NGHIÊN CỨU PHÂN TÍCH, SO SÁNH, ĐÁNH GIÁ HIỆU SUẤT CỦA TƯỜNG LỬA THẾ HỆ MỚI: TRƯỜNG HỢP PALO ALTO VÀ FORTIGATE FIREWALL

Nguyễn Ngọc Hoan, Lê Hoàng Hiệp, Đỗ Đình Lực
Trường Đại học Công nghệ thông tin và Truyền thông, Đại học Thái Nguyên
Ngày nhận bài 08/4/2022, ngày nhận đăng 22/6/2022
DOI : https://doi.org/10.56824/vujs.2022nt08

Tóm tắt: Bài báo tập trung phân tích so sánh và đánh giá hiệu suất của tường lửa thế hệ tiếp theo là Palo Alto Firewall và Fortinet Firewall trên thực tế thông qua việc triển khai các tình huống, kịch bản mô phỏng thực nghiệm đó là sử dụng tấn công mạng kiểu TCP, UDP Flood; đánh giá chức năng SSL/TLS Inspection, Application Control; kiểm tra lưu lượng, độ trễ, thời gian phản hồi gói tin và giá trị thông lượng trung bình trên đường truyền trên mỗi hệ thống mạng có tích hợp riêng một tường lửa của từng hãng. Kết quả quá trình xử lý thông tin đầu vào sau đó thu được định lượng số liệu đầu ra dựa trên phân tích, so sánh và thực nghiệm mô phỏng cho thấy cả hai loại tường lửa có hiệu suất vượt trội so với các loại tường lửa thế hệ cũ nói chung và Fortinet Firewall có điểm nổi trội hơn so với Palo Alto Firewall nói riêng. Kết quả nghiên cứu sẽ là tài liệu cần thiết cho nhà thiết kế, đảm bảo an toàn, an ninh hệ thống mạng và cho các học viên, sinh viên chuyên ngành công nghệ thông tin, an toàn thông tin tham khảo để đưa ra các quyết định phù hợp khi sử dụng hai loại tường lửa thế hệ tiếp theo này.

Từ khóa: Khoa học máy tính; an ninh mạng; tường lửa Palo Alto; tường lửa Fortinet; tấn công mạng

1. Giới thiệu

Các hệ thống, hạ tầng mạng máy tính hiện nay đang đóng vai trò cực kỳ quan trọng trong việc thúc đẩy phát triển mở rộng và lợi ích kinh tế đối với bất kỳ một đơn vị nào ở cả trong và ngoài nước. Trước các mối đe dọa, tấn công mạng ngày càng tinh vi thì việc đảm bảo an toàn dữ liệu và an ninh hệ thống mạng cho các hạ tầng mạng của cơ quan, tổ chức, doanh nghiệp là vấn đề được ưu tiên hàng đầu hiện nay [1]-[3]. Có nhiều giải pháp đã được triển khai nhằm bảo vệ hệ thống, hạ tầng mạng doanh nghiệp trước các mối đe dọa như sử dụng các hệ thống công cụ phần mềm (tường lửa mềm) hoặc các hệ thống, thiết bị phần cứng (tường lửa cứng) hoặc là kết hợp cả hai phương án này trên hệ thống mạng doanh nghiệp [4]-[7]. Trong đó, phương án sử dụng tường lửa cứng gần như rất phổ biến tại bất kỳ hạ tầng hệ thống mạng nào, bởi nó đem tới những ưu điểm và sức mạnh, hiệu quả vượt trội trên thực tế. Các thế hệ tường lửa mới (thế hệ tiếp theo của tường lửa truyền thống - *Next Generation Firewall/ NGFW*) đã được nâng cấp, cải tiến rất nhiều nhằm bắt kịp và đáp ứng đủ các yêu cầu bảo vệ hệ thống cũng như hạ tầng mạng doanh nghiệp tính tới thời điểm hiện tại [8]-[11]. Các nghiên cứu đã công bố về hiệu suất của tường lửa đối với các hệ thống mạng cụ thể trên thực tế thông qua việc so sánh chi tiết, cụ thể các chức năng và hiệu quả như trong nghiên cứu này là chưa có. Vì

Email: lhhiep@ictu.edu.vn (L. H. Hiệp)

vậy, trong nghiên cứu này, hai phiên bản tường lửa thế hệ tiếp theo khá phổ biến của hãng *Palo Alto* và *Fortinet* được sử dụng làm trọng tâm nghiên cứu. Bài báo này tập trung phân tích so sánh và đánh giá hiệu suất của tường lửa thế hệ tiếp theo Ploalto Firewall và Fortinet Firewall trên thực tế thông qua việc triển khai các tình huống, kịch bản mô phỏng thực nghiệm đó là: sử dụng tấn công mạng kiểu TCP, UDP Flood; đánh giá chức năng SSL/TLS Inspection, Application Control; Kiểm tra lưu lượng, độ trễ, thời gian phản hồi gói tin và giá trị thông lượng trung bình trên đường truyền trên mỗi hệ thống mạng có tích hợp riêng một tường lửa của từng hãng. Các kết quả của nghiên cứu này có thể dùng làm tài liệu nghiên cứu, tham khảo chuyên sâu cho sinh viên các ngành học về công nghệ thông tin, an toàn thông tin.

