Kỷ yếu Hội nghị Quốc gia lần thứ VIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR); Hà Nội, ngày 9-10/7/2015
DOI: 10.15625/vap.2015.000187

NGHIÊN CỨU ỨNG DỤNG MỘT SỐ GIẢI PHÁP CÔNG NGHỆ TRONG THIẾT KẾ THIẾT BỊ ĐIỀU KHIỂN LƯU LƯỢNG MẠNG SDN

Nguyễn Ái Việt, Lưu Thị Huy, Lâm Thị Sen và Nguyễn Văn Nghiệp

Viện Công nghệ thông tin, Đại học Quốc gia Hà Nội và

Trường Đại học CNTT&TT, Đại học Thái Nguyên

June 16, 2015

TÓM TẮT *- Công nghệ SDN đã trở nên chín muồi và đang là cơ hội để xây dựng các thiết bị mạng mới. Trên cơ sở đó, thiết bị điều khiển lưu lượng mạng VNTC [1] được đề nghị thay thế các tường lửa thế hệ cũ nhằm bảo vệ các mạng LAN, trung tâm dữ liệu IDC và hạ tầng tính toán mây. Chúng tôi nghiên cứu phối hợp các công nghệ khác nhau được thiết kế tối ưu để tăng tốc độ xử lý với giá thành cho sản phẩm hợp lý.*

I. ĐẶT VẤN ĐỀ

Công nghệ mạng nội bộ (LAN) truyền thống được xây dựng để chia sẻ dùng chung tài nguyên và thiết bị trong một tổ chức. Trước hết, LAN giảm đầu tư phần cứng, do chia sẻ các thiết bị ngoại vi như máy in, kết nối internet. Một số ứng dụng và dữ liệu dùng chung cũng được chia sẻ tại các máy chủ, cho phép không phải đầu tư nhiều lần và tiện lợi. Cuối cùng việc bảo hành bảo trì, cấu hình từ xa, được tiết kiệm tối đa. Tuy nhiên, ngay từ đầu, mạng LAN đã không được thiết kế để an toàn. Ngày nay, việc phơi nhiễm mạng LAN đối với các cuộc tấn công phá hoại từ internet là nguyên nhân chính gây ra tổng thiết hại hàng trăm tỷ đô la mỗi năm. Hầu như các tài nguyên quý của các tổ chức đều có trong mạng LAN. Bảo vệ an toàn mạng LAN là một trong những hướng nghiên cứu chính của Viện CNTT và VIEGRID JSC, trong khuôn khổ của dự án phát triển sản phẩm công nghệ cao quốc gia.

Hiện nay, đa số mạng LAN sử dụng công nghệ máy chủ Windows trên thế giới được bảo vệ bằng tường lửa của Microsoft Forefront TMG 2010 và tiền thân của nó trước kia là tường lửa ISA. Tuy nhiên từ ngày 14 tháng 4 năm 2015, Microsoft đã tuyên bố ngừng hỗ trợ chung cho sản phẩm này (vốn đã ngừng bán từ năm 2012), mọi trách nhiệm hỗ trợ kỹ thuật mở rộng của Microsoft với sản phẩm này sẽ chấm dứt vào năm 2020. Thực tế này bắt buộc các tổ chức phải đi tìm cho mình một giải pháp mới. Đồng thời đây cũng là một cơ hội thị trường cho các sản phẩm tường lửa.

Việc Microsoft rút lui ra khỏi thị trường tường lửa là việc thị trường này đang dịch chuyển sang tường lửa thế hệ tương lai NGF, mà các nhà sản xuất các thiết bị phát hiện và ngăn chặn xâm nhập (IDS và IPS) sẽ có ưu thế cạnh tranh hơn. Tuy nhiên, có lẽ lý do quan trọng trong việc Microsoft từ bỏ thị trường này là trong tương lai, các thiết bị mạng nói chung và thiết bị tường lửa nói riêng sẽ là một thành phần trong bộ điều khiển mạng trong mạng SDN.

