HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
*****

TRẦN QUỐC TRUNG

GIẢI PHÁP CHỐNG TẤN CÔNG TRONG MẠNG ĐỊNH NGHĨA BẰNG PHẦN MỀM

Chuyên ngành : Kỹ thuật viễn thông
Mã số: 8.52.02.08

TÓM TẮC LUẬN VĂN THẠC SĨ

Hà Nội – 2019

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

TS. NGÔ ĐỨC THIỆN

Phản biện 1:

Phản biện 2:

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn Thạc sĩ tại Học viện Công nghệ Bưu chính Viễn Thông.
Vào lúc:..... giờ ..... ngày ..... tháng .... năm .....

.

Có thể tìm hiểu luận văn tại:

1. Thư viện Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

1. Lý do chọn đề tài

Với sự phát triển không ngừng của Internet ngày nay, nhu cầu mở rộng mạng ngày càng tăng, đòi hỏi về số lượng các thiết bị mạng ngày càng lớn, từ đó kiến trúc mạng truyền thống đã bộc lộ ra nhiều khuyết điểm. Sự phức tạp trong hệ thống, khả năng mở rộng mạng kém, chính sách không nhất quán, chi phí triển khai tốn kém, nhiều điểm yếu về bảo mật.

Nhu cầu đặt ra cần có một kiến trúc mạng đảm bảo được sự tích hợp linh hoạt, kết hợp với các giải pháp bảo mật an toàn cho hệ thống. Chính vì vậy, công nghệ mạng định nghĩa bằng phần mềm (SDN) ra đời như một giải pháp cho hệ thống mạng trong tương lai. Bên cạnh đó, SDN còn là lựa chọn cho việc triển khai các giải pháp đảm bảo an ninh mạng, trước sự phức tạp của những cuộc tấn công không ngừng thay đổi về cách thức cũng như độ nguy hại, cản trở nhiều hoạt động giao dịch, các dịch vụ mạng.

Những hạn chế về bảo mật của kiến trúc mạng truyền thống đã để lộ ra những lỗ hổng cho kẻ tấn công, những tổ chức tội phạm có thể thực hiện hành vi phá hoại tới những hệ thống, gây hậu quả cho các doanh nghiệp, cơ quan, tổ chức, các nhà cung cấp dịch vụ. Vì lý do đó em xin chọn đề tài "*Giải pháp chống tấn công trong mạng định nghĩa bằng phần mềm*" làm đề tài luận văn tốt nghiệp.

2. Tổng quan về vấn đề nghiên cứu

SDN ra đời vào năm 2008 tại Đại học Stanford và tạo ra một cuộc cách mạng trong giới công nghệ. Ưu điểm của SDN là việc tách phần logic điều khiển mạng khỏi các bộ chuyển mạch, thúc đẩy điều khiển tập trung và cung cấp khả năng lập trình cho mạng. Hiện tại, Google và Facebook đều đầu tư rất mạnh cho SDN và dự đoán trong 5 năm tới sẽ thay thế toàn bộ mạng truyền thống.

Vấn đề nghiên cứu về mạng SDN được nghiên cứu rộng rãi trên thế giới trong những năm gần đây. Từ nhiều năm trở lại đây, đã có các bài báo trên thế giới đã đưa ra rất nhiều giải pháp nhằm nâng cao hiệu quả cho quá trình sử dụng mạng Internet.

Trong đó SDN là một trong những giải pháp được kỳ vọng cao. Tại Việt Nam, đã có các công trình nghiên cứu và áp dụng SDN vào việc thiết kế và áp dụng cho việc điều khiển mạng.

Luận văn sẽ nghiên cứu về công nghệ SDN/OpenFlow, các ưu điểm mà SDN cung cấp so với cấu trúc mạng truyền thống. Bên cạnh đó tìm hiểu các hình thức tấn công SDN và cách phòng chống các hình thức tấn công này. Từ đó đưa ra phương thức phòng chống tấn công dựa trên công nghệ SDN/OpenFlow.

3. Mục đích nghiên cứu

Nghiên cứu các phương pháp phòng chống tấn công SDN và áp dụng công nghệ SDN/OpenFlow vào việc phòng chống tấn công, nâng cao bảo mật.

