TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

THÁI NGUYÊN

ĐỒ ÁN TỐT NGHIỆP

CHUYÊN NGÀNH MẠNG MÁY TÍNH

ĐỀ TÀI

NGHIÊN CỨU ĐÁNH GIÁ HIỆU NĂNG CỦA MỘT SỐ FIREWALL THẾ HỆ MỚI, ÁP DỤNG TRIỂN KHAI TRÊN HẠ TẦNG MẠNG CỦA CÔNG TY CÔNG NGHỆ MỚI BẢO THẮNG - HÀ NỘI.

SVTH: HOÀNG TRUNG DŨNG

LỚP: CNTT-K16K

GVHD: THS. LÊ HOÀNG HIỆP

Thái Nguyên, tháng 2 năm 2022

MỤC LỤC

LỜI CẢM ƠN

Sau hơn bốn tháng nỗ lực tìm hiểu, nghiên cứu và thực hiện, đề tài "***Nghiên cứu đánh giá hiệu năng của một số Firewall thế hệ mới, Áp dụng triển khai trên hạ tầng mạng của Công ty Công nghệ mới Bảo Thắng - Hà Nội***" đã được hoàn thành