TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

Đề tài:

XÂY DỰNG HỆ THỐNG PHÁT HIỆN VÀ GIẢM THIỂU TẤN CÔNG DDOS DỰA TRÊN CÔNG NGHỆ MẠNG ĐIỀU KHIỂN BẰNG PHẦN MỀM

Sinh viên thực hiện: VƯƠNG BÁ NAM

Lớp ĐT-TT06 – K58

NGUYỄN MẠNH QUYỀN

Lớp ĐT-TT05 – K58

Giảng viên hướng dẫn: PGS.TS NGUYỄN HỮU THANH

Hà Nội, 06-2018

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

Đề tài:

XÂY DỰNG HỆ THỐNG PHÁT HIỆN VÀ GIẢM THIỂU TẤN CÔNG DDOS DỰA TRÊN CÔNG NGHỆ MẠNG ĐIỀU KHIỂN BẰNG PHẦN MỀM

Sinh viên thực hiện: VƯƠNG BÁ NAM

Lớp ĐT-TT06 – K58

NGUYỄN MẠNH QUYỀN

Lớp ĐT-TT05 – K58

Giảng viên hướng dẫn: PGS.TS NGUYỄN HỮU THANH

Cán bộ phản biện :

Hà Nội, 06-2018

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho giảng viên hướng dẫn)

Giảng viên đánh giá: PGS. TS. Nguyễn Hữu Thanh

Họ và tên sinh viên: Nguyễn Mạnh Quyền MSSV: 20133190

Tên đồ án: Xây dựng hệ thống phát hiện và giảm thiểu tấn công DDoS dựa trên công nghệ mạng điều khiển bằng phần mềm.

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5

9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

3. Nhận xét thêm của Thầy/Cô (*giảng viên hướng dẫn nhận xét về thái độ và tinh thần làm việc của sinh viên****)***

.....

.....

.....

.....

.....

.....

Ngày: / /2018

Người nhận xét

(Ký và ghi rõ họ tên)

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho cán bộ phản biện)

Giảng viên đánh giá:.....

Họ và tên sinh viên: Nguyễn Mạnh Quyền MSSV: 20133190

Tên đồ án: Xây dựng hệ thống phát hiện và giảm thiểu tấn công DDoS dựa trên công nghệ mạng điều khiển bằng phần mềm.

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5

9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

3. Nhận xét thêm của Thầy/Cô

.....

.....

.....

.....

.....

.....

Ngày: / /2018

Người nhận xét

(Ký và ghi rõ họ tên)

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho giảng viên hướng dẫn)

Giảng viên đánh giá: PGS. TS. Nguyễn Hữu Thanh

Họ và tên sinh viên: Vương Bá Nam MSSV: 20132719

Tên đồ án: Xây dựng hệ thống phát hiện và giảm thiểu tấn công DDoS dựa trên công nghệ mạng điều khiển bằng phần mềm.

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5

9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

3. Nhận xét thêm của Thầy/Cô (*giảng viên hướng dẫn nhận xét về thái độ và tinh thần làm việc của sinh viên****)***

.....

.....

.....

.....

.....

.....

Ngày: / /2018

Người nhận xét

(Ký và ghi rõ họ tên)

Đánh giá quyển đồ án tốt nghiệp

(Dùng cho cán bộ phản biện)

Giảng viên đánh giá:.....

Họ và tên sinh viên: Vương Bá Nam MSSV: 20132719

Tên đồ án: Xây dựng hệ thống phát hiện và giảm thiểu tấn công DDoS dựa trên công nghệ mạng điều khiển bằng phần mềm.

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5
6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5

9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				
Điểm tổng		**/50**				
Điểm tổng quy đổi về thang 10						

3. Nhận xét thêm của Thầy/Cô

.....

.....

.....

.....

.....

.....

Ngày: / /2018

Người nhận xét

(Ký và ghi rõ họ tên)

LỜI NÓI ĐẦU

Trong thế kỉ 21, hệ thống mạng Internet ở nước ta nói riêng và thề giới nói chung và đóng một vai trò cực kỳ quan trọng trong cuộc sống cũng như trong công việc. Sự phát triển nhanh chóng đó cũng kéo theo rất nhiều hệ lụy gây thiệt hại lớn về kinh tế như các lỗ hổng bảo mật dễ bị tin tặc khai thác dẫn đến mất an toàn thông tin. Một trong những loại hình tấn công đơn giản mà hiệu quả là tấn công từ chối dịch vụ phân tán (DDoS). Loại hình tấn công này đã xuất hiệt từ khá lâu nhưng vẫn được các tin tặc sử dụng để tấn công vào các máy chủ cung cấp dịch vụ của các doanh nghiệp do hiện nay vẫn chưa có cách nào có thể phát hiện và phòng chống hiệu quả.

Với sự ra đời và phát triển của công nghệ mạng mạng định nghĩa bằng phần mềm (SDN) với ưu điểm là dễ quản lý và giám sát hệ thống mạng. Từ đó, việc áp dụng các giải pháp giảm thiểu hậu quả của tấn công DDoS cũng dễ dàng hơn.

Dưới sự hướng dẫn của thầy **PGS.TS Nguyễn Hữu Thanh** nhóm nghiên cứu chúng em quyết định chọn hướng nghiên cứu và làm việc về "**Xây dựng hệ thống phát hiện và giảm thiểu tấn công DDoS dựa trên công nghệ mạng điều khiển bằng phần mềm".**

Trong quá trình thực hiện đề tài do sự hạn chế về thời gian và kiến thức nên không thể tránh khỏi những thiếu sót. Em rất mong thầy cô tham gia đóng góp phê bình để đồ án của chúng em được hoàn thiện hơn.

Em xin chân thành cảm ơn **PGS.TS Nguyễn Hữu Thanh**, người đã trực tiếp hướng dẫn chúng em thực hiện đồ án này, đã dìu dắt, giúp đỡ và tận tình chỉ bảo chúng em trong suốt thời gian thực hiện đồ án.

TÓM TẮT ĐỒ ÁN

Sự phát triển và mở rộng nhanh chóng của mạng Internet với hàng tỷ thiết bị tham gia đã tạo điều kiện cho các cuộc tấn công DDoS ngày càng nhiều và quy mô cũng lớn hơn. Tấn công DDoS có thể xảy ra một cách nhanh chóng và bất ngờ khiến hệ thống của chúng ta có thể ngừng bất cứ lúc nào, vì vậy chúng ta cần một cách thức phát hiện và giảm thiểu tấn công đủ nhanh, hiệu quả và có thể kịp thời ngăn chặn. Trong đồ án này sẽ trình bày một phương pháp phát hiện và giảm thiểu tấn công DDoS dựa trên nền tảng SDN bằng việc xây dựng thêm khối thu thập thông số mạng để đưa lên thuật toán đặt trên khối điều khiển, khối điều khiển đưa ra quyết định và đưa ra chính sách giảm thiểu hoặc ngăn chặn tấn công xảy ra. Đồng thời xây dựng một testbed hoàn chỉnh cho việc phát lưu lượng mô phỏng tấn công DDoS, đo đạc đánh giá khả năng đáp ứng của hệ thống phát hiện và giảm thiểu tấn công như thực tế xảy ra. Những kết quả thu được cho thấy tốc độ phát hiện nhanh, biện pháp ngăn chặn tấn công là hiệu quả và kịp thời.

ABSTRACT

The rapid development and expansion of the Internet with billions of technology devices, it provides more opportunites for the attackers to perform DDos attacks on a global scale. Nowadays, DDos attacks can happen quickly and easily to shut down our system at any moment, so we need a solution to detect and minimize attacks quickly enough, effectively and in a timely manner. This project will present a method for detecting and minimizing Ddos attacks based on the SDN platform , by a way we add a network analyzer block to put the algorithms on the controller block then the controller decide and implement policies to minimize or prevent attacks. Moreover, we build a complete testbed for the Ddos attack simulation traffic, measuring the response capability of the detection system and minimizing the attack as it actually does. The results show that the speed of detection is fast, effective measures to prevent attacks are effective and timely.

MỤC LỤC

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH ẢNH

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Ý nghĩa
DDoS(Distributed Denial of Service)	Tấn công từ chối dịch vụ phân tán
Attacker	Kẻ tấn công DDoS
Botnet	Máy tính bị điều khiển tham gia tấn công
Control Plane	Mặt phẳng điều khiển
Forwarding Plane	Mặt phẳng chuyển tiếp
IAT(Inter-arrival time)	Tỷ lệ thời gian đến giữa hai packet nằm trong khoảng 0-0,2 ms
PpF(Packet per flow)	Tỷ lệ luồng có 1 packet
SDN (Software defined Networking)	Mạng định nghĩa bằng phần mềm
WanEm (Wan Emulator)	Phần mềm giả lập mạng Wan
Bonesi (Botnet Simulator)	Phần mềm giả lập mạng botnet
Testbed	Hệ thống thử nghiệm

PHẦN MỞ ĐẦU

Sự phát triển ngày càng mạnh của Internet luôn đi kèm với những yêu cầu khắt khe hơn trong các vấn đề về bảo mật, hiệu suất và năng lượng của cơ sở hạ tầng mạng. Trong lĩnh vực an ninh mạng, Internet đang bị đe dọa bởi rất nhiều loại tấn công mạng khác nhau. Trong số này, tấn công từ chối dịch vụ (DDoS) là một trong những loại hình tấn công phổ biến nhất và là một vấn đề kéo dài suốt hàng thập kỷ qua. Theo báo cáo của Verisign [2], hoạt động tấn công DDoS đã tăng trong quý 3-2017 đã đạt đến mức rất lớn và trải rộng hơn 89 quốc gia trên thế giới. Verisign cũng quan sát tấn công đỉnh cao là 34 gigabit / giây (Gbps) và 30 triệu gói tin / giây (Mpps) đối với loại hình tấn công TCP (Transmission Control Protocol) trong Quý 3 năm 2017.

Khó khăn trong việc phát hiện tấn công DDoS nằm ở sự giống nhau giữa lưu lượng truy cập bình thường và tấn công. Do đó, rất khó phân biệt được đâu là cuộc tấn công lưu DDoS và đâu là lượng truy cập thông thường. Bên cạnh đó, theo các báo cáo của Verisign, số lượng các gói dữ liệu trong suốt cuộc tấn công DDoS là rất lớn và quá trình giám sát và phân tích sẽ hết sức khó khăn. Do đó cần thiết phải có cơ chế phát hiện tấn công DDoS dựa trên lưu lượng có thể được áp dụng linh hoạt cho mạng lưới theo dõi toàn cầu. Trong đồ án này, chúng em giới thiệu giải pháp phát hiện tấn công DDoS dựa trên công nghệ SDN. Chúng em tập trung về việc tối ưu hóa các cách tiếp cận phân loại DDoS và làm rõ được các vấn đề sau:

Thứ nhất, chúng em đề xuất kiến trúc phát hiện tấn công và triển khai thuật toán phát hiện tấn công. Các testbed của kiến trúc này được triển khai bởi sử dụng hệ thống switch ảo là Open vSwitch và bộ tạo lưu lượng truy cập theo bộ dữ liệu CAIDA.

Thứ hai, chúng em phân tích lưu lượng trong mạng để đưa ra trạng thái của mạng là bị tấn công hay bình thường. Từ đó đưa ra các giải pháp phù hợp để giảm thiểu hậu quả của tấn công DDoS.

Cấu trúc đồ án:

- Chương 1: Giới thiệu các khái niệm cơ bản về tấn công DDoS, phân loại và thống kê DDoS Attack trên thế giới trong thời gian gần đây
- Chương 2: Giới thiệu công nghệ mạng SDN bao gồm cấu trúc, cơ chế hoạt động, ưu điểm và nhược điểm của mạng SDN
- Chương 3: Đưa ra kiến trúc mạng, thuật toán phát hiện và giảm thiểu tấn công DDoS. Các thành phần trong kiến trúc mạng, cách xây dựng thuật toán dựa trên phân tích dữ liệu và các biện pháp giảm thiểu tấn công phù hợp.
- Chương 4: Tập trung phân tích một cuộc tấn công DDoS ở đây là CAIDA 2007 để đưa ra các đặc tính của một cuộc tấn công DDoS từ đó đưa ra cách thức mô phỏng một cuộc tấn công DDoS xảy ra trong thực tế .
- Chương 5: Xây dựng mô hình thử nghiệm gồm hệ thống mạng doanh nghiệp, bộ gateway sử dụng công nghệ SDN, bộ phát lưu lượng rồi đưa ra kết quả đạt được khi áp dụng giải pháp đã nói ở chương 3 và hướng phát triển .

CHƯƠNG 1. TỔNG QUAN VỀ TẤN CÔNG DDOS

Tấn công từ chối dịch vụ (DDoS) là một trong những cách thức tấn công vào hệ thống mạng máy tính của các doanh nghiệp rất hiệu quả. Nó gây ra thiệt hại rất lớn đối với các doanh nghiệp bị tấn công. Vì thế, chương này chúng em xin trình bày một số khái niệm cơ bản, phân loại và nguyên tắc hoạt động, cách thức tấn công của loại tấn công nguy hiểm này. Thống kê số liệu trong quý 3/2017 chúng ta có thể thấy được sự lớn mạnh của loại hình tấn công này trong thời gian qua.

1.1 DDoS là gì?

1.1.1 Khái niệm tấn công DDoS

Một cuộc tấn công DoS (Denial of Service) là một cuộc tấn công vào một hay nhiều máy chủ nạn nhân nhằm làm cạn kiệt băng thông hay tài nguyên của nạn nhân làm cho máy chủ nạn nhân từ chối một phần hoặc toàn bộ các yêu cầu hợp pháp của người dùng. Nguồn của một cuộc tấn công thường phát sinh từ một nguồn duy nhất[1].

Tấn công từ chối dịch vụ phân tán (DDoS -Distributed Denial of Service) là một dạng cải tiến của DoS. Thay vì sử dụng một nguồn thì attacker sử dụng rất nhiều nguồn khác nhau để tấn công. Kẻ tấn công có thể sử dụng các công cụ (tool) để giả mạo nguồn hoặc sử dụng các máy tính trên mạng Internet đã bị kẻ tấn công chiếm quyền diều khiển. Điều này làm cho các nhà quản trị mạng khó có thể tìm được nguồn tấn công.

1.1.2 Các bước để thực hiện một cuộc tấn công DDoS

- *Khái niệm botnet*

Botnet là các mạng máy tính được tạo lập từ các máy tính được kết nối Internet mà ke tấn công có thể điều khiển từ xa. Các máy tính trong mạng botnet là máy đã bị nhiễm malware và tiếp tục lây lan sang các máy tính chưa bị nhiễm trong cùng một mạng. Một mạng botnet có thể có tới hàng trăm ngàn, thậm chí là hàng triệu máy tính.

Sau khi chiếm được quyền điều khiển thì kẻ tấn công có thể sử dụng các botnet vào nhiều mục đích khác nhau.

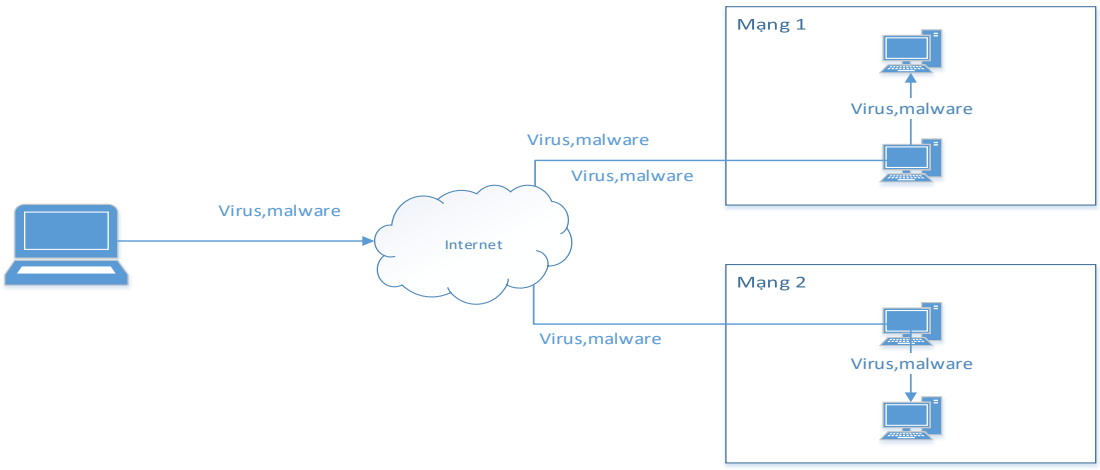
- Thực hiện các cuộc tấn công DDoS
- Đào bitcoin
- Phát tán malware
- Spam quảng cáo

➢ *Các bước thực hiện tấn công DDoS*

Gồm 2 giai đoạn chính:

- **Giai đoạn thiết lập mạng botnet**

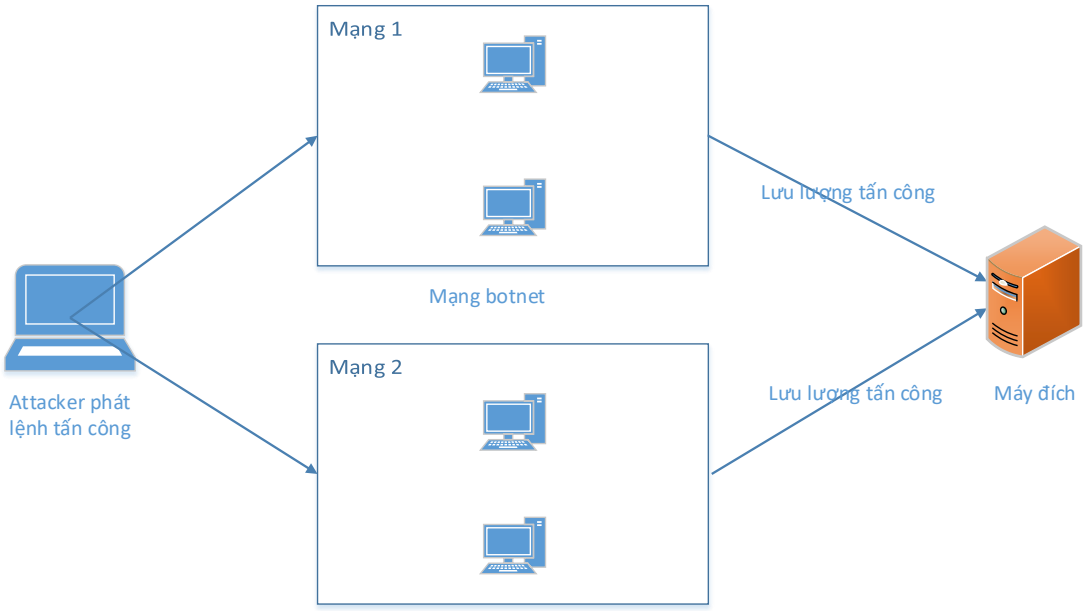
Kẻ tấn công xác định các lỗ hổng trong một hay nhiều mạng để cài đặt các chương trình phần mềm độc hại để có thể điều khiển chúng từ xa. Chúng cũng có thể phát tán virus, malware, mã độc… trên mạng Internet thông qua các trang web có nội dung không lành mạnh hay các phần mềm crack được cài đặt. Sau khi một hoặc nhiều máy trong mạng bị nhiễm virus hay malware thì chúng sẽ tiếp tục phát tán đến tất cả các máy tính trong mạng nội bộ.



Hình 1.1: Attacker phát tán malware trên mạng Internet để xây dựng mạng botnet

- **Phát lệnh tấn công**

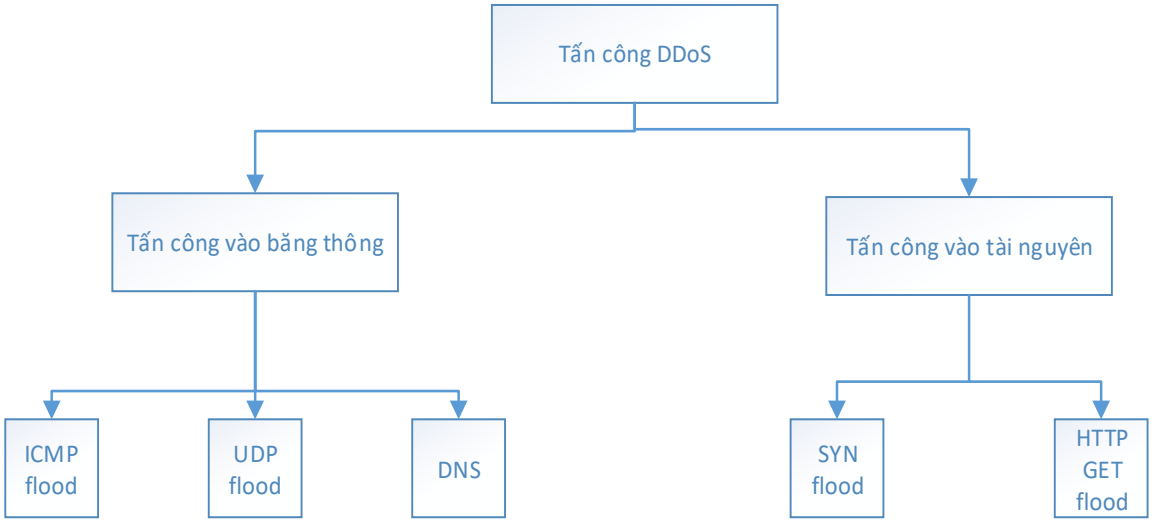
Attacker điều khiển các máy tính trong botnet cùng một lúc gửi rất nhiều gói tin đến máy nạn nhân làm cho nạn nhân không còn khả năng phục vụ những người dùng hợp pháp. Tùy thuộc vào mục đích tấn công của kẻ tấn công mà các máy trong mạng botnet sẽ gửi các gói tin với giao thức khác nhau.



