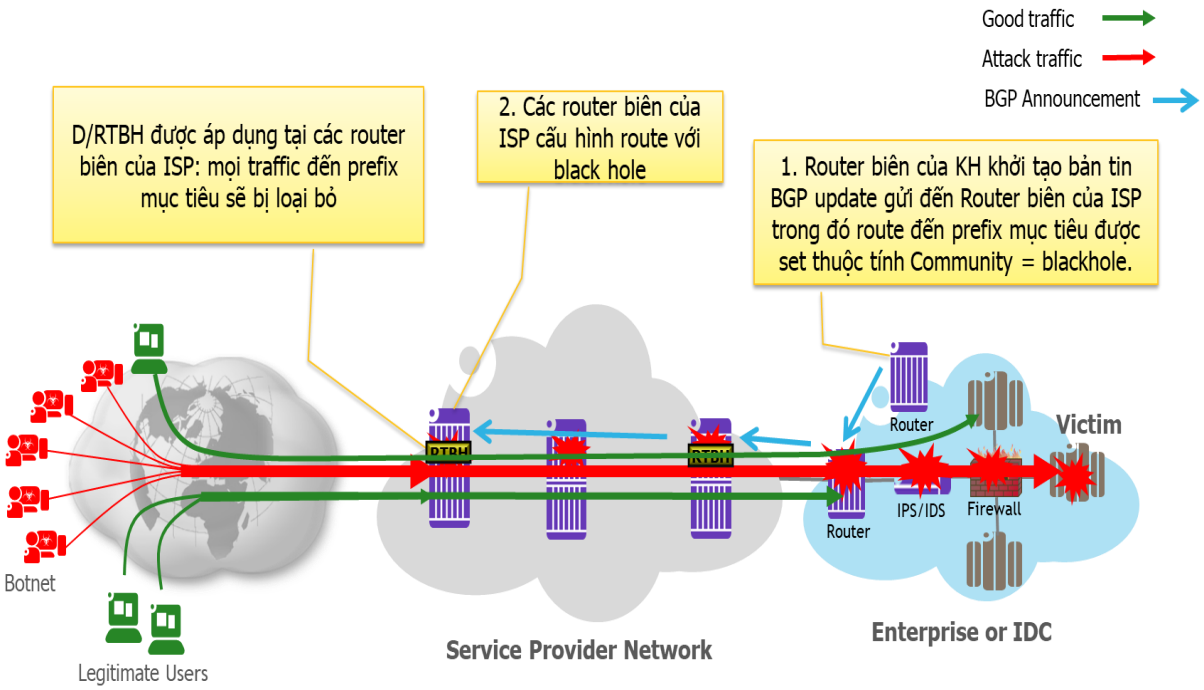
Trong các thiết bị trên, router đóng vai trò chủ đạo trong việc phòng chống DDoS tại các hệ thống mạng của các ISP, doanh nghiệp. Router là vị trí phòng thủ đầu tiên trong toàn bộ hệ thống mạng, router có thể giảm thiểu các cuộc tấn công DDoS ngay tại lớp biên mạng. Router có thể sử dụng các kỹ thuật định tuyến nâng cao để điều khiển lưu lượng các cuộc tấn công sang 1 hướng khác. Các kỹ thuật được áp dụng trước đây là: ACL, D/RTBH, S/RTBH và một kỹ thuật mới được nghiên cứu trong thời gian gần đây là BGP Flowspec.

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):



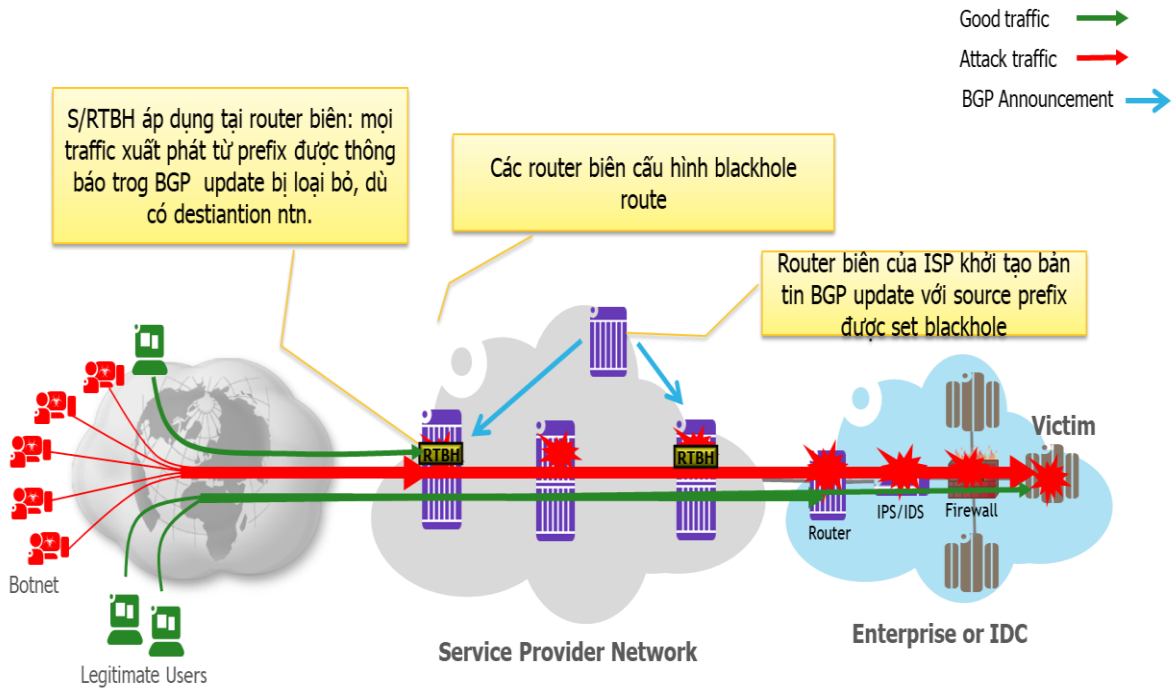
Hình 2.4: Kỹ thuật D/RTBH

Khi cuộc tấn công DDoS xảy ra, router biên của mạng khách hàng (hoặc ISP) khởi tạo 1 bản tin BGP update gửi đến router biên của ISP; trong đó route đến prefix của máy chủ mục tiêu được thiết lập thuộc tính BGP community = blackhole. Các router biên của ISP sau khi nhận được bản tin BGP update, sẽ cấu hình route này gửi đến blackhole. Điều đó có nghĩa là mọi traffic hướng đến prefix mục tiêu sẽ bị các router biên loại bỏ. Kỹ thuật D/RTBH đã được chuẩn hóa trong tiêu chuẩn RFC 3882, RFC 5635.

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

Tương tự kỹ thuật D/RTBH nhưng route được thiết lập community = blackhole trong bản tin BGP update là các prefix nguồn của các cuộc tấn công. Kỹ thuật D/RTBH đã được chuẩn hóa trong tiêu chuẩn RFC 5635.

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: Không linh hoạt, do traffic của các cuộc tấn công DDoS xuất phát từ nhiều nguồn khác nhau.

Kết luận:

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

Kỹ thuật BGP Flowspec là 1 kỹ thuật mới được nghiên cứu áp dụng trong thời gian gần đây nhằm ngăn chặn các cuộc tấn công DDoS. Kỹ thuật BGP Flowspec hoạt động dựa trên các luật áp dụng cho từng luồng lưu lượng cụ thể (BGP Flow Specification Rule). Các chính sách này bao gồm 2 phần:

- **Phần Flow Specification** gồm 1 chuỗi có thứ tự các tiêu chí ở lớp 3, lớp 4 trong mô hình OSI nhằm xác định 1 luồng lưu lượng cụ thể. Một luồng lưu lượng được coi là khớp với 1 Flow Specification nếu các gói tin của luồng khớp với toàn bộ các tiêu chí trong Flow Specification đó. Các tiêu chí này khi mã hóa phải được sắp xếp theo đúng thứ tự quy định trước để hai phía BGP flowspec peering hiểu được. Các tiêu chí này bao gồm:
  - 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**: hành động tương ứng áp dụng cho luồng lưu lượng được xác định bởi Flow Specification. Action có thể là loại bỏ hoàn toàn luồng lưu lượng; áp dụng QoS cho luồng lưu lượng; hạn chế tốc độ hoặc điều hướng luồng lưu lượng đến 1 thiết bị làm sạch (Scrubbing center).

Khi cuộc tấn công DDoS xảy ra, các BGP Flow Specification Rule này được phân phối đến toàn bộ các router biên (BGP peer) từ 1 hệ thống quản lý tập trung (Controlller) thông qua bản tin BGP Update. Trong đó, phần Flow Specification được mã hóa trong định dạng mới của trường NLRI; phần Action được mã hóa trong thuộc tính BGP Community tương ứng với trường NLRI.

<u>Ưu điểm của kỹ thuật này là:</u>

➢ 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.

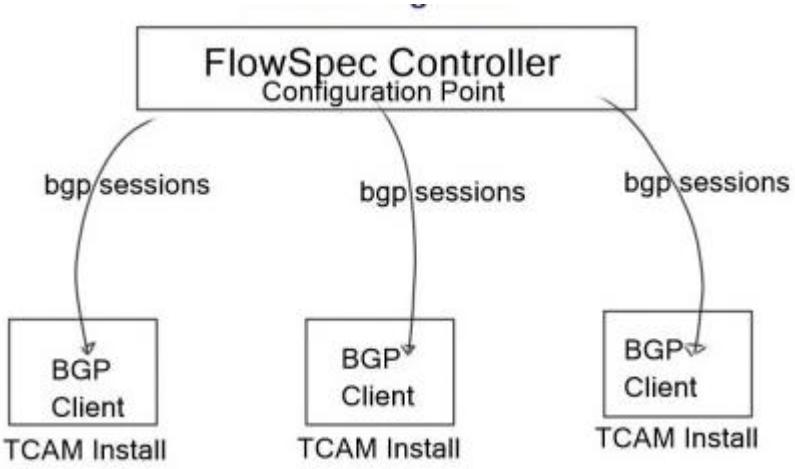
Thông tin về các dòng sản phẩm thiết bị hỗ trợ BGP Flowspec:

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

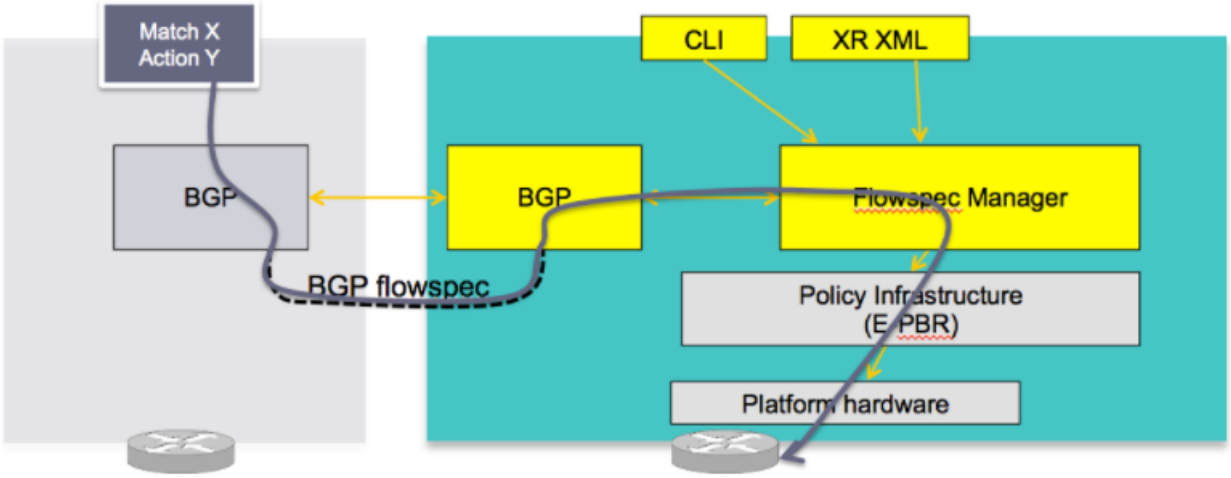
2.3.2.1. Mô hình



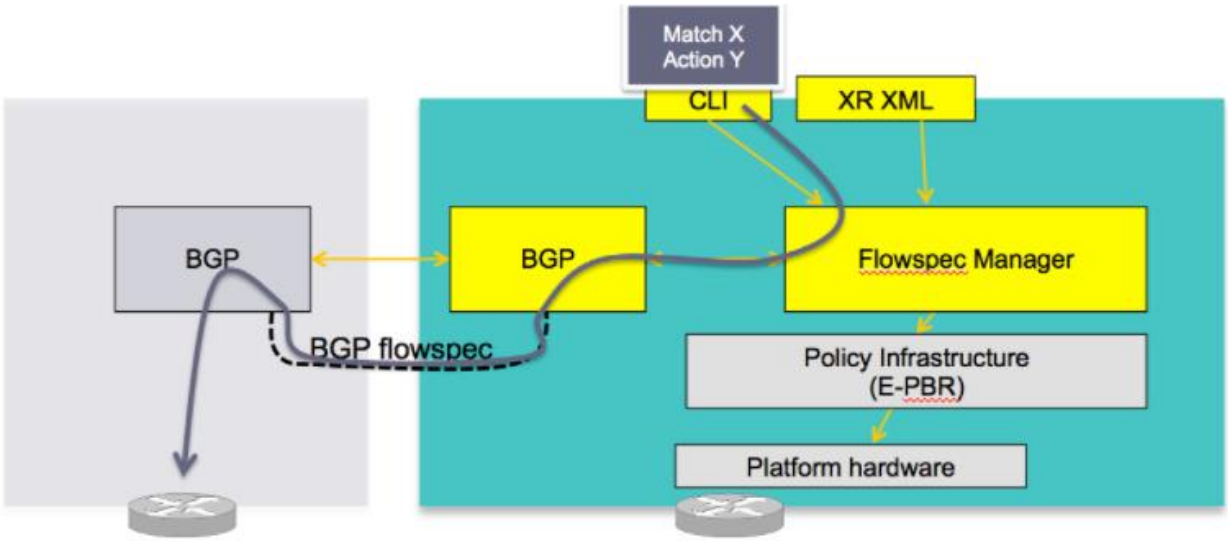
Hình 2.6: Mô hình hoạt động của BGP Flowspec

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.

BGP Flowspec Server sẽ thực hiện phân phối các Flowpsec Rule đồng thời đến các thiết bị BGP Flowspec Client. Tại BGP Flowspec Server, người quản trị có thể nhập các thông tin qua giao diện dòng lệnh hoặc giao diện GUI. Thông tin này qua bộ xử lý Flowspec Manager sẽ tạo thành các Flowpsec Rule gửi sang Client qua giao thức BGP. Các thiết bị Client nhận được Flowspec Rule qua giao thức BGP này, sẽ gửi đến bộ xử lý Flowspec Manager cài đặt vào bộ xử lý chính sách định tuyến nâng cao (E-PBR). Tại đây, sẽ thực hiện xử lý phần cứng trên các giao diện của router biên, đảm bảo tốc độ xử lý ở mức cao nhất.



Hình 2.7: Mô hình hoạt động của BGP Flowspec Client



Hình 2.8: Mô hình hoạt động của BGP Flowsec Server

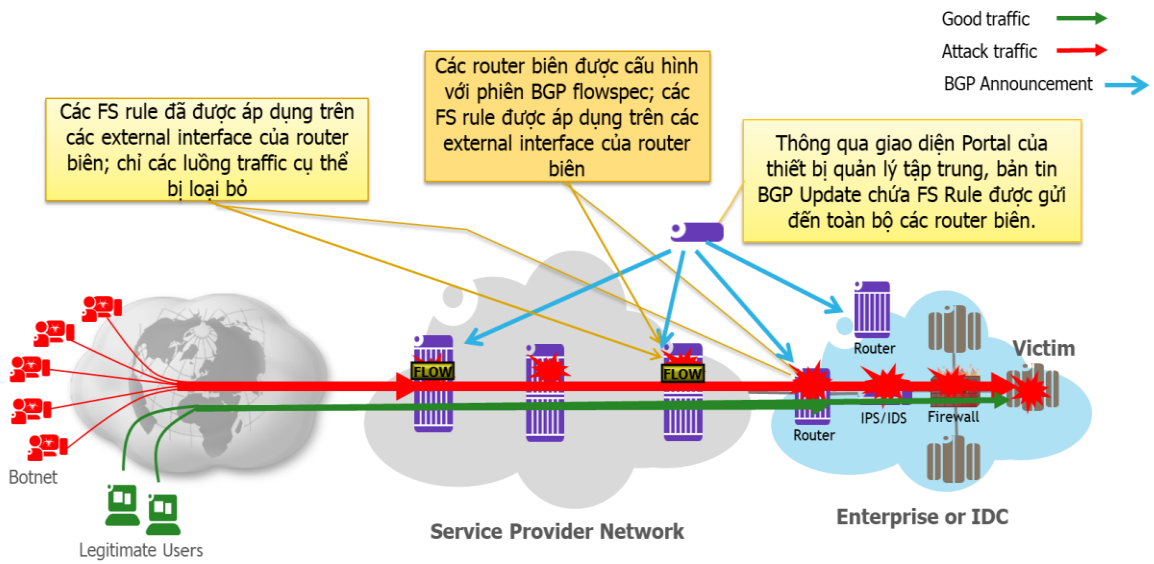
Kỹ thuật BGP Flowspec có thể hoạt động với cả 2 mô hình intra-domain và inter-domain:

- Intra-domain: thiết bị Controller và các Client cùng thuộc 1 AS. Do BGP flowspec can thiệp vào chính sách định tuyến của các router biên nên mô hình này được ưu tiên và dễ triển khai hơn. Theo đó, các ISP hoặc các mạng khách hàng tự chủ động triển khai BGP Flowspec Controller cho các router biên của mình nhằm phòng chống tấn công DDoS. Ngoài ra, các ISP cũng có thể triển khai Controller để điều khiển, tác động các router biên của mình; đồng thời phân quyền cho phép các khách hàng truy cập vào giao diện portal của Controller, chủ động ngăn chặn khi có tấn công DDoS hướng đến mạng của mình. Tuy nhiên, điều này đòi hỏi sự đồng thuận, tin tưởng rất lớn giữa các ISP và khách hàng.

- Inter-domain: thiết bị Controller và các Client nằm ở các AS khác nhau. Theo đó, khách hàng có thể chủ động triển khai Controller và tác động đến router biên của ISP thông qua eBGP flowspec peering. Khi có tấn công DDoS xảy ra, khách hàng sẽ chủ động sử dụng Controller để gửi rule đến router biên của ISP nhằm ngăn chặn luồng tấn công DDoS. Tuy nhiên, mô hình này không phổ biến vì thường các ISP không cho phép khách hàng tác động đến router biên của mình.

Hiện nay, tại Việt Nam hầu hết các ISP đều chưa triển khai BGP Flowspec. Do vậy, giải pháp đề xuất là VNNIC tự chủ động triển khai BGP Flowspec Controller và điều khiển các router biên của mình.

2.3.2.2. Nguyên lý hoạt động



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

Khi 1 cuộc tấn công DDoS xảy ra, đầu tiên cần phải xác đinh được các đặc điểm lớp 3, lớp 4 (Flow Specification) của luồng traffic DDoS đang tấn công hệ thống mạng. Việc phát hiện, xác định này thông qua các công cụ giám sát và phân tích lưu lượng (ví dụ: Netflow).

Sau khi xác định được Flow Specification, người quản trị thực hiện nhập các đặc điểm này vào thiết bị BGP FS Controller thông qua giao điện dòng lệnh hoặc giao diện portal. Đồng thời, người quản trị cũng nhập hành động muốn áp dụng với luồng traffic này. Các thông tin trên tạo thành 1 BGP FS Rule hoàn chỉnh.

BGP FS Controller thực hiện mã hóa các thông tin BGP FS Rule vào trường NLRI và thuộc tính Community. Sau đó, các thông tin mã hóa này sẽ được gửi đến toàn bộ các BGP FS Client 1 cách đồng thời thông qua bản tin BGP Update.

Các BGP FS Client nhận được bản tin BGP Update này, đọc thông tin và lập trình các Flowspec Rule này vào các bộ xử lý phần cứng chuyên dụng trên các interface tương ứng.

Khi đó, các luồng lưu lượng tấn công DDoS không hợp lệ sẽ bị xử lý ngay tại các cổng kết nối phía ngoài của các router biên; trong khi các luồng lưu lượng hợp lệ khác vẫn được chuyển tiếp đến máy chủ dịch vụ đích. Như vậy, cuộc tấn công DDoS đã bị xử lý kịp thời, hạn chế đến mức thấp nhất ảnh hưởng đến dịch vụ. Thời gian xử lý (response time) tương đối nhanh, trong phạm vi của 1 chu kì cập nhật bản tin BGP Update.

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

Trong các mục trên đã nghiên cứu, nguyên lý hoạt động của BGP Flowspec là phân phối đồng thời các Flowspec Rule từ server đến các client thông qua bản tin BGP Update. Trong mục này sẽ trình bày cụ thể quá trình mã hóa lại các thành phần trong bản tin BGP Update (bao gồm trường NLRI, các thuộc tính) để mang các thông tin thành phần của Flowspec Rule (Flow Specification, Action) theo đúng RFC.