2. Nhận diện đặc điểm của tường lửa truyền thống và tường lửa thế hệ tiếp theo

2.1. Ưu điểm so với tường lửa truyền thống

Các dòng tường lửa thế hệ tiếp theo là phiên bản tiên tiến hơn của tường lửa truyền thống và chúng mang lại những lợi ích cao hơn. NGFW là thiết bị tường lửa dựa trên xác thực người dùng, có khả năng xác thực dựa trên các ứng dụng hoặc nội dung. Với cơ chế này, người quản trị dễ dàng nhận dạng các ứng dụng, nội dung bên trong luồng dữ liệu với các mức độ nguy cơ đe dọa xuất phát từ người sử dụng nào. Sự khác biệt rõ ràng nhất giữa hai loại này là NGFW có khả năng lọc các gói dựa trên các ứng dụng. NGFW có thể chặn phần mềm độc hại xâm nhập vào mạng, điều mà tường lửa truyền thống sẽ không bao giờ có thể đạt được. Chúng được trang bị tốt hơn để giải quyết các mối đe dọa liên tục nâng cao. NGFW có thể là một lựa chọn chi phí thấp cho các công ty muốn cải thiện bảo mật cơ bản vì họ có thể kết hợp công việc của phần mềm chống vi-rút, tường lửa và các ứng dụng bảo mật khác vào một giải pháp. Các tính năng khác biệt của tường lửa thế hệ tiếp theo tạo ra nhiều lợi ích tối ưu hơn cho các khách hàng sử dụng chúng. Bên cạnh đó, tường lửa truyền thống còn có những nhược điểm sau:

• Không thể đọc hiểu chi tiết từng loại thông tin và không phân tích nội dung tốt hay xấu của thông tin đó mà chỉ có thể ngăn chặn sự xâm nhập của những thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

• Không thể ngăn chặn một cuộc tấn công mạng nếu cuộc tấn công này đi qua bên ngoài nó, ví dụ như những cuộc tấn công từ bên trong.

• Không thể hoặc khó chống lại các cuộc tấn công bởi virus, mã độc.

• Chỉ có thể nhận diện và kiểm soát được mức thông lượng từ giao thức và cổng dịch vụ, nhưng không nhận diện được các ứng dụng, đặc biệt là các ứng dụng web có sử dụng chung giao thức HTTP và cổng dịch vụ 80.

Từ những hạn chế, nhược điểm của mô hình bảo mật mạng sử dụng tường lửa truyền thống, cùng với sự phát triển mạnh và ngày càng tinh vi của hacker nên yêu cầu phải có một mô hình bảo mật có hiệu suất tối ưu và cao hơn so với mô hình cũ để có thể giúp hệ thống của khách hàng hạn chế, ngăn chặn các mối đe dọa an ninh mạng. Đây là lý do để ra đời các hệ thống tường lửa thế hệ kế tiếp theo.

2.2. Tường lửa Palo Alto

Các thiết bị *Palo Alto Next Generation Firewall* với kiến trúc tiên tiến và mạnh mẽ được cải tiến, kết hợp cùng hệ thống phần cứng chuyên biệt tốc độ cao, đã giúp cung cấp các chức năng, tính năng bảo mật hệ thống vượt trội, giúp khắc phục những nhược điểm, hạn chế của mô hình bảo mật Firewall truyền thống và có khả năng đáp ứng tốt hơn yêu cầu về bảo mật trong thời điểm hiện tại, trở thành một trong những giải pháp bảo mật hiệu quả, phổ biến hiện nay trong hạ tầng mạng doanh nghiệp. Các ưu điểm của tường lửa Palo Alto là:

• Cho phép hệ thống tự động hóa nhận dạng và thực thi các mối đe dọa trên đám mây, không gian mạng và thiết bị đầu cuối của hệ thống.

• Giúp hạn chế, giảm các bề cuộc tấn công và có thể ngăn chặn các mối đe dọa bằng cách bật/cho phép ứng dụng hoạt động một cách an toàn.

• Giúp cung cấp một số chính sách tự động với thời gian thực cho mọi môi trường, hạ tầng mạng.

• Có chức năng mở rộng: bảo vệ an toàn cho các công nghệ mới và mạng ảo.

• Có khả năng tự động cập nhật các phát triển mới từ nhà sản suất một cách nhanh chóng.

2.3. Tường lửa Fortinet

Tường lửa Fortinet cung cấp đến khách hàng giải pháp toàn diện trong việc đảm bảo an toàn, an ninh thông tin, dữ liệu cho khách hàng. Các thiết bị tường lửa thế hệ tiếp theo của FortiGate sử dụng các bộ, chức năng xử lý được xây dựng dựa trên mục đích và dịch vụ bảo mật ngăn chặn các mối đe dọa thông minh. Một số chức năng chính của dòng sản phẩm FortiGate của Fortinet đó là:

• Ngăn chặn tất cả các truy cập trái phép, sau đó phân vùng truy cập và bộ lọc gói tin một cách rõ rang, triệt để.

• Các kết nối mạng riêng ảo: giúp cung cấp các kết nối bảo mật đến những tài nguyên quan trọng (Ipsec & SSL VPN).

• URL Filtering: tính năng lọc URL.

• Antivirus/AntiSpyware: chống lại các thành phần gián điệp mạng nội bộ, ngăn các nội dung độc hại lan truyền trong mạng cục bộ LAN.

• Antispam: lọc và loại bỏ tin rác đi vào trong hệ thống mạng nội bộ.

• Cung cấp các công nghệ thông tin thế hệ tiếp theo, kiểm soát ứng dụng (Application Control).