Hình 1.2. Attacker phát lệnh tấn công

1.2 Phân loại tấn công DDoS

Dựa trên mục đích tấn công của kẻ tấn công mà ta có thể chia làm 2 loại tấn công chính[1].



Hình 1.3: Phân loại tấn công DDoS

1.2.1 Tấn công vào băng thông mạng

- *Tấn công lũ lụt*

Trong phương pháp này băng thông mạng của máy chủ nạn nhân bị chiếm hết bởi lưu lượng tấn công từ mạng botnet. Các máy tính trong mạng botnet bị điều khiển bởi attacker thực hiện gửi liên tục rất nhiều bản tin có dung lượng lớn đến máy chủ nạn nhân làm tắc nghẽn mạng của nạn nhân dẫn đến các người dùng hợp pháp không thể sử dụng được dịch vụ của nạn nhân.

Có 2 loại giao thức chính trong phương pháp này:

Tấn công sử dụng ICMP Flood: Giao thức ICMP được thiết kế nhằm mục đích kiểm tra, quản lý kết nối mạng. Nhưng trong trường hợp này, một số lượng cực lớn máy tính trong mạng botnet gửi một loạt các bản tin ICMP Echo Request đến máy chủ nạn nhân buộc nạn nhân trả lời bằng các bản tin ICMP Echo Reply làm cho băng thông

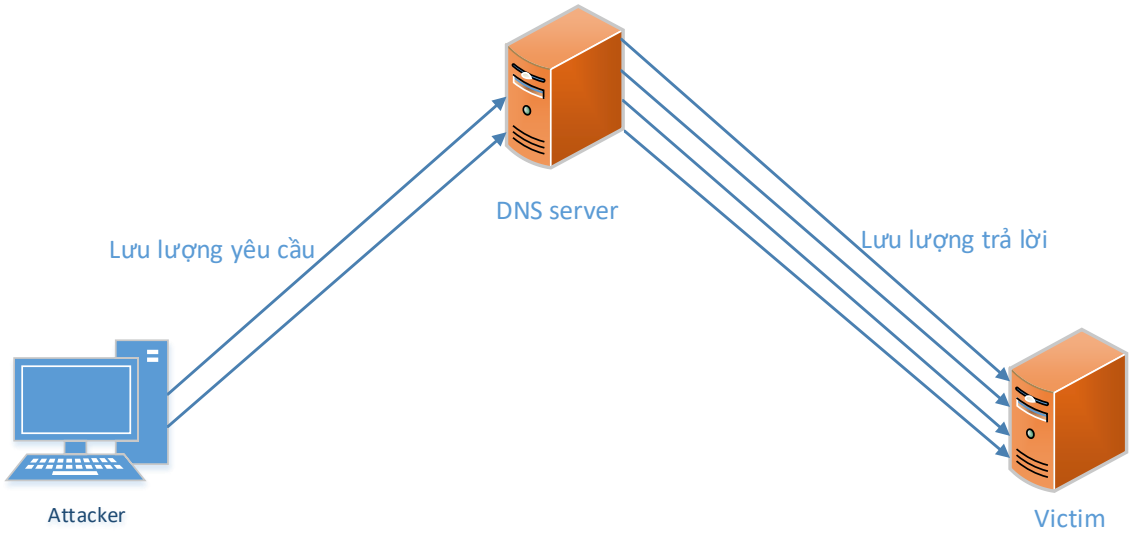
mạng của nạn nhân bị tắc nghẽn hoặc giảm đáng kể khiến cho dịch vụ mà nạn nhân cung cấp không đảm bảo chất lượng.

Tấn công sử dụng UDP Flood: Giao thức UDP là loai giao thức không hướng kết nối nên một máy client có thể gửi liên tục các bản tin UDP đến máy chủ và máy client này sẽ chiếm 1 lượng băng thông của máy chủ. Lợi dụng điều này kẻ tấn công sử dụng mạng botnet gửi liên tục các bản tin UDP làm cho băng thông trong mạng của nạn nhân bị bão hòa dẫn đến người dùng hợp pháp không thể sử dụng được dịch vụ của nạn nhân.

- *Tấn công khuếch đại*

Một số giao thức có bản tin trả lời lớn hơn rất nhiều so với bản tin request. Sử dụng sơ hở này kẻ tấn công có thể tạo ra lưu lượng tấn công cực kỳ lớn mà lưu lượng thực sự mà kẻ tấn công tạo ra không lớn.

Tấn công khuếch đại DNS: Attacker gửi các bản tin DNS request đến các máy chủ DNS public trên Internet nhưng các bản tin này đã được kẻ tấn công giả mạo địa chỉ nguồn là địa chỉ của máy nạn nhân. Khi máy chủ DNS trả lời trở lại máy nạn nhận thì lưu lượng trả về rất lớn (do bản tin trả lời có lưu lượng lớn gấp nhiều lần so với bản tin yêu cầu) khiến cho băng thông của nạn nhân bị chiếm hết. Trong kiểu tấn công này, kẻ tấn công không cần sử dụng mạng botnet lớn vẫn có thể tạo ra cuộc tấn công có lưu lượng lớn.



Hình 1.4 Cách thức tấn công khuếch đại DNS

1.2.2 Tấn công vào tài nguyên

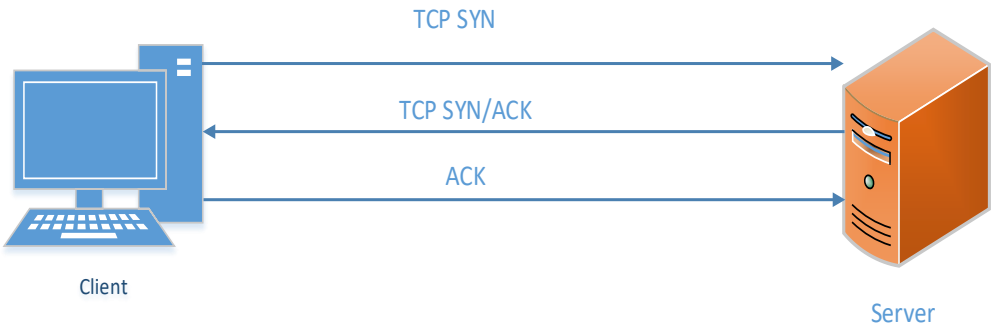
- *Tấn công TCP SYN flood*

Ở phương pháp này kẻ tấn công lợi dụng lỗ hổng trong quá trình bắt tay 3 bước của giao thức TCP để thực hiện tấn công. Quá trình bắt tay 3 bước được thực hiện như sau.

Bước 1: Client gửi bản tin TCP SYN đến server để thiết lập kết nối

Bước 2: Server phản hồi lại bằng bản tin TCP SYN/ACK để báo nhận cho gói tin SYN và chờ bản tin ACK từ client.

Bước 3: Client trả lời bằng bản tin ACK để hoàn thành việc thiết lập kết nối



Hình 1.5 Quá trình bắt tay 3 bước

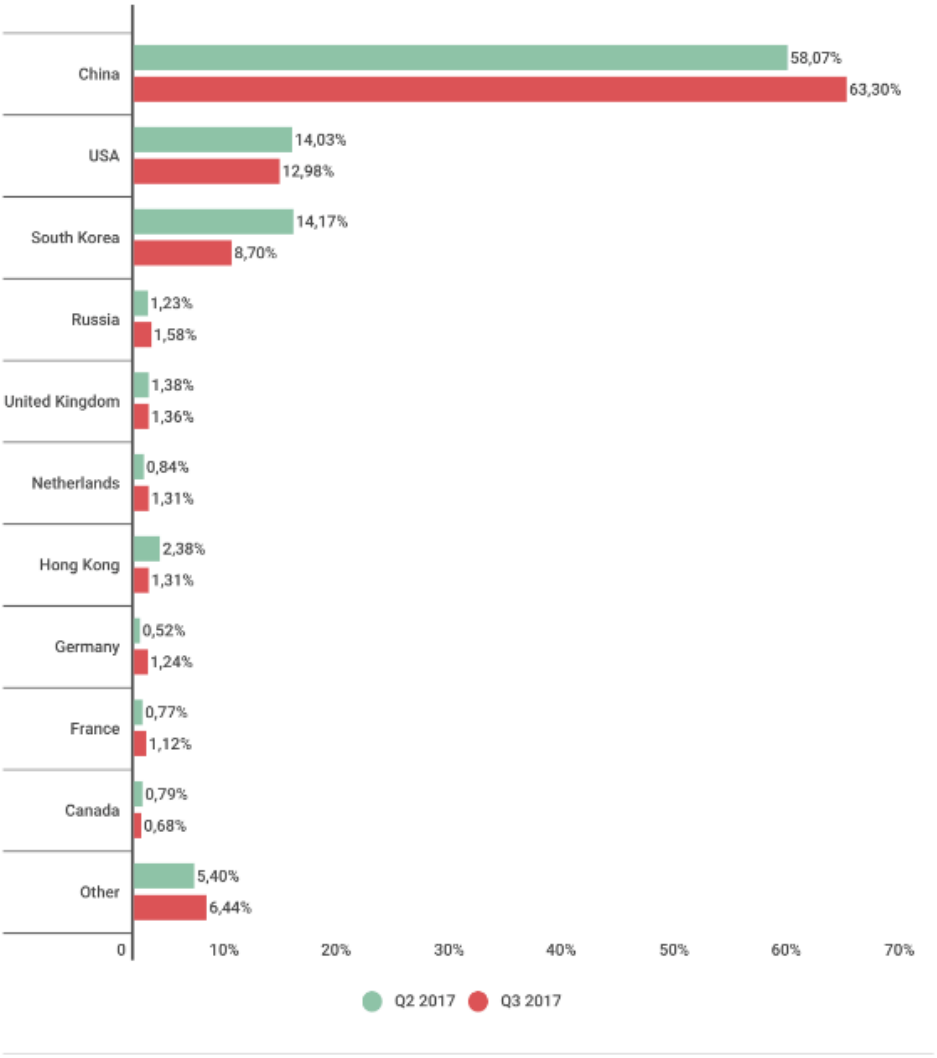
Tại bước thứ 2, sau khi server nhận được bản tin TCP SYN từ client thì server sẽ phản hồi bằng bản tin TCP SYN/ACK và sử dụng một phần tài nguyên để lưu trữ kết nối đó. Lợi dụng lỗ hổng này kẻ tấn công gửi rất nhiều bản tin TCP SYN nhằm chiếm hết tài nguyên của máy chủ nạn nhân khiên cho người dùng hợp pháp không thể truy cập được.

1.3. Thống kê các cuộc tấn công DDoS trên toàn cầu

Tấn công từ chối dịch vụ phân tán (DDoS) ngày càng gia tăng mạnh mẽ. Theo thống kê của Viettel IDC trong quý 3/2017 [2] thì số lượng các vụ tấn công DDoS ở Trung Quốc, Mỹ Hàn Quốc và Nga tăng lên. Số vụ tấn công tăng đột ngột (450 vụ mỗi ngày) và mức độ lên đến 15,8 triệu gói tin/giây đã được xác định thuộc "khu vực của Úc".

- *Các khu vực bị tấn công*

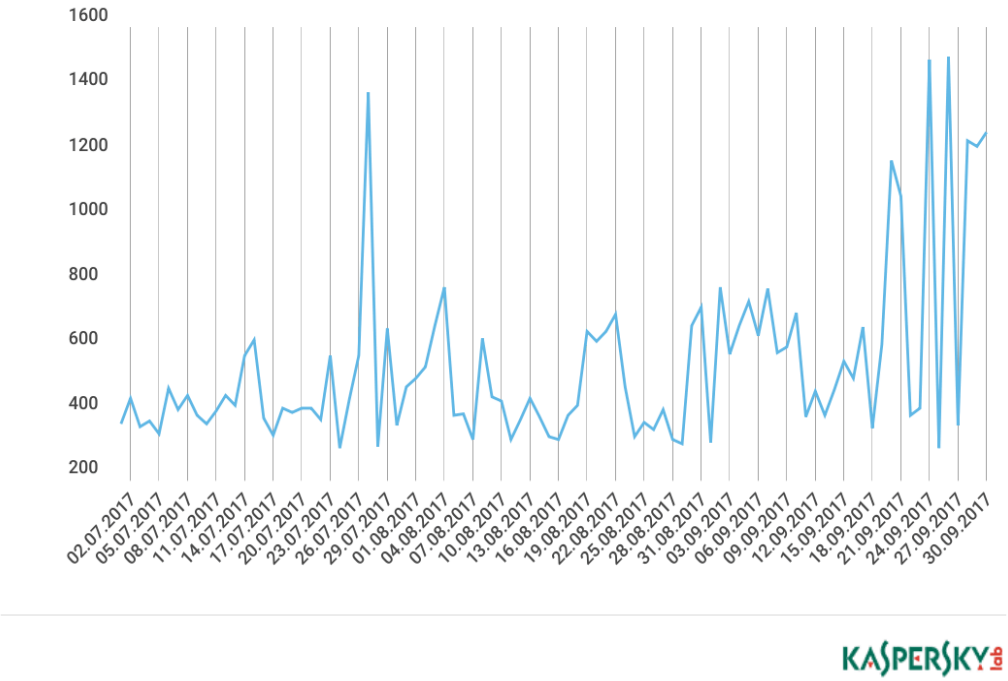
Số lượng các cuộc tấn công nhằm vào Trung Quốc tăng lên từ 58,07% trong quý 2 lên 63,30% trong quý 3. Theo sau là Mỹ (12,98%) và Hàn Quốc (8,70%)



Hình 1.6: Thống kê các khu vực bị tấn công

- *Tần suất các cuộc tấn công DDoS*

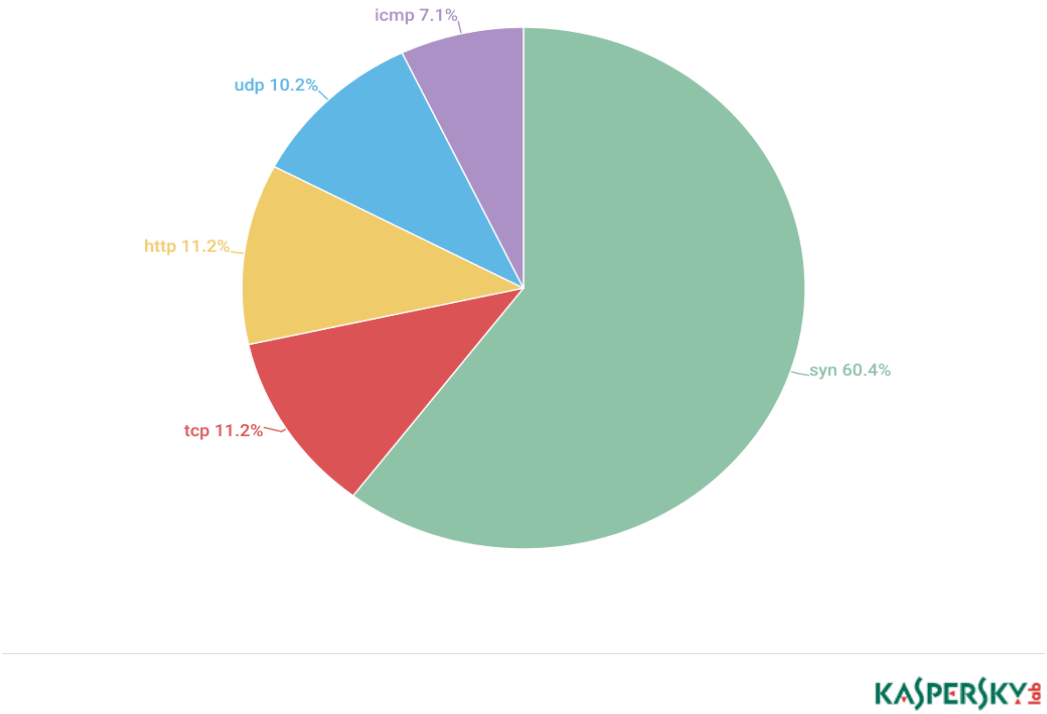
Số lượng các cuộc tấn công mỗi ngày dao động từ 296 (24 tháng 7) đến 1508 (26 tháng 9) trong quý 3 năm 2017. Cao nhất là vào ngày 27 tháng 7 (1.399) và 24 tháng 9 (1.497). Thấp nhất vào ngày 28 tháng 7 (300), 31 Tháng Năm (240), và ngày 25 tháng 9 (297).



Hình 1.7: Tần suất các cuộc tấn công

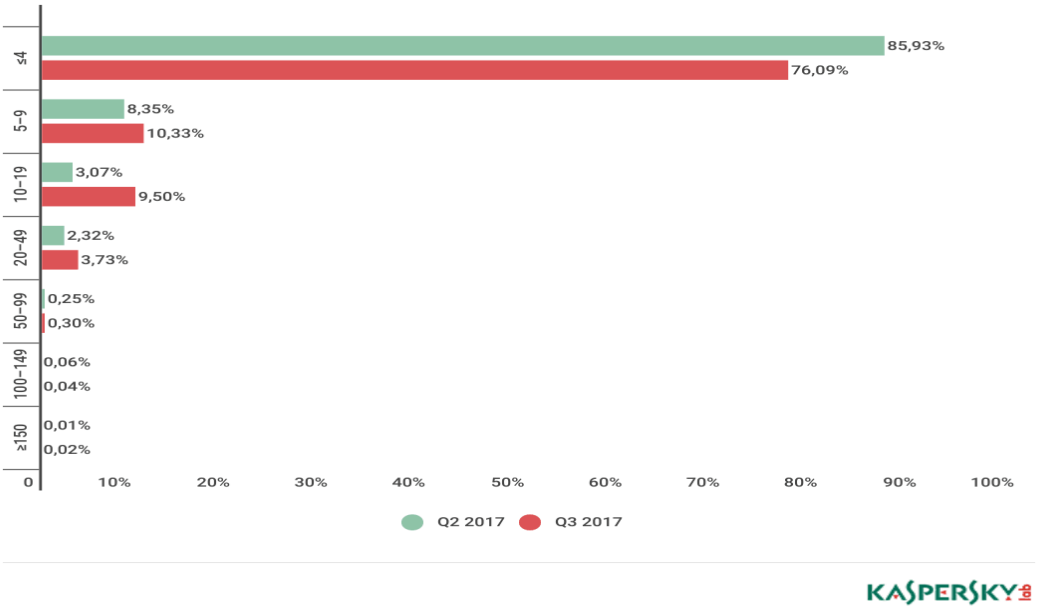
- *Hình thức và thời gian tấn công*

Các cuộc tấn công TCP SYN Flood tiếp tục tăng từ từ 53,26% lên 60,43% vào quý 3 năm 2017.



Hình 1.8: Hình thức tấn công DDoS

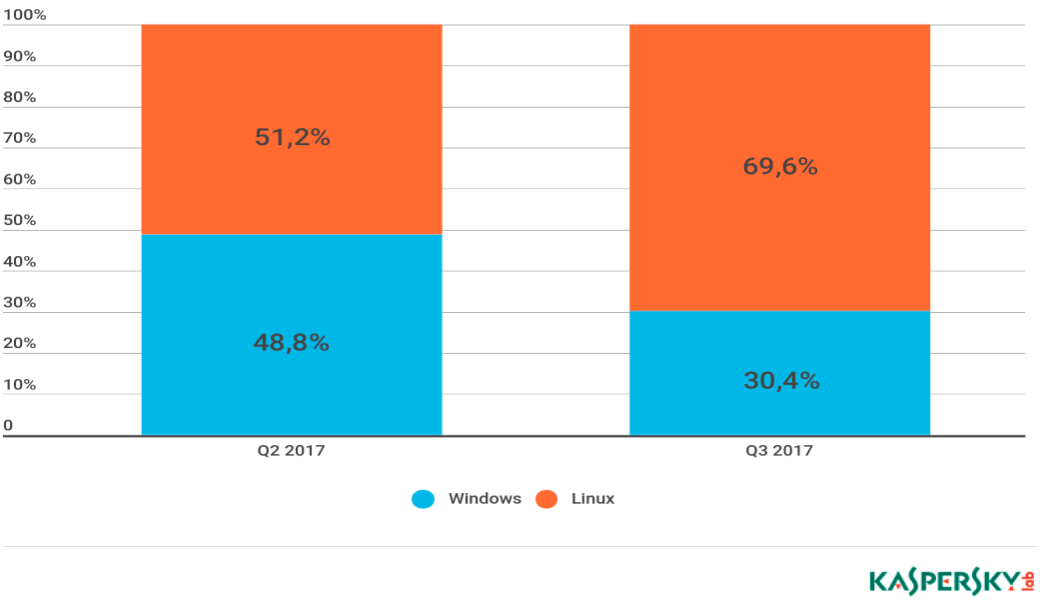
Thời gian của các cuộc tấn công dài hạn hầu như không thay đổi trong quý 3 (0,02 % trong quý 2 và 0,01% trong quý 3). Trong khi đó các cuộc tấn công có thời lượng nhỏ hơn 4 tiếng giảm từ 85,93% trong quý 2 xuống 76,09% trong quý 3



Hình 1.9: Thời gian các cuộc tấn công

- *Hệ thống botnet*

Trong quý 3 các botnet chạy trên hệ điều hành Linux tiếp tục tăng



Hình 1.10: Hệ thống botnet

1.4 Kết luận

Ở chương này, chúng ta đã có cái nhìn khái quát nhất về tấn công từ chối dịch vụ phân tán (DDoS). Tình hình thống kê các cuộc tấn công DDoS trong quý 3/2017 của Viettel IDC cho ta thấy được sự gia tăng mạnh mẽ của loại hình tấn công này. Tấn công DDoS gây thiệt hại rất nhiều cho các công ty đặc biệt là các công ty hoạt động ở lĩnh vực giải trí. Tấn công DDoS vẫn đang được sử dụng phỏ biến trong các cuộc tấn công mạng và rất khó để phòng chống vì rất khó để phân biệt lưu lượng tấn công và lưu lượng của người dùng hợp pháp. Qua đó ta thấy được tầm quan trọng của việc phát hiện và giảm thiểu thiệt hại của tấn công DDoS.