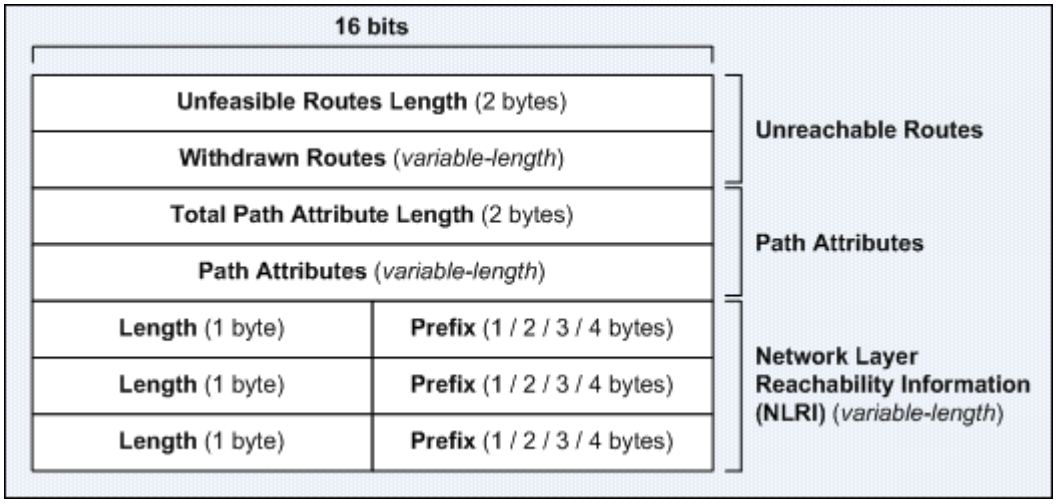
2.3.3.1. . Nhắc lại bản tin BGP Update

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:

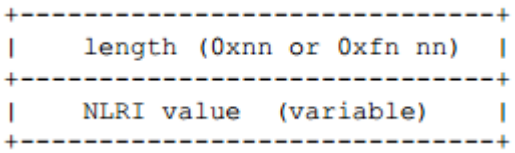


Hình 2.10: Định dạng bản tin BGP Update

2.3.3.2. Mã hóa flow specification trong trường NLRI

Để có thể phân phối thông tin flow specification đến các router biên, RFC 5575 đã đưa ra định dạng mã hóa Flow specification NLRI type để mã hóa lại trường NLRI trong bản tin BGP Update.

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.



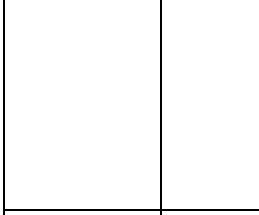
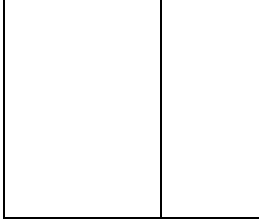
Hình 2.11: flowspec NLRI

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:

Loại flowspec NLRI	**Chỉ tiêu so sánh**	**Mô tả**	**Định dạng mã hóa**
Type 1	Địa chỉ IPv4 đích	Xác định địa chỉ đích để so sánh. Địa chỉ được mã hoá như trong bản tin UPDATE BGP: bao gồm thông tin chiều dài (bit) được mã hóa trong 1 octet; theo sau là các octet đủ để mã hóa thông tin địa chỉ.	<type (1 octet), prefix length (1 octet), prefix>
Type 2	Địa chỉ IPv4 nguồn	Xác định địa chỉ nguồn để so sánh.	<type (1 octet), prefix-length (1 octet), prefix>
Type 3	IPv4 protocol	Bao gồm các cặp (operation, value) để so sánh với trường Protocol trong mào đầu gói tin. Operation (1 byte) được mã hóa theo định dạng sau: 0 1 2 3 4 5 6 7 +---+---+---+---+---+---+---+---+ | e | a | len | 0 | lt | gt | eq | +---+---+---+---+---+---+---+---+ Value là giá trị dùng để so sánh cho các tham số trong Operation.	<type (1 octet), [op, value]+>
Type 4	IPv4 port nguồn hoặc đích	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với TCP/UDP port nguồn hoặc đích trong gói tin IP. Các cặp này cũng được mã hóa	<type (1 octet), [op, value]+>

		tương tự theo định dạng trong type 3. Trường giá trị được mã hóa trong 1 hoặc 2 byte.	
Type 5	IPv4 port đích	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với TCP/UDP port đích trong gói tin IP. Các cặp này cũng được mã hóa tương tự theo định dạng trong type 3. Trường giá trị được mã hóa trong 1 hoặc 2 byte.	<type (1 octet), [op, value]+>
Type 6	IPv4 port nguồn	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với TCP/UDP port nguồn trong gói tin IP. Các cặp này cũng được mã hóa tương tự theo định dạng trong type 3. Trường giá trị được mã hóa trong 1 hoặc 2 byte.	<type (1 octet), [op, value]+>
Type 7	IPv4 ICMP type	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với trường type trong gói tin ICMP. Giá trị value được mã hóa trong 1 byte.	<type (1 octet), [op, value]+>
Type 8	IPv4 ICMP code	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với trường code trong gói tin ICMP. Giá trị value được mã hóa trong 1 byte.	<type (1 octet), [op, value]+>
Type 9	IPv4 TCP flags	Giá trị bitmask có thể được mã hóa trong 1-2	<type (1 octet), [op, bitmask]+>

		byte. Nếu 1 byte, nó sẽ đối chiếu với byte 13 trong mào đầu TCP. Nêu 2 byte nó sẽ đối chiếu với byte 12, 13 trong mào đầu TCP. Bitmask được mã hóa theo định dạng như sau:  	
Type 10	IPv4 packet length	So sánh tổng độ dài cảu gói tin IP (không bao gồm mào đầu lớp 2 nhưng bao gồm cả mào đầu IP). Value có độ dài 1-2 byte.	<type (1 octet), [op, value]+>
Type 11	IPv4 DSCP	Xác định 1 danh sách các cặp (operation, value) dùng để so sánh với trường DSCP. Value có độ dài 1 byte.	<type (1 octet), [op, value]+>
Type 12	IPv4 Fragmentation bit	Sử dụng định dạng bitmask được mô tả ở type 9:  	<type (1 octet), [op, bitmask]+>

Bảng 2.4: Các loại thành phần con của mã hóa Flow specification NLRI

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:

Type	Extended Community	Hành động	Mô tả
0x8006	traffic-rate 0 traffic-rate <rate>	Loại bỏ lưu lượng. Thiết lập giới hạn tốc độ lưu lượng	Hai octet đầu tiên mang id của 2-octet, có thể được gán từ một số AS có độ dài 2 byte. Khi một số AS có độ dài 4 byte có thể sử dụng 2 byte có ý nghĩa nhất trong 4 byte. 4 octet còn lại mang thông tin tốc độ theo định dạng mô tả trong IEEE.754.1985 , đơn vị là byte/s. Tốc độ lưu lượng là 0 tức mọi lưu lượng bị loại bỏ.
0x8008	redirect-vrf	Điều hướng lưu lượng	Giá trị này của thuộc tính mở rộng community hương dẫn phía nhận điều hướng lưu lượng đến 1 VRF routing được chỉ ra trong phần route-target của policy. Thuộc tính mở rộng community này sử dụng cùng kiểu mã hóa trong thuộc tính Route Target community (RFC 4360).
0x8009	traffic-marking	Thiết lập DSCP để áp dụng QoS	Giá trị này của thuộc tính mở rộng community hướng dẫn phía nhận sửa đổi các bit DSCP của các gói tin khớp với flow specification theo giá trị tương ứng.

Bảng 2.5: Mã hóa các hành động trong Flowspec Rule bằng thuộc tính Community

Như vậy, toàn bộ các thành phần của Flowspec Rule đã có thể được mã hóa trong bản tin BGP Update. Như vậy, thông qua mối quan hệ flowspec peering, controller đã có thể gửi các Flowspec Rule đến các client. Các client nhận được Flowspec Rule này, sẽ cập nhật vào các bộ xử lý định tuyến phần cứng nâng cao (ePBR), xử lý chính xác các luồng lưu lượng tấn công DDoS.

2.3.4. Kỹ thuật điều hướng lưu lượng trong BGP Flowspec

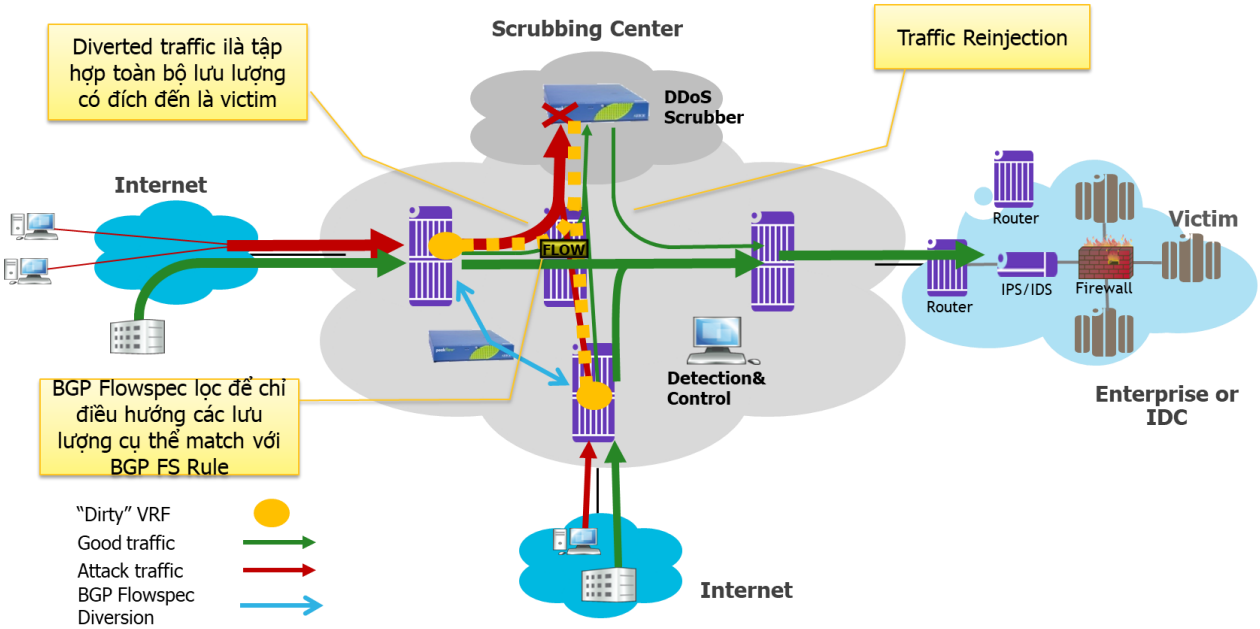
Một kỹ thuật nâng cao của BGP Flowspec là điều hướng lưu lượng DDoS đến 1 hệ thống làm sạch DDoS (DDoS Scrubber). DDoS Scrubber là các thiết bị chuyên dụng có khả năng hạn chế các cuộc tấn công DDoS phức tạp ở lớp ứng dụng bằng cách kết hợp nhiều kỹ thuật khác nhau như: DPI (Deep Packet Inspection –

kiểm tra gói tin ở cả phần dữ liệu lẫn phần mào đầu); signature matching (So sánh với các mẫu lưu lượng), behavior analysis (phân tích hành vi), protocol authentication….Các thiết bị này được đặt tại 1 vùng gọi là Trung Tâm làm sạch dữ liệu (Scrubbing Center).