3. Triển khai phân tích, so sánh và đánh giá hiệu suất tường lửa

3.1. Đặt vấn đề

Với các sản phẩm khi đưa ra thị trường, các hãng thường có các tài liệu giới thiệu các thông số kỹ thuật cho sản phẩm của mình. Tuy nhiên, để có thể đánh giá toàn diện được hiệu quả của hai tường lửa một cách khách quan trên thực tế, nhóm tác giả tham khảo các chức năng chính do nhà sản xuất đưa ra, sau đó thực nghiệm mô phỏng

một số tính năng chính thường được sử dụng trên thực tế trên mô hình mạng (trong phòng thí nghiệm). Thông qua nhiều lần lặp lại, kết quả phân tích đánh giá được trình bày kỹ ở các phần tiếp theo của nghiên cứu để có kết quả định lượng có tính chính xác cao nhất có thể. Từ đó mới có kết luận chuẩn xác về hiệu suất sản phẩm tường lửa với các số liệu cụ thể, tăng độ tin cậy cho người dùng khi muốn lựa chọn loại tường lửa cho hệ thống của mình [12]-[15].

3.2. Triển khai phân tích, so sánh

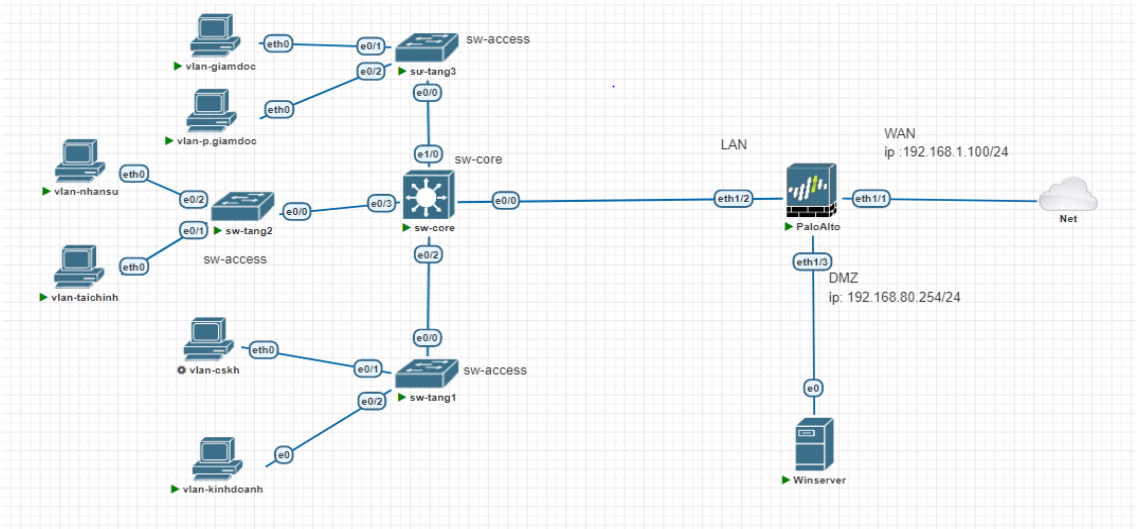
Trong phạm vi nghiên cứu này, nhóm tác giả sử dụng phiên bản Fortigate FG-30E và Palo Alto PA-200. Đây là hai sản phẩm cùng phân khúc được thiết kế để cung cấp các giải pháp bảo mật phù hợp cho các doanh nghiệp vừa và nhỏ với các tính năng tương tự nhau.

Để kết luận được định lượng đầu ra (output) của nghiên cứu này, nhóm tác giả thực hiện việc phân tích, so sánh hiệu suất hai loại tường lửa dựa trên:

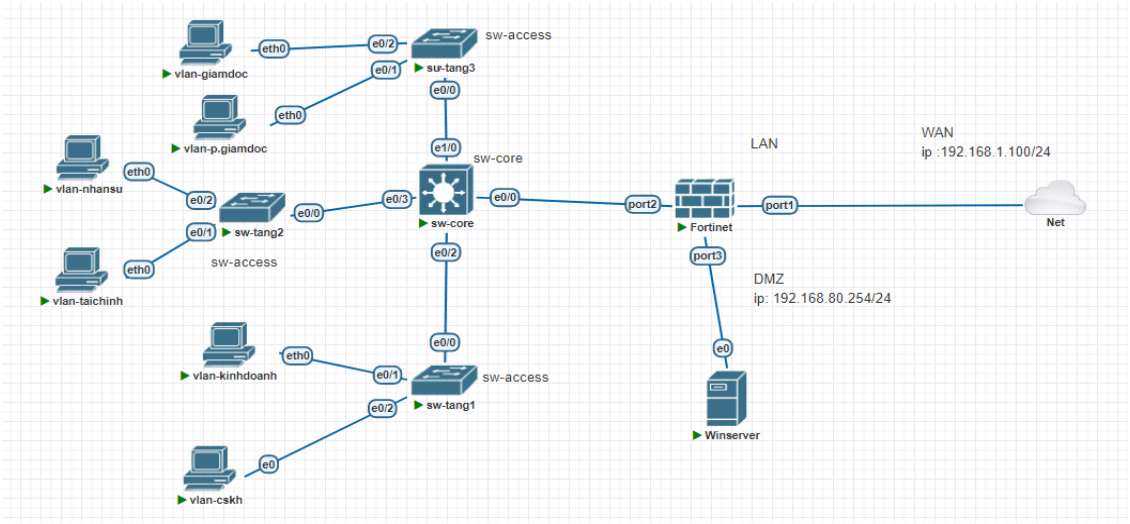
- *Kịch bản tấn công hệ thống mạng kiểu UDP Flood và TCP Flood*
- *So sánh chức năng SSL/TLS Inspection*
- *So sánh chức năng Application Control*
- *Kiểm tra lưu lượng gói tin*
- *Độ trễ của gói tin*
- *Thời gian phản hồi gói tin*
- *Thông lượng trung bình*