CHƯƠNG 2 GIỚI THIỆU VỀ CÔNG NGHỆ MẠNG SDN (SOFTWARE DEFINE NETWORKING)

Hệ thống mạng máy tính và Internet phát triển rất mạnh mẽ trong những năm qua. Vì thế mà mô hình mạng của các doanh nghiệp ngày càng cồng kềnh và khó quản lý. Đòi hỏi một công nghệ mạng mới ra đời giúp các nhà quản trị mạng có thể kiểm soát hệ thống mạng của mình một cách dễ dàng và linh hoạt hơn. Đó chính là SDN (Software defined Networking). Trong chương này chúng em sẽ giới thiệu SDN là gì? Vì sao chúng ta nên dùng SDN thay thế cho mạng truyền thống? Cấu trúc và nguyên tắc hoạt động của SDN.

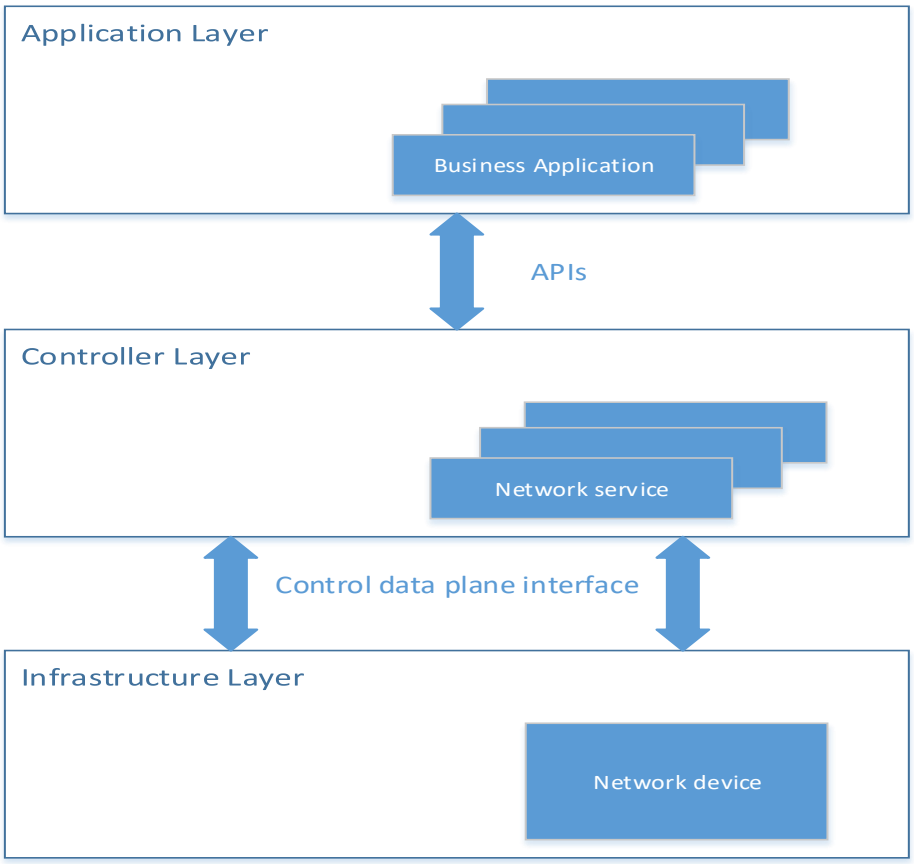
2.1 Giới thiệu về SDN

2.1.1 Khái niệm SDN

Software Defined Network (SDN) là một công nghệ mạng mới cho phép người quản trị mạng có thể điều khiển, cấu hình các thiết bị mạng một cách linh hoạt và hiệu quả. Về mặt bản chất thì SDN tách riêng 2 thành phần có sẵn trong cách thiết bị mạng là control plane và forwarding plane [3].

Control plane và forwarding plane là 2 dạng tiến trình mà các thiết bị mạng đều thực hiện. Trong mạng truyền thống, control plane của mỗi thiết bị mạng sẽ được phân tán và hoạt động độc lập với control plane của các thiết bị khác. Trong SDN thì phần control plane sẽ được tách khỏi thiết bị mạng và được tập trung lại thành một thiết bị gọi là controller các thiết bị mạng chỉ còn nhiệm vụ chuyển tiếp dữ liệu.

2.1.2 Kiến trúc mạng SDN



Hình 2.1: Cấu trúc mạng SDN

Mạng SDN gồm 3 thành phần chính:

Tầng ứng dụng: Là các ứng dụng kinh doanh, theo dõi lưu lượng mạng và được kết nối tới tầng điều khiển thông qua các API, cung cấp khả năng cấu hình, đặt lại các thông số mạng như băng thông, độ trễ, định tuyến … thông qua lớp điều khiển.

Tầng điều khiển: Là tầng tập trung các bộ điều khiển thực hiện yêu cầu từ tầng ứng dụng. Tầng này cung cấp các API cho phép giao tiếp với tầng ứng dụng. Ngoài ra tầng này còn điều khiển tầng cơ sở hạ tầng thông qua các cơ chế như OpenFlow, ForCES, PCEP, NETCONF, SNMP…

Tầng cơ sở hạ tầng: Bao gồm tất cả các thiết bị mạng chịu sự điều khiển của tầng điều khiển. Tầng này có nhiệm vụ chuyển tiếp các gói tin trong mạng theo sự điều khiển của tầng điều khiển.

2.1.3 Cơ chế hoạt động của SDN

Khi một gói tin được gửi đến thiết bị chuyển mạch thì thiết bị này sẽ kiểm tra trong bảng định tuyến có luồng nào phù hợp không. Nếu có thì gói tin sẽ được chuyển đến cổng tương ứng có trong bảng định tuyến. Nếu không có thì thiết bị chuyển mạch sẽ gửi một yêu cầu đến thiết bị điều khiển để xử lý. Sau đó thiết bị điều khiển sẽ gửi một bản tin yêu cầu thiết bị mạng thêm một luồng dữ liệu tương ứng với gói tin đến. Sau đó thiết bị chuyển mạch sẽ thiết lập luồng sữ liệu mới này vào bảng định tuyến và chuyển tiếp các gói tin của người dùng.

Cơ chế này có nhược điểm là độ trễ xử lý gói tin ban đầu, đây là lỗ hổng để tin tặc có thể tấn công vào gây mất an toàn thông tin.

2.1.4 Ưu nhược điểm của SDN so với mạng truyền thống

Ưu điểm:

- Các thiết bị chuyển mạch hoạt động đơn giản và hiệu quả hơn vì các chức năng điều khiển đã được lược bỏ.
- Sự khác biệt giữa các nhà sản xuất khác nhau không ảnh hưởng tới hệ thống mạng do việc điều khiển được tập trung tại tầng điều khiển.

Nhược điểm:

- Trễ xử lý bản tin đầu là một lỗ hổng mà tin tặc có thể tấn công.

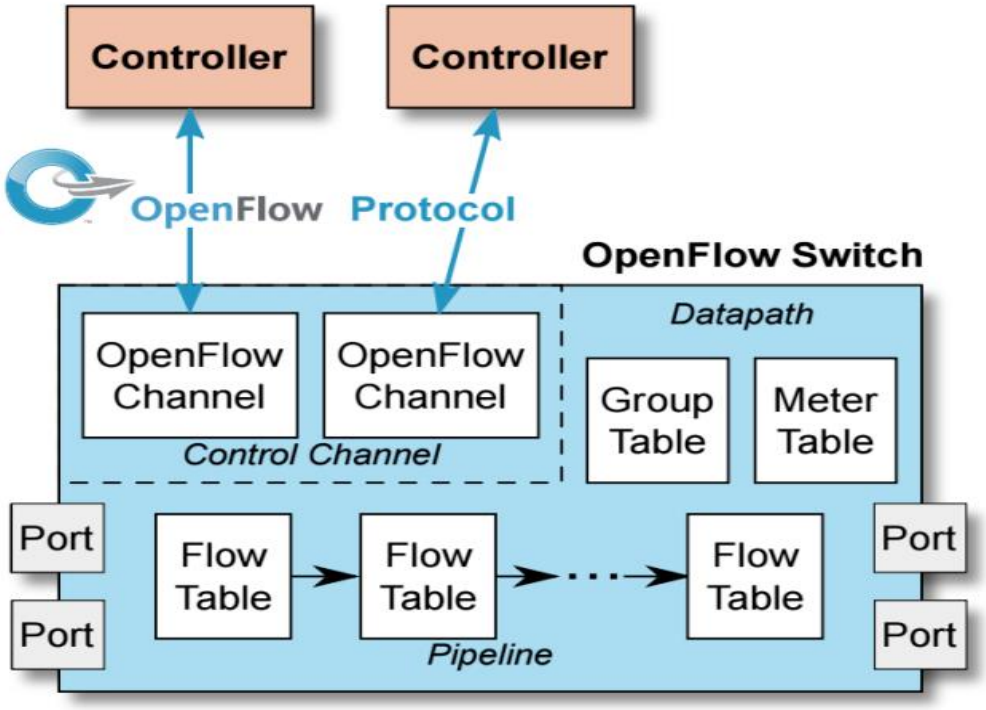
2.2. Giao thức OpenFlow

Là giao thức để giao tiếp giữa tầng điều khiển và tầng vật lý (thiết bị mạng) trong cấu trúc mạng SDN.

2.2.1 Giới thiệu về OpenFlow Controller

Đây là phần quan trọng nhất trong mạng SDN chịu trách nhiệm điều khiển các thiết bị trong mạng. OpenFlow controller nằm độc lập với thiết bị mạng và giao tiếp với thiết bị mạng thông qua giao thức OpenFlow. Trong một hệ thống mạng có thể có một hoặc nhiều OpenFlow Controller, các OpenFlow Controller có thể giao tiếp với nhau thông qua các API được định nghĩa sẵn trong tầng điều khiển.

2.2.2 Giới thiệu về OpenFlow Switch



Hình 2.2: OpenFlow Switch [3]

Mỗi OpenFlow Switch có thể có một hoặc nhiều bảng Flow Table. Flow Table giống như bảng định tuyến của router nó chứa các thông tin định tuyến của các luồng dữ liệu. Khi một gói tin đến thì thiết bị chuyển mạch sẽ dựa vào bảng Flow Table để chuyển tiếp gói tin.

Mỗi Flow Table chứa rất nhiều Flow Entry. Mỗi Flow Entry bao gồm các thành phần sau.

Matching Fields	Action	Counter

Các thành phần của Matching Field.

Một số Action trong Flow Entry

- Loại bỏ bản tin (Drop packet): Khi một Flow Entry có action này thì bất cứ gói tin nào có thông tin trong trường Matching Field giống với Flow Entry nào thì đều bị loại bỏ.
- Gửi lên Controller: Flow Entry có Action này sẽ nằm ở cuối bảng Flow Table. Khi mà tất cả các Flow Entry hiện có trong Flow Table đều không tương ứng với bản tin đến thì thiết bị mạng sẽ gửi lên controller yêu cầu xử lý.
- Chuyển gói tin đến một cổng của OpenFlow Switch:

Các thông tin thống kê trong trường counter:

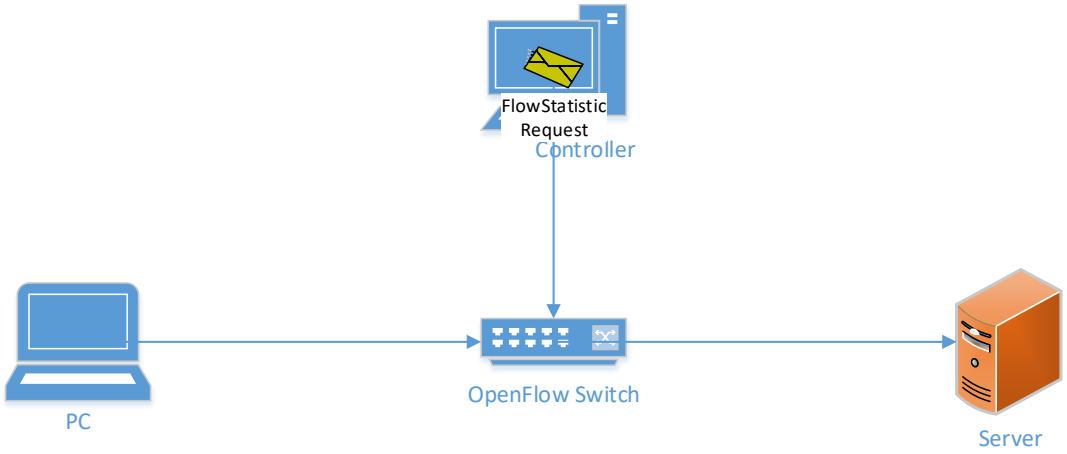
- Packet_count : Đếm số gói tin đã đi qua thiết bị chuyển mạch tương ứng với một Flow Entry
- Byte_count : Đếm số byte dữ liệu đã đi qua thiết bị chuyển mạch tương ứng với một Flow Entry
- Duration_sec : Thời gian tồn tại của Flow Entry tính bằng giây

- Duration_nsec : Thời gian tồn tại của Flow Entry tính bằng nano giây

2.3 Thống kê thông tin lưu lượng

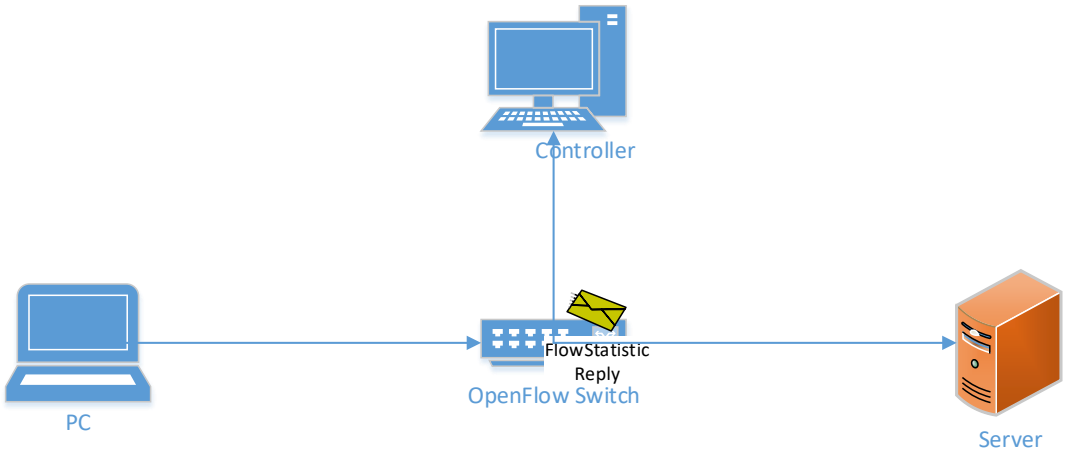
Trong phần này, chúng em trình bày các bước để thống kê thông tin lưu lượng trong mô hình SDN [4].

Bước 1: Controller gửi bản tin FlowStatistic Request xuống Switch yêu cầu Switch gửi thông tin của các flow trong bảng flow table



Hình 2.3: Controller gửi bản tin FlowStatistic Request xuống Switch

Bước 2: Switch gửi bản tin FlowStatistic Reply cho Controller. Thông tin của mỗi flow entry chứa các thông tin thống kê về số lượng gói tin, lưu lượng của mỗi flow…



Hình 2.4: Switch trả lời Controller bằng bản tin FlowStatistic Reply

Bước 3: So sánh thông tin mỗi flow ở thời điểm t+1 vs thời điểm t để xem sự thay đổi của flow giữa 2 thời điểm.

VD: Ở thời điểm t thì ta có 2 flow là:

Flow1 có 2 packets,

Flow2 có 5 packets.

Thời điểm t+1 ta có 3 flow là

Flow1 có 5 packets,

Flow2 có 10 packets,

Flow3 có 7 packets

Vậy trong khoảng thời gian từ t đến t +1 thì Flow1 có 3 packets đi qua Switch, Flow2 có 5 packets, Flow3 có 7 packets.

Như vậy, so sánh sự thay đổi giữa lần đo liên tiếp nhau thì ta sẽ được thông tin thống kê của mỗi flow.

2.4 Kết luận

Qua chương này chúng em đã trình bày khái quát về công nghệ mạng SDN (Software defined Networking). Những ưu điểm nào có thể giúp cho SDN thay thế cho hệ thống mạng truyền thống trước đây trong tương lai. Chúng em cũng đã trình bày về giao thức OpenFlow và cách thức hoạt động của các thiết bị (OpenFlow Switch) sử dụng OpenFlow trong SDN.

CHƯƠNG 3 ĐỀ XUẤT KIẾN TRÚC MẠNG SDN, GIẢI PHÁP PHÁT HIỆN VÀ GIẢM THIỂU TẤN CÔNG DDOS

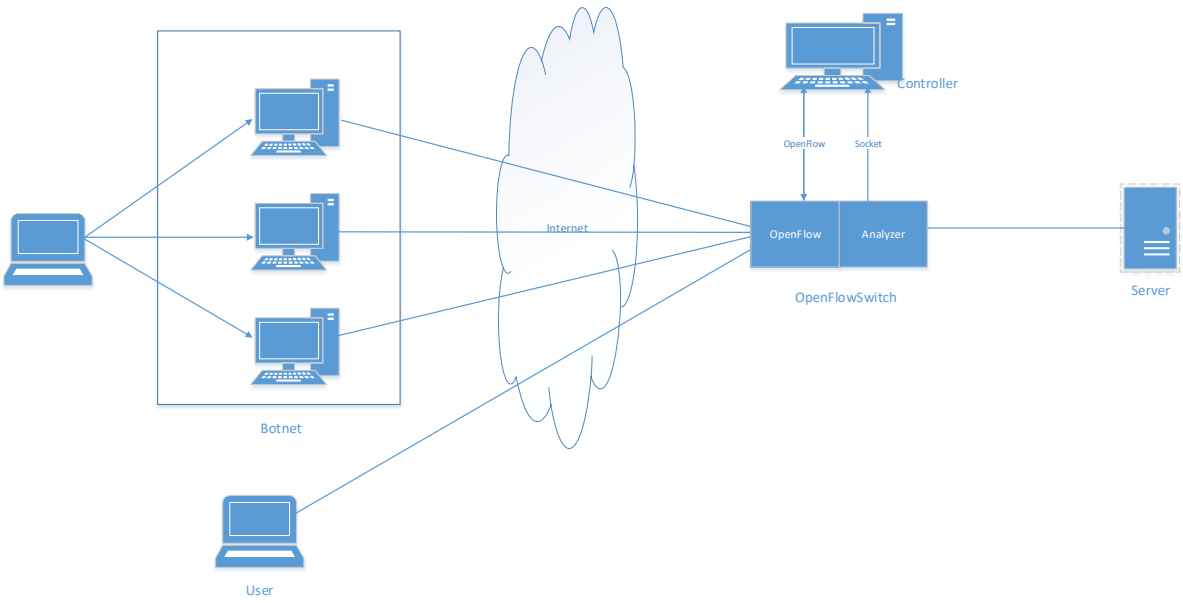
Trong chương này, chúng em trình bày về kiến trúc mạng SDN phù hợp để phát hiện và giảm thiểu tấn công DDoS. Kiến trúc này sử dụng thêm một khối chức năng trên

OpenFlow Switch để thống kê lưu lượng mạng đến server theo thời gian thực rồi gửi kết quả cho Controller (nơi chạy thuật toán để đưa ra quyết định) thông qua giao diện Socket.

Trên Controller chúng em sử dụng thuật toán Fuzzy-logic-based [5] để phát hiện tấn công và quyết định chính sách phù hợp để giảm thiểu tác dụng của cuộc tấn công. Thuật toán Fuzzy-logic-based dựa trên lưu lượng truy cập đến máy chủ để xác định các truy cập thuộc về lưu lượng tấn công. Thuật toán này được xây dựng dựa trên Sugeno FIS (Fuzzy Inference System)[6].

Sau khi phát hiện ra tấn công, thì các biện pháp giảm thiểu sẽ được thực hiện ngay sau đó. Dựa vào đặc điểm của lưu lượng mạng trong thời điểm hiện tại thì chúng em sẽ áp dụng các phương pháp khác nhau.