Các traffic bất thường khi đi vào hệ thống mạng sẽ được điều hướng đến Scrubbing Center và bị xử lý bởi các thiết bị Scrubber trước khi đến hệ thống mạng của doanh nghiệp, trung tâm dữ liệu.

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.

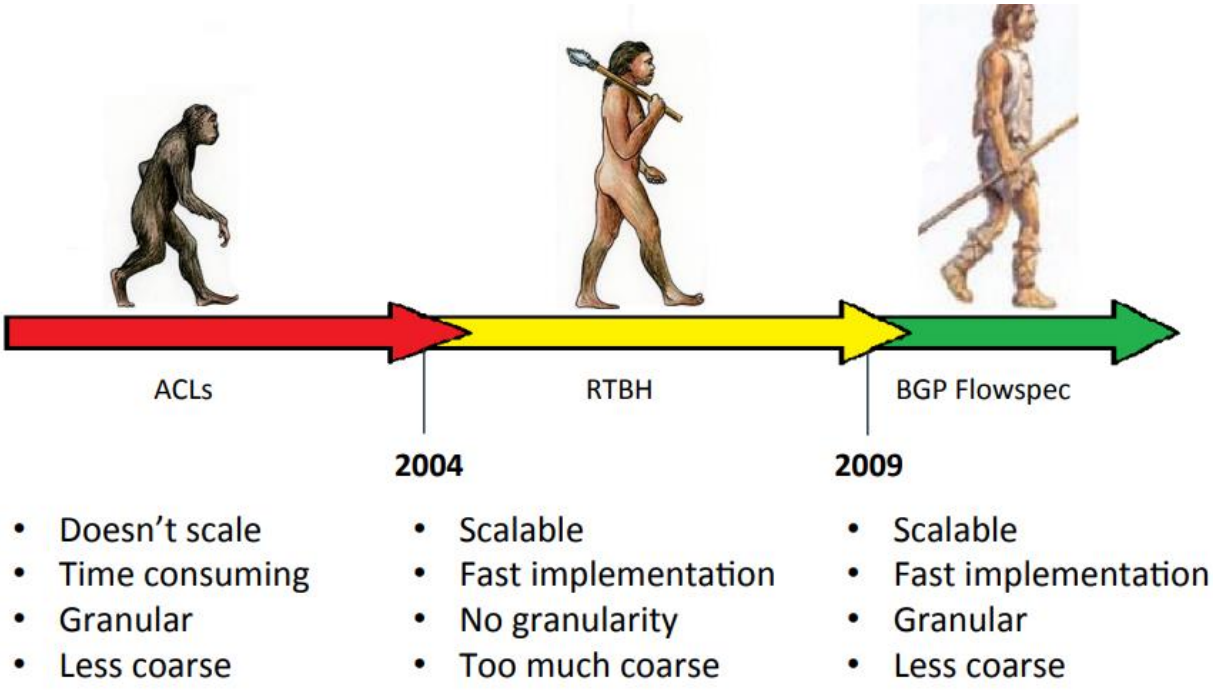
Kỹ thuật Reinjection hay Onramping: điều hướng các lưu lượng sạch từ Scrubbing Center quay trở lại đích đến ban đầu. Kỹ thuật Reinjection thường sử dụng đường hầm hoặc VRF để chuyển hướng các lưu lượng sạch về lại đích dự kiến mà không bị loop.



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

2.3.3.5. 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

ExaBGP là 1 công cụ mã nguồn mở do tác giả Thomas Magnin phát triển theo hướng mạng định nghĩa bằng phần mềm (Software Defined Network); cho phép các nhà quản trị mạng có thể dễ dàng tương tác với các hệ thống mạng sử dụng giao thức BGP. Nguyên tắc hoạt động của ExaBGP là chuyển đổi các bản tin BGP về dạng văn bản hoặc định dạng JSON; từ đo có thể dễ dàng điều khiển, tương tác, can thiệp bằng các script đơn giản. Hiện tại, mã nguồn của ExaBGP được cung cấp và hỗ trợ miễn phí tại: https://github.com/exa-networks/exabgp

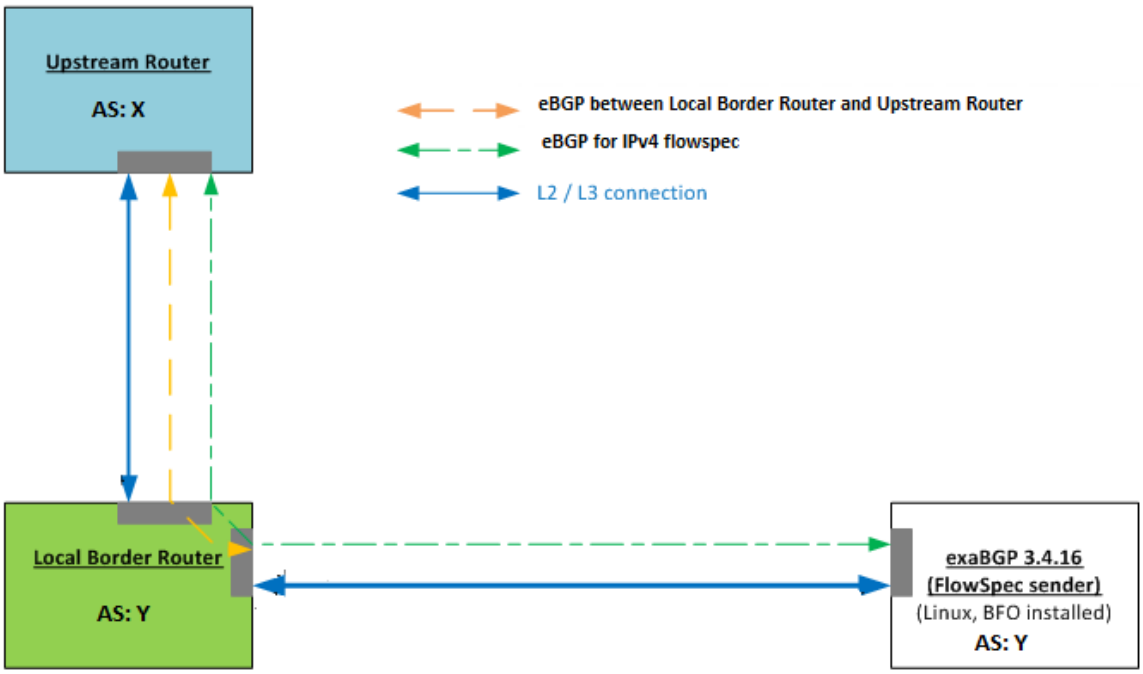
ExaBGP có thể được ứng dụng trong một số trường hợp sau:

- Đóng vai trò làm BGP Flowspec Controller, hoạt động theo RFC 5575 nhằm ngăn chặn, hạn chế tấn công DDoS vào các hệ thống mạng sử dụng giao thức BGP. Hiện tại, ExaBGP là mã nguồn mở duy nhất cho phép inject và lan truyền các BGP Flowspec rule.
- Cân bằng tải cho hệ thống mạng.

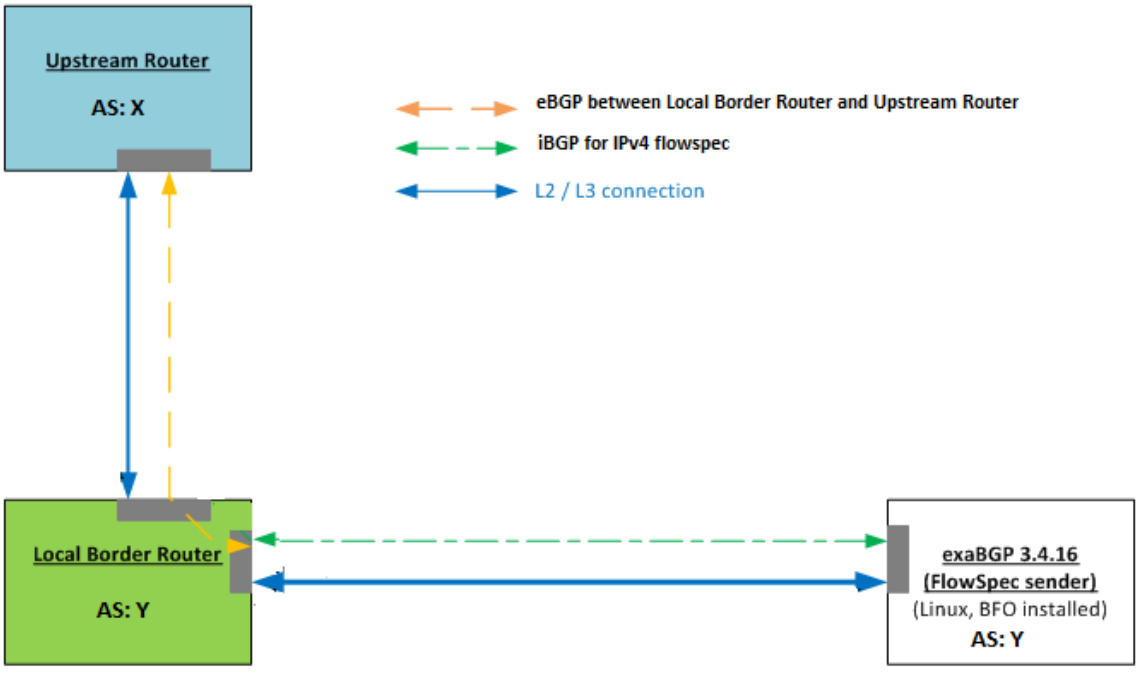
Hiện nay, ExaBGP được rất nhiều các tổ chức hỗ trợ, sử dụng để làm BGP Flowspec Controller như: AMS-IX, Alcatel Lucent, BBC, Blablacar, Cisco Systems, CloudFlare, Dailymotion, Facebook, MaxCDN, Microsoft, OpenDNS, Oracle, PowerDNS, RIPE NCC....

Công cụ ExaBGP được cài đặt trên 1 máy chủ chạy hệ điều hành Linux (Ubuntu, Redhat, Debian…). Hiện có 2 phiển bản ExaBGP chủ yếu là 3.4.5 và 4.0.