4. Đối tượng và phạm vi nghiên cứu

Đối tượng: Công nghệ mạng định nghĩa bằng nội dung (SDN).

Phạm vi: Phòng chống tấn công trong SDN dựa trên SDN/OpenFlow.

5. Phương pháp nghiên cứu

Nghiên cứu tìm hiểu lý thuyết từ các tài liệu, bài báo, công trình nghiên cứu về SDN và tấn công trong SDN. Xây dựng một kiến trúc mạng sử dụng trong phòng chống tấn công SDN, tiến hành mô phỏng tấn công trên server testbed của Mobifone, sử dụng các card phần cứng và phầm mềm, công cụ hỗ trợ. Dựa trên kết quả mô phỏng đưa ra giải pháp giảm thiểu các tấn công vào SDN.

6. Nội dung đề tài

Nội dung của luận văn bao gồm 3 chương với cấu trúc như sau:

Chương 1. Tổng quan về SDN:

Chương 2. Xây dựng kiến trúc mạng SDN/OpenFlow sử dụng trong phòng chống tấn công

Chương 3. Kết quả mô phỏng chống tấn công trong SDN

CHƯƠNG 1. TỔNG QUAN VỀ SDN

1.1. Tổng quan về SDN

1.1.1. Định nghĩa

Software-Definded Networking (SDN) là một cách tiếp cận mới trong việc thiết kế, xây dựng và quản lý hệ thống mạng. Về cơ bản, SDN chia tách độc lập hai cơ chế hiện đang tồn tại trong cùng một thiết bị mạng: Cơ chế điều khiển (Control Plane *controller – thành phần điều khiển*), cơ chế chuyển tiếp dữ liệu (Data Plane - data forwarding plane – thành phần chuyển tiếp dữ liệu) nhằm tối ưu nhiệm vụ và chức năng của hai thành phần này (Hình 1.1). Mục đích của sự phân tách này là tạo ra mạng có thể được lập trình và quản lý một cách tập trung.

SDN là một kiến trúc mạng linh hoạt, dễ quản lý, hiệu suất cao, khả năng chịu lỗi và thích nghi tốt,… Điều đó làm cho công nghệ này thật sự lý tưởng cho các ứng dụng đòi hỏi băng thông cao và cần sự linh hoạt hiện nay. Mục đích cơ bản của truyền thông mạng là truyền tải thông tin từ điểm này tới các điểm khác nhưng với SDN thì dữ liệu trong mạng sẽ được truyền tải giữa các node với sự hỗ trợ từ các ứng dụng và dịch vụ nên việc truyền thông trở nên hiệu quả và tối ưu hơn rất nhiều.

1.1.2. Kiến trúc của SDN

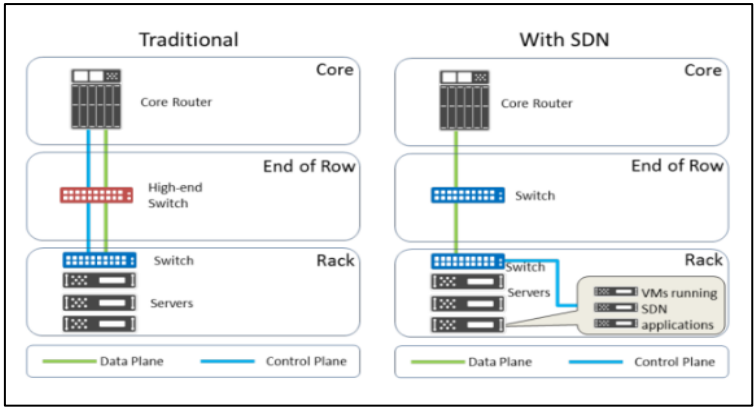
Kiến trúc của SDN gồm 3 lớp riêng biệt: lớp ứng dụng, lớp điều khiển, và lớp cơ sở hạ tầng (lớp chuyển tiếp).

Lớp ứng dụng: Là các ứng dụng kinh doanh được triển khai trên mạng, được kết nối tới lớp điều khiển thông qua các API, cung cấp khả năng cho phép lớp ứng dụng lập trình lại (cấu hình lại) mạng (điều chỉnh các tham số trễ, băng thông, định tuyến, …) thông qua lớp điều khiển.

Lớp điều khiển: Là nơi tập trung các bộ điều khiển thực hiện việc điều khiển cấu hình mạng theo các yêu cầu từ lớp ứng dụng và khả năng của mạng. Các bộ điều khiển này có thể là các phần mềm được lập trình.

Lớp cơ sở hạ tầng: Là các thiết bị mạng thực tế (vật lý hay ảo hóa) thực hiện việc chuyển tiếp gói tin theo sự điều khiển của lớp điều khiển. Một thiết bị mạng có thể hoạt động theo sự điều khiển của nhiều bộ điều khiển khác nhau, điều này giúp tăng cường khả năng ảo hóa của mạng.

1.1.3. So sánh kiến trúc mạng truyền thống và kiến trúc SDN



Hình 1.1. So sánh mạng SDN và mạng truyền thống

Mô hình so sánh giữa kiến trúc mạng truyền thống và kiến trúc SDN trên (hình 1.1) cho thấy trong kiến trúc mạng truyền thống Control Plane và Data Plane đều được ghép chung vào trong Network Node. Trong đó Control Plane có nhiệm vụ cấu hình các Node mạng và lập trình đường đi (định tuyến) để vận chuyển Data Flow. Data Flow (luồng dữ liệu) sẽ được đẩy xuống Data Plane thông qua các API và chuyển tiếp tới các thiết bị phần cứng dựa trên các thông tin điều khiển trên Control Plane.

Trong kiến trúc mạng truyền thống khi chính sách Forwarding đã được thông qua thì cách duy nhất để điều chỉnh lại các chính sách này theo ý muốn là phải đi cấu hình lại trên tất cả thiết bị vật lý (Switch, Router, Firewall, …). Điều này không chỉ mất thời gian mà còn khá là phiền toái bởi trong kiến trúc hệ thống mạng truyền thống đặc biệt đối với hệ thống mạng quy mô trong doanh nghiệp thì việc xác định vị trí thiết bị và tiến hành cấu hình điều chỉnh rất là phức tạp và có nhiều rủi ro sai sót có thể ảnh hưởng tới nhiều hoạt động quan trọng khác trong hệ thống mạng.

1.1.4. Lợi ích của SDN

SDN đem lại các lợi ích sau:

Giảm CapEx: SDN giúp giảm thiểu các yêu cầu mua phần cứng theo mục đích xây dựng các dịch vụ, phần cứng mạng trên cơ sở ASIC, và hỗ trợ mô hình pay-as-you-grow (trả những gì bạn dùng) để loại bỏ lãng phí cho việc dự phòng.

Giảm OpEx: thông qua các phần tử mạng đã được gia tăng khả năng lập trình, SDN giúp dễ dàng thiết kế, triển khai, quản lý và mở rộng mạng. Khả năng phối hợp và dự phòng tự động không những giảm thời gian quản lý tổng thể, mà còn giảm xác suất lỗi do con người tới việc tối ưu khả năng và độ tin cậy của dịch vụ.

Truyền tải nhanh chóng và linh hoạt: giúp các tổ chức triển khai nhanh hơn các ứng dụng, các dịch vụ và cơ sở hạ tầng để nhanh chóng đạt được các mục tiêu kinh doanh.

Cho phép thay đổi: cho phép các tổ chức tạo mới các kiểu ứng dụng, dịch vụ và mô hình kinh doanh, để có thể tạo ra các luồng doanh thu mới và nhiều giá trị hơn từ mạng.

1.1.5. Ứng dụng của SDN

- *Áp dụng trong mạng doanh nghiệp*: Mô hình tập trung, điều khiển và dự phòng tự động của SDN hỗ trợ việc hội tụ dữ liệu, voice, video, cũng như là việc truy cập tại bất kỳ thời điểm nào, bất kỳ đâu. Điều này được thực hiện thông qua việc cho phép nhân viên IT thực thi chính sách nhất quán trên cả cơ sở hạ tầng không dây và có dây. Hơn nữa, SDN hỗ trợ việc quản lý và giám sát tự động tài nguyên mạng, xác định bằng các hồ sơ cá nhân và các yêu cầu của ứng dụng, để đảm bảo tối ưu trải nghiệm người dùng với khả năng của mạng.
- *Áp dụng trong Data Center (DC)*: Việc ảo hóa các thực thể mạng của kiến trúc SDN cho phép việc mở rộng trong DC, di

cư tự động các máy ảo, tích hợp chặt chẽ hơn với kho lưu trữ, sử dụng server tốt hơn, sử dụng năng lượng thấp hơn, và tối ưu băng thông.