3.1 Đề xuất kiến trúc mạng



Hình 3.1 Kiến trúc mạng SDN đề xuất

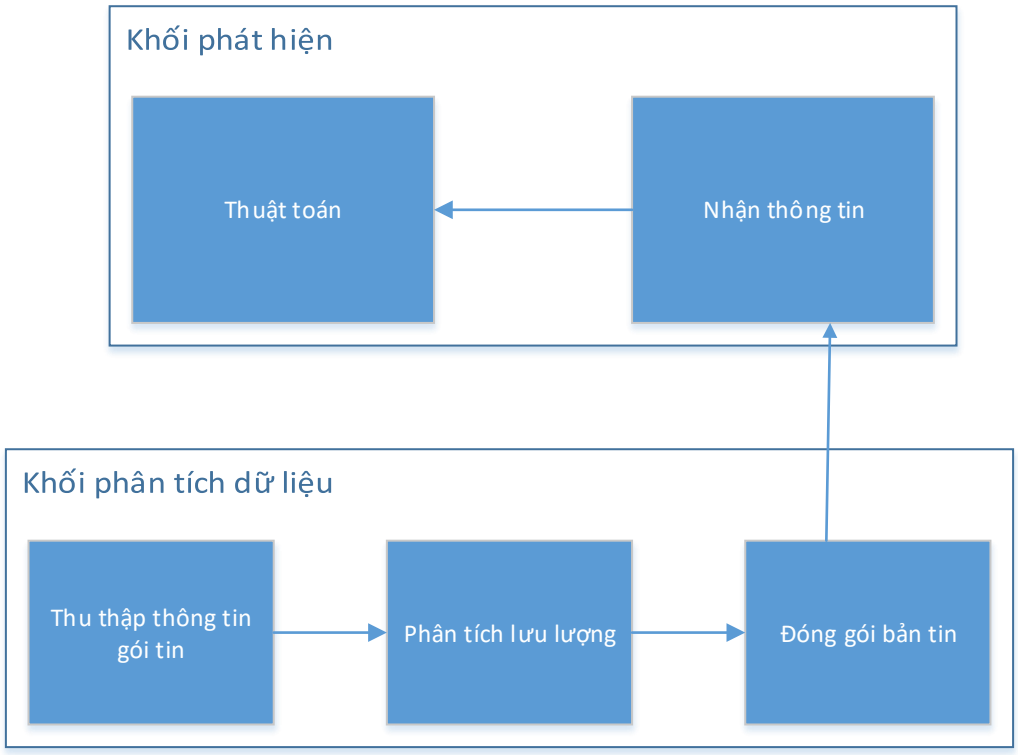
Các thành phần trong kiến trúc trong Hình 3.1:

- Botnet: Hệ thống các máy tính bị chiếm quyền điều khiển bởi kẻ tấn công.
- User: Người dùng bình thường.
- OpenFlow Switch: Là thiết bị chuyển mạch được hỗ trợ giao thức OpenFlow.
- Controller: Là thiết bị điều khiển lưu lượng mạng đi qua thiết bị chuyển mạch.
- Server: Là web server, nạn nhân tấn công của kẻ tấn công.

Kiến trúc mạng trong Hình 3.1 cho phép lưu lượng đến Server được thống kê theo thời gian thực và các thông tin thống kê được gửi cho SDN Controller thông qua giao diện Socket. Tại SDN Controller, thuật toán được áp dụng với đầu nhận được qua giao diện Socket, đầu ra của thuật toán sẽ quyết định xem trạng thái của mạng là đang bị tấn công hay không.

3.2 Các khối chính và chức năng

Các khối chính trong hệ thống:



Hình 3.2 Các khối trong kiến trúc mạng

3.2.1 Khối phân tích dữ liệu

Khối phân tích dữ liệu được phát triển dưới OpenFlow Switch có chức năng chính là thống kê lưu lượng trong mạng để đưa lấy thông tin đầu vào cho khối phát hiện.

Trong khối này, chúng em chia làm 3 thành phần nhỏ hơn:

- **Thu thập thông tin gói tin**: Trong thành phần này, bất kỳ gói tin nào đi qua OpenFlow Switch đều được giữ lại thông tin như time_stamp, ip source, ip destination, port source, port destination, protocol. Các thông tin này được đưa đến thành phần tiếp theo để xư lý tiếp.
- **Phân tích lưu lượng**: Từ thông tin của các gói tin đi vào mạng, thành phần này sẽ tính toán và đưa ra các thông số là đầu vào của thuật toán.

- **Đóng gói bản tin**: Đóng gói các thông tin từ khối phân tích lưu lượng vào gói tin TCP qua giao diện Socket

3.2.2. Khối phát hiện

Khối phát hiện được phát triển trên SDN Ctroller có chức năng chính là đưa các thông số nhận được vào thuật toán để đưa ra tráng thái của mạng có bị tấn công hay không.

Khối này được xây dựng dựa trên hai thành phần sau:

- **Nhận thông tin**: Thành phần này có nhiệm vụ lắng nghe trên giao diện Socket để bắt thông tin mà khối phân tích dữ liệu gửi lên. Khi bắt được thông tin thì thành phần tiếp theo sẽ được gọi đến
- **Thuật toán**: Dựa vào các thông số đầu vào, thuật toán sẽ được áp dụng để phát hiện tấn công

3.3 Phân tích dữ liệu mẫu

3.3.1 Tại sao phải phân tích dữ liệu

Như đã giới thiệu ở chương 1, để tổ chức một cuộc tấn công DDoS thì kẻ tấn công phải huy động rất nhiều các máy botnet để truy cập vào server cùng một thời điểm làm cho dịch vụ của server bị gián đoạn. Khi tấn công xảy ra thì các thông số trong mạng thay đổi đột ngột trong khoảng thời gian ngắn.

Để biết được sự thay đổi của các thông số mạng từ bình thường sang tấn công thì ta phải phân tích các dữ liệu mẫu có nhãn để thấy được sự khác biệt khi bình thường và tấn công. Trong chương này, chúng em phân tích bộ dữ liệu CaiDa 2007 tại thời điểm trạng thái của mạng chuyển từ bình thường sang tấn công. Chúng em thống kê hai thông số là tỉ lệ flow có 1 gói tin và tỉ lệ số packet inter-arrival time (khoảng thời gian đến giữa hai gói tin liên tiếp) nằm trong dải giá trị [0 - 0.2 ms].

Lý do em chọn hai thông số này:

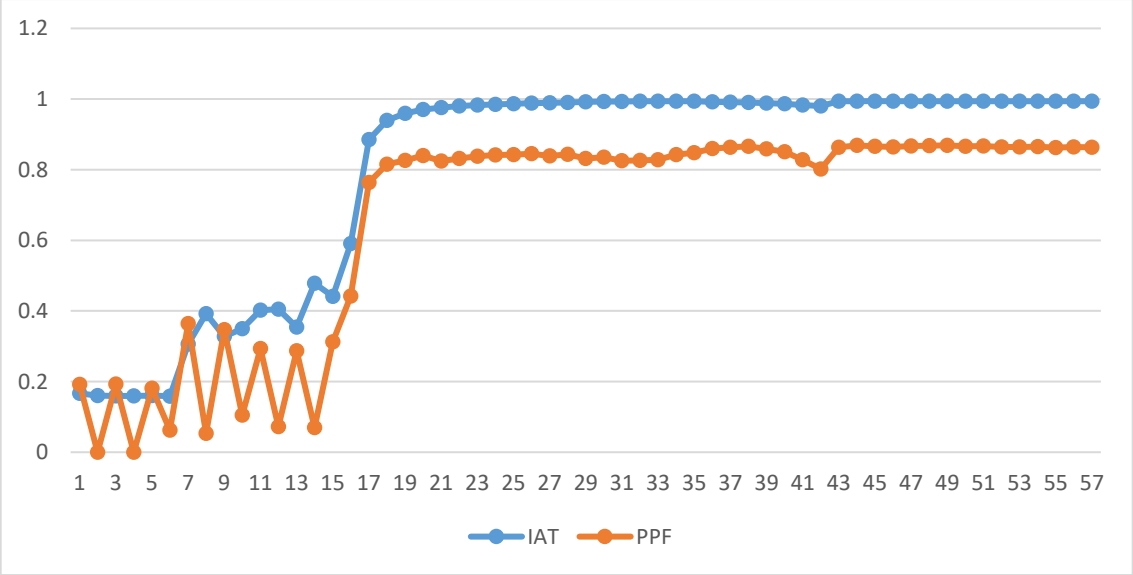
(1) Kẻ tấn công sử dụng rất nhiều các botnet trên internet trong khi các botnet này phát ra tốc độ gói không cao

(2) Khi bị tấn công thì số lượng gói tin đến tại một thời điểm là rất lớn vì các botnet cùng tấn công một thời điểm.

3.3.2 Kết quả phân tích dữ liệu

Trong phần này, chúng em phân tích bộ dữ liệu CAIDA 2007. Chúng em sẽ giới thiệu trong Chương 4.

Trong bộ dữ liệu này thì 80s đầu là lưu lượng bình thường, trừ giây thứ 80 thì trạng thái của mạng là tấn công. Các thông số trên được thống kê 5s một lần.



Hình 3.3 Kết quả phân tích dữ liệu CaiDa 2007

Hai thông số mà chúng em phân tích là:

- IAT (Inter arrival time): Tỉ lệ số packet inter-arrival time (khoảng thời gian đến giữa hai gói tin liên tiếp) nằm trong dải giá trị [0 - 0.2 ms].
- PpF (Paket per flow): Tỉ lệ flow có 1 gói tin.

Từ hình 3.3 cho thấy khi bình thường thì hai thông số trên khá thấp nằm trong khoảng từ 0% đến 40%. Nhưng khi bị tấn công thì hai thông số này tăng lên rất cao >80%.

3.4 Thuật toán Fuzzy-logic-based

3.4.1 Chọn các thông số đầu vào cho thuật toán

Dựa vào kết quả phân tích lưu lượng trong chương 3. Chúng em sử dụng hai thông sô là:

(1) Tỉ lệ flow có 1 gói tin. (PpF – paket per flow)

(2) Tỉ lệ số packet inter-arrival time (khoảng thời gian đến giữa hai gói tin liên tiếp) nằm trong dải giá trị [0 - 0.2 ms]. (IAT – Inter arrival time)

Để dễ dàng đưa ra các giải pháp giảm thiểu tấn công phù hợp các các loại tấn công khác nhau thì chúng em đề xuất lấy thêm 1 thông số nữa đó là:

(3) Giao thức có tỉ lệ gói tin cao nhất (MaxRateProtocol).

Mỗi thông số trên được thống kê trong khoảng thời gian 5s.

3.4.2 Xây dựng các quy tắc đánh giá

Quy tắc của thuật toán có thể được phát biểu như sau:

Quy tắc 1: Nếu lưu lượng truy cập hiện tại của mạng có hai thông số (PpF, IAT) đều nằm dưới ngưỡng bình thường thì ta có thể kết luận là lưu lượng hiện tại là lưu lượng bình thường.

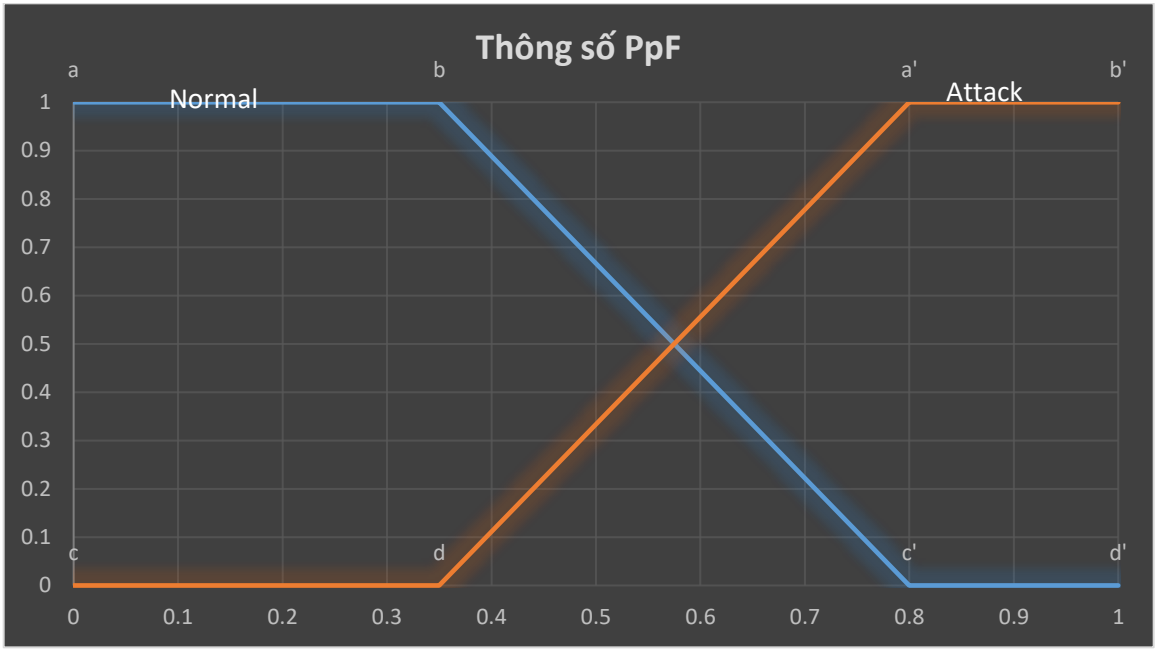
Quy tắc 2: Nếu cả hai giá trị nằm trên ngưỡng tấn công thì ta có thể kết luận là lưu lượng hiện tại là lưu lượng tấn công.

Quy tắc 3: Nếu hai giá trị nằm giữa ngưỡng tấn công và bình thường tức là hiện tại có cả lưu lượng tấn công và lưu lượng bình thường, lúc đó ta sẽ sử dụng các công thức để tính ra một số Z đại diện cho phần trăm lưu lượng tấn công dựa trên PpF và IAT.

3.4.3 Định nghĩa các miền cho thống số đầu vào

Đầu vào của thuật toán là mức độ của hai thông sô IAT và PpF, được xác định là Normal và Attack. Để xây dựng được hai thông số đầu vào em dựa trên kết quả phân tích dữ liệu ở trên.

- Thông số PpF



Hình 3.4 Thông số PpF

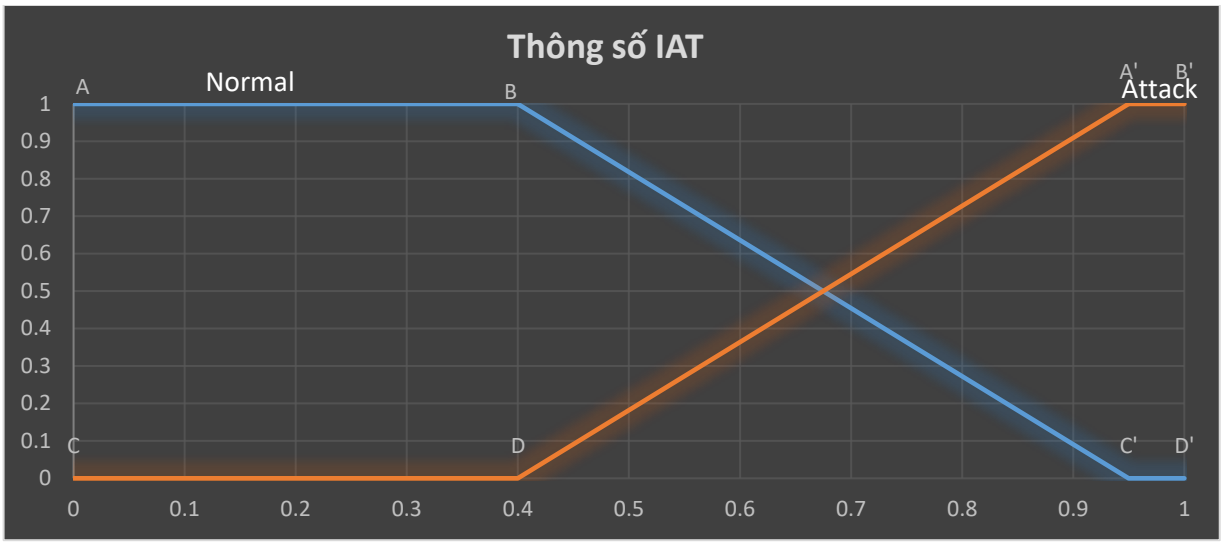
Thông số PpF được biểu diễn như hình trên:

- Nếu PpF < 0.35 tức là PpF đang ở mức Normal (mức bình thường). Nếu PpF > 0.8 tức là PpF đang ở mức Attack(mức tấn công).
- Nếu 0.35 < PpF < 0.8 thì ta chưa chắc chắn PpF đang ở mức nào thì mức độ đầu vào của mức Normal và Attack được tính như sau:

$$F_{Normal}(PpF) = \max[\min\left(\frac{PpF - c}{c - a}, 1, \frac{c' - PpF}{c' - b}\right), 0]$$

$$F_{Attack}(PpF) = \max[\min\left(\frac{PpF - d}{a' - d}, 1, \frac{d' - PpF}{c' - b'}\right), 0$$

- Thông số IAT



Hình 3.5 Thông số IAT

Thông số IAT được biểu diễn như hình trên:

- Nếu IAT < 0.4 tức là IAT đang ở mức Normal (mức bình thường). Nếu IAT > 0.95 tức là IAT đang ở mức Attack.
- Nếu 0.4 < IAT < 0.95 thì ta chưa chắc chắn IAT đang ở mức nào thì mức độ đầu vào của mức Normal và Attack được tính như sau:

$$F_{Normal}(IAT) = \max[\min\left(\frac{IAT - C}{C - A}, 1, \frac{C' - IAT}{C' - B}\right), 0]$$

$$F_{Attack}(IAT) = \max[\min\left(\frac{IAT - D}{A' - D}, 1, \frac{D' - IAT}{C' - B'}\right), 0]$$

Các quy tắc để đưa ra hành động là:

- Nếu PpF = Normal và IAT = Normal thì F_w= 0
- Nếu PpF = Normal và IAT = Attack thì D_r= 1
- Nếu PpF = Attack và IAT = Normal thì D_r= 1
- Nếu PpF = Attack và IAT = Attack thì D_r= 1

Độ mạnh của các quy tắc trên được tính như sau:

W_1 = min[F_{Normal} (IAT), F_{Normal} (PpF)]

W_2 = min[F_{Normal} (IAT), F_{Attack} (PpF)]

W_3 = min[F_{Attack} (IAT), F_{Normal} (PpF)]

W_4 = min[F_{Attack} (IAT), F_{Attack} (PpF)]

Dựa vào các quy tắc trên mà ta có thể đưa ra các quyết định hợp lý. Các hành động được biểu diễn bởi: F_w = 0 thì thông báo là bình thường, D_r= 1 thì thông báo là tấn công.

3.4.4 Đưa ra quyết định dựa trên các quy tắc đánh giá

Khi lưu lượng mạng của hệ thống rơi vào Quy tắc 3, tức là hiện tại đang có cả lưu lượng tấn công và lưu lượng bình thường. Vậy ta có thể tính ra hệ số Z của thuật toán bằng công thức:

$$Z = \frac{W_1.F_w + W_2.D_r + W_3.D_r + W_4.D_r}{W_1 + W_2 + W_3 + W_4}$$

Với Z nằm trong khoảng [0, 1] thể hiện phần trăm lưu lượng tấn công đang có trong mạng.

3.5 Các phương pháp giảm thiểu tấn công

Khi phát hiện trạng thái của mạng đang bị tấn công thì chúng em dựa vào thông số (MaxRateProtocol) để đưa ra các phương pháp phù hợp.

- MaxRateProtocol = ICMP

  Giao thức ICMP được sử dụng rất ít trong các server cung cấp dịch vụ trên Internet nên giải pháp được đưa ra là thêm một flowEntry với action là drop vào bảng flowTable của OpenFlowSwitch để loại bỏ hết các bản tin ICMP.

- MaxRateProtocol = TCP

Với tấn công TCP thì ta áp dụng giải pháp sau:

- ✓ Nếu Z ≤PpF(tỉ lệ flow có 1 gói tin) thì ta xóa hết các luồng có 1 gói tin.
- ✓ Nếu Z > PpF thì ta loại bỏ một số luồng cho tới tỉ lệ Z (ưu tiên các luồng có ít gói tin).

3.6 Kết luận

Qua chương này, chúng em thấy được tầm quan trong của việc phân tích thống kê lưu lượng mẫu trong việc phát hiện tấn công DDoS. Chúng em cũng hiểu được cách xây dựng và cách hoạt động của thuật toán Fuzzy logic based dựa trên hai thông số đầu vào là IAT và PpF.

CHƯƠNG 4 MÔ PHỎNG MỘT CUỘC TẤN CÔNG DDOS

Chương 4 tập trung phân tích một cuộc tấn công DDoS ở đây là CAIDA 2007 để đưa ra các đặc tính của một cuộc tấn công DDoS từ đó đưa ra cách thức mô phỏng một cuộc tấn công DDoS xảy ra trong thực tế .

4.1 Bộ dữ liệu CAIDA

4.1.1 Giới thiệu bộ dữ liệu CAIDA

Để mô phỏng một cuộc tấn công DDoS trong thực tế, ở đây em đã chọn tập dữ liệu "DDoS Attack 2007"[7] của CAIDA để đưa vào hệ thống thử nghiệm của nhóm. Bộ dữ liệu này chứa traffic traces khoảng hơn một giờ vụ tấn công từ chối dịch vụ DDoS vào ngày 4 tháng 8 năm 2007. Loại tấn công DDoS này nhằm ngăn chặn truy cập vào các máy chủ mục tiêu bằng cách tiêu thụ tài nguyên máy tính trên máy chủ và tiêu thụ tất cả băng thông của mạng kết nối với máy chủ đó.

4.1.2 Phân tích bộ dữ liệu CAIDA đưa ra đặc tính mô phỏng

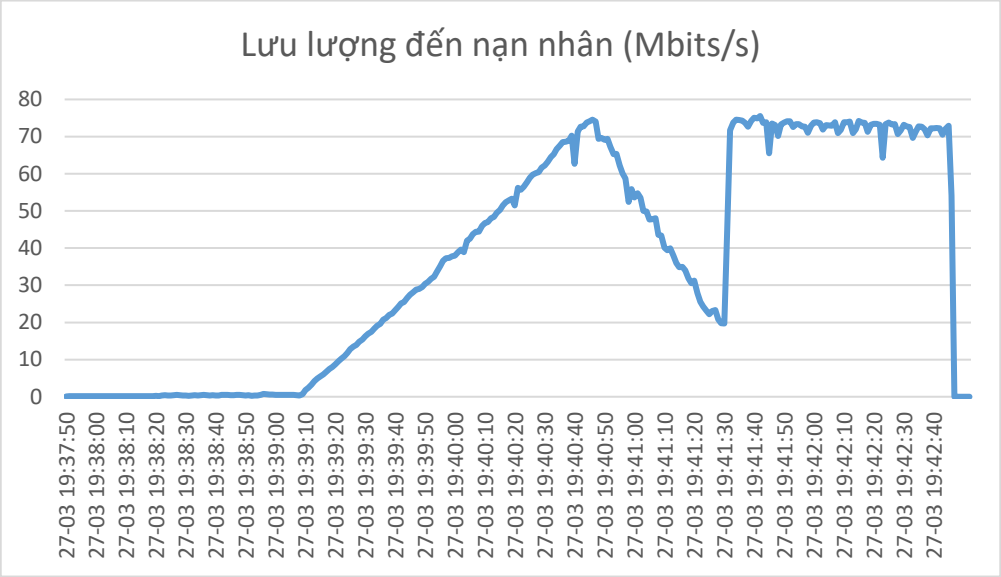
Chúng em sử dụng công cụ chuyên cho phân tích gói tin Wireshark để đưa ra kết quả thống kê .Nhìn vào đồ thị bên dưới ta có thể thấy rõ ràng số luồng ICMP và số địa chỉ IP tăng dần theo thời gian chứng tỏ của việc đang chịu sự tấn công của kẻ tấn công.