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

Công cụ ExaBGP có thể hoạt động trong 2 mô hình: intra-domain và inter-domain như hình vẽ bên trên. Trong mô hình inter-domain, ExaBGP đặt tại mạng

của khách hàng đóng vai trò Controller điều khiển upstream router của ISP qua flowspec. Trong mô hình intra-domain, ExaBGP đặt tại mạng của khách hàng đóng vai trò Controller điều khiển local router của khách hàng qua flowspec.

Trong cả 2 mô hình, ExaBGP đều hỗ trợ BGP flowspec hoạt động theo tiêu chuẩn RFC 5575.

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;
```

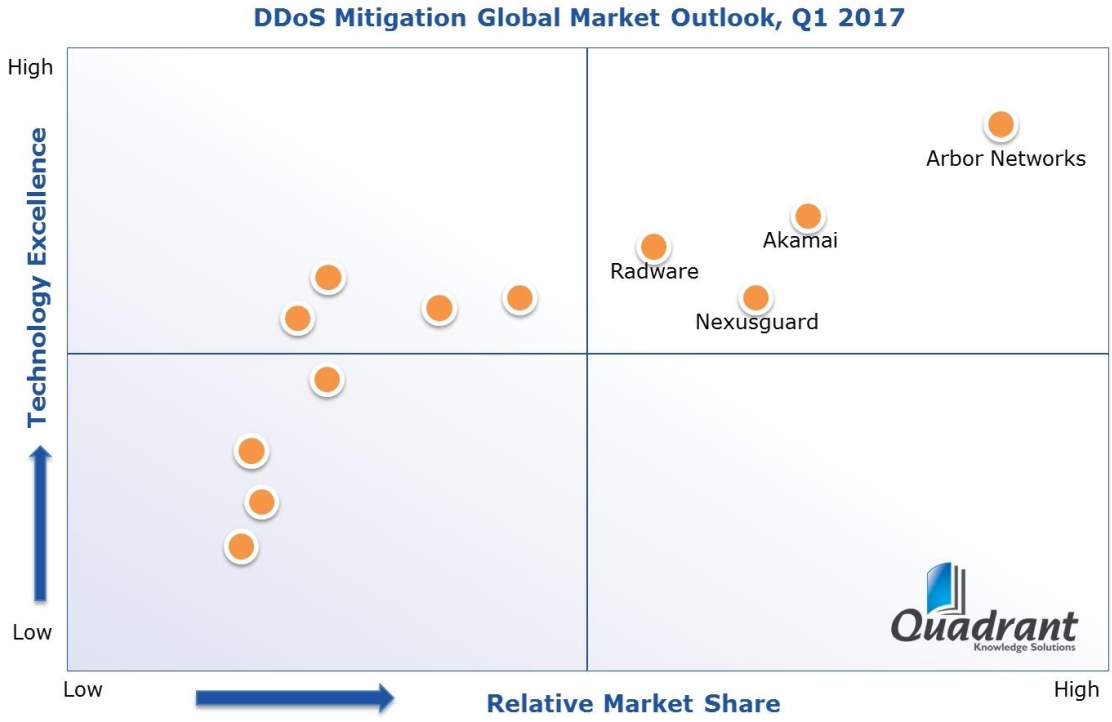
- Cấu hình các Flowspec rule dưới dạng static hoặc dynamic. Trong trường hợp cấu hinh tĩnh các Flowspec rule trong file config, mỗi lần thay đổi các rule này sẽ thiết lập lại mối quan hệ Flowspec peering. Ngược lại, trong trương hợp sử dụng script động dynamic.sh; có thể thay đổi và inject các Flowspec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

- Hiện tại, hệ thống mạng VNNIC đang sử dụng các thiết bị router gateway của hãng Cisco.
- Arbor là hãng duy nhất có giải pháp đồng bộ, tổng thể kết hợp với các thiết bị router của Cisco trong việc áp dụng kỹ thuật BGP Flowspec vào ngăn chặn tấn công DDoS.
- Arbor là hãng dẫn đầu thị trường về giải pháp ngăn chặn, hạn chế tấn công DDoS (theo đánh giá của Gartner 2017):



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

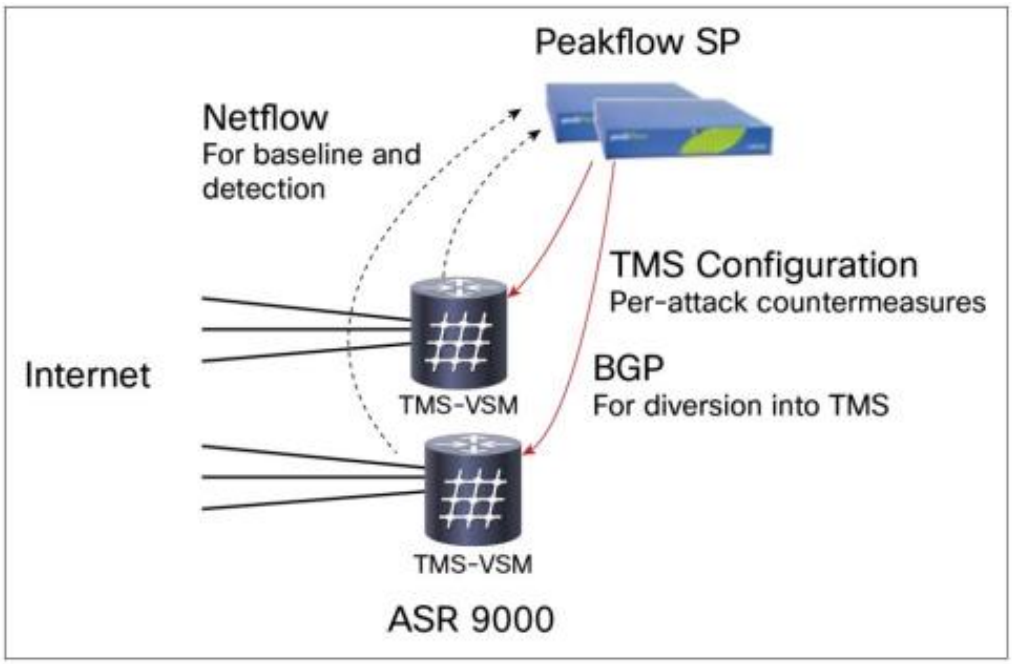
b) Nguyên lý hoạt động

Giải pháp Arbor Peakflow cho phép bảo vệ các hệ thống mạng trước cả 2 kiểu tấn công DDoS: kiểu volumetric và kiểu tấn công tầng ứng dụng. Giải pháp này xây dựng 1 mức giới hạn (baseline) của mạng. Nếu nhận thấy các bất thường của mạng vượt ngoài baseline thì nó sẽ tự động loại bỏ các lưu lượng không mong muốn và cho phép các lưu lượng hợp lệ. Quá trình này được thực hiện bằng ACL, hạn chế tốc độ, các thực các phiên kết nối và giám sát lưu lượng. Nguyên lý hoạt động của giải pháp này như sau:

- Đầu tiên, hệ thống sẽ giám sát tại các điểm lưu lượng đi vào hệ thống mạng bằng Netflow và BGP, từ đó tạo ra 1 mức giới hạn (baseline) của mạng và các mẫu lưu lượng.
- Tiếp theo, hệ thống tiếp tục giám sát để phát hiện ra các bất thường và đánh đấu nó các cuộc tấn công tiềm năng.
- Những cuộc tấn công tiềm năng này được thông báo đến cán bộ quản trị mạng thông qua GUI, email, SNMP…cho phép thực hiện các hành động phù hợp: thực hiện 1 hành động đối phó (response) hoặc coi sự kiện đó là cảnh báo giả. Các hành động đối phó chính như sau:

- Cập nhật định tuyến mạng để điều hướng tất cả lưu lượng đến đích đi qua hệ thống TMS-VMS, nơi có thể loại bỏ các lưu lượng không mong muốn. Việc điều hướng này được Peakflow SP đóng vai trò Controller điều khiển các router ASR 9K đóng vai trò Client bằng kỹ thuật BGP Flowspec. Giải pháp này tuân thủ đúng kỹ thuật BGP Flowspec được mô tả trong RFC 5575.
- Làm sạch lưu lượng tối đa có thể mà không ngăn chặn nhầm các lưu lượng hợp lệ.

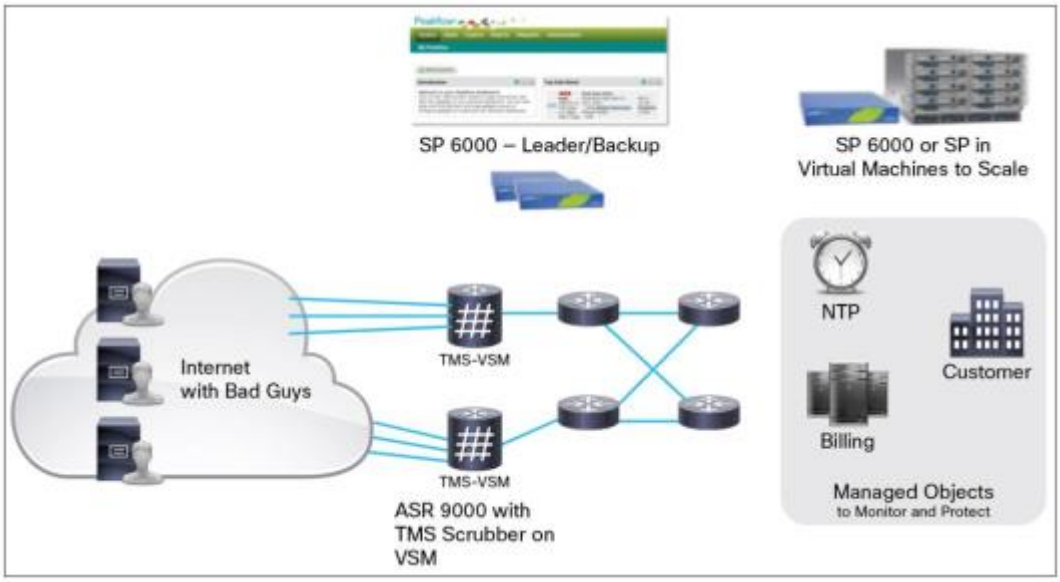
Trong giải pháp kết hợp với Arbor, Cisco ASR 9K đã tích hợp chức năng làm sạch lưu lượng vào bên trong router.



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.

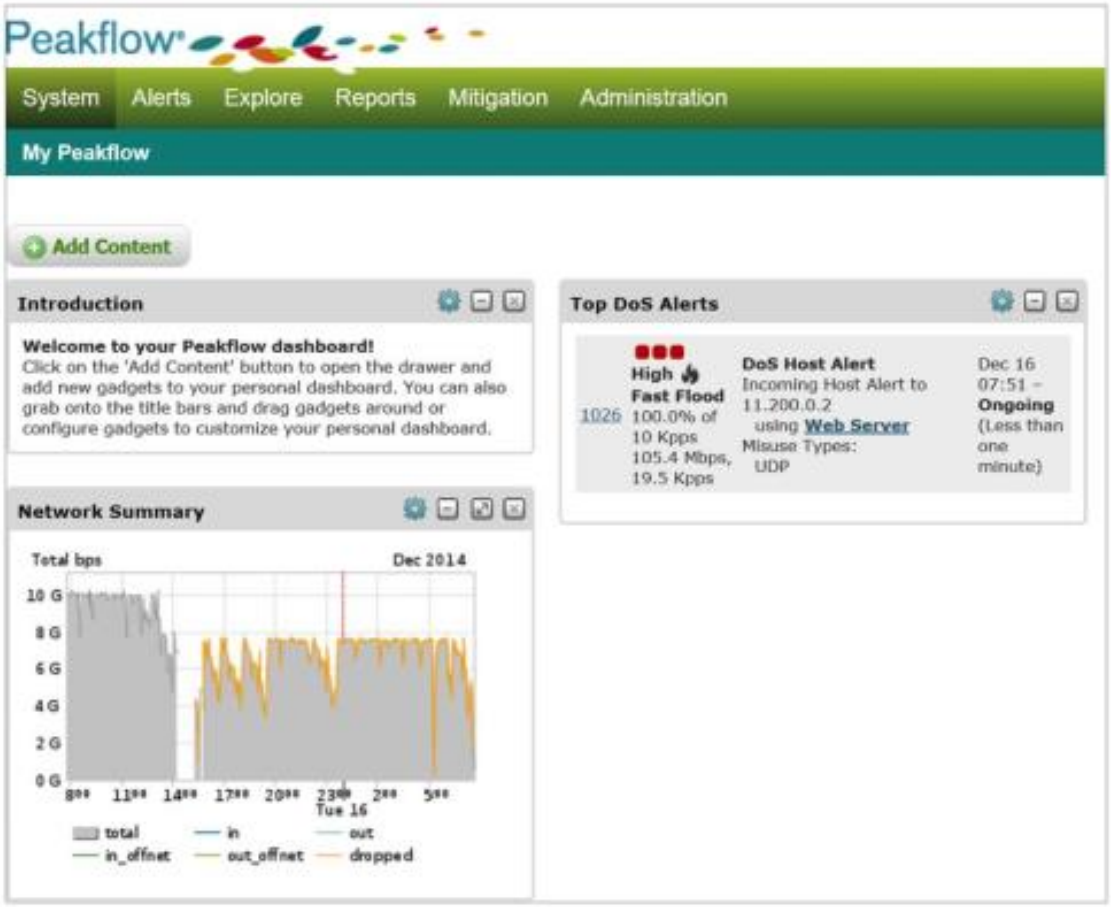


Hình 2.17: Các thành phần của giải pháp Arbor Peakflow

Peakflow SP: là thành phần thực hiện chức năng điều khiển của giải pháp Peakflow, thực hiện các công việc như giám sát mạng, phát hiện các cuộc tấn công và phối hợp phản ứng lại các cuộc tấn công. Thành phần Peakflow SP có thể chạy kết hợp trên thiết bị phần cứng của Arbor (VD: SP 6000) và máy chủ ảo hóa nhằm mở rộng khả năng xử lý. Bắt đầu từ phiên bản Peakflow SP 7.0.3, thành phần này có thể chạy hoàn toàn trên máy chủ ảo hóa. Trong giải pháp ASR 9K vDDoS, Cisco chỉ chấp nhận cài đặt Peakflow SP trên máy ảo hóa. Trước đây, để thực hiện chức năng Peakflow SP cần 1 loạt các phần cứng sau: Collector Platform (CP), Flow Sensor (FS), Portal Interface (PI), Business Intelligence (BI). Peakflow SP thực hiện các chức năng sau:

- 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): viết tắt là Peakflow SP TMS là thành phần thực hiện chức năng chuyển mạch dữ liệu, thực hiện việc loại bỏ các cuộc tấn công DDoS. Thành phần TMS chạy trên card VSM trên router Cisco ASR 9K. Peakflow TMS thực hiện các chức năng sau:

- 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: đóng vai trò làm BGP Flowpsec Client; nhận các Flowspec Rule từ Peakflow SP và thực hiện xử lý lưu lượng bằng bộ xử lý định tuyến phần cứng nâng cao (ePBR). Trong giải pháp này, trên router ASR 9K cũng đồng thời tích hợp luôn card VMS thực hiện vai trò của 1 scrubbing center.

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

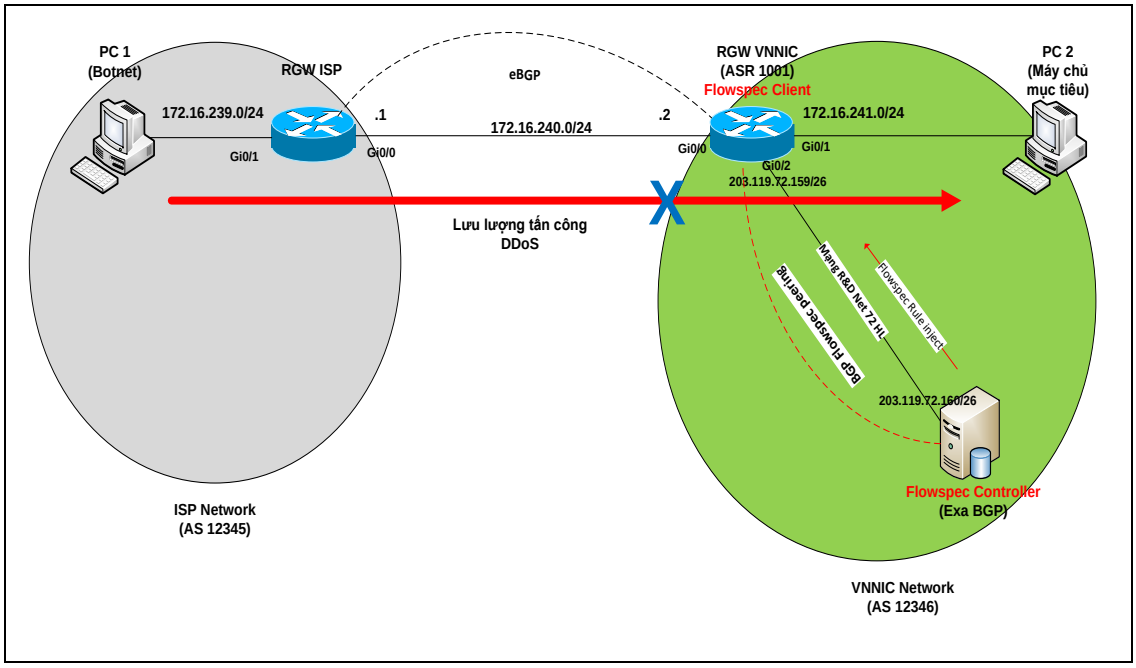
3.1.1. Mục tiêu thử nghiệm

- 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

Để đạt được các mục tiêu trên nhóm đề tài đã xây dựng hệ thống thử nghiệm theo đúng mô hình hoạt động của hệ thống mạng VNNIC. Theo đó, mô hình gồm có gồm 2 ASN được mô tả như sơ đồ bên dưới:

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



Hình 3.1: Mô hình thử nghiệm BGP Flowspec

STT	Thiết bị	Phần mềm	Gao diện/Địa chỉ IP	Chức năng
1	ASR 1001	Cisco ASR1001 IOS XE UNIVERSAL (asr1001-universalk9.03.08.01.S.153-1.S1.bin)	Gi 0/0: 172.16.240.2/24: Kết nối eBGP to RGW ISP. Gi 0/1: 172.16.241.1/24: Kết nối đến PC-02. Gi 0/2: 203.119.72.159/26: Kết nói BGP Flowspec với ExaBGP	Mô phỏng RGW mạng VNNIC – đóng vai trò BGP Flowspec Client
2	PC-02	Window 10	IP: 172.16.241.2/24 GW: 172.16.241.1	Mô phỏng máy chủ mục tiêu của VNNIC
3	Máy ảo VMWare ExaBGP	HĐH: Ubuntu. ExaBGP 3.4.5	203.119.72.160/26	Mô phỏng công cụ BGP Flowspec Controller
4	ASR 1001	Cisco ASR1001 IOS XE UNIVERSAL (asr1001-	Gi 0/0: 172.16.240.1/24: Kết nối eBGP to	Mô phỏng router biên của ISP – kết nối

		universalk9.03.08.01.S.153-1.S1.bin)	RGW VNNIC. Gi 0/1: 172.16.239.1/24: Kết nối đến PC-01.	định tuyến cho mạng VNNIC đi ra Internet
5	PC-01	Window 10	IP: 172.16.239.2/24 GW: 172.16.239.1	Mô phỏng máy tính trên Internet đóng vai trò botnet gửi lưu lượng tấn công DDoS đến PC-02

Bảng 3.1: Các thành phần của mô hình thử nghiệm BGP Flowspec

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

RGW mạng VNNIC sẽ được cấu hình eBGP peering với RGW của ISP. RGW VNNIC quảng bá vùng địa chỉ 172.16.241.0/24 của mạng VNNIC; RGW ISP quảng bá các cùng mạng trên Internet cho RGW VNNIC (ở đây sử dụng vùng mạng 172.16.239.0/24). Kết quả trong điều kiện hoạt động bình thường:

- 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).

Công cụ ExaBGP được cài đặt trên 1 máy ảo hóa chạy hệ điều hành Ubuntu Linux có địa chỉ 203.119.72.160/26 thuộc mạng R&D-72. Trên RGW VNNIC cũng cấu hình 1 giao diện có địa chỉ chỉ thuộc mạng R&D-72 203.119.72.159/26. Máy chủ ExaBGP Server và RGW VNNIC được cấu hình để thiết lập mối quan hệ BGP Flowpsec peering với nhau; trong đó ExaBGP Server đóng vai trò làm Flowspec Controller điều khiển RGW VNNIC.

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
```