Bên cạnh đó, công nghệ mạng xác định bởi phần mềm SDN (Software Defined Network) cũng đang khởi động một cuộc cách mạng thực sự về công nghệ mạng trên nền tảng hạ tầng tính toán đám mây và xu hướng ảo hóa thiết bị.

Trong bài báo [1], các tác giả đã đề xuất việc sản xuất thiết bị điều khiển lưu lượng mạng VNTC (Viegrid Network Traffic Controller) đáp ứng yêu cầu này của thị trường. Bên cạnh các chức năng tường lửa thế hệ mới, có khả năng phân tích các đợt tấn công hướng ứng dụng, thiết bị mới này có thêm các chức năng điều khiển lưu lượng hướng tới các máy chủ ứng dụng. Các công nghệ cốt lõi được nghiên cứu áp dụng và phát triển, cải tiến để phục vụ cho thiết bị này là:

a. Phân tích dữ liệu lớn với tốc độ cao để phát hiện sớm các mẫu hình tấn công. Đồng thời, thu thập và khai thác các cơ sở dữ liệu lớn về mẫu hình tấn công.

b. Tối ưu các chức năng của tường lửa thế hệ mới trong giải pháp truy cập internet an toàn cho các mạng LAN V-AZUR [2], trao quyền mã hóa và giải mã cho các giao thức an toàn như https.

c. Bắt gói tin để xử lý tốc độ cao ngay tại card mạng.

d. Tăng tốc tốc độ xử lý của thiết bị nhờ ứng dụng tính toán GPU, công nghệ nhúng FPGA và một số phần cứng.

e. Thiết bị VNTC được thiết kế phù hợp với các chuẩn mới của mạng SDN, nhằm chuẩn bị cho việc thiết bị này tham gia vào cuộc cách mạng công nghệ mạng. Trong bài này chúng tôi báo cáo một số kết quả nghiên cứu các công nghệ liên quan tới việc phát triển thiết bị VNTC.

II. TỔNG QUAN VỀ SDN

2.1. Xu hướng đổi mới công nghệ mạng

Truyền thông xã hội, thiết bị di động, phân tích dữ liệu lớn và tính toán đám mây (SMAC) đang đòi hỏi thay đổi có tính chất cách mạng đối với công nghệ mạng truyền thống.

Trên hạ tầng đám mây, việc tính toán và lưu dữ liệu đã có rất nhiều đổi mới công nghệ trong việc ảo hóa và tự động hóa. Tuy nhiên đã đến lúc việc đổi mới này đã bị sự lạc hậu về công nghệ mạng cản trở.

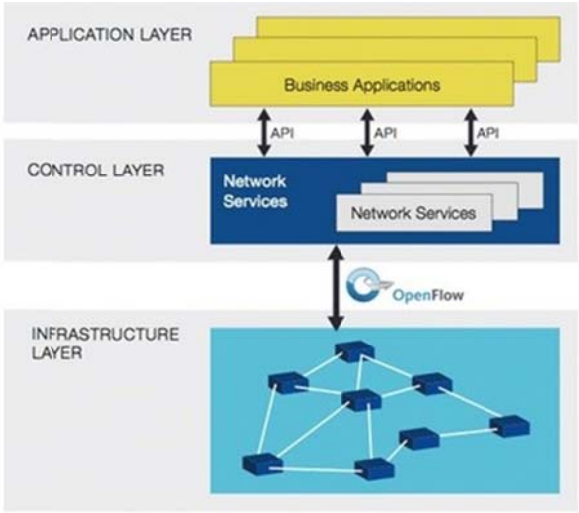
Các nhà quản trị mạng có thể tạo ra và cấu hình rất nhiều máy chủ, máy trạm ảo, tạo ra các cơ sở dữ liệu dự phòng, thậm chí toàn bộ hạ tầng tính toán trong thời gian ngắn. Tuy nhiên, việc quản trị mạng vẫn phải làm bằng tay trên các thiết bị có khi mất nhiều tuần cho một thay đổi.

SDN cho phép làm một cuộc cách mạng đối với các trung tâm dữ liệu, cho phép việc điều khiển các mạng bằng các thiết bị mạng và đặc biệt là bộ điều khiển ảo giống như đối với máy chủ, máy trạm và cơ sở dữ liệu.