Hình ảnh dưới đây là một phần của bộ dữ liệu CAIDA có độ dài khoảng 5 phút đồng hồ. Trong đoạn dữ liệu có sự chuyển biến từ trạng thái thường sang trạng thái tấn công rõ rệt có thể thấy bằng mắt thường.

Trong khoảng từ giây thứ 10 lưu lượng tấn công tăng tuyến tính nhanh chóng từ 0 Mb/s lên đến 70 Mb/s trong vòng 30s khiến chúng ta nghi ngờ có sự bất thường ở đây , tiếp tục nhìn đồ thị tiếp theo ta thấy số lượng IP nguồn cũng tăng tuyến tính theo lưu lượng khiến ta nghi ngờ đây có thể là do botnet tạo ra .Cuối cùng đồ thị tỷ lệ gói tin cho ta thấy lượng gói ICMP gia tăng đột ngột và chiếm đại đa số đưa ra kết luận đây là tấn công DDoS ICMP.

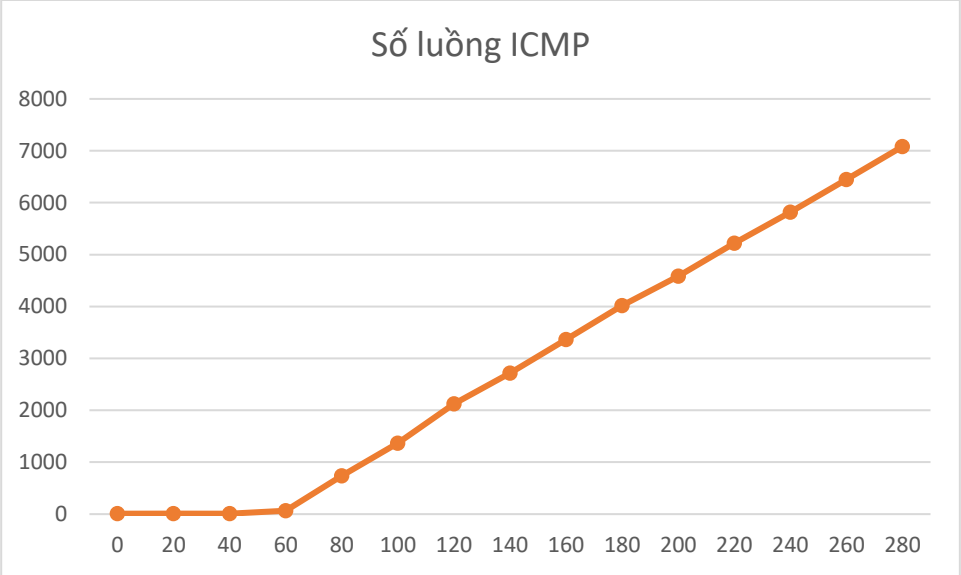
Từ các đặc điểm ở trên ta có để đưa ra kết luận về đặc tính của tấn công DDoS thực tế như sau:

- Lưu lượng đến tăng nhanh và tuyến tính



Hình 4.1: Lưu lượng bộ dữ liệu CAIDA trong khoảng 5 phút

- Số lượng địa chỉ ip nguồn cũng tăng nhanh và tuyến tính theo lưu lượng đến.



Hình 4.2: Số luồng ICMP CAIDA trong khoảng 5 phút

- Đối với tấn công ICMP số lượng gói ICMP đến nhiều chiếm đại đa số.

Hình 4.3: Tỷ lệ gói ICMP CAIDA trong khoảng 5 phút

Từ đó ta có thể dựa theo các đặc tính này và mô phỏng lại chính xác một cuộc tấn công.

4.2 Xây dựng hệ thông mô phỏng tấn công DDoS

4.2.1 Công cụ phát gói Bonesi

Công cụ Bonesi (botnet simulator)[8] là một công cụ phát gói mã nguồn mở , có thể mô phỏng một cuộc tấn công ddos với nhiều loại thông số :

- Số địa chỉ IP nguồn
- Số gói phát ra mỗi giây
- Kích thước gói tin
- Giao thức tấn công

Ưu điểm: dễ sử dụng với câu lệnh ngắn gọn, mã nguồn mở có thể can thiệp vào.

Nhược điểm: Chỉ phát được cố định một số lượng gói tin và số lượng địa chỉ IP cụ thể.

Cách sử dụng:

bonesi -i 50k-bots -d lo -r 50000 -s 1400 -p icmp 127.0.0.1:22

Trong đó:

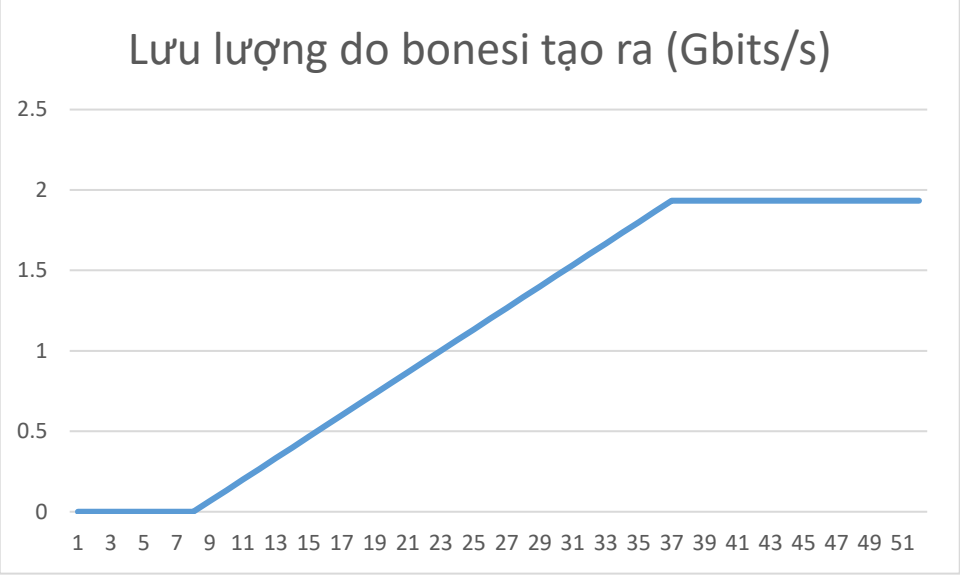
- -i : tên file chứa địa chỉ IP mô phỏng mạng botnet
- -d : tên cổng mạng muốn phát gói qua
- -r : số lượng gói tin muốn phát trong 1 giây
- -s : kích thước gói tin bytes (đối với tấn công udp, icmp)
- -p : giao thức tấn công muốn thực hiện (có tcpsyn , http, udp,icmp)

Do nhược điểm chỉ phát được một lượng gói tin cố định và địa chỉ IP cụ thể mỗi giây,chúng em đã phát triển công cụ Bonesi lên để có khả năng với gói tăng liên tục với lượng địa chỉ IP cũng gia tăng theo. Giải pháp sử dụng đó là chạy nhiều tiến trình song song dưới mức hệ điều hành sao cho mỗi tiến trình sẽ thực thi một tiến trình phát gói sử dụng bonesi với tương ứng một file IP botnet khác nhau để số lượng botnet và gói có thể tăng tuyến tính theo thời gian.

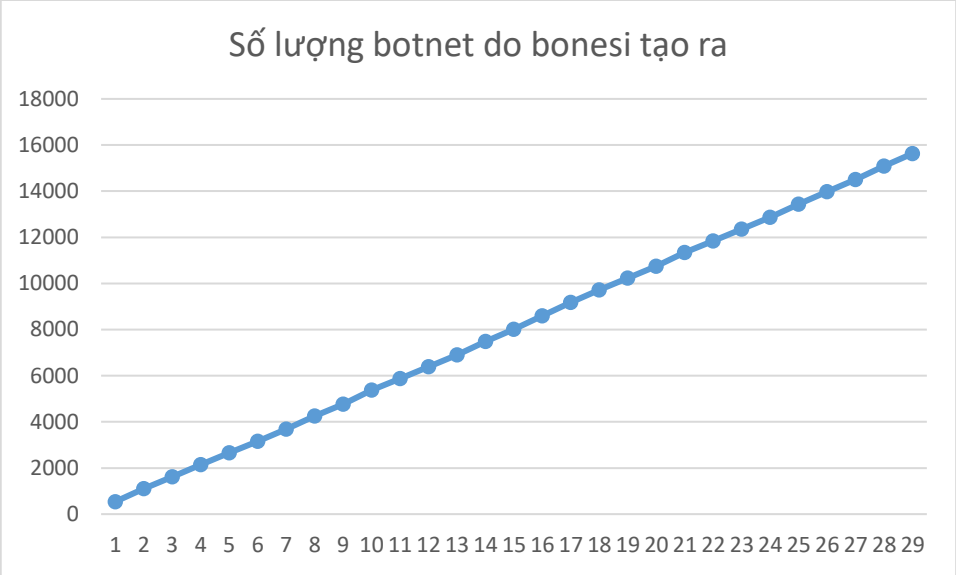
Chúng em đã sử dụng tiến trình chạy ngầm của hệ điều hành Linux để thực hiện điều trên và sau đây là kịch bản chúng em sử dụng.

```
max=30
for i in `seq 1 $max`
do
    r=$(( $RANDOM % 1000 + 5000 ))
    screen -dmS mutilbonesi bonesi -i $i -d lo -r $r -s 1400 -p icmp 127.0.0.1:22
    sleep 5
```

Kết quả lưu lượng khi chúng em sử dụng kịch bản tấn công ICMP flood ở trên so với kịch bản thông thường.



Hình 4.4 Lưu lượng sử dụng bonesi mô phỏng theo thời gian



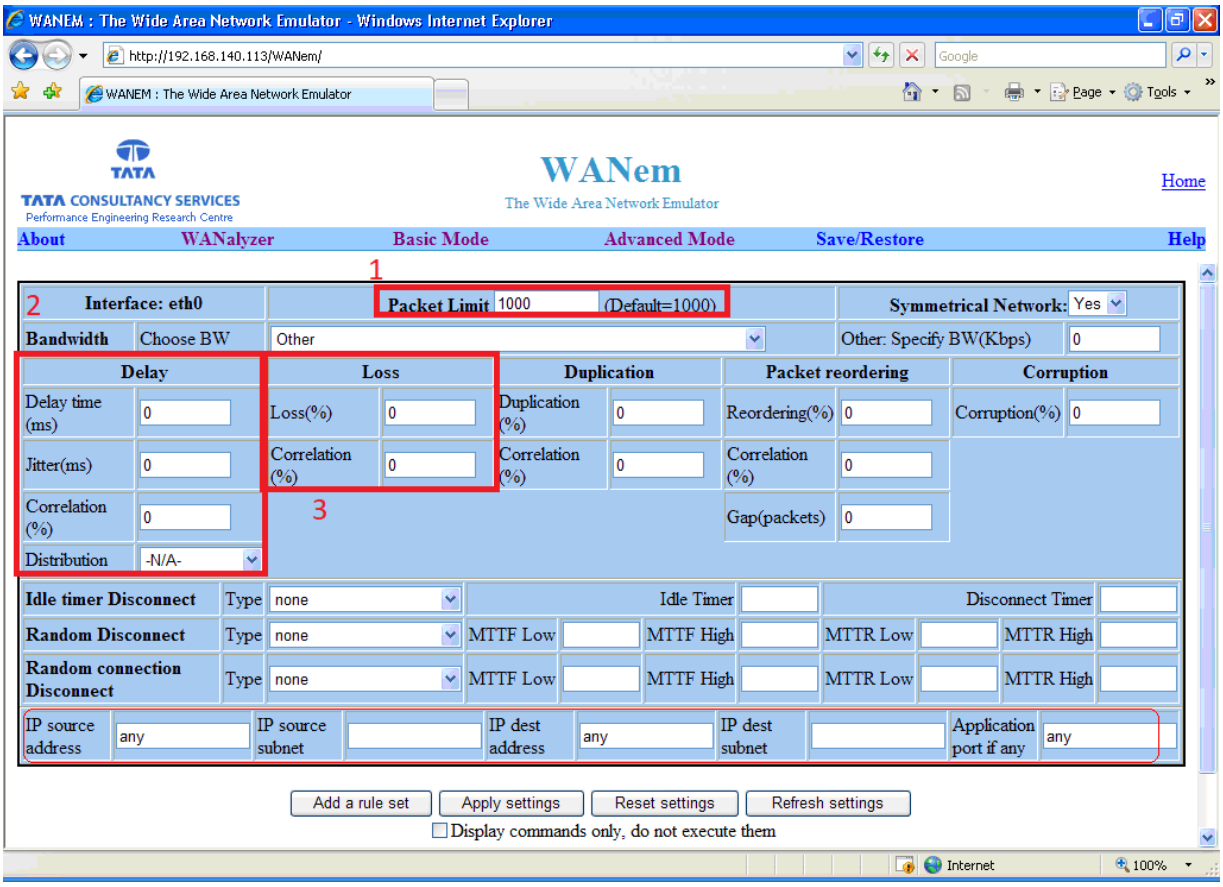
Hình 4.5 Lượng botnet sử dụng bonesi mô phỏng theo thời gian

Từ 2 đồ thị trên ta có thể thấy lưu lượng do bonesi cũng tăng tuyến tính theo thời gian , đồng thời lượng botnet tham gia tấn công cũng tăng theo giống với các đặc điểm của tấn công Ddos.

4.2.2 Công cụ tạo độ trễ gói tin WanEm

Cộng cụ WanEm (Wan Emulator)[9] là một công cụ mã nguồn mở có chức năng mô phỏng một mạng Wan ở giữa mục đích để tạo một số thông số cho gói tin khi đi qua mạng Wan đó với hiệu năng cao cho phép một lượng gói tín lớn đi qua với độ trễ , tỉ lệ mất gói ,… ngẫu nhiên hoặc tuân theo một phân bố cụ thể nào đó .

Quay lại với thực tế khi một cuộc tấn công mạng xảy ra các botnet có thể phân tán từ các vùng và quốc gia khác nhau từ đó dẫn đến một vấn đề xảy ra đó là khi các luồng dữ liệu đến từ các quốc gia khác nhau đến nạn nhân sẽ có độ trễ và tỉ lệ mất gói khác nhau do phải đi qua các nút mạng trung gian mới có thể đến đích đó là lí do chúng em đưa công cụ WanEm để mô phỏng một mạng Wan đứng giữa , lưu lượng khi đi qua mạng Wan này hay chính xác các nút mạng trung gian trong mạng Wan sẽ có độ trễ và tỉ lệ mất gói khác nhau .

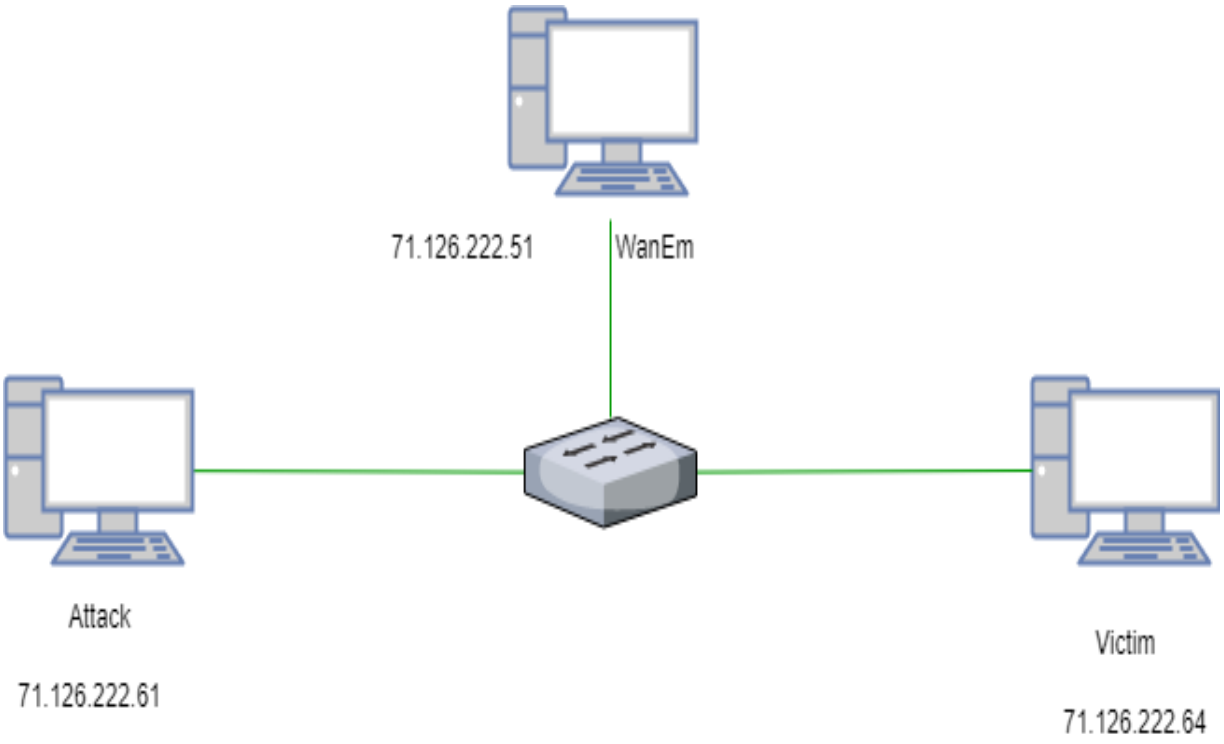


Hình 4.6: Bảng điều khiển của WanEm

Hình 4.6 là bảng điều khiển của WanEm chúng em sử dung các chức năng được khoanh trong ô đỏ.

1. Packet Limit: Số lượng gói cho phép đi qua
2. Delay: Tạo đỗ trễ cho các gói tin và nguồn phát gói tin (đơn vị mili giây ms)
3. Loss: Tỉ lệ mất gói (đơn vị phần trăm %)

Mô hình WanEm



Hình 4.7 Mô hình lắp đặt WanEm

Chúng em thực hiện cấu hình route sao cho lưu lượng từ máy tính tấn công (ở đây sử dụng cách phát bonesi nêu ở trên) đi qua máy tính cài đặt WanEm trên máy tính này ta sẽ điều chỉnh các thông số liên quan đến độ trễ và tỷ lệ mất gói rồi đi đến hệ thống nạn nhân chi tiết sẽ như sau.

Ở đây chúng em sử dụng nền tảng ảo hóa KVM để tạo 2 máy tính ảo cài hệ điều hành Ubuntu và 1 máy tính ảo cài WanEm, 1 switch ảo KVM (sử dụng openvswitch chế độ thường).

Bước 1: Đặt IP lần lượt cho các máy tính như trên hình.

Bước 2: Nối các máy tính ảo với switch ảo sử dụng lệnh của openvswitch

$ sudo ovs-vsctl add-br br0

$ sudo ovs-vsctl add-port br0 vnet1

Trong đó br0 là tên openvswitch và lệnh đầu tiên là để khởi tạo openvswitch trong môi trường KVM, tiếp theo là câu lệnh thêm các cổng ảo vào openvswitch ở đây là các cổng máy tính ảo tấn công, WanEm, nạn nhân.