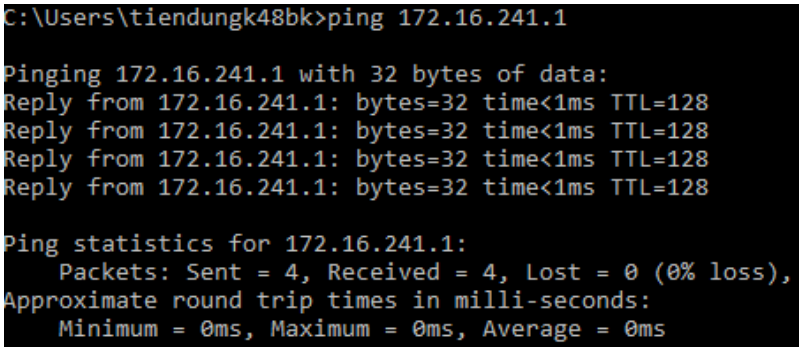
```
# command and watchdog name are case sensitive

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:



Sau đó, giả xử PC-01 bị nhiễm độc, tham gia vào mạng lưới bots tấn công DDoS PC-02. Lúc này, xác định các lưu lượng xuất phát từ PC-01 đến PC-02 là tấn công DDoS; cần phải ngăn chặn.

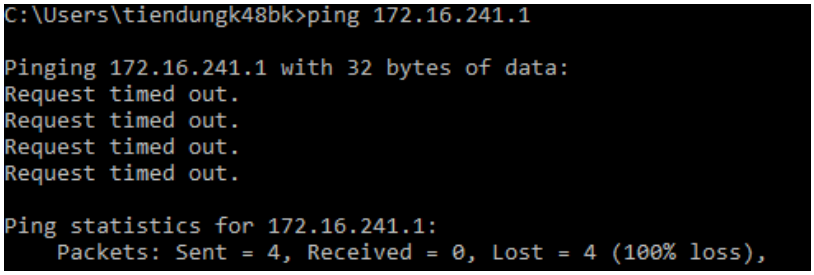
Tiến hành cấu hình trên exaBGP điều khiển RGW VNNIC bằng Flowpsec rule: thực hiện drop các lưu lượng đến từ vùng địa chỉ của PC-01 *(tham khảo chi tiết phụ lục 01).*