- *Áp dụng đối với dịch vụ Cloud*: Khi được sử dụng để hỗ trợ một môi trường đám mây riêng hoặc tích hợp, SDN cho phép các tài nguyên mạng được cấp phát theo phương thức linh hoạt cao, cho phép dự phòng nhanh các dịch vụ đám mây và hand off linh hoạt hơn với các nhà cung cấp đám mây bên ngoài. Với các công cụ để quản lý an toàn các mạng ảo của mình, các doanh nghiệp và các đơn vị kinh doanh sẽ tin vào các dịch vụ đám mây hơn.

1.2. Giao thức OpenFlow

1.2.1. Định nghĩa

OpenFlow là giao thức chuẩn mở cho phép các nhà nghiên cứu có thể thử nghiệm, kiểm chứng các giao thức mạng mới trong môi trường thực tế với quy mô lưu lượng thật, giúp cho việc học tập, nghiên cứu được dễ dàng và có thể kiểm nghiệm được mà không cần các thiết bị thật phức tạp. OpenFlow là giao thức giúp bộ điều khiển có thể giao tiếp, cấu hình, điều khiển các bộ chuyển mạch ở phía dưới, cung cấp một giao diện đồng nhất cho các thiết bị của nhiều hãng khác nhau có thể hoạt động được trên cùng một bộ điều khiển.

1.2.2. Kiến trúc của OpenFlow Switch

Một thiết bị chuyển mạch OpenFlow bao gồm ít nhất 3 thành phần: Bảng luồng (Flow table), Kênh an toàn (Secure Chanel) và Giao thức Openflow (OpenFlow Protocol).

1.2.3. Hoạt động của OpenFlow Switch

Giao thức OpenFlow mô tả bản tin trao đổi giữa OpenFlow Controller và một OpenFlow switch. Giao thức này được triển khai trên Secure Socket Layer (SSL) hoặc Transport Layer Security (TLS), cung cấp kênh OpenFlow bảo mật. Giao thức OpenFlow cho phép controller thực hiện các thao tác bổ sung, cập nhật và xóa các hành động vào các flow entry trong các flow tables.

1.3. Các bản tin trao đổi OpenFlow

1.3.1. Bản tin PacketIn

PacketIn là bản tin được gửi từ switch lên Controller. Có hai lý do để thực hiện điều này: Một gói tin match với một flow entry và flow entry đó có action gửi lên Controller hoặc một gói tin match với table_miss và trong table_miss có action là gửi lên Controller.

1.3.2. Bản tin PacketOut

Bản tin PacketOut được gửi từ Controller tới Switch dùng để hướng dẫn gói tin đi như thế nào trong mạng. Bản tin này không dùng để thiết lập entry trên Switch mà chỉ gửi gói tin ra ngoài Switch.

1.3.3. Bản tin FlowRemoved

FlowRemoved là bản tin được gửi tới Controller từ Switch khi có flow entry trong flow table bị xóa.

1.3.4. Bản tin FlowMod

Đây là một trong những bản tin chính hay được sử dụng giữa Controller và Switch. Nó được gửi từ Controller xuống Switch cho phép Controller sửa đổi trạng thái của Openflow Switch.

1.3.5. Bản tin StatsRequest

Bản tin StatsRequest được sử dụng để yêu cầu về thông tin của từng flow, từng table trên Switch.

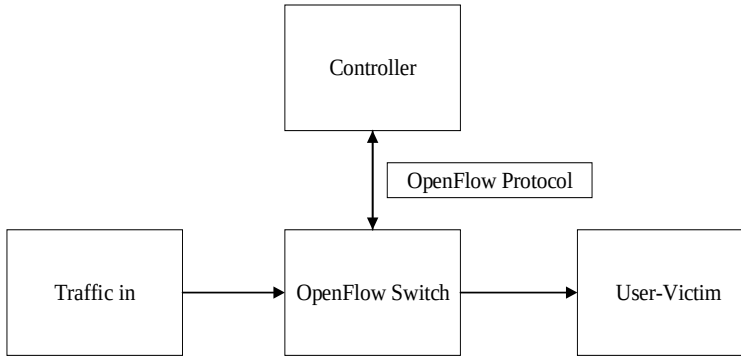
1.3.6. Bản tin StatsResponse

StatsResponse dùng để trả lời bản tin StatsRequest.

CHƯƠNG 2. XÂY DỰNG KIẾN TRÚC MẠNG SDN/OPENFLOW SỬ DỤNG TRONG PHÒNG CHỐNG TẤN CÔNG

2.1. Giả lập kiến trúc mạng SDN/OpenFlow

Kiến trúc tổng quan của hệ thống được thể hiện như bên dưới (Hình 2.1)



Hình 2.1. Kiến trúc mạng SDN/OpenFlow giả lập

2.2. Nguyên lý hoạt động của hệ thống

2.2.1. Cách thức hoạt động của Controller

Bộ điều khiển SDN Controller có nhiệm vụ ra quyết định cho khối chuyển mạch OpenFlow Switch thực thi thông qua giao thức OpenFlow. Nhận thông báo về những phân tích các flow entry đi vào mạng, khi xảy ra tấn công, SDN Controller sẽ nhận được một thông báo và kèm theo đó là một dãy các địa chỉ IP của nguồn tin truy

vấn có tần suất cao tới hệ thống, đa số đều là các nguồn tin đang thực hiện việc tấn công hệ thống, đều cần phải được ngăn chặn. Khi đã nhận được thông báo đang có tấn công cùng với danh sách địa chỉ IP, SDN Controller sẽ gửi một bản tin điều khiển xuống khối chuyển mạch OpenFlow Switch để làm rớt tất cả các gói tin đi từ những địa chỉ IP đang bị nghi ngờ, từ đó lưu lượng đi qua bộ chuyển mạch được khống chế, đảm bảo cho các thiết bị ở phía người dùng không bị ảnh hưởng. SDN Controller sẽ gửi bản tin FlowMod xuống cho bộ chuyển mạch để thực hiện việc hủy bỏ các gói tin.

2.2.2. Cách hoạt động của chuyển mạch OpenFlow Switch

Bộ chuyển mạch sẽ thực hiện việc chuyển tiếp lưu lượng lưu thông trong mạng, lưu giữ các bảng trạng thái. Khi các Flow entry đi đến bộ chuyển mạch OpenFlow Switch sẽ được đối chiếu với bảng trạng thái Flow table để thực hiện việc định tuyến và chuyển tiếp các gói tin, tất cả mọi hoạt động đều chịu sự giám sát của SDN Controller, các giao tiếp giữa Controller với chuyển mạch OpenFlow Switch đều được thực hiện thông qua giao thức OpenFlow. Bên cạnh đó, trên bộ chuyển mạch còn tích hợp thêm khối giám sát lưu lượng sFlow, các gói tin đến sẽ được lấy mẫu để theo dõi, kiểm soát và xử lý, phân tích dữ liệu và gửi lên controller theo định kỳ để đảm bảo kịp thời phát hiện khi có tấn công xảy ra.

2.2.3. Cách thức hoạt động của bộ kiểm soát lưu lượng sFlow – Network Monitoring

Bộ kiểm soát lưu lượng có chức năng thực hiện giám sát và kiểm soát và phân tích lưu lượng đi vào hệ thống mạng, và chuyển tiếp toàn bộ thông tin phân tích được lên bộ điều khiển. Là phần mềm sẽ được nhúng trong khối OpenFlow Switch trên nền tảng NetFPGA. Hoạt động dựa trên công nghệ sFlow với cấu trúc Agent – Collector. Các sFlow Agent sẽ thực hiện nhiệm vụ thu thập lưu lượng theo một chu kỳ thời gian lấy mẫu, rồi đưa lên khối sFlow Collector, giúp Collector có thể bao quát toàn bộ lưu lượng trong mạng theo thời gian thực.

2.3. Kịch bản tấn công và giải pháp giảm thiểu tấn công khuyếch đại DNS

2.3.1. Xây dựng hệ thống

Hệ thống bao gồm các thiết bị : 1 SDN Controller, 1 OpenFlow Switch trên nền tảng NetFPGA(tích hợp khối Network Monitoring), 1 máy phát lưu lượng giả lập như lưu lượng thời gian thực (bao gồm cả lưu lượng tấn công và lưu lượng bình thường), 1 Server đóng vai trò là nạn nhân của cuộc tấn công (Victim).

2.3.2. Công cụ hỗ trợ

Các công cụ hỗ trợ bao gồm: Bonesi, Wireshark, TCPReplay, Moba Sterm, Editcap, Speedometer, Tcpdump.

2.3.3. Kịch bản phát tấn công

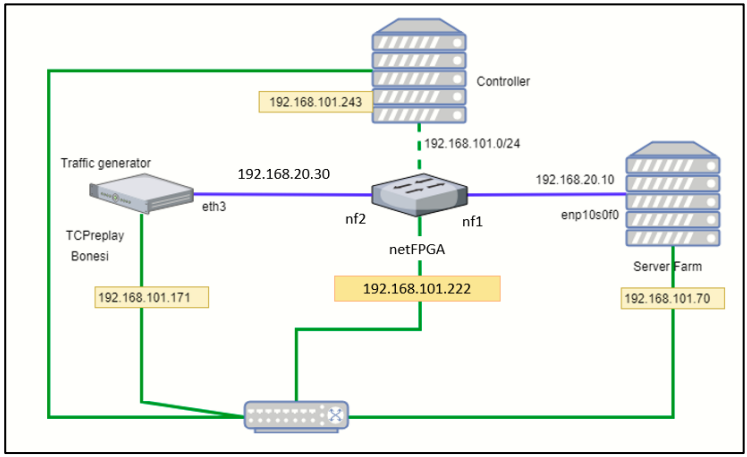
Sử dụng công cụ Bonesi để phát tấn công trực tiếp vào FPT Server đóng vai trò là máy nạn nhân, đồng thời dùng Wireshark để thu thập dữ liệu lưu lại dưới dạng file pcap. Tác giả đã có được một bộ dữ liệu tấn công giống đặc tính của mạng Botnet. Sử dụng TCPReplay để phát lại bộ lưu lượng đó từ máy phát lưu lượng vào hệ thống giả lập đã xây dựng, tiến hành tấn công máy FPT Server. Lưu lượng phải được chuyển tiếp qua OpenFlow Switch và được kiểm soát bởi controller. Tiến hành phát và ghi lại kết quả trong hai trường hợp : không chạy giải pháp giảm thiểu tấn công và trường hợp có chạy giải pháp giảm thiểu tấn công trên Floodlight Controller. Sử dụng công cụ Speedometer để đo thông lượng của lưu lượng ở đầu vào cũng như đầu ra của khối chuyển mạch và công nghệ sFlow để giám sát lưu lượng.

CHƯƠNG 3. KẾT QUẢ MÔ PHỎNG CHỐNG TẤN CÔNG TRONG SDN

3.1. Mô hình xây dựng hệ thống

3.1.1. Tổng quan hệ thống

Tác giả đã xây dựng được mô hình giả lập tấn công như đã nghiên cứu phần lý thuyết. Hình 3.1 cho thấy được các khối chức năng trong hệ thống giả lập.



Hình 3.1. Mô hình lý thuyết

3.1.2. Triển khai hệ thống

Traffic Generator: Chúng ta tiến hành bật traffic generator lên để chuẩn bị cho việc phát lưu lượng mẫu. Kiểm tra lại các kết nối mạng từ traffic generator ra mạng internet để bắt đầu dùng MobaXterm để SSH vào điều khiển máy này.

OpenFlow Switch (super-switch): Sau khi tiến hành bật máy lên, chúng ta phải tiến hành nạp code cho NetFPGA, bước đầu là để máy tính có thể nhận các cổng của NetFPGA là cổng của máy.

Sau khi tiền hành nạp file code đầu tiên, chúng ta phải khởi động lại máy để máy hoàn thành tác vụ chuyển các cổng của FPGA thành cổng của máy. Sau khi máy bật lên trở lại, chúng ta tiến hành nạp file code thứ hai

Sau khi chạy xong file nạp code trên, chúng ta đã cấu hình để máy tính này có thể hoạt động như một OpenFlow Switch.

ServerFarm: Sau khi máy ServerFarm được bật, chúng ta tiến hành bật Wireshark lên và chuẩn bị tiến hành đo lưu qua cổng enp10s0f0.

3.2. Mô phỏng tấn công và biện pháp giảm thiểu tấn công

Trước tiên sử dụng Bonesi để phát lưu lượng giả lập, trong đó chứa các nguồn địa chỉ IP khác nhau từ file 50k-bots với tối độ 1500 gói/s tới địa chỉ của Victim 192.168.20.30

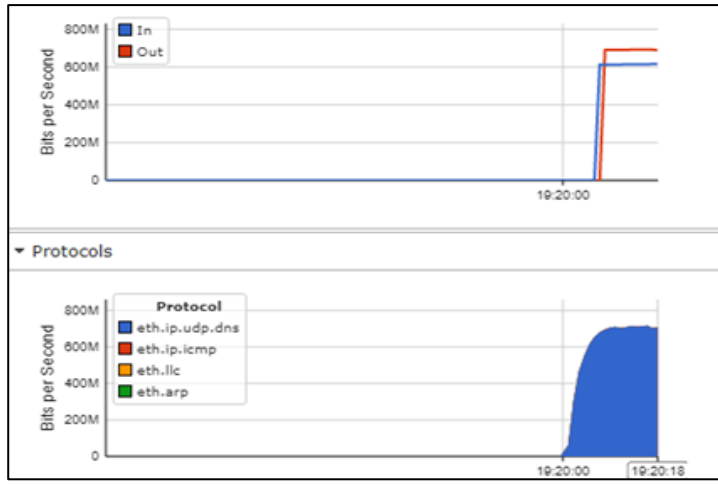
Đồng thời dùng phần mềm wireshark thu lại lịch sử của những kết nối trong khi phát tấn công thành file dns.pcap.

Sau khi thu được file dns.pcap đóng vai trò như file chứa lưu lượng tấn công cho mô hình giả lập. Tiếp theo tác giả sẽ sử dụng công cụ TCPReplay để phát lại file dns.pcap kia vào mô hình.

3.2.1. Phát lưu lượng bình thường không có giải pháp giảm thiểu

Trước khi tiến hành phát lưu lượng, chúng ta tiến hành bật controller và tiến hành gửi lưu lượng từ OpenFlow Switch lên

controller. Sau đó, chúng ta tiến hành chạy controller mà trên đó không có bất cứ giải pháp giảm thiểu nào.



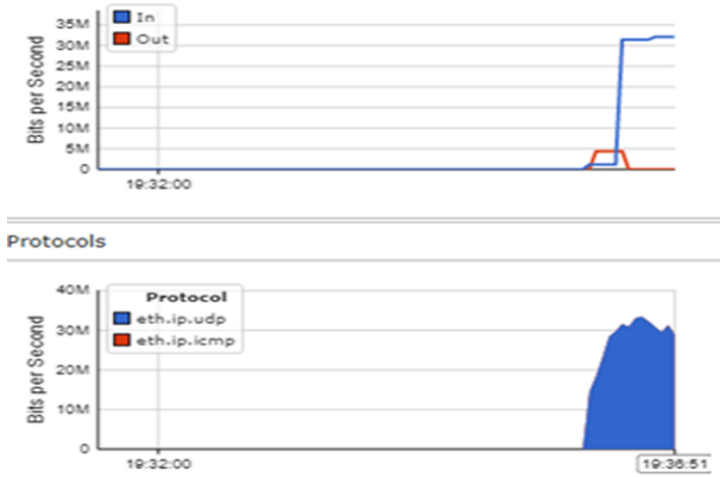
Hình 3.1. Lưu lượng tấn công khi chưa chạy giải pháp giảm thiểu

3.2.2. Hệ thống khi sử dụng giải pháp giảm thiểu

Quy trình tương tự như khi phát lưu lượng bình thường, nhưng lúc này trên SDN Controller ta bắt đầu chạy giải pháp phát hiện và giảm thiểu tấn công.

cho ta thấy sự khác biệt giữa trường hợp sử dụng giải pháp phát hiện và giảm thiểu tấn công và trường hợp không sử dụng. Ta thấy rằng, đối với file 50k-bots với tối độ 1500 gói/s khi không sử dụng giải pháp giảm thiểu tấn công, số lượng flow-entry trên switch rất lớn và lớn nhất khoảng 700Mb/s và thời gian tồn tại của flow entry trên Switch kéo dài. Điều này có thể gây tốn tài nguyên trên Switch và nếu tấn công với cường độ lưu lượng lớn có thể dẫn tới Switch sẽ không còn khả năng xử lý. Trong đó khi sử dụng giải pháp

giảm thiểu tấn công với file 50k-bots với tối độ 1500 gói/s thì số lượng flow-entry trên Switch rất ít khi tấn công xảy ra và đạt giá trị lớn nhất khoảng 5Mb/s. Ngoài ra trạng thái flow tồn tại trên Swich cũng ngắn hơn so với trường hợp không sử dụng giải pháp giảm thiểu.



Hình 3.2. Lưu lượng tấn công khi chạy qua giải pháp giảm thiểu

3.3. Nhận xét và kiến nghị

Hệ thống giả lập được xây dựng khá hiệu quả trong việc phát hiện và phòng chống tấn công. Dựa trên kiến trúc mạng SDN/OpenFlow cùng với công nghệ sFlow, hệ thống đã phát hiện được các truy vấn giả mạo để thực hiện ngăn chặn tấn công trong một thời gian ngắn, nhanh chóng giảm thiểu được các flow entry đi vào bộ chuyển mạch OpenFlow Switch, giúp Server nhanh phục hồi để phục vụ các dịch vụ thông thường ngay trong khi cuộc tấn công xảy ra.

Qua đề tài luận văn này, ta nhận thấy hiệu quả trong việc phát hiện và phòng chống tấn công của hệ thống giả lập. Tác giả xin được kiến nghị được thử nghiệm mô hình hệ thống này vào các hệ thống SDN đang hoạt động tại các đơn vị trong thời gian tới.

KẾT LUẬN

Các kết quả chính của đề tài luận văn:

- Đưa ra cái nhìn tổng quan về kiến trúc mạng SDN, giao thức OpenFlow và các bản tin trao đổi giữa OpenFlow Switch và Controller.

- Xây dựng kiến trúc mạng SDN/OpenFlow trên server testbed. Đồng thời giả lập một cuộc tấn công trên hệ thống mô phỏng, các kỹ thuật giám sát lưu lượng và giảm thiểu tấn công đã được tích hợp.

- Hệ thống mô phỏng đã phát hiện và ngăn chặn cuộc tấn công trong thời gian ngắn, giúp server nhanh chóng phục hồi để phục vụ các dịch vụ ngay trong khi cuộc tấn công xảy ra.

Hướng phát triển của đề tài:

Thử nghiệm mô hình với các bộ dữ liệu đã được thu thập từ thực tế chứa nhiều hình thức tấn công hơn, để có thể đánh giá hiệu năng của hệ thống giả lập cũng như phát triển các giải pháp phòng chống các loại tấn công khác trên SDN Controller. Đồng thời, nâng cấp cấu hình Controller để tăng tốc độ xử lý các gói tin trong các cuộc tấn công, giảm thời gian đáp ứng của hệ thống, tối ưu hóa hiệu năng của hệ thống, cung cấp một hệ thống hoàn thiện.

DANH MỤC TÀI LIỆU THAM KHẢO

[1]. Thuyết minh dự thảo tiêu chuẩn quốc gia – Các yêu cầu và hướng dẫn bảo mật DNS (DNSSEC)-2016.

[2]. Open Networking Foundation, Software-Defined Networking: The New Norm for Networks, April 13, 2012

[3]. OpenFlow Specification v1.3.0, June 25, 2012

[4]. Marios Anagnostopoulos, Georgios Kambourakis, Panagiotis Kopanos, Georgios Louloudakis, Stefanos Gritzalis, DNS Amplification Attack Revisited, An article in Computer&Security, December 2013

[5]. FERGUSON, P., AND SENIE, D.BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827, May 2000.

[6]. Muhammad Afaq, Shafqat Rehman, Wang-Cheol Song, Large Flows Detection, Marking, and Mitigation based on sFlow Standard in SDN, Journal of Korea Multimedia Society Vol. 18, No. 2, February 2015 (pp. 189-198).