3.2.1. Kịch bản tấn công hệ thống mạng kiểu UDP Flood và SYN Flood

Thực hiện tấn công đứng từ bên ngoài Internet tấn công vào vùng mạng nội bộ của công ty để xem Firewall có ngăn chặn được các cuộc tấn công hay không, cụ thể ở đây là tấn công *UDP Flood và SYN Flood* trên hai loại tường lửa. Mô hình mạng tích hợp mỗi loại tường lửa được thể hiện như Hình 1 và Hình 2:



Hình 1: *Mô hình tích hợp Firewall Palo Alto*



Hình 2: *Mô hình tích hợp Firewall Fortinet*

a. Trên Palo Alto Firewall

Thực hiện tấn công UDP Flood:

Trước khi tấn công: Truy cập vào một website bất kỳ, ví dụ trong nghiên cứu này sử dụng www.dantri.com.vn ta thấy máy chủ của trang web này vẫn phản hồi và hoạt động bình thường. Tiếp đến chúng ta sử dụng công cụ LOIC (Low Orbit Ion Cannon) để tấn công UDP Flood tới địa chỉ của Palo Alto Firewall là 192.168.1.100.

Sau khi tấn công: Sử dụng công cụ Glasswire để xem lại thông số lưu lượng Card mạng thì có thể thấy máy nạn nhân đã nhận tới 400 kb/s dữ liệu và hiệu suất CPU lên tới mức 98% tuy nhiên dung lượng RAM không thay đổi là bao, cụ thể ở đây là 28%. Bên cạnh đó, để xem máy nạn nhân có còn truy cập được web nữa không chúng ta thử kiểm tra truy cập lại website ban đầu. Kết quả cho thấy tốc độ truy cập của máy nạn nhân bị giảm do dung lượng CPU đã tăng cao khi bị tấn công.

Thực hiện tấn công TCP Syn Flood:

Tương tự như trên, trước khi tấn công truy cập vào một website bất kỳ, ví dụ trong nghiên cứu này sử dụng www.dantri.com.vn ta thấy máy chủ của trang web này vẫn phản hồi và hoạt động bình thường. Tiếp đến chúng ta sử dụng công cụ TCP Syn-flood để tấn công tới địa chỉ của Palo Alto Firewall là 192.168.1.100. Sau khi tấn công, kiểm tra kết quả ta thấy trên máy nạn nhân: vẫn truy cập website ban đầu bình thường; lưu lượng Card mạng tăng lên 60 kb/s; CPU sử dụng hết 39% và RAM sử dụng hết 26%.

b. Trên Fortinet Firewall

Thực hiện kỹ thuật tương tự như phần trên đến website www.dantri.com.vn, kết quả thu được như sau:

Thực hiện tấn công UDP Flood: Kiểm tra trên máy nạn nhân sau khi bị tấn công: lưu lượng Card mạng có tăng nhưng không đáng kể cụ thể là 60 kb/s; CPU tiêu thụ hết 88%, RAM tiêu thụ hết 23%; ngoài ra khi kiểm tra trên giao diện của Firewall ta thấy đã phát hiện cũng như chặn được cuộc tấn công UDP Flood.

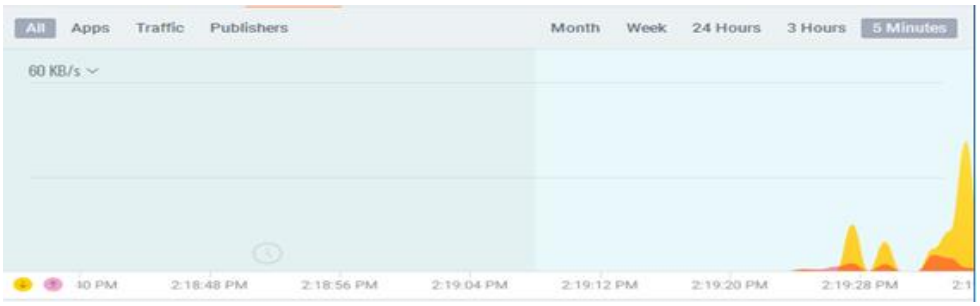
Thực hiện tấn công TCP Syn Flood: Kiểm tra trên máy nạn nhân sau khi bị tấn công: lưu lượng Card mạng tăng lên 20 kb/s; CPU tiêu thụ hết 42%, RAM tiêu thụ hết 23%.

c. Kết luận đánh giá

Thông qua các số liệu thu được từ kết quả của các cuộc tấn công vào máy nạn nhân trong mỗi trường hợp khác nhau sử dụng hai loại tường lửa, ta có được:

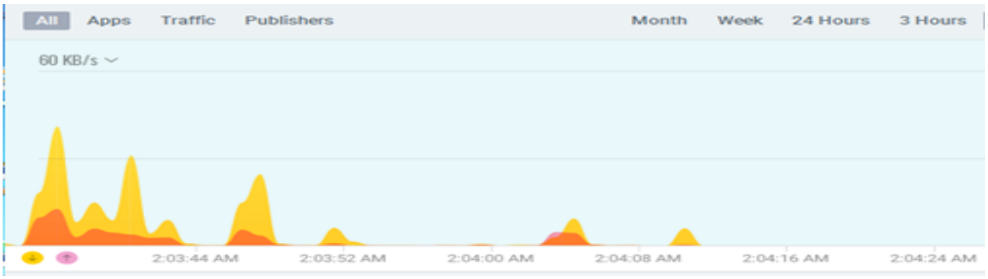
Biểu đồ so sánh tấn công kiểu *UDP Flood* như trong Hình 3 và Hình 4:

Hình 3. *Kiểm tra lưu lượng Card mạng tấn công UDP trên Palo Alto Firewall*

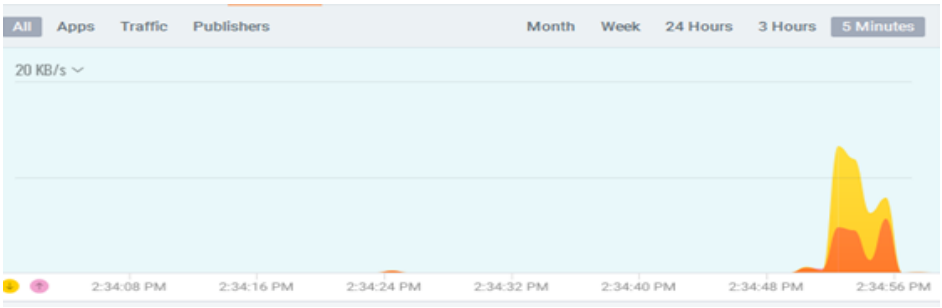


Hình 4: *Kiểm tra lưu lượng Card mạng tấn công UDP trên Fortinet Firewall*

Biểu đồ so sánh kiểu tấn công *TCP Flood* như trong Hình 5 và Hình 6:

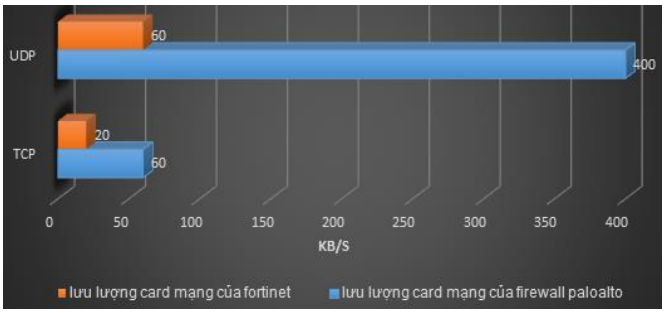


Hình 5: *Kiểm tra lưu lượng Card mạng tấn công TCP trên Firewall Palo Alto*

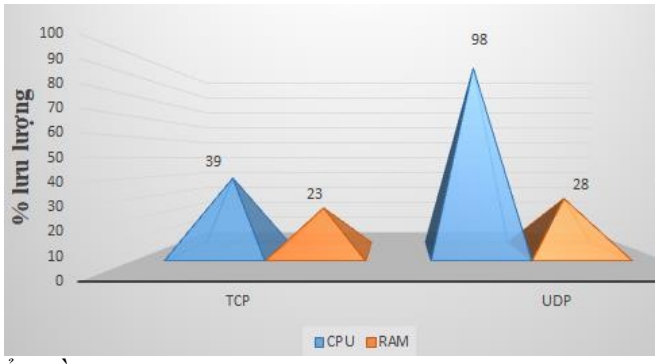


Hình 6: *Kiểm tra lưu lượng Card mạng tấn công TCP trên Firewall Fortinet*

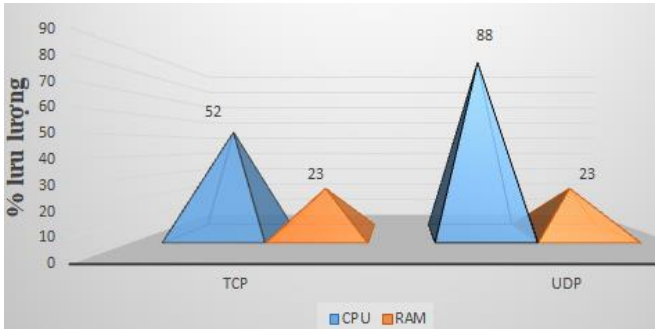
Biểu đồ so sánh lưu lượng Card mạng, CPU/RAM như trong Hình 7, Hình 8 và Hình 9:



Hình 7: *Biểu đồ lưu lượng Card mạng sử dụng trên Palo Alto & Fortinet Firewall*



Hình 8: *Biểu đồ lưu lượng CPU và RAM sử dụng trên Firewall Palo Alto*



Hình 9: *Biểu đồ lưu lượng CPU và RAM sử dụng trên Firewall Fortinet*

Từ các số liệu thu thập được và thông qua biểu đồ này ta có thể đưa ra nhận xét như sau: cả hai Firewall trong hai trường hợp bị tấn công TCP và UDP thì đều có khả năng ngăn chặn cuộc tấn công nhưng ở trên Fortinet Firewall có khả năng ngăn chặn tốt hơn Palo Alto Firewall.

3.2.2. So sánh chức năng SSL/TLS Inspection

Tính năng SSL/TLS Inspection giúp hệ thống giám sát được tất cả lưu lượng hoạt động trong mạng với Web và App sử dụng các giao thức mã hoá trên Internet (SSL, TLS…) từ đó có thể phát hiện được các mối đe doạ, Virus, Ransomware được truyền qua các kết nối được mã hoá và thực thi các kết nối an toàn giữa Client và Server trên Internet. Để tiến hành so sánh thì ta dựa trên việc đưa ra các trang Web có tiềm ẩn Virut

và xem thử trên các Firewall có thể ngăn chặn được không. Cụ thể ta đứng ở vùng DMZ (theo sơ đồ mạng) có Window Sever để thực nghiệm. Nghiên cứu này sử dụng một trang web tiềm ẩn virus như *www.eicar.org* để thử xem khả năng ngăn chặn của hai Firewall trước và sau khi tiến hành cấu hình SSL/TLS Inspection. Sau khi thực hiện các thử nghiệm, kết quả cho thấy: trên cả Palo Alto Firewall và Fortinet Firewall sau khi cấu hình SSL/TLS Inspection, các Firewall đã phát hiện ra mối nguy hại và tiến hành chặn luôn trang web.