```
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:



3.1.5. Kết quả thử nghiệm

a) Kết quả:

Sau khi tiến hành thử nghiệm theo đúng kịch bản nêu trên, kết quả cho thấy ExaBGP đã điều khiển RGW VNNIC bằng các flowspec rule ngăn chặn thành công luồng lưu lượng tấn công từ PC-01 hướng đến PC-02.

b) Đánh giá:

- Việc triển khai kỹ thuật BGP Flowspec theo mô hình intra-domain vào mạng VNNIC trong giai đoạn ngăn chặn tấn công DDoS sau khi phát hiện, xác định được tấn công là khả thi; phù hợp với mô hình mạng.
- Công cụ ExaBGP đáp ứng tốt vai trò Controller điều khiển các router Cisco đóng vai trò Client trong mô hình triển khai áp dụng BGP Flowspec.

c) Đề xuất:

Triển khai giải pháp BGP Flowspec theo mô hình intra-domain áp dụng chính thức cho hệ thống mạng VNNIC. Trong đó, VNNIC tự xây dựng các Controller sử dụng công cụ ExaBGP; điều khiển các RGW của mạng VNNIC tại các site nhằm ngặn khi có tấn công DDoS xảy ra.

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

- Tiếp tục nâng cấp năng lực xử lý của các thiết bị định tuyến tại các phân mạng VNNIC. Đồng thời, nâng cấp các cổng kết nối ra Internet bên ngoài (với ISP, VNIX) trên các thiết bị này lên 10 Gbps.
  (Tham khảo: Kế hoạch triển khai quy hoạch RGW mạng VNNIC 2017).
- Cập nhật kịp thời các bản update, các bản patch vá lỗi , lỗ hổng cho các hệ điều hành, phần mềm của máy chủ, thiết bị mạng khi có khuyến nghị từ nhà sản xuất.

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

- Giám sát chặt chẽ lưu lượng các cổng kết nối trên router, firewall tại 1 cửa sổ riêng tại các NOC 3 miền. Khi có dấu hiệu bất thường, KTV khai thác lập tức thông báo cho cán bộ khai thác ATBM theo đúng quy trình (tham khảo chi tiết phụ lục 05).

- Thiết lập các ngưỡng cảnh báo tự động bằng âm thanh, hình ảnh trên các hệ thống giám sát (Cacti, Solarwind) cho các interface kết nối của RGW mạng VNNIC. Cơ sở để thiết lập ngưỡng là căn cứ thống kê lưu lượng max từng phân mạng trong 1 năm trở lại đây (tham khảo chi tiết phụ lục 05).

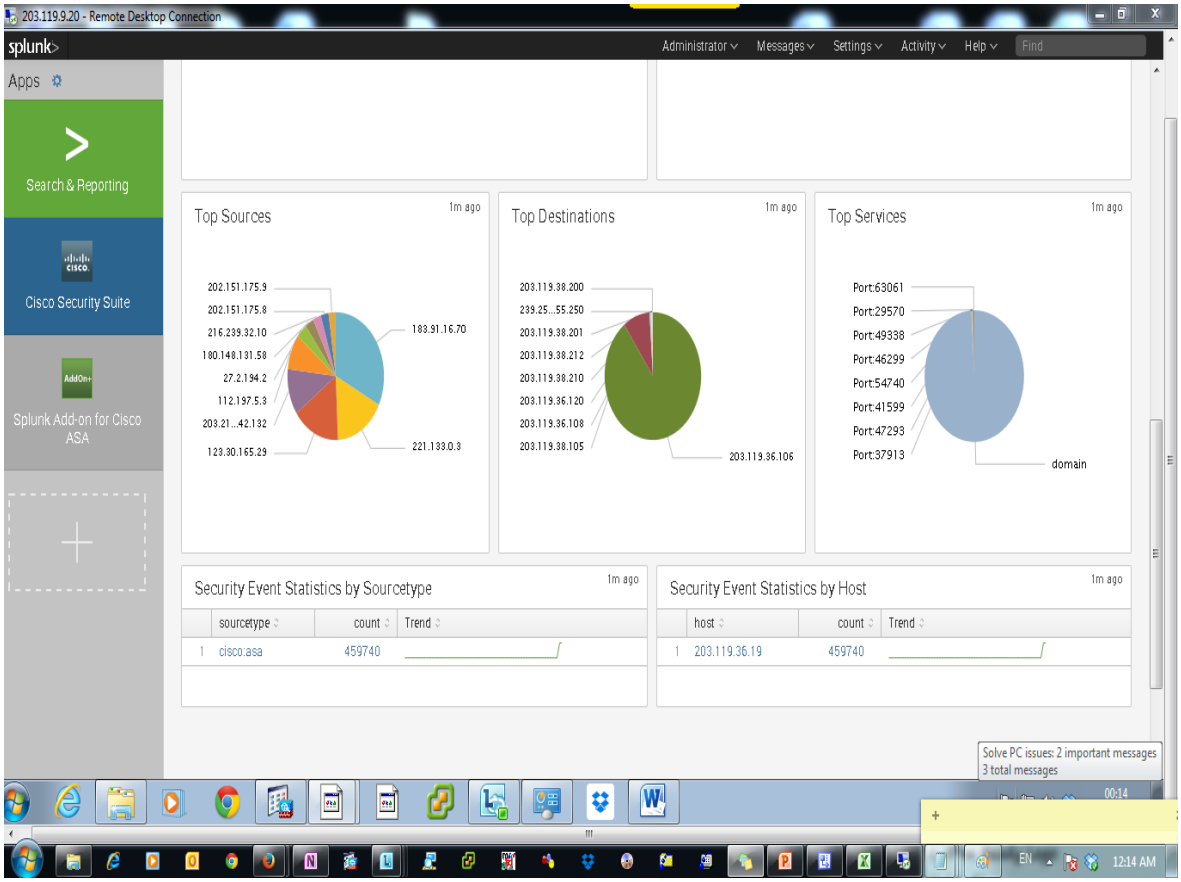
STT	RGW	Interface	Lưu lượng max	Ngưỡng cảnh báo
1	RGW-Net8-HL-01	Gi0/1	28.53 Mbps	100 Mbps
2	RGW-Net72-HL-01	Te0/0/0	94 Mbps	150 Mbps
3	RGW-Net64-AD-01	Gi0/0/0	8.14 Mbps	50 Mbps
4	RGW-Net36-TT-01	Gi0/0/0	39.55 Mbps	100 Mbps
5	RGW-Net117-TT-01	Te0/0/0	14 Mbps	100 Mbps

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

- Xem xét nghiên cứu, thiết lập thêm các công cụ phát hiện sớm tấn công DDoS (SourceFire….); các công cụ phát hiện tấn công dựa trên mẫu lưu lượng, hành vi của lưu lượng….

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

- Triển khai hệ thống phân tích lưu lượng cho tất cả các phân mạng VNNIC; đưa ra khai thác tại các NOC, SOC. Hiện tại, có một số giải pháp, công cụ phân tích lưu lượng tương đối hiệu quả, có thể triển khai ngay như splunk, netflow, sflow, firewall…. Khi xảy ra tấn công DDoS, cán bộ khai thác ATBM có thể nhanh chóng tìm ra các địa chỉ nguồn tấn công, địa chỉ đích tấn công, đặc điểm của lưu lượng tấn công thông qua các hệ thống PTLL này. Từ đó, nhanh chóng thực hiện các giải pháp xử lý, ngăn chặn các cuộc tấn công DDoS:



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

- Ngoài ra khi xảy ra tấn công DDoS có thể trao đổi trực tiếp với ISP, sử dụng công cụ PTLL của hệ thống VNIX để tìm đặc điểm của lưu lượng tấn công.

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

- Xây dựng trước các quy trình, kịch bản để xử lý nhanh chóng, kịp thời, hiệu quả các cuộc tấn công.
- Xây dựng hệ thống ngăn chặn DDoS cho mạng VNNIC sau khi đã phát hiện, xác định lưu lượng tấn công DDoS:

- GĐ 1: Triển khai giải pháp áp dụng kỹ thuật BGP Flowspec theo mô hình intra-domain. Trong đó, sử dụng công cụ ExaBGP đóng vai trò Controller; các RGW mạng VNNIC đóng vai trò client.
- GĐ 2: Tiếp tục nghiên cứu, thử nghiệm, đánh giá giải pháp của Arbor/Cisco.

e) Triển khai xử lý sau tấn công

- Phối hợp với các đơn vị chuyên trách như VNCERT, CSIRT, Cục An toàn thông tin…truy tìm đâu vết của cuộc tấn công DDoS. Đối với các trường hợp tấn công có chủ đích nếu tìm ra nguồn tấn công cần xử lý theo quy định pháp luật.
- Thực hiện phân tích log file trên các thiết bị liên quan để tìm nguồn tấn công.
- Thực hiện các báo cáo sự cố theo đúng QTQĐ.
- Nghiên cứu, đào tạo chuyên sâu cho cán bộ chuyên trách ATBM về kỹ thuật truy tìm dấu vết.