Bước 3: Trên máy tính phát lưu lượng cấu hình route đến máy tính cài đặt WanEm

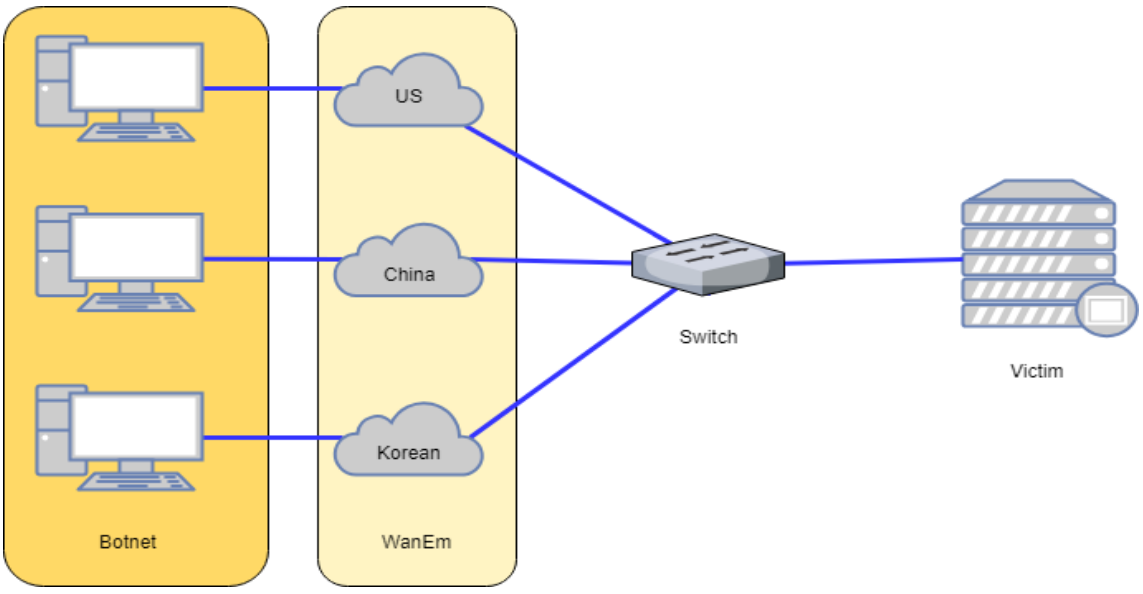
$ *route add –host 71.126.222.64 gw 71.126.222.51 dev ens4*

Trong đó 71.126.222.64 là địa chỉ máy tính nạn nhân và gateway 71.126.222.51 là địa chỉ của máy tính WanEm, ens4 là tên cổng mạng nối từ máy tấn công đến máy tính WanEm

Bước 4: Thực hiện điều chỉnh các thông số trên WanEm

4.2.3 Hệ thống và kết quả mô phỏng tấn công DDoS

Tiếp theo, chúng em sẽ kết hợp 2 công cụ bonesi và WanEm lại với nhau để xây dựng lên một mô hình mô phỏng tấn công DDoS hoàn chỉnh



Hình 4.8: Mô hình mô phỏng sử dụng WanEm

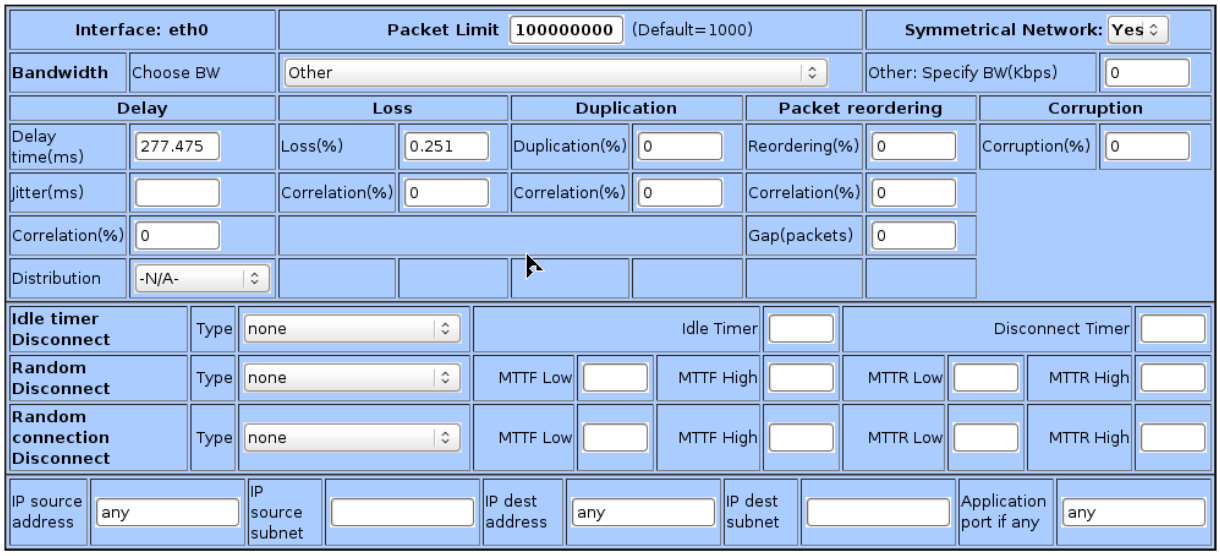
Trong mô hình trên chúng em sử dụng nền tảng ảo hóa KVM để xây dựng trong đó 3 máy ảo mô phỏng các botnet đến từ các quốc gia tham gia tấn công nhiều nhất là Mỹ,

Trung Quốc ,Hàn Quốc và lưu lượng từ các quốc gia này đến Việt Nam sẽ có độ trễ và tỷ lệ mất gói khác nhau cụ thể ở bảng phía dưới .Các máy ảo Ubuntu 16.04 được cài đặt công cụ bonesi và được route lưu lượng đến các máy WanEm .

Thông số	US	China	Korean
Đỗ trễ (ms)	**277.475**	**93.145**	**73.555**
Tỷ lệ mất gói (%)	**0.251**	**0.378**	**0.020**

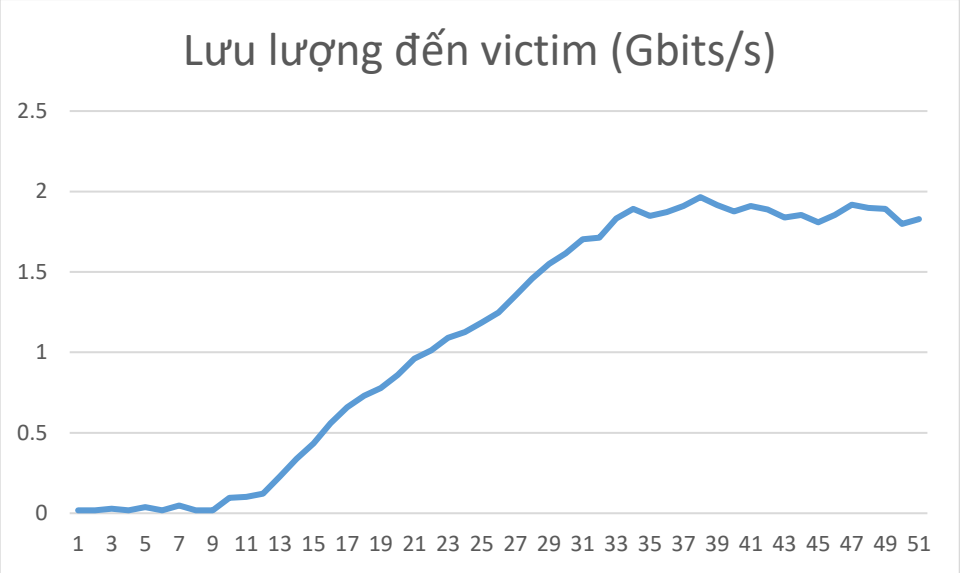
Bảng 4.1 Đỗ trễ và tỷ lệ mất gói đến Việt Nam

Chi tiết cấu hình WanEm như hình bên dưới, ở đây em chọn thông số từ Mỹ sang Việt Nam vào khoảng thời gian tháng 5 năm 2018 [10].



Hình 4.9: Cấu hình trên WanEm

Kết quả thu được tại nạn nhân khi kết hợp Bonesi và WanEm.



Hình 4.10: Lưu lượng đo được trên máy nạn nhân

Nhận xét thấy lưu lượng đến tăng nhanh một cách tuyến tính và kết hợp sự can thiệp của WanEm khiến lưu lượng có tính ngẫu nhiên giống với thực tế hơn. Cụ thể mô phỏng ở đây là mô phỏng tấn công ICMP Flood với kích thước gói tin lên đến 1400 bytes .Lưu lượng tăng nhanh từ điểm thứ 11 đến điểm thứ 33 và từ xấp xỉ 0 Gb/s lên đến 2 Gb/s xấp xỉ một cuộc tấn công thực tế hiện nay.

Kết quả lưu lượng phát đến nạn nhân sẽ được công cụ Tcpdump cài đặt trên thiết bị switch mục đích là thu lại các lưu lượng đi qua thành một file .pcap cho việc tái sử dụng và kết hợp phát với lưu lượng thường sẽ được nói ở chương sau.

4.3 Kết luận.

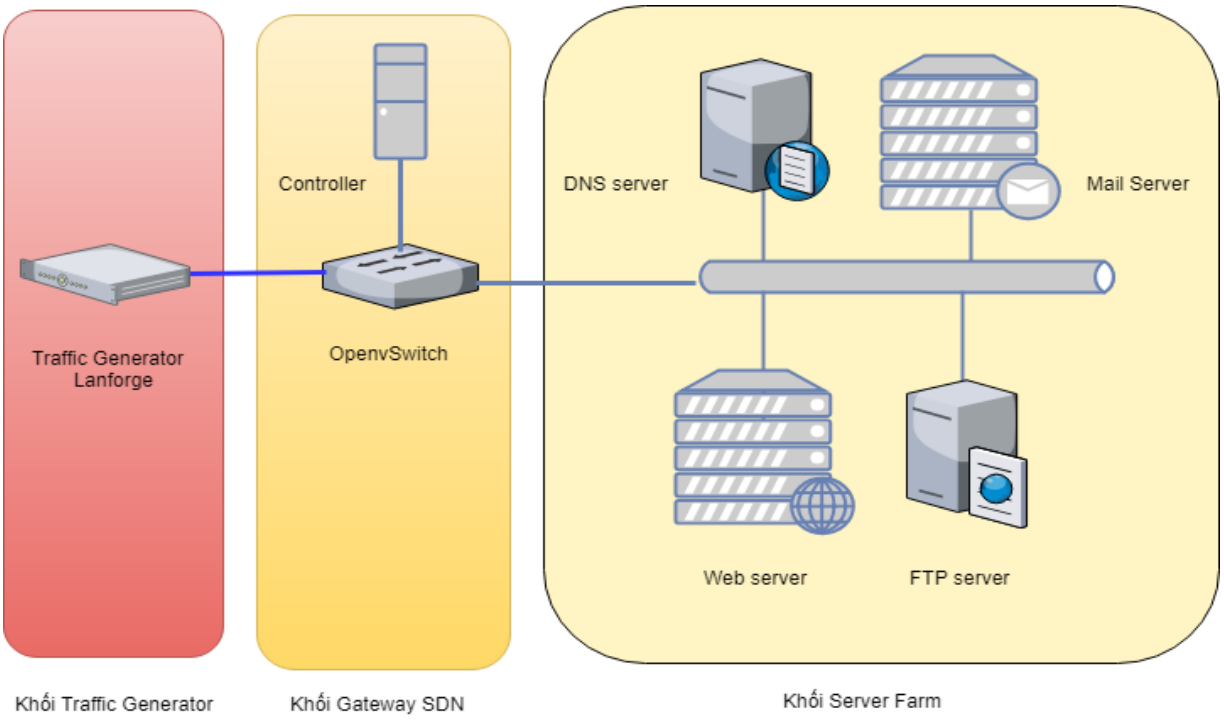
Chương 4 tập trung phân tích đặc tính lưu lượng từ bộ dữ liệu thật CAIDA từ đó đưa ra các đặc điểm, kết hợp sử dụng nhiều loại công cụ khác nhau để xây dựng lên một hệ thống giả lập lưu lượng một cách chính xác nhất có thể của một cuộc tấn công DDos đến các máy chủ.

CHƯƠNG 5 XÂY DỰNG MÔ HÌNH THỬ NGHIỆM VÀ KẾT QUẢ ĐO ĐẠC

Mục đích trong chương này nhằm xây dựng mô hình thử nghiệm gồm hệ thống mạng doanh nghiệp, bộ gateway sử dụng công nghệ SDN, bộ phát lưu lượng rồi đưa ra kết quả đạt được khi áp dụng giải pháp đã nói ở chương 3 và đưa ra phân tích, hướng phát triển

5.1 Tổng quan mô hình thử nghiệm

Sau khi tham khảo một số tài liệu xây dựng hệ thống mạng doanh nghiệp kết hợp với giải pháp đề xuất bên trên nhóm chúng em đã xây dựng lên mô hình thử nghiệm với các thành phần bên dưới để kiểm tra hiệu quả phương pháp đề xuất đưa ra kết quả và hướng phát triển sau này.



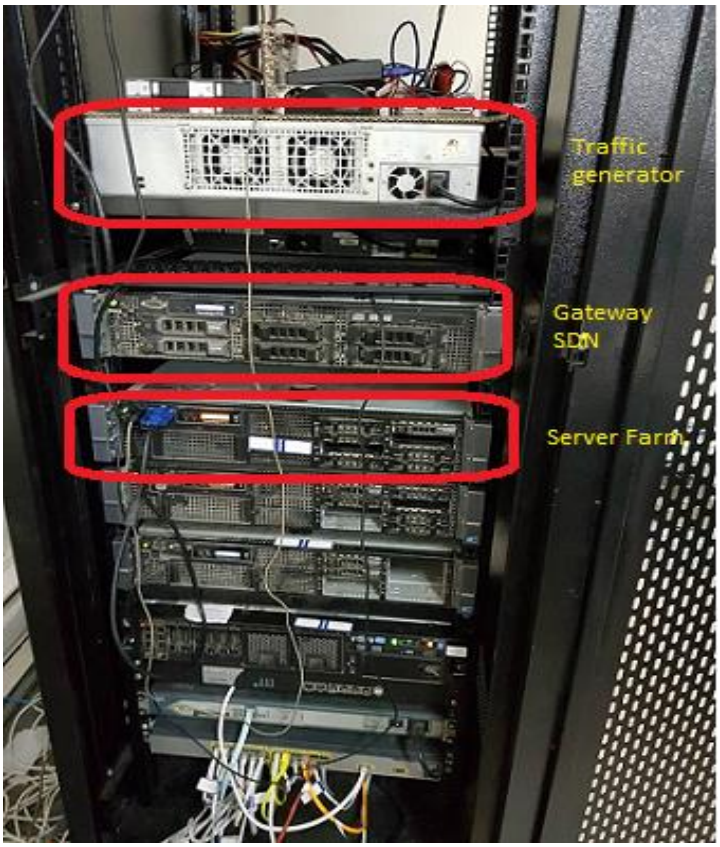
Hình 5.1: Mô hình testbed thử nghiệm hệ thống chống tấn công DDoS

Việc xây dựng testbed trên đòi hỏi lượng tài nguyện lớn chi tiết trong bảng dưới.

Tên khối	Tên thiết bị	Cấu hình
Traffic Generator	Lanforge CT503-MIX [11]	• 16GB RAM • 120GB SSD • Quad-Core Intel processor
Gateway SDN	Dell PowerEdge R730 server	• 32GB RAM • Intel E5-2620 v3 Xeon Six-Core 2.4GHz CPU's • 1TB HDD
Server Farm	IBM server x3650 M5	• 64GB RAM • Xeon 8C E5-2620 v4 85W 2.1GHz/2133MHz • 2 TB HDD

Bảng 5.1 Cấu hình hệ thống testbed

Mô hình thực tế của hệ thống.



Hình 5.2: Hệ thống testbed xây dựng trên các server thực tế

5.2 Xây dựng chi tiết từng khối trong mô hình thử nghiệm

5.2.1 Khối Server Farm:

Mục đích trong phần này nhằm xây dựng hệ thống mạng doanh nghiệp để thử nghiệm các cuộc tấn công và sức chịu đựng của các server. Nhóm chúng em xin trình bày bản thiết kế các thành phần và chức năng trong hệ thống mạng này.

Các thành phần trong đồ hình mạng ServerFarm**:**

- DNS Server
- Web Server
- FTP Server

- Mail Server
- Switch (ở đây nhóm chúng em sử dụng switch ảo của KVM)

Ở đây nhóm chúng em sử dụng môi trường KVM để xây dựng nên đồ hình mạng này .Công nghệ KVM với độ ổn định và hiệu năng cao hỗ trợ trong việc tạo quản lý các máy ảo và hạ tầng mạng ảo nên nhóm quyết định sử dụng công nghệ này.KVM được cài đặt trực tiếp lên các server, tại đó nhóm chúng em sẽ sử dụng và tạo nên nhiều máy ảo mỗi máy ảo phục vụ tương ứng một dịch vụ phía trên. Mục đích nhóm chúng em xây dựng nhiều loại hình dịch vụ là để có thể các nhóm tiếp theo dựa trên mô hình thử nghiệm nhiều loại tấn công khác nhau trên các loại hình dịch vụ khác nhau.

➢ Thành phần Webserver:

Web server là máy chủ được dùng để xử lý các truy cập được gửi từ máy khách thông qua giao thức HTTP. Các truy cập HTTP này thường được gửi từ các chương trình duyệt web trên máy tính cá nhân. Thuật ngữ web server có thể được sử dụng để để cập tới 2 khía cạnh là phần cứng hoặc phần mềm. Với khía cạnh phần cứng thì web server về bản chất cũng là 1 loại máy chủ giống như các máy chủ khác, tuy nhiên máy chủ này cần phải được cài đặt ít nhất một phần mềm giúp xử lý các truy cập gửi tới thông qua giao thức HTTP .

Web server cung cấp các dịch vụ cho người dùng có thể là một web thương mại điện tử , bán hàng trực tuyến , hoặc mạng xã hội … là đối tượng chính trong cuộc tấn công DDos nhắm tới .

Nhóm chúng em sử dụng Web Server Apache ,lí do Apache dễ cài đặt và tính phổ biến trên thị trường .

➢ Thành phần DNS Server:

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên nhiều thông tin đa dạng với tên miền được gán cho những người tham gia. Quan

trọng nhất là, DNS chuyển tên miền có ý nghĩa cho con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới.

Hệ thống tên miền giúp cho nó có thể chỉ định tên miền cho các nhóm người sử dụng Internet trong một cách có ý nghĩa, độc lập với mỗi địa điểm của người sử dụng. Bởi vì điều này, World-Wide Web (WWW) siêu liên kết và trao đổi thông tin trên Internet có thể duy trì ổn định và cố định ngay cả khi định tuyến dòng Internet thay đổi hoặc những người tham gia sử dụng một thiết bị di động. Tên miền internet dễ nhớ hơn các địa chỉ IP như là 208.77.188.166 (IPv4).

Mọi người tận dụng lợi thế này khi họ thuật lại có nghĩa các URL và địa chỉ email mà không cần phải biết làm thế nào các máy sẽ thực sự tìm ra chúng.

Các hệ thống Server Farm lớn đều cần một DNS server của riêng nó nhằm mục đích phần giải tên miền tốt hơn .

- Thành phần Mail Server:

Ngày nay, thư điện tử (email) là 1 công cụ vô cùng hữu ích và thiết thực trong đời sống hàng ngày cũng như công việc kinh doanh của doanh nghiệp. Bên cạnh đó tên miền thư điện tử cũng là đại diện thương hiệu cho 1 doanh nghiệp, 1 tổ chức, thể hiện sự chuyên nghiệp và tôn trọng khách hàng thay vì 1 địa chỉ mail cá nhân. Do đó việc xây dựng một hệ thống thư điện tử với tên miền riêng là rất quan trọng đối với 1 công ty, doanh nghiệp. Với hệ thống này nhà quản trị có thể tự quản lý các địa chỉ mail, truyền thông nội bộ vô cùng hiệu quả và an toàn bảo mật.Email Server – hay còn gọi là Máy chủ thư điện tử là máy chủ dùng để gửi và nhận thư điện tử, là một giải pháp Email dành cho các doanh nghiệp để quản lý và truyền thông nội bộ, thực hiện các giao dịch thương mại yêu cầu sự ổn định, tính liên tục và với tốc độ nhanh, đồng thời đảm bảo tính an toàn của dữ liệu, khả năng backup cao….Hệ thống thư điện tử Email server sẽ giải quyết được các vấn đề như mail bị virus, spam, bị đưa vào blacklist, không check được webmail, check online/offline, không thể kiểm soát nội dung…

- Thành phần FTP Server:

FTP là chữ viết tắt của File Transfer Protocol (Giao thức chuyển nhượng tập tin), đây là một giao thức giúp bạn dễ dàng trao đổi các dữ liệu giữa máy tính của bạn với host và ngược lại. Tại FTP, bạn sẽ có quyền quản lý toàn bộ các dữ liệu dạng tập tin và thư mục có trên host ngoại trừ database. Tất cả các gói host bạn mua có hỗ trợ control panel cPanel, DirectAdmin, … đều hỗ trợ sẵn FTP qua cổng kết nối 21.FTP có cơ chế xác thực nhưng không mã hóa trong lúc đăng nhập, cũng có thể không cần đăng nhập nếu được cấu hình cho phép như thế (anonymous). Để kết nối vào FTP trên host bạn cần phải sử dụng một ứng dụng chuyên làm việc này, nó được gọi là FTP Client. Hiện nay, bạn có thể sử dụng phần mềm FileZila vì đây là FTP Client miễn phí tốt nhất hiện tại, hỗ trợ hầu hết mọi hệ điều hành hiện nay.

Tất cả server dịch vụ phía trên bọn em xây dựng lên nhằm mục đích đưa ra một hệ thống server farm khá hoàn chỉnh và giống thực tế nhất phục một số nghiên cứu sau này trên các loại hình tấn công khác.

Tài nguyên cấp phát và dịch vụ cài trên các máy ảo chi tiết ở dưới bảng sau:

Bảng 5.2 Chi tiết cấu hình hệ thống server farm

Tên thành phần	Hệ điều hành	Gói dịch vụ	Cấu hình
Web server	Ubuntu server 16.04	Apache	• 4 GB Ram • 4 VCpu
DNS server	Ubuntu server 16.04	Bind9	• 4 GB Ram • 4 VCpu
FTP server	Ubuntu server 16.04	ProFTPD	• 4 GB Ram • 4 VCpu
Mail server	Ubuntu server 16.04	Mdaemon	• 4 GB Ram • 4 VCpu

5.2.2 Khối Gateway SDN:

Khối Gateway SDN là khối chịu trách nhiệm trực tiếp chuyển tiếp các gói tin từ hệ thống mạng bên ngoài vào bên trong mạng nội bộ Server Farm .Công nghệ chuyển mạch được sử dụng ở đây là SDN (software define networking), các thuật toán xử lý dữ liệu, phát hiện tấn công, đưa ra chính sách giảm thiểu ngăn chặn tấn công sẽ được khối này thực hiện có thể khối này chính là khối mang nhiều ý nghĩa nhất trong đồ án này.