SDN thay đổi công nghệ điều khiển lưu lượng mạng hiện tại của Cisco bằng cách tách phần điều khiển khỏi phần chuyển dữ liệu. Phần điều khiển trong mạng SDN được tập trung và tối ưu hóa. Chính vì vậy hiệu năng được nâng cao rất nhiều.

2.2. Kiến trúc SDN và Open Flow

Trong mọi mô hình SDN, bộ điều khiển SDN được tập trung hóa, đưa ra quyết định tối ưu toàn cục thay cho thuật toán best-effort tại mỗi thiết bị định tuyến. Bộ điều khiển SDN tập trung được gắn với hai giao diện lập trình ứng dụng (API) hướng Nam và hướng Bắc [3].



a. Bộ API hướng Nam: Sử dụng một giao thức riêng gọi là Open Flow để gửi thông tin điều khiển cho các chuyển mạch và định tuyến.

b. Bộ API hướng Bắc: Giao tiếp với các trình ứng dụng để xây dựng các ứng dụng giúp các nhà quản trị cấu hình, thiết lập các quy tắc mạng.

Ngày nay, việc chuyển sang SDN cho phép các cơ quan và doanh nghiệp sang một hạ tầng mạng mới, với các chức năng mạng được ảo hóa, tối ưu và cung cấp theo nhu cầu.

2.3. Ảo hóa chức năng mạng NFV

NFV là phương pháp thiết kế, triển khai và quản trị các dịch vụ mạng mới trong các mạng SDN. NFV tách các chức năng mạng như dịch địa chỉ mạng (NAT), tường lửa, phát hiện xâm nhập, dịch vụ tên miền (DNS) ra khỏi các thiết bị mạng truyền thống và triển khai chúng bằng phần mềm [4].

Như vậy với NFV người ta sẽ có một môi trường hạ tầng được ảo hóa hoàn toàn từ máy chủ, lưu trữ và mạng ảo hóa. Hiện nay, NFV đã hình thành được một chuẩn công nghiệp cho phép:

a. Giảm chi phí đầu tư: Không cần phải mua các phần cứng có các chức năng định sẵn như trước, hỗ trợ mô hình chỉ triển khai khi có nhu cầu, tránh việc đầu tư vào các chức năng chưa cần.

b. Giảm chi phí vận hành: Giảm yêu cầu về chỗ, năng lượng và làm lạnh, đơn giản hóa việc triển khai và quản trị mạng.

c. Rút ngắn thời gian triển khai: Triển khai các dịch vụ mạng không mất thời gian, chớp thời cơ và giảm thiểu rủi ro khi thử nghiệm và triển khai công nghệ mới.

d. Linh hoạt: Có thể mở rộng hoặc thu hẹp các dịch vụ theo yêu cầu thay đổi, hỗ trợ các cải tiến mới về thiết bị, bớt sự phụ thuộc vào phần cứng chuyên dụng.

2.4. Vấn đề an ninh mạng trong SDN

Trong mạng SDN, vấn đề an ninh là quan trọng ở mọi chỗ và cần được xây dựng ngay trong kiến trúc. Do đó, vấn đề an ninh có thể khắc phục được các khó khăn về an ninh từ gốc của mạng LAN. An toàn an ninh mạng cần được xem như một dịch vụ bảo vệ tính sẵn sàng, toàn vẹn và riêng tư đối với mọi tài nguyên và thông tin được kết nối [5].

Truy cập các bộ điều khiển tập trung cần an toàn hơn. Khi bộ điều khiển SDN bị tấn công (chẳng hạn bởi DDoS), toàn bộ mạng sẽ bị đánh sập. Việc triển khai các quy định an toàn mạng sẽ thống nhất và đồng bộ. Khi xảy ra sự cố việc khắc phục sẽ dễ dàng và chỉ một lần.