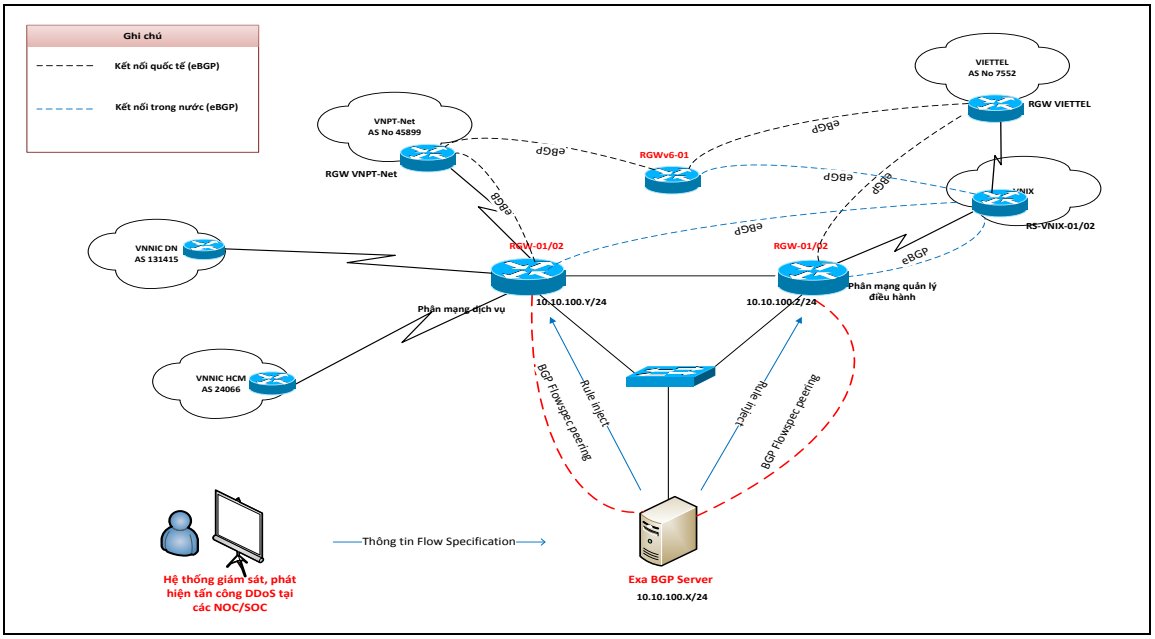
3.2.2. Mô hình đề xuất

Như đã phân tích bên trên, hiện tại ở Việt Nam chưa có ISP nào triển khai giải pháp BGP Flowspec, các ISP cũng không đồng ý cho phép tác động đến chính sách định tuyến trên router biên của mình. Do đó, nhóm đề tài đề xuất VNNIC tự chủ động triển khai áp dụng giải pháp BGP Flowspec theo mô hình intra-domain nhằm ngăn chặn tấn công DDoS cho hệ thống mạng VNNIC. Mặc dù với mô hình này, lưu lượng DDoS vẫn ảnh hưởng đến đường kết nối hướng lên (uplink) và các RGW nhưng phù hợp với hiện trạng mạng VNNIC. Mô hình đề xuất gồm 2 thành phần sau:

- 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.

Tại mỗi site (tương ứng với mỗi ASN) của mạng VNNIC sẽ triển khai 1 máy chủ ảo hóa cài đặt phần mềm công cụ Exa BGP. Máy chủ này cần phải triển khai phân tán tại từng site do:

- 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

Máy chủ này sau khi cài đặt xong công cụ sẽ được cấu hình địa chỉ và kết nối đến vlan Management của mạng VNNIC (Tại HN: 10.10.100.0/24). Lí do các máy chủ này sử dụng vlan Management:

- 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.

Các RGW tại các phân mạng VNNIC cũng được nâng cấp lên các dòng thiết bị hỗ trợ tính năng BGP Flowspec Client. Trên các RGW cũng cấu hình 1 giao diện có địa chỉ và kết nối đến vlan Management.

Exa BGP Server và từng RGW sẽ được cấu hình thiết lập mối quan hệ BGP flowspec peering. Khi sự cố tấn công DDoS xảy ra, cán bộ quản trị xác định đặc điểm của luồng lưu lượng tấn công (Flow Specification); truy cập vào Exa BGP Servers tạo script cập nhật Flowspec rule, inject đồng thời các Flowspec rule này đến tất cả RGW tại site đó. Sau khi nhận được các Flowspec rule này, các RGW sẽ loại bỏ các lưu lượng tấn công DDoS ngay tại lớp biên mạng, không gây ảnh hưởng đến hoạt động của hệ thống mạng VNNIC.

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.

Danh sách thiết bị triển khai:

STT	Tên thiết bị	Mô tả	Vai trò
1	Exa BGP Server HN	- Phần cứng: RAM: 4GB; CPU: 2 GHz, HDD: 50 Gbps. - Hệ điều hành: Linux (Ubuntu, Redhat….) - Phần mềm: ExaBGP 3.4.5.	Flowspec Server cho RGW-Net8-HL-01; RGW-Net72-HL-01
2	Exa BGP Server DN		Flowspec Server cho RGW-Net64-AD-01
3	Exa BGP Server HCM		Flowspec Server cho RGW-Net36-TT-01; RGW-Net117-TT-01
4	RGW-Net8-HL-01	ASR 1001-X	Flowspec Client
5	RGW-Net72-HL-01	ASR 1001-X	Flowspec Client
6	RGW-Net64-AD-01	ASR 1001-X	Flowspec Client
7	RGW-Net36-TT-01	ASR 1001-X	Flowspec Client
8	RGW-Net117-TT-01	ASR 1001-X	Flowspec Client

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.

TÀI LIỆU THAM KHẢO

[1] https://viettelidc.com.vn/bao-cao-tan-cong-tu-choi-dich-vu-ddos-quy-2-2017-tren-the-gioi.html

[2] https://lp.incapsula.com/rs/804-TEY-921/images/2015-16%20DDoS%20Threat%20Landscape%20Report.pdf

[3] https://www.verisign.com/assets/infographic-ddos-trends-Q22017.pdf

[4] https://telecombigdata.blogspot.com/2015/01/ddos-mitigation-using-flowspec-with.html

[5] https://labs.ripe.net/Members/thomas_mangin/content-exabgp-new-tool-interact-bgp

[6] https://www.netcraftsmen.com/bgp-flowspec-step-forward-ddos-mitigation/

[7] RFC 5575 – Dissemination of Flow Specification Rules

[8] https://supportforums.cisco.com/t5/service-providers-documents/asr9000-xr-understanding-bgp-flowspec-bgp-fs/ta-p/3139916

[9] https://supportforums.cisco.com/t5/xr-os-and-platforms/bgp-flowspec-server/td-p/3080075

[10] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/bgp_flowspec_route-reflector_support.html

[11] https://www.arbornetworks.com/blog/insight/2017-market-technology-leader-global-ddos-mitigation-market/

[12] https://www.chrisk.de/blog/2016/05/exabgp-4-0-getting-started

[13] https://r2079.wordpress.com/2016/11/22/what-is-exa-bgp/

[14] Comparing DDoS Mitigation Techniques - C.J.T.M. Schutijser
- University of Twente

[15] Cisco ASR 9000 vDDoS Protection Solution –White paper- Cisco

[16] Playing with off-Ramp / On-Ramp - Ferran Orsola – Arbor

[17] BGP Flowspec – Alcatel

[18] BGP Flowspec(RFC5575) Case study and Discussion - Shishio Tsuchiya – Cisco

[19] Implementing BGP Flowspec – Cisco System

[20] Flowspec compability between vendor lab – Ripe

[21] Brocade Flow Optimizer Use Cases – Broadcade

[22] https://www.corero.com/resources/glossary.html

[23] http://network-insight.net/2015/12/bgp-flowspec-ddos-mitigation/

PHỤ LỤC

I. PHỤ LỤC 01: Hướng dẫn cài đặt, cấu hình công cụ ExaBGP

3.3. Bước 1: Tải và cài đặt công cụ ExaBGP

• 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

Kiểm tra lại quá trình cài đặt:

/usr/bin/exabgp --h

3.4. Bước 2: Sửa nội dung của file config trong exaBGP như sau

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;

process service-dynamic {

run /data/Indu/exabgp-3.4.5/etc/exabgp/processes/dynamic-1.sh; ## the script chứa các flow mà ta muốn quảng bá (announce) hoặc loại bỏ.

}

}

3.5. Bước 3: Tạo file script có nội dung như sau:

#!/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
```

3.6. Bước 4: Chạy ExaBGP với file config như trên:

```
/data/Indu/exabgp-3.4.5/sbin/exabgp  /data/Indu/exabgp-
3.4.5/etc/exabgp/flowspec_conf_dynamic.txt
```

3.7. Bước 5: Khi muốn inject 1 flowspec rule mới ta thực hiện như sau:

a) Thêm flowspec rule mới vào file script dynamic.sh:

```
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"
```

b) Tìm forked process-id của dynamic.sh và kill nó:

```
[root@BR-140 configs]# ps -aef | grep -i bgp | grep -v grep

nobody 19576 9574 0 10:53 pts/38 00:00:01 /usr/bin/python2.6 /data/Indu/exabgp-
3.4.5/lib/exabgp/application/bgp.py --folder /data/Indu/exabgp-3.4.5/etc/exabgp
/data/Indu/exabgp-3.4.5/etc/exabgp/flowspec_conf_dynamic.txt

nobody 30642 19576 0 10:55 pts/38 00:00:00 /bin/sh /data/Indu/exabgp-
3.4.5/etc/exabgp/processes/dynamic.sh

& run kill -9   ## kill -9 30642
```

c) Trên router, thực hiện kiểm tra xem flowspec rule đã được thêm vào chưa:

```
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

4. PHỤ LỤC 02: Hướng dẫn cấu hình trên router

4.1. Cấu hình trên RGW ISP

```
Interface GigabitEthernet0/0/0
description PeerRGW-VNNIC
 ip address 172.16.240.1 255.255.255.0
 ipv6 enable
!
Interface GigabitEthernet0/0/1
description To-PC01
 ip address 172.16.239.1 255.255.255.0
 ipv6 enable
!
router bgp 12345
 no bgp log-neighbor-changes
 neighbor 172.16.240.2 remote-as 12346
 neighbor 172.16.240.2 description peerVNNIC
address-family ipv4
  network 172.16.239.0 mask 255.255.255.0
  neighbor 172.16.240.2 active
```

4.2. Cấu hình trên RGW

```
Interface GigabitEthernet0/0/0
description PeerRGW-ISP
 ip address 172.16.240.2 255.255.255.0
 ipv6 enable
!
Interface GigabitEthernet0/0/1
description To-PC02
 ip address 172.16.241.1 255.255.255.0
 ipv6 enable
!
```

```
Interface GigabitEthernet0/0/2
description To-ExaBGP
 ip address 203.119.72.159 255.255.255.0
 ipv6 enable
!
router bgp 12346
 no bgp log-neighbor-changes
 neighbor 172.16.240.1 remote-as 12345
 neighbor 172.16.240.1 description peerISP
address-family ipv4
  network 172.16.241.0 mask 255.255.255.0
  neighbor 172.16.240.1 active
```

4.3. Cấu hình RGW VNNIC BGP flowspec peering với ExaBGP Server

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