3.2.3. So sánh chức năng Application Control

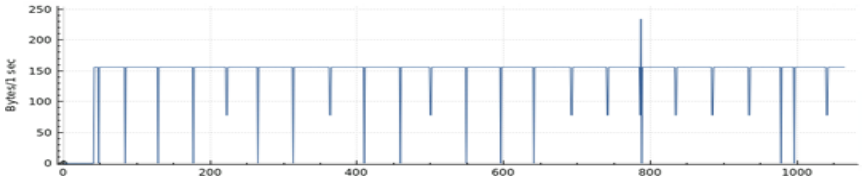
Trên tường lửa thế hệ mới, chức năng Application Control cung cấp khả năng hiển thị rộng rãi cho việc sử dụng ứng dụng trong thời gian thực, cũng như xu hướng quản lý theo thời gian thông qua chế độ hiển thị và báo cáo. Có thể sử dụng Application Control để cho phép những ứng dụng phần mềm nào được chạy trên hệ thống, giảm bớt khó khăn trong quá trình triển khai và cập nhật thông tin danh sách ứng dụng một cách liên tục. Thực hiện kiểm tra chức năng này trên hai tường lửa như sau: Giả sử muốn chặn một host không được sử dụng ứng dụng này nhưng vẫn có thể sử dụng các ứng dụng khác (ví dụ chặn ứng dụng *youtube* và cho phép sử dụng *facebook* bằng việc thiết lập các cấu hình trên giao diện của hai tường lửa) kết quả cho thấy số liệu như Bảng 1:

Bảng 1: *Bảng thông tin so sánh chức năng Application Control trên hai loại tường lửa*

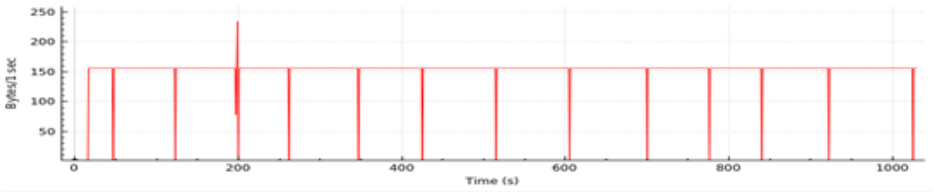
Thực hiện chức năng	Fortinet Firewall	Palo Alto Firewall
Khả năng chặn các ứng dụng	*Có*	*Có*
Khả năng kiểm soát ứng dụng và giám sát ứng dụng	*Có*	*Không*

Thông qua việc thiết lập, triển khai cấu hình và thực nghiệm cho thấy Fortinet Firewall tiên tiến hơn cũng như tối ưu hơn khi cho phép người quản trị có thể kiểm soát ứng dụng được tốt hơn trên thực tế. Thực hiện gửi 1000 gói tin từ máy (host) có tên *vlan-taichinh* thuộc vùng mạng LAN đến máy Server thuộc vùng DMZ có dải địa chỉ 192.168.70.1/24 sau đó sử dụng Wireshask để bắt gói tin trên đường truyền.

3.2.4. Lưu lượng gói tin trên đường truyền

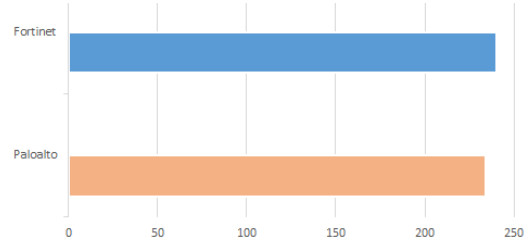


Hình 10: *Lưu lượng gói tin trên Palo Alto Firewall*



Hình 11: *Lưu lượng gói tin trên Fortinet Firewall*

Như trong Hình 10 và Hình 11, chúng ta có thể thấy rằng lưu lượng gói tin trên đường truyền của từng hệ thống khi sử dụng mỗi Firewall là không khác nhau nhiều nhưng ở trên Palo Alto Firewall có sự ổn định hơn, cao nhất là 234 byte/s thấp nhất là 0 byte/s; còn trên Fortinet Firewall cao nhất là 240 byte/s, thấp nhất là 0 byte/s. Biểu đồ so sánh như trong Hình 12:



Hình 12: *Biểu đồ so sánh lưu lượng gói tin*

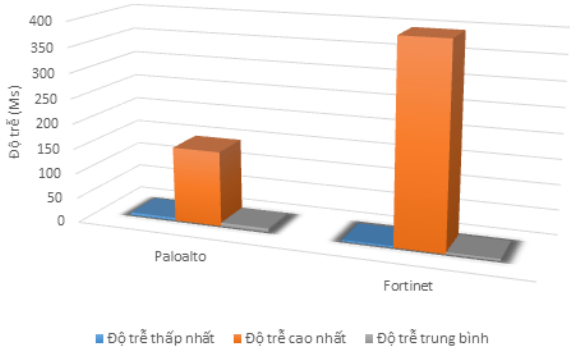
3.2.5. Độ trễ của gói tin

Thông qua việc phân tích các thông số từ việc sử dụng lệnh Ping với số gói tin gửi đi là 1000 gói (packet), ta lập được bảng thông tin chi tiết như trong Bảng 2:

Bảng 2: *Thông tin về độ trễ gói tin sau khi thu thập từ hệ thống*

Thông tin	Palo Alto	Fortinet
Số gói tin gửi	*1000*	*1000*
Số gói tin nhận	*1000*	*1000*
Tỉ lệ mất gói	*0%*	*0%*
Độ trễ thấp nhất	*5 ms*	*3 ms*
Độ trễ cao nhất	*150 ms*	*397 ms*
Độ trễ trung bình	*7 ms*	*4 ms*

Thông qua Bảng 2, ta xây dựng được biểu đồ như trong Hình 13:



Hình 13: *Biểu đồ so sánh độ trễ gói tin khi sử dụng hai loại tường lửa khác nhau*

Qua bảng số liệu và biểu đồ so sánh ta thấy rằng rằng độ trễ trên đường truyền thấp nhất của Fortinet Firewall là 3 ms thấp hơn so với Palo Alto Firewall là 5 ms ; độ trễ cao nhất của Fortinet Firewall (397 ms) cao hơn của Palo Alto Firewall (150 ms); độ trễ trung bình của Fortinet Firewall (4 ms) thấp hơn của Palo Alto Firewall (7 ms). Từ đó có thể thấy rằng độ trễ trên đường truyền của Fortinet Firewall là tối ưu hơn của Palo Alto Firewall.

3.2.6. Thời gian phản hồi gói tin

Sử dụng Wireshark bắt thông tin về việc gửi và nhận gói tin, ta thu được Bảng 3:

Bảng 3: *Thời gian phản hồi gói tin với mỗi hệ thống sử dụng tường lửa*

Thông số	Palo Alto Firewall	Fortinet Firewall
Thời gian phản hồi gói tin	*1021.76 (ms)*	*1011.34(ms)*

Có thể thấy khi gửi 1000 gói tin từ máy PC nguồn đến máy PC đích trên hai mô hình sử dụng Fortinet Firewall và Palo Alto Firewall, ta thấy hệ thống có sử dụng Fortinet Firewall tối ưu trong việc phản hồi gói tin hơn Palo Alto Firewall (thời gian phản hồi nhanh hơn trong thực nghiệm này là 10,42 ms).

3.2.7. Thông lượng trung bình

Cũng thông qua việc gửi số lượng gói tin là 1000 và sử dụng Wireshark để truy vết, lấy thông tin ta có được Bảng 4:

Bảng 4: *Thông tin về thông lượng trung bình của hệ thống khi sử dụng hai tường lửa*

Thông số	Palo Alto	Fortinet
Thông lượng trung bình	*320.57 byte/s*	*328.56 byte/s*

Qua bảng số liệu ta thấy được thông lượng trung bình trên Fortinet Firewall (là 328.56 byte/s) cao hơn Palo Alto Firewall là (320.57 byte/s). Ở phần so sánh này thì Palo Alto Firewall tốt hơn Fortinet Firewall.

3.3. Đánh giá tổng hợp

Dưới đây là các bảng so sánh hiệu suất mỗi tường lửa khi tiến hành các kịch bản mô phỏng thực nghiệm đã thực hiện ở các phần trên, số liệu cụ thể được thể hiện như trong Bảng 5, Bảng 6, Bảng 7, và Bảng 8:

Bảng 5: *Kết quả khi so sánh cuộc tấn công TCP và UDP flood*

Thông số	Tấn công TCP trên Palo Alto Firewall	Tấn công UDP trên Palo Alto Firewall	Tấn công TCP trên Fortinet Firewall	Tấn công UDP trên Fortinet Firewall
Lưu lượng Card mạng	*60kb/s*	*400kb/s*	*20kb/s*	*60kb/s*
Lưu lượng Cpu sử dụng	*39%*	*98%*	*42%*	*88%*
Lưu lượng Ram sử dụng	*26%*	*28 %*	*23%*	*23%*
Làm ngừng truy cập mạng	*Không*	*Không*	*Không*	*Không*
Chặn đứng các cuộc tấn công	*Có*	*Một phần*	*Có*	*Có*
Phát hiện các cuộc tấn công	*Có*	*Có*	*Có*	*Có*

Bảng 6: *Kết quả so sánh dựa trên tính năng của hai Firewall*

Chức năng	Palo Alto Firewall	Fortinet Firewall
Tính năng SSL/TLS Inspection	*Có*	*Có*
Tính năng Application Control	*Có nhưng không chi tiết*	*Có chi tiết*
Tính năng giám sát và kiểm soát ứng dụng	*Không*	*Có*
NAT	*Có*	*Có*
Mức độ nhận biết ứng dụng	*Một phần*	*Có*
VPN	*Có*	*Có*

Bảng 7: *Hiệu xuất sử dụng khi gửi gói tin từ Client đến Server đi qua Firewall*

Thông số	Firewall Palo Alto	Firewall Fortinet
Số gói tin	*1000*	*1000*
Số gói nhận	*1000*	*1000*
Tỉ lệ mất gói	*0%*	*0%*
Độ trễ thấp nhất	*5 ms*	*3 ms*
Độ trễ cao nhất	*150 ms*	*397 ms*
Độ trễ trung bình	*7 ms*	*4 ms*
Thời gian phản hồi gói tin	*1021.76 (s)*	*1011.34(s)*
Thông lượng trung bình	*320.57 byte/s*	*byte/s*

Bảng 8: *Giá thành sản phẩm*

Tham số	Firewall Palo Alto	Firewall Fortinet
Giá thành sản phẩm	*Đắt hơn*	*Rẻ hơn*

Thông qua các phần so sánh với số liệu thu thập được như đã trình bày có thể đưa ra nhận xét: cả hai loại/hãng đều là những tường lửa có tính ưu việt và đáng sử dụng nhưng có một phần nào đó trên Fortinet Firewall có điểm nổi trội hơn so với Palo Alto Firewall.