Khối Gateway SDN sẽ gồm 2 phần chính đó là: khối chuyển mạch switch và khối điều khiển controller. Sau nhiều khảo sát các công nghệ chúng em đưa ra các so sánh và quyết định lựa chọn sử dụng chuyển mạch openvswitch, khối điều khiển sử dụng floodlight controller vì dễ sử dụng và dễ phát triển thêm các chức năng, thực hiện các thuật toán xử lý dữ liệu thống kê. Ngoài ra trong khối này còn trình bày thêm về công cụ đo đạc băng thông sflow để tiến hành lấy kết quả.

a. Openvswitch [12]

❖ Tổng quan về OpenvSwitch

OpenvSwitch còn gọi tắt là OVS là multilayer software switch được cấp giấy phép bởi Apache2. OVS được thiết kế tương thích với Switch hiện đại. Open vSwitch là software switch, một trong ba công nghệ cung cấp switch ảo trong hệ thống Linux-based (bên cạnh Linux bridge và Macvlan), giải quyết các vấn đề ảo hóa network bên trong các máy vật lý. OpenvSwitch hỗ trợ công nghệ ảo hóa trên Linux-based bao gồm: Xen/XenServer, KVM (Kernel-based Virtual Machine) và VirtualBox.

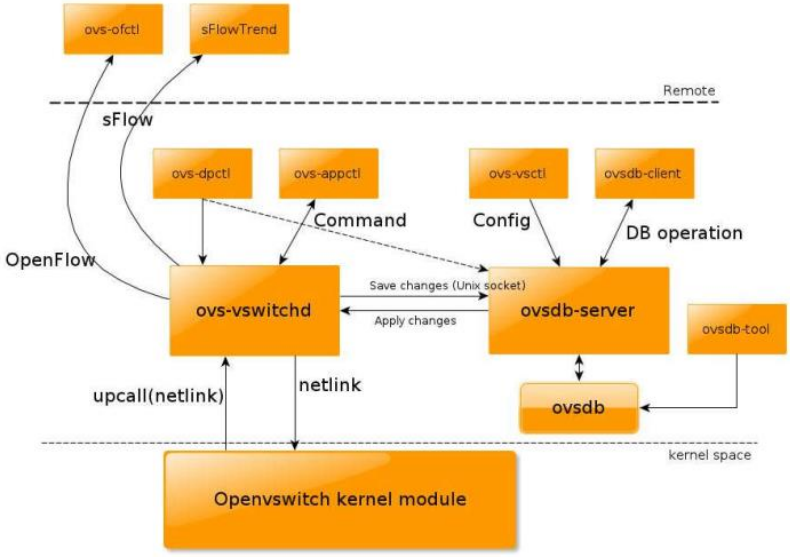
❖ Một số tính năng của OVS

Open vSwitch được dùng ngôn ngữ C là chủ yếu để viết, độc lập với nền tảng và dễ dàng di chuyển giữa các môi trường. Với các phiên bản mới, vừa ra đời gần đây có hỗ trợ các tính năng như sau đây:

- Hỗ trợ tính năng VLAN chuẩn 802.1q với các cổng Trunk, cổng Access

- Hỗ trợ NIC bonding (network interface card bonding) có hoặc không có LACP trên cổng uplink switch
- Hỗ trợ Netflow, sFlow(R) và mirroring để tăng khả năng hiển thị
- Hỗ trợ cấu hình QoS (quality of Service) và các chính sách khác
- Hỗ trợ tạo tunnel Geneve, GRE, VXLAN, STT, và LISP
- Hỗ trợ chuẩn 802.1ag connectivity fault management
- Hỗ trợ OpenFlow 1.0 trở lên
- Cấu hình cơ sở dữ liệu bằng ngôn ngữ C và Python
- Hiệu suất forwarding cao sử dụng module trong nhân Linux

❖ Các thành phần của OVS



Hình 5.3: Các thành phần của OVS

❖ Một số các thành phần chính của Open vSwitch có thể liệt kê như ở dưới đây

- ovs-vswitchd là một daemon switch thực thực hiện các chức năng chuyển mạch với module của nhân Linux phục vụ cho flow-based switching
- ovsdb-server là database của Open vSwitch mà ovs-vswitchd truy vấn để lấy cấu hình
- ovs-dpctl là một công cụ để cấu hình switch kernel module
- ovs-vsctl là công cụ thực hiện truy vấn và cập nhật các cấu hình của ovsvswitchd

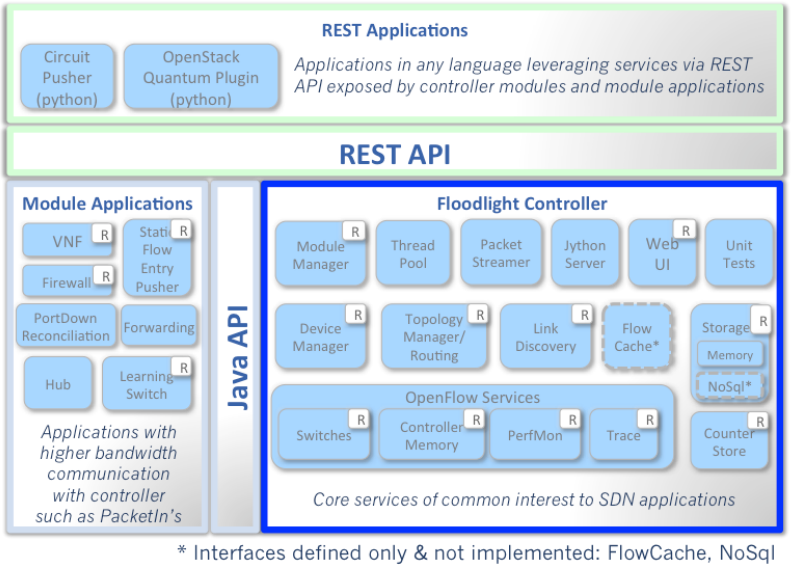
- ovs-appctl, là công cụ để gửi câu lệnh để chạy Open vSwitch daemons
- ovs-ofctl, là công cụ để truy vấn và điều khiển OpenFlow switches và controllers
- ovs-pki, là công cụ để tạo và quản lý public-key infrastructure của OpenFlow switches

b. SDN controller

- Floodlight controller [13] là gì?

- Là SDN controller dựa trên nền tảng mã nguồn mở đươc phát triển bởi nhóm BigSwitch Network.
- Được viết bằng ngôn ngữ java
- Hỗ trợ giao thức OpenFlow
- Cho phép người phát triển có thể viết ứng dụng cho Floodlight controller dựa trên các API (application programming interface) mà nó cung cấp.

- Kiến trúc của Floodlight controller



Hình 5.4: Kiến trúc của floodlight controller

- Một số module chính

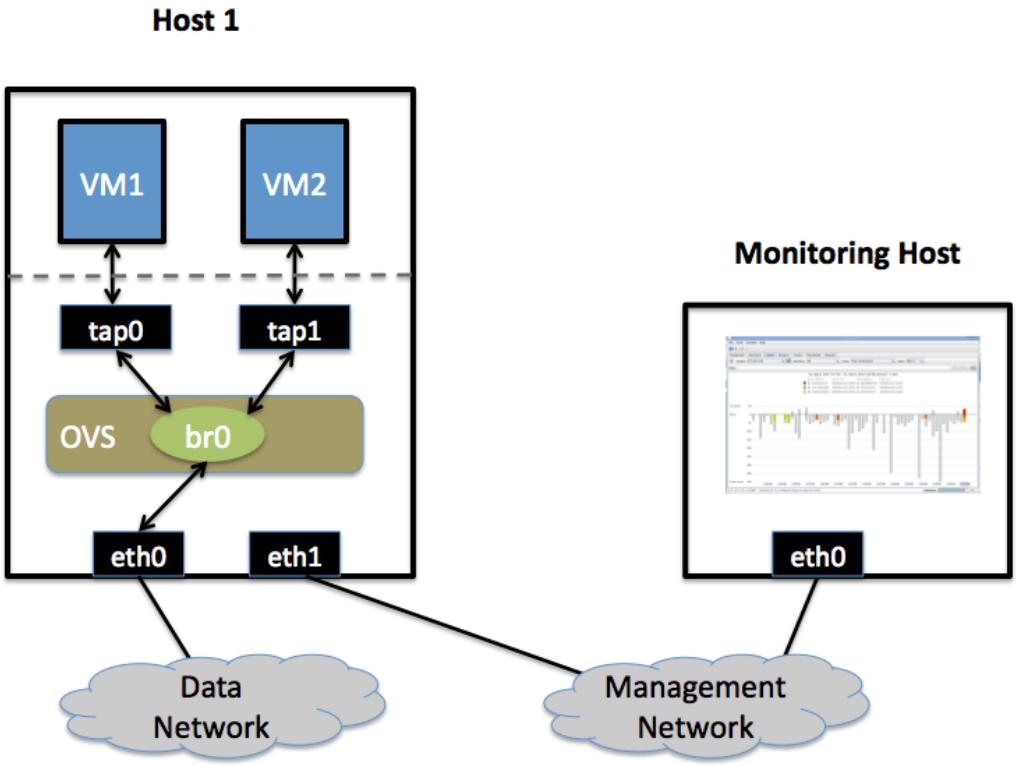
➢ Floodlight Provider: Nó xử lý các kết nối đến switch là và biến các message của giao thức OpenFlow thành các sự kiện để các module khác có thể lắng nghe là xử lý và quyết định thứ tự các bản tin OpenFlow được gửi đến các module khác. Các module có thể chuyển sang các module khác hoặc có thể xử lý gói tin luôn.

➢ Forwarding: Khi có một gói tin mới đi đến SDN switch thì module này có chức năng hướng dẫn SDN switch chuyển tiếp gói tin theo cổng nào của switch để gói tin có thể đi đến đích bằng cách thêm một Flow entry vào bảng Flowtable của SDN switch.

➢ Link Discovery Manager: Chức năng chính của module này là phát hiện và cập nhật topology của mạng khi có thay đổi. Để phát hiện sự thay đổi trong mạng thì SDN switch sẽ gửi đi một trong hai bản tin LLDP (Link layer discovery protocol) hoặc broadcast packet. Với bản tin LLDP thì địa chỉ MAC đích là 01:80:c2:00:00:0e còn bản tin broadcast thì MAC đích sẽ là ff:ff:ff:ff:ff:ff . Một liên kết trực tiếp sẽ được thiết lập nếu một bản bản tin LLDP được gửi đi trên một cổng và nhận lại một bản tin LLDP giống bản tin gửi đi trên một cổng khác.

c. Công cụ sflow [14]:

Công cụ sflow là một công cụ mã nguồn mở cho phép thống kê băng thông trên các thiết bị mạng, cho phép cài như một agent lên openvswitch để thuận tiện giám sát lưu lượng từ xa. Dưới đây là mô hình chúng em sử dụng tham khảo



Hình 5.5: Mô hình sử dụng sflow giám sát lưu lượng trên openvswitch

5.2.3 Khối Traffic Generator:

Khối Traffic Generator có nhiệm vụ phát lại lưu lượng mạng đi vào một Server farm một cách chính xác nhất có thể bao gồm cả lưu lượng thường (lưu lượng người dùng) và lưu lượng tấn công (đã được tạo ra nhờ các công cụ ở chương trước). Với sự trợ giúp của giảng viên hướng dẫn bọn em đã có một file lưu lượng thường từ bộ công an, kết hợp với file pcap lưu lượng tấn công tạo ở trên, chúng em phát đồng thời hai loại lưu lượng này với nhau để thử nghiệm lên mô hình này.

Khi thực hiện việc giả lập để tạo lưu lượng mạng các vấn đề cần được quan tâm như là công cụ thực hiện có khả năng tạo lưu lượng lớn, có khả năng phát lại các file pcap giống với thực tế (như có đủ số lượng gói tin, timestamp…). Vì vậy, công cụ mà chúng

em sử dụng đó là Traffic Generator đồng thời cũng sử dụng thêm công cụ TCP-Replay để phát lại file pcap.

- Sơ lược về Traffic Generator.
  - Model: CT503-MIX.
  - Hình ảnh về máy:

Hình 5.6: Traffic Generator

  - Thông số kỹ thuật của Traffic Generator.
    - High-End Intel Multi-Core 2U rackmount server.
    - Hệ điều hành: Fedora Linux.
    - Vi xử lý Intel Quad-Core.
    - 16GB RAM
    - Ổ cứng SSD 120GB.
    - Điện hoạt động: 100-240VAC, 50-60Hz, 7-3Amps.
    - Các cổng NIC bao gồm: 4-port 10/100/1000 copper, 2-port 10/100/1000 copper, 2-port 1Gbps fiber, 2-port 10Gbps fiber, 2-port 10Gbps copper (CX4).

❖ Tổng quan

- CT503-MIX bao gồm một hệ thống LF1011 2U với 12 SFP 1Gbps và 2 giao diện SFP+Ethernet 10Gbps.
- Máy có thể phát và nhận với tốc độ khoảng 24Gbps.
- Máy hỗ trợ chuẩn VGA, bàn phím, chuột để dễ dàng truy cập, điều khiển và kết nối với màn hình vào hệ thống.
- Quản lý hệ thống bằng một phần mềm là LANforge-GUI.

➢ Sơ lược về TCP-Replay

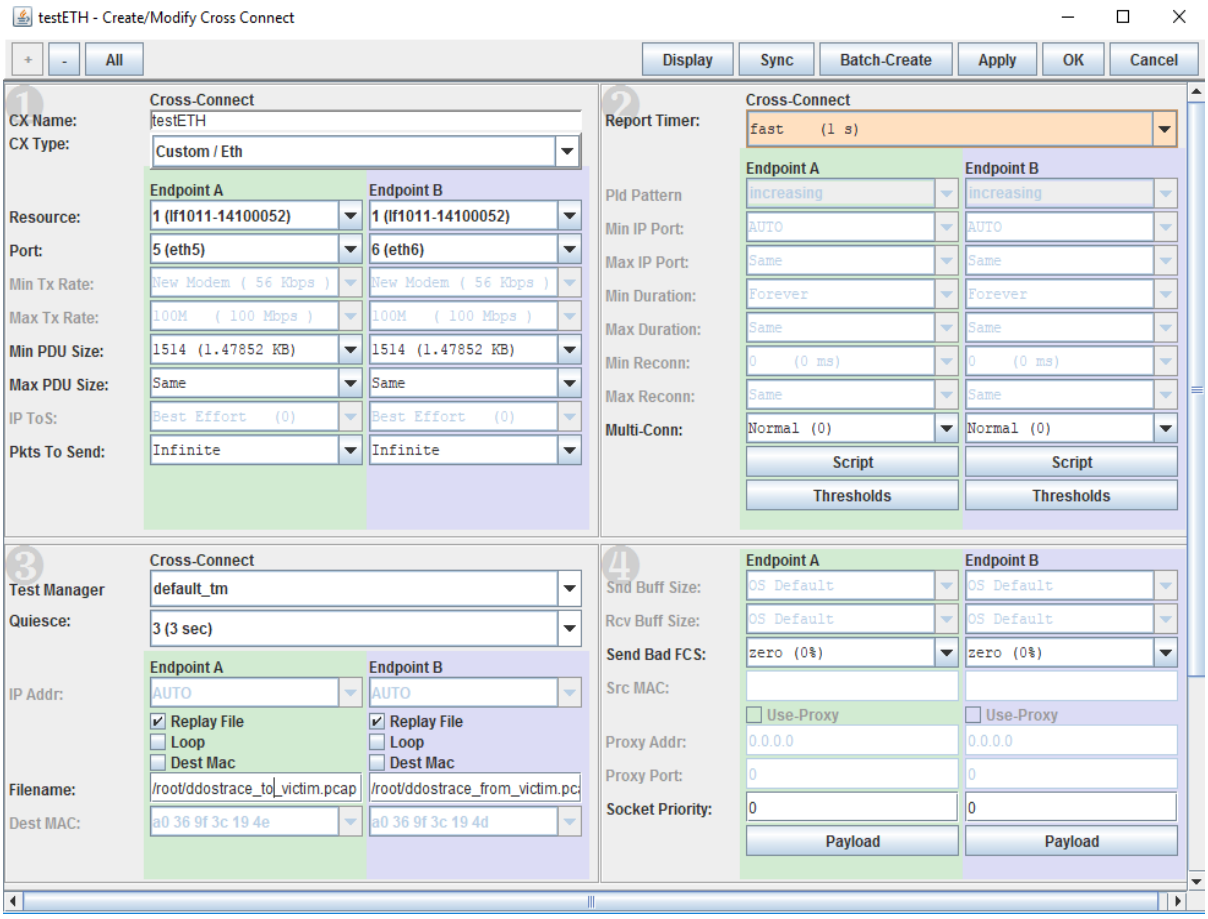
❖ Tcpreplay (Transmission Control Protocol Replay) là một mã nguồn mở và các dự án phần mềm miễn phí được thực hiện trong C và được thiết kế để hoạt động như một công cụ dòng lệnh đó bao gồm một số tiện ích cho hệ điều hành * NIX, cho phép người sử dụng để kiểm tra một loạt các thiết bị mạng bằng cách sử dụng qua các thư viện libpcap.

❖ TCP-Replay được cấp phép của GPLv3 cho hệ đều hành UNIX để chỉnh sửa và phát lại lưu lượng mạng mà trước đó được bắt lại bằng các công cụ như tcpdump, Ethereal/Wireshark.

➢ Quá trình phát lại file .pcap

❖ Cấu hình trên Traffic Generator.

Giao diện chính khi truy cập vào Traffic Generator



Hình 5.8: GUI chính của Traffic Generator

❖ Các thông số cơ bản trên Lanforge GUI.

✓ **CX Name**: tên nhận diện trong cấu hình LANforge.

✓ **CX Type**:

- **Ethernet**: kiểm tra gói tin bình thường ở mức Ethernet, nó hiển thị nhiều loại lỗi lớp Link.
- **Custom Ethernet**: Xác định đúng kích thước bytes để truyền vào dây Ethernet, bao gồm cả Ethernet header. LANforge có thể phát lại các gói tin mà được bắt bởi LANforge-ICE, Wireshark (định dạng file pcap). Khi chọn vào replay thì

LANforge đóng gói chính xác như file pcap bao gồm Ethernet header, tốc độ truyền…

- **UDP**: dùng trong các giao thức thời gian thực, video, music.
- **UDP6**: tương tự như UDP nhưng dùng IPv6.
- **Custom UDP**: cho phép thiết lập chính xác kích thước gói tin UDP.
- **TCP**: Tạo kết nối bằng cách bắt tay 3 bước, truyền lại gói tin bị drop.
- **TCP6**: tương tự như TCP nhưng dùng cho IPv6.
- **Custom TCP**: cho phép thiết lập chính xác kích thước gói tin gửi qua kết nối TCP/IP.
- **SCTP**: một giao thức với sự kết hợp các tính năng tương tự từ UDP và TCP.
- **SCTP6**: tương tự như SCTP nhưng dùng cho IPv6.
  - ✓ **Report Timer**: chỉ định tuần suất các máy phát dữ liệu LANforge gửi thông tin cập nhật đến máy chủ LANforge.
  - ✓ **Test Manager**: sử dụng để phân biệt một hệ thống LANforge bởi nhiều người sử dụng. Việc để CX là *default_tm* là tốt.
  - ✓ **Quiesce**: Khi người dùng click vào button 'quiesce' để ngăn chặn một test, thay vì chỉ 'Stop'. LANforge sẽ dừng Endpoint truyền và chờ đợi số giây lựa chọn rồi mới bắt đầu phát tiếp.
  - ✓ **Filename**: Chỉ ra đường dẫn tới file pcap mà người sử dụng muốn phát đi.
  - ✓ Các thông số còn lại đều để ở chế độ mặc định.

❖ Thiết lập kết nối đầu cuối (Layer 3).

- ✓ **Resource**: Thiết bị đầu cuối.
- ✓ **Port**: Giao diện vật lý hoặc ảo mà liên kết với thiết bị đầu cuối.
- ✓ **Min Tx Rate**: tốc độ truyền tối thiểu mà Lanforge sẽ gửi đi (bit/s).
- ✓ **Max Tx Rate**: tốc độ truyền tối đa mà Lanforge sẽ gửi đi được (bit/s).
- ✓ **Min/Max PDU Size**: kích thước bản ghi tính bằng bytes và chỉ bao gồm các bytes mà giao thức được chọn. Ví dụ, khi lựa chọn gói tin có kích thước là 1472 byte cho kết nối UDP, thì Ethernet frame có chiều dài thực tế là 1514 bytes cộng thêm cả 14 bytes của Ethernet header.

- ✓ **IP ToS**: Dành cho các giao thức dựa trên IP và có thể chỉ định các bits ToS trong IP header. Việc này sẽ rất hữu ích cho việc kiểm tra chất lượng dịch vụ.
- ✓ **Pkts to Send**: Sẽ chỉ định số lượng gói tin gửi đi trước khi LANforge tự động quiesce các bài kiểm tra.
- ✓ **TTL**: xác định thời gian tồn tại khi cấu hình multicast endpoints.
- ✓ **Replay file**: Chọn tính năng này để phát lại file pcap dành cho kết nối Custom Ethernet.
- ✓ **Loop**: Sẽ phát lại file pcap nhiều lần cho tới khi người dùng muốn dừng.

➢ Phát lại file pcap sử dụng TCP-Replay.

❖ **Cách sử dụng cơ bản:** cho việc phát lại một file pcap và phát qua cổng 'eth0'.

$ *tcpreplay --intf1=eth0 sample.pcap*

❖ Ngoài ra còn có thể phát lại file pcap khác tốc độ trong file pcap gốc.