Cho đến nay vẫn có hai cách tiệm cận về việc bảo vệ an toàn trong mạng LAN: cách thứ nhất là bảo vệ an toàn an ninh ngay trong mạng, cách thứ hai là bảo vệ ngay trong các máy chủ và các thiết bị tính toán.

Trong cả hai trường hợp, môi trường thế hệ tương lai sẽ bảo vệ an ninh xác định bằng phần mềm SDSec, tách việc điều khiển an toàn khỏi việc xử lý an toàn hoàn toàn tương tự với kiến trúc SDN. Do đó, các chức năng điều khiển của các thiết bị an toàn truyền thống cũng sẽ được tách ra và tập trung hóa.

Vấn đề là phải có những thiết bị mới được xây dựng để hướng tới giải quyết vấn đề an ninh hiện tại của mạng LAN, trung tâm dữ liệu tích hợp (IDC) và hướng tới các hạ tầng đám mây với SDN trong tương lai đảm phải tính đơn giản, tiết kiệm và an toàn.

III. KIẾN TRÚC CỦA VNTC

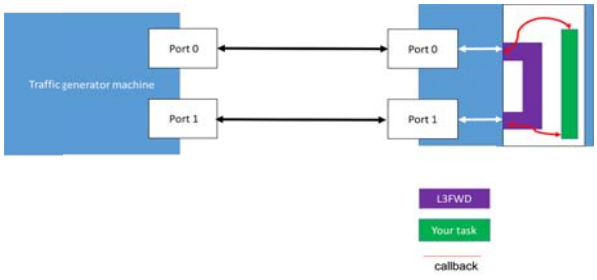
Trong tương lai VNTC sẽ hướng tới một bộ điều khiển lưu lượng mạng tập trung bao gồm nhiều chức năng với tốc độ cao, có thể chạy trên bất cứ môi trường nào. Trước mắt, VNTC vẫn phải ứng dụng trong mạng LAN, các trung tâm tích hợp dữ liệu, phòng máy chủ. Do đó, chúng tôi đề nghị tập trung một số chức năng của tường lửa thế hệ mới, chuyển chức năng mã và giải mã phiên trên máy chủ sang tường lửa để tăng tính bảo mật và linh hoạt. Chúng tôi cũng đề nghị tách việc lọc, định tuyến gói tin theo các bộ luật ra khỏi việc phát hiện các mẫu hình tấn công và xây dựng tập luật mới. Do đó, VNTC là thiết bị bảo vệ các máy chủ ứng dụng, các mạng bên trong, bằng cách giảm tải cho các máy chủ bên trong, vừa có chức năng tường lửa thế hệ mới vừa lọc các gói tin theo ứng dụng.

Trong thực tế, VNTC sẽ được phối hợp với giải pháp V-AZUR đang triển khai để thành một bộ giải pháp bảo vệ các mạng LAN có chất lượng và hiệu năng cao. Vì vậy, VNTC đã được đề nghị triển khai theo kiến trúc thiết kế như trong hình vẽ sau [1].

Việc ngăn chặn các đợt tấn công vào mạng cần được xử lý nhanh bằng các giải pháp có giá thành hợp lý. Do đó, chúng tôi tập trung vào việc sử dụng các giải pháp tăng tốc, phù hợp.

IV. CHỌN CÔNG NGHỆ BẮT GÓI TIN TRÊN CARD MẠNG

Việc phân tích các gói tin có thể tiến hành bằng các ứng dụng cài đặt trên hệ điều hành. Do đó tốc độ có thể tương đối chậm. Intel đã phát triển một công cụ bắt gói tin ngay trên card mạng là dpdk để tăng tốc độ xử lý các gói tin ở mức cao nhất. Chúng tôi đã tiến hành triển khai việc bắt các gói tin theo kiến trúc như sau [6].



Trên cùng một máy, chúng tôi mô phỏng tương tác giữa máy và một tường lửa che chắn cho một máy chủ. Chúng tôi tiến hành bắt gói tin trên tường lửa tại các cổng 0 và 1.

Chúng tôi sử dụng một máy chủ với cấu hình 16 core, 32 GB RAM, có 2 card mạng, chạy trên hệ điều hành tinh giản TinyOS, để đảm bảo tối ưu về tốc độ.