4. Kết luận

Bài báo đã phân tích, so sánh đầu vào (input) và tìm được kết quả đầu ra (output) với các thông số định lượng rõ ràng. Trong phạm vi nghiên cứu này sử dụng hai tường lửa cùng phân khúc của hai hãng phù hợp với các hệ thống mạng vừa và nhỏ tại Việt Nam. Dựa trên các phân tích và số liệu thu được ta thấy mỗi loại sản phẩm đều có ưu, nhược điểm riêng. Do đó trên thực tế, dựa trên các kịch bản đã trình bày tùy vào từng trường hợp cụ thể mà người sử dụng có thể lựa chọn sản phẩm nào cho hệ thống của mình để đạt được hiệu quả cao nhất. Kết quả nghiên cứu sẽ là tài liệu cần thiết cho nhà thiết kế, đảm bảo an toàn, an ninh hệ thống mạng và cho các học viên, sinh viên chuyên ngành công nghệ thông tin, an toàn thông tin tham khảo để đưa ra các quyết định phù hợp khi sử dụng hai loại tường lửa thế hệ tiếp theo này.

Lời cảm ơn: Nhóm tác giả xin được bày tỏ lòng biết ơn đến Trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên đã hỗ trợ một phần kinh phí cho nghiên cứu này theo đề tài cấp cơ sở mã số T2022-07-08.

TÀI LIỆU THAM KHẢO

[1] T. Plens, *Mastering Palo Alto Networks*, Packt Publishing, 2020.

[2] O. Shmueli, *Fortigate Firewall Admin Pocket Guide*, FortiTip, 2021.

[3] R. Baloch, *Ethical Hacking and Penetration Testing Guide*, CRC Press, 2015.

[4] T. Hayajneh et al., "Performance and Information Security Evaluation with Firewalls," *International Journal of Security and Its Applications, SERSC*, Vol. 7, No. 6, pp. 355-372, 2013.

[5] F. Malecki, "Next-generation Firewalls: Security with performance," *Network Security*, Vol. 2012, No. 12, pp.19-20, 2012.

[6] K. Neupane, "Next Generation Firewall for Network Security: A Survey," *Conference: SoutheastCon 2018*, 2018. DOI:10.1109/SECON.2018.8478973.

[7] M. Faizan et al., "Comparison between Cisco ASA and Fortinet FortiGate", *Journal of Electrical and Computer Engineering*, Vol. 21, No. 3, pp. 34-36, 2019.

[8]. A. Maraj et al., "Testing of network security systems through DoS attacks," *Embedded Computing (MECO), 6th Mediterranean Conference on. IEEE, 2017.*

[9] A. Maraj *et al.*, "Testing techniques and analysis of SQL injection attacks," *Knowledge Engineering and Applications (ICKEA), 2017 2nd International Conference on. IEEE*, 2017.

[10] D. Loganathan, and K. Ramesh, "Prevention Mechanism for Denial of Service in Web Applications Services," *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, No. 4, pp. 480-484, 2015.

[11] G. Weidman, *Penetration Testing: A Hands-on Introduction to Hacking*, No Starch Press, 2014.

[12] L. H. Hiep et al., "Improve network security system in Vietnam using reverse method", *TNU Journal of Science and Technology*, Vol. 225, No. 09, pp. 125-133, 2020.

[13] L. H. Hiep et al., "Study to applying Blockchain technology for preventing of spam email," *TNU Journal of Science and Technology*, Vol. 208, No. 15, pp. 161-167, 2019.

[14] A. Alhasan and N. Surantha, "Evaluation of Data Center Network Security", *International Journal of Advanced Computer Science and Applications*, Vol. 12, No. 9, pp. 518-525, 2021.

[15] B. Soewito, "Next-generation Firewall for improving security in company and IoT network". *Conference: 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 2019. DOI:10.1109/ISITIA.2019.8937145.

SUMMARY

STUDY TO ANALYSE, COMPARE AND EVALUATE THE PERFORMANCE OF NEXT GENERAL FIREWALLS: CASE OF PALO ALTO AND FORTIGATE FIREWALL

Nguyen Ngoc Hoan, Le Hoang Hiep, Do Dinh Luc
University of Information and Communication Technology, Thai Nguyen University
Received on 08/4/2022, accepted for publication on 22/6/2022

The article focuses on analyzing, comparing, and evaluating the performance of the next-generation firewalls, case of Palo Alto Firewall and Fortinet Firewall in practice through the deployment of simulated situations and experimental scenarios that are: using network attacks such as TCP, UDP Flood; evaluate the function of SSL/TLS Inspection, Application Control; check traffic, latency, packet response time and average throughput values on each network system with each separate firewall. The result shows that both types of firewalls have outstanding performance compared with older generation firewalls and Fortinet Firewall has more outstanding points than Palo Alto Firewall in particular. The research results will be necessary documents for designers, ensuring network safety and security of the network system, and for students and students majoring in Information Technology and Information Security as a reference to make appropriate decisions when using these two types of next-generation firewalls.

Keywords: Computer science; network security; Palo alto firewall; Fortigate firewall; network attack.