- ✓ Phát với tốc độ nhanh nhất có thể:

$ *tcpreplay --topspeed --intf1=eth0 sample.pcap*

- ✓ Phát với tốc độ là 10Mbps:

$ *tcpreplay --mbps=10.0 --intf1=eth0 sample.pcap*

- ✓ Phát với tiêu chí là 25 packets per second:

$ *tcpreplay --pps=25 --intf1=eth0 sample.pcap*

- ✓ Phát lại file pcap 10 lần:

$ *tcpreplay --loop=10 --intf1=eth0 sample.pcap*

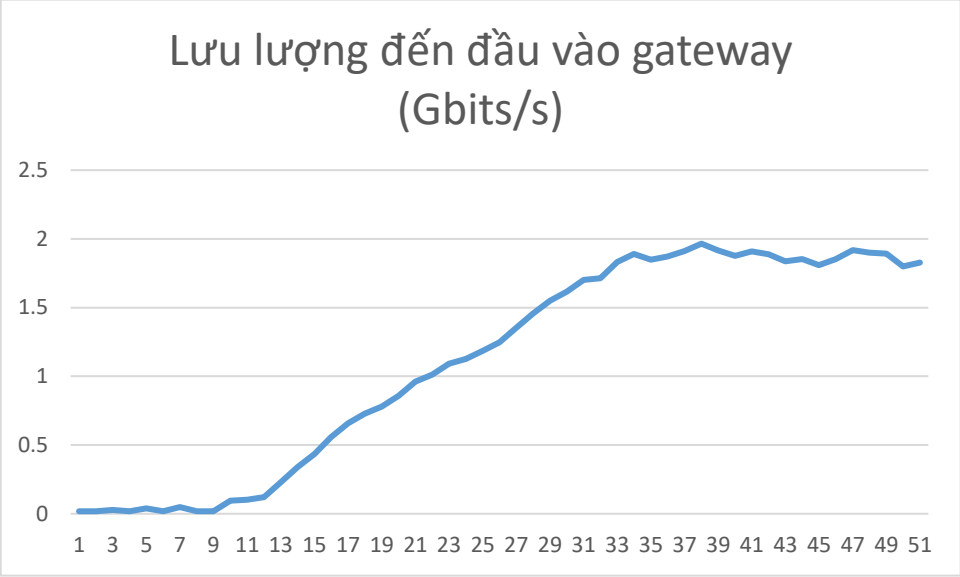
Với Traffic Generator Lanforge việc thực phát lưu lượng tấn công và lưu lượng thường trở nên dễ dàng và có thể phát đến nhiều hệ thống khác nhau sau này.

5.3 Phân tích đánh giá kết quả

Sau khi xây dựng mô hình thử nghiệm thành công, nhóm chúng em tiến hành đo đạc và kiểm nghiệm mô hình cụ thể ở đây chúng em sử dụng Traffic Generator phát lưu lượng thường vào hệ thống trước sau đó tiến hành phát lượng tấn công ICMP flood vào hệ thống xây dựng phía trên với thuật toán Fuzzy Logic được thực hiện trên controller Floodlight.

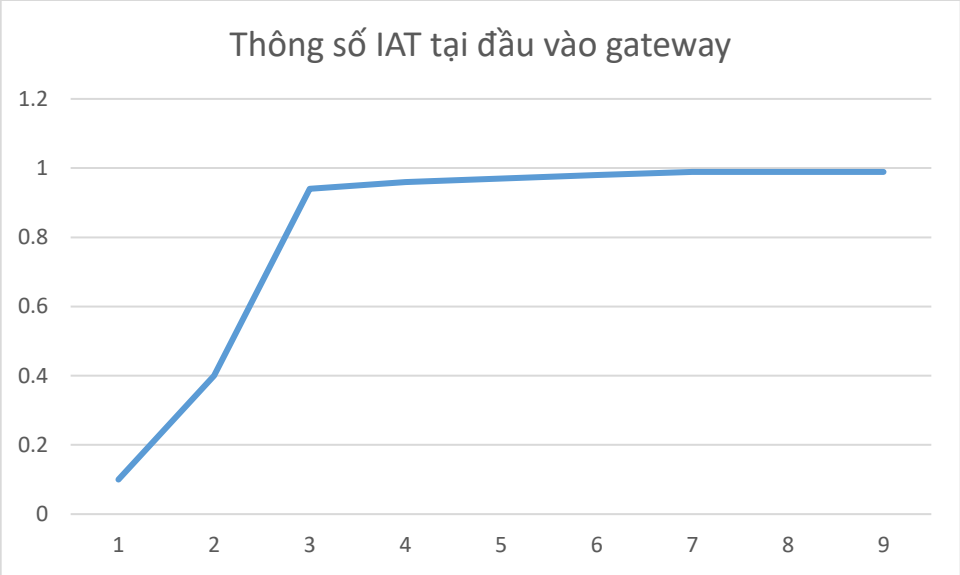
Sau đây chúng em xin ra kết quả đo trên đầu vào và đầu ra của gateway nhằm mục đích kiểm tra tính đúng đắn của hệ thống.

- Kết quả tại đầu vào gateway

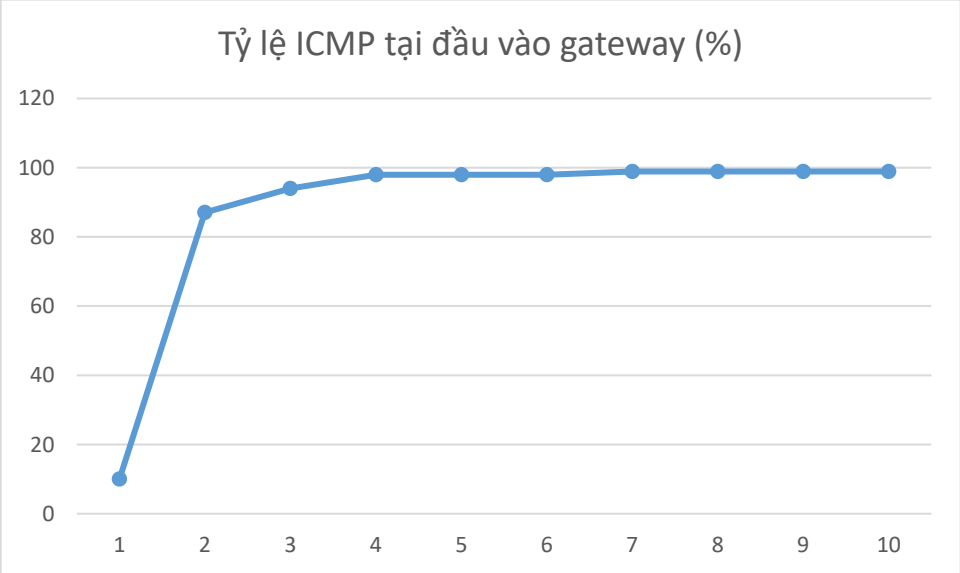


Hình 5.9 Lưu lượng đo tại đầu vào gateway

Vì lưu lượng thường so với lưu lượng tấn công tại đầu vào gateway là rất ít nên việc nhận biết lưu lượng thường bằng mắt thường trên đồ thị khá là khó khăn nhưng ta có thể nhận thấy rõ băng thông đang tăng dần theo thời gian.



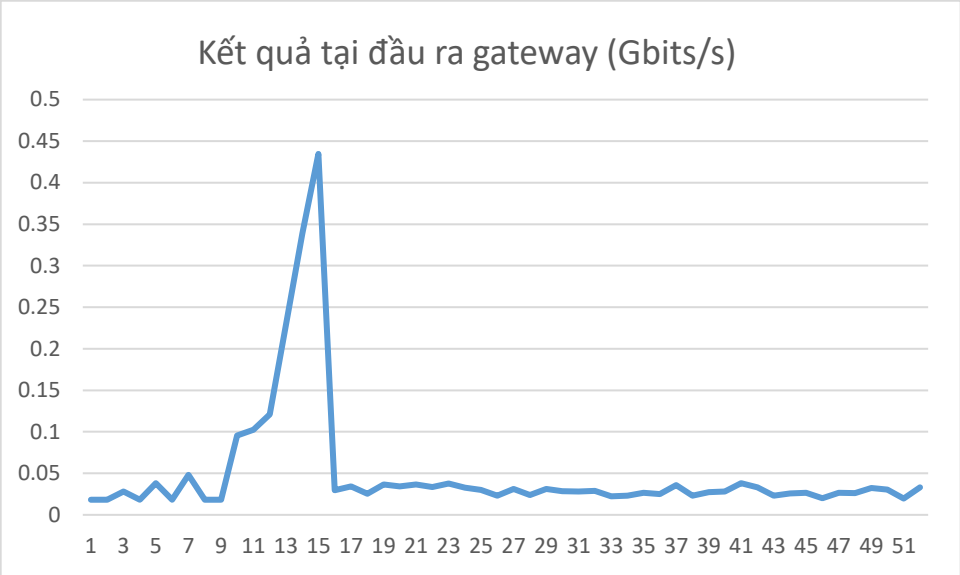
Hình 5.10 Thông số IAT tại đầu vào gateway



Hình 5.11 Tỷ lệ ICMP tại đầu vào gateway

Số IAT và tỷ lệ ICMP được thống kê 5 giây một lần cũng phản ánh rõ ràng việc số lượng gói đến rất nhanh và bị nghi ngờ tấn công tại giây thứ 15 do IAT và tỷ lệ ICMP đã gần xấy xỉ 1.

➢ Kết quả tại đầu ra gateway

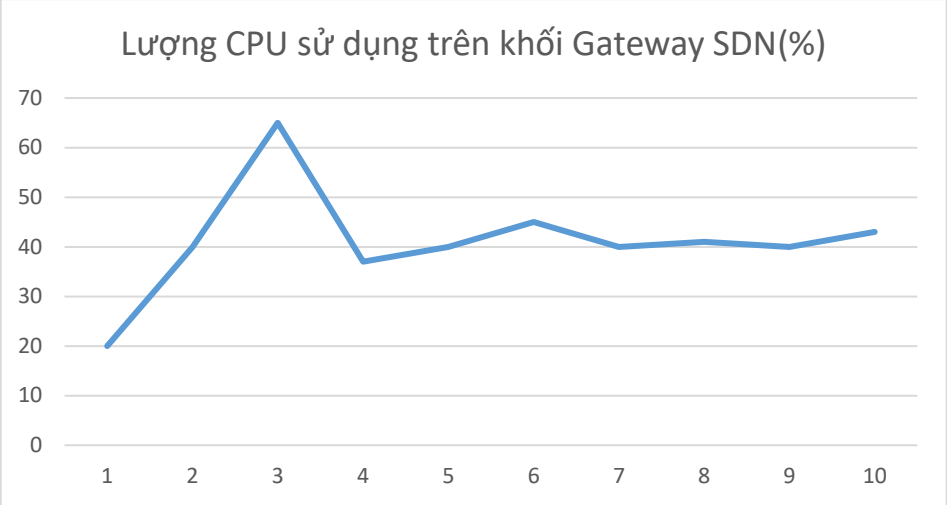


Hình 5.12 Lưu lượng tại đầu ra gateway

Sau khi chúng em áp dụng thuật toán Fuzzy logic based và áp dụng các chính sách đã được trình bày trong Chương 3 thì chúng em nhận được kết quả như Hình 5.14. Chính sách mà chúng em đã áp dụng ở đây là chặn tất cả các luồng ICMP trong vòng 5s.

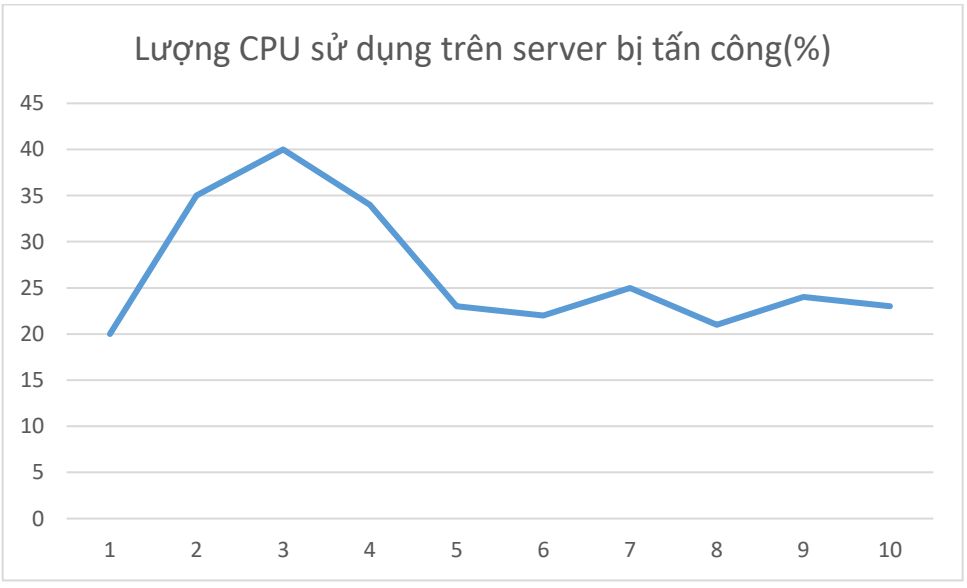
Lưu lượng đầu ra cho thấy việc lưu lượng giảm đột ngột chứng tỏ khối controller đã can thiệp vào việc chuyển phát gói tin bằng cách chặn những luồng ICMP bị coi là tấn công đến gateway các luồng lưu lượng thường vẫn đi qua bình là các khoảng nhỏ phía sau do lưu lượng ít hơn nhiều so với lưu lượng tấn công. Kết luận hệ thống đã hoạt động một cách chính xác và hiệu quả, dưới dây là hình ảnh thực tế lưu lượng đi qua gateway sử dụng công cụ giám sát sflow.

Ngoài ra để đánh giá thêm hiệu quả nhóm chúng em đánh giá thêm các thông số trên khối gateway SDN và phía web server nạn nhân.



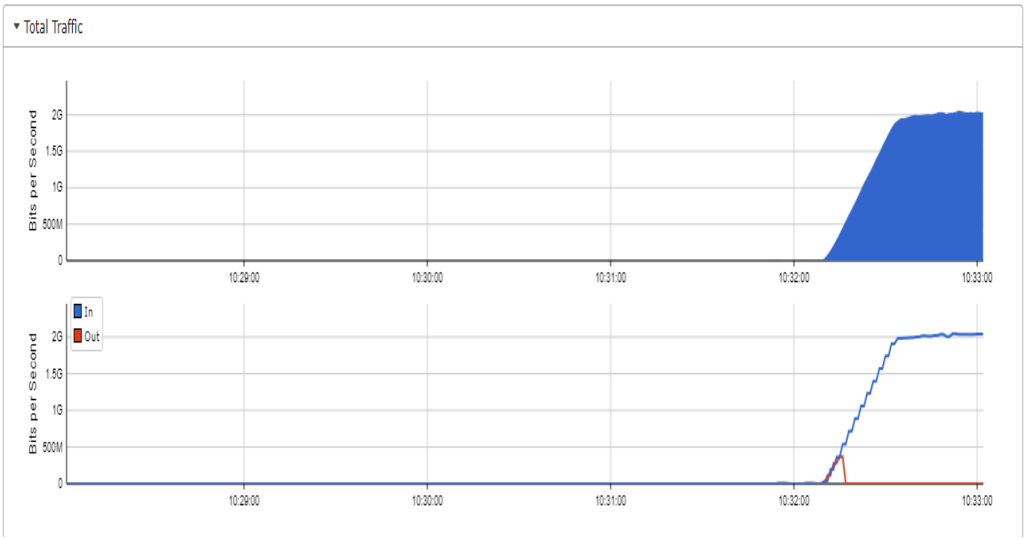
Hình 5.13. Lượng CPU sử dụng trên khối Gateway SDN (%)

Khối Gateway SDN bao gồm cả controller vào openvswicth trên cùng một máy nên có thể thấy khi lượng gói tin đến lớn openvswicth sẽ gửi một lượng lớn request lên hỏi controller về việc chuyển tiếp gói tin nên lượng CPU sử dụng tăng lên, sau đó việc loại bỏ các gói tin được áp đặt lên openvswitch được đặt cùng trên controller nên việc này cũng chiếm một lượng CPU nhất định.



Hình 5.14. Lượng CPU sử dụng trên server bị tấn công

Mặc dù mục đích chính không phải tấn công vào tài nguyên CPU nhưng do sử phải đáp trải quá nhiều request ICMP một lúc làm cho server phải tiêu tốn một lượng tài nguyên.



Hình 5.15: Sử dụng công cụ giám sát sflow hiển thị lưu lượng trên gateway

Nhìn hình trên, ta có thể thấy lưu lượng đi vào là đường màu xanh da trời vọt lên rất cao và nhanh còn lưu lượng đi ra là đường màu đỏ nhờ sự can thiệp của controller nên các lưu lượng bị coi là tấn công bị ngăn chặn không cho đi qua.

5.4 Hướng phát triển

➢ Hệ thống thử nghiệm :

- Hệ thống thử nghiệm mô phỏng gần chính xác những gì của một tấn công xảy ra.
- Việc phát hiện tấn công và đưa ra chính sách giảm thiểu là nhanh chóng kịp thời. Tuy nhiên, với khoảng cách 5s lấy thông số một lần vẫn cần phải thử nghiệm thêm để có thể phát hiện tốt hơn nữa.
- Hệ thống đưa ra là nền tảng để đưa nhiều loại thuật toán khác vào.
- Hướng phát triển: Mở rộng mô hình giám sát trên nhiều gateway hoặc switch để đưa các phát hiện sớm và chính xác hơn.

➢ Thuật toán :

- Thuật toán phát hiện tấn công nhanh và hiệu quả.
- Các thông số đưa vào thuật toán còn phụ thuộc nhiều vào dataset
- Hướng phát triển: giúp thuật toán thông minh hơn khi kết hợp với một số thuật toán học máy khác để phát hiện nhiều loại tấn công khác.

KẾT LUẬN CHUNG

Trong thời đại bùng nổ công nghệ thông tin như hiện nay, khi mà mỗi ngày có hàng tỉ thiết bị đang kết nối vào mạng Internet toàn cầu thì thách thức trước vấn đề bảo mật nói chung ngày càng gia tăng trở thành vấn để không của riêng cá nhân tổ chức nào. Một trong những vấn đề bảo mật nổi cộm đó là tấn công DDoS với cơ chế đơn giản nhưng hiệu quả, dù không đánh cắp dữ liệu nhưng lại có thể gây thiệt hại lớn về kinh tế và uy tín cho các doanh nghiệp bằng cách làm từ chối dịch vụ do doanh nghiệp cung cấp. Nhận thấy những thách thức đó, chúng em đã tìm cách xây dựng một hệ thống phát hiện tấn công DDoS dựa trên những ưu điểm vượt trội của nền tảng SDN. Mục đích xây dựng một hệ thống thử nghiệm thực cho việc thử nghiệm khả năng phát hiện tấn công DDoS thực tế của thuật toán và sự linh động trong việc giảm thiểu tấn công của công nghệ SDN. Đề tài đã đưa ra một hệ thống thử nghiệm thực tế cho việc thử nghiệm mô phỏng tấn công Ddos từ đó có thể đưa các thuật toán phát triển vào để so sánh, đồng thời đã đưa ra các biện pháp ngăn chặn tấn công cách lấy những thông số và xử lí dữ liệu . Tuy nhiên, trong quá trình thực hiện đề không thể tránh được những thiếu sót như:

- Bản OpenFlow còn ở version thấp hạn chế tính năng
- File dataset còn đơn giản, chưa cập nhật
- Các OpenFlow Switch cài trên các máy tính nên chưa đạt tối đa hiệu năng
- Công cụ phát gói chưa đạt được tốc độ tối đa như trong file dataset
- Các thuật toán chạy chưa tối ưu tối đa tham số cần tìm

Những thiếu sót này có thể sẽ trở thành những khía cạnh cho việc tiếp tục nghiên cứu phát triển tiếp theo.

TÀI LIỆU THAM KHẢO

[1] DDoS surviral handbook [Online]. https://security.radware.com/uploadedfiles/resources_and_content/ddos_handbook/ddos_handbook.pdf

[2]https://viettelidc.com.vn/bao-cao-tan-cong-tu-choi-dich-vu-ddos-quy-3-2017-tren-the-gioi.html, truy cập lần cuối 25/05/2018.

[3] https://overlaid.net/2017/02/15/openflow-basic-concepts-and-theory/, truy cập lần cuối 25/05/2018.

[4] http://flowgrammable.org/sdn/openflow/message-layer/statsrequest/ , truy cập lần cuối 25/05/2018

[5] Phan Van Trung, Truong Thu Huong, Dang Van Tuyen, Duong Minh Duc, Nguyen Huu Thanh, "A multi-criteria-based DDoS-attack prevention solution using software defined networking", International Conference on Advanced Technologies for Communications, pp.308 – 313, 2015.

[6]M. Sugeno, Industrial Applications of Fuzzy Control. Elsevier, 1985.

[7] https://www.caida.org/data/passive/ddos-20070804_dataset.xml , truy cập lần cuối 25/06/2018

[8] https://github.com/Markus-Go/bonesi , truy cập lần cuối 25/05/2018

[9] http://wanem.sourceforge.net , truy cập lần cuối 25/05/2018

[10]http://wwwwanmon.slac.stanford.edu/cgiwrap/pingtable.pl?file=throughput&by=bysite&size=100&tick=monthly&from=S.E.+Asia&to=Vietnam&ex=none&only=all&dtaset=hep&pecentage=any, truy cập lần cuối 25/05/2018

[11] https://www.candelatech.com/ , truy cập lần cuối 25/05/2018

[12] http://www.openvswitch.org/ , truy cập lần cuối 25/05/2018

[13]https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/1343542/Getting+Started , truy cập lần cuối 25/05/2018

[14] http://docs.openvswitch.org/en/latest/howto/sflow/ , truy cập lần cuối 25/05/2018

PHỤ LỤC

Phân công công việc trong đồ án

	Họ và tên	Công việc
1	Vương Bá Nam	• Xử lý lấy dữ liệu từ controller • Lấy thông tin lưu lượng từ Switch • Xây dựng các biện pháp giảm thiểu tấn công trên SDN Controller
2	Nguyễn Mạnh Quyền	• Phân tích CAIDA • Mô phỏng dữ liệu tấn công • Xây dựng Traffic Generator ,Gateway SDN ,Server Farm