Mô hình này có ưu điểm là bắt gói tin khá linh hoạt và có thể tùy biến theo các giao thức ở các tầng khác nhau. Các gói tin bắt được, một mặt sẽ được chuyển tiếp theo các luật của một tường lửa thế hệ mới, mặt khác sẽ được chuyển tới một bộ phân tích. Khi phát hiện ra mẫu hình tấn công, bộ phân tích sẽ cập nhật lại các bộ luật.

V. CÁC CHỨC NĂNG TƯỜNG LỬA VÀ MÃ HÓA

Sau khi phân tích các chức năng của bộ tường lửa thế hệ mới mã nguồn mở Suricata [7] chúng tôi quyết định sử dụng công nghệ này làm cơ sở để phát triển các chức năng tường lửa của VNTC.

Trong giải pháp V-AZUR, mạng LAN được chia làm mạng trong và mạng ngoài, do đó VNTC sẽ được áp dụng tại vị trí của tường lửa trong và tường lửa ngoài.

Hiện tại, V-AZUR áp dụng một chính sách an toàn an ninh rất chặt chẽ do đó chỉ sử dụng các chức năng tường lửa ở tầng thấp. Tuy nhiên, trong một số trường hợp, chẳng hạn khi phát triển các ứng dụng Web, hoặc các ứng dụng cần có kết nối mạng, do đó cần sử dụng các chức năng tường lửa ở tầng ứng dụng.

Chúng tôi đã xem xét thiết kế VNTC cho phù hợp với kiến trúc của VAZUR. Thậm chí, việc chuyển chức năng mã hóa cho các giao thức an toàn như https cũng được chuyển về VNTC. VNTC cũng có chức năng phân tải, cho trường hợp cần nhiều máy chủ có hiệu năng lớn tham gia vào việc điều khiển lưu lượng mạng.

VI. CÁC GIẢI PHÁP TĂNG TỐC

Trên thế giới hiện nay, việc xây dựng các bộ điều khiển hiệu năng cao đều sử dụng các phần mềm nhúng chuyên dụng, do đó giá thành khá cao (khoảng 1-2 triệu USD một bộ điều khiển). Tuy nhiên, trong hạ tầng của các doanh nghiệp và tổ chức, đặc biệt tại Việt Nam, không tới 10% các chức năng của các bộ điều khiển này là cần thiết và được sử dụng.

VNTC nhằm đáp ứng các nhu cầu cấp thiết của các hạ tầng mạng của cơ quan doanh nghiệp, trước mắt là nhu cầu thay thế tường lửa của Microsoft và tường lửa ASA của Cisco. Với mức giá thành phù hợp, chúng tôi sẽ phát triển các công nghệ tăng tốc VNTC theo các hướng sau đây:

a. Chọn một nhân hệ điều hành tối thiểu và tối ưu hóa dần dần: Qua nghiên cứu chúng tôi đã chọn TinyOS là hệ điều hành mã nguồn mở gốc Linux đã được tối ưu hóa, với quy mô cực nhỏ gọn, tốc độ tốt, chạy ổn định, có khả năng nhúng được vào các chip chuyên dụng hoặc sử dụng FPGA.

b. Sử dụng công nghệ Hadoop, phân tích dữ liệu song song theo thuật toán Map&Reduce.

c. Sử dụng công nghệ tính toán GPU để tăng tốc tính toán tại các thiết bị VNTC.

d. Chuyển một số chức năng lên xử lý ngay trên card mạng được lập trình nhúng FPGA.

Hiện nay, chúng tôi đã làm chủ được công nghệ Hadoop và đang tiếp tục phát triển việc phân tích dữ liệu lớn của các gói tin với tốc độ cao.

Trong thời gian qua, có một số kết quả trong việc tăng tốc nhờ ứng dụng tính toán GPU, có triển vọng áp dụng vào VNTC.

VII. ỨNG DỤNG CÔNG NGHỆ TÍNH TOÁN GPU

Do việc mã hóa được chuyển về VNTC để tiến hành kiểm soát lọc ở tầng ứng dụng đối với các gói tin sử dụng các giao thức an toàn như https. Chúng tôi tiến hành nghiên cứu việc sử dụng GPU để tăng tốc cho việc mã hóa trên VNTC.

Chúng tôi thử nghiệm so sánh thời gian tính toán cho mã hóa và giải mã dùng thuật toán AES trên CPU và GPU.

Kết quả được trình bày trong các bảng sau:

Bảng 1. So sánh thời gian mã hóa trên CPU và GPU

Size	CPU	GPU
1.1Mb	0,834	0,215
5.2Mb	18,552	0,504
9.84Mb	36,957	0,797
21.55Mb	79,289	1,608
29.05Mb	109,881	2,174
39.25 Mb	148,290	2,864
50.21 Mb	191,045	3,673
62.22 Mb	237,291	4,368
70.59 Mb	269,187	4,922
84.98 Mb	326,418	5,839

Bảng 2. So sánh thời gian giải mã trên CPU và GPU

Size	CPU	GPU
1.1Mb	8,703	0,2180
5.2Mb	45,497	0,653
9.84Mb	85,154	1,056
21.55Mb	189,704	2,014
29.05Mb	257,100	2,704
39.25 Mb	349,593	3,645
50.21 Mb	447,036	4,620
62.22 Mb	551,862	5,613
70.59 Mb	640,422	6,311
84.98 Mb	805,386	8,010

VIII. KẾT LUẬN

VNTC là một thiết bị cần thiết hiện nay có khả năng thay thế các tường lửa của Microsoft đã ngừng hỗ trợ và của Cisco, bằng các bổ sung các tính năng của tường lửa thế hệ tương lai. Việc tăng tốc bằng các giải pháp phù hợp có thể giảm giá thành của thiết bị.

SDN cũng đem lại nhiều công cụ và tư tưởng thiết kế mới, để VNTC có thể có tương lai ứng dụng lâu dài khi chuyển sang hạ tầng mạng với công nghệ mới.

IX. TÀI LIỆU THAM KHẢO

[1] Nguyen Ai Viet and Ngo Doan Lap, Application of SDN in the Information Security Protection for the IDC and the cloud computing infrastructure, in Proceedings of International Symposium on GIS and Advanced Technologies 2014, Thai Nguyen (2014).

[2] Công ty VIEGRID, Tài liệu hướng dẫn sử dụng giải pháp V-AZUR (2012), Bằng sáng chế được bảo hộ do Cục Sở hữu trí tuệ cấp (2015).

[3] Open Networking Foundation Software-Defined Networking: The New Norm for Networks White paper (2012).

[4] ETSI *Network Functions Virtualisation* - Introductory White Paper (2012).

[5] S.Scott-Hayard, G.O-Callaghan and S. Seizer, *A survey: SDN security* IEEE Communication Magazine (2013).

[6] Nguyễn Văn Nghiệp, *Nghiên cứu việc ứng dụng phần mềm nguồn mở DPDK để theo dõi lưu lượng mạng SDN* Luận án Kỹ sư CNTT, trường Đại học CNTT&TT, Đại học Thái Nguyên (2015).

[7] Lưu Thị Huy, *"Nghiên cứu các chức năng của tường lửa thế hệ mới Suricata và ứng dụng trong mạng nội bộ doanh nghiệp"*, Luận án Kỹ sư CNTT, trường Đại học CNTT&TT, Đại học Thái Nguyên (2015).

[8] Giorgos Vasiliadis, Spiros Antonatos, Michalis Polychronakis, Evangelos P, Sotiris Ioannidis, *Gnort: High performance network intrusion detection using graphics processors* in Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection (2009).

[9] S. Singh and S. Sikalari, *A Survey of Cyber Attack Detection Systems* International Journal of Computer Science and Network Security 9 (2009), 1.

[10] Lâm Thị Sen, *Tìm hiểu về GPU Computing và ứng dụng,* Luận án Kỹ sư CNTT, Trường Đại học CNTT&TT, Đại học Thái Nguyên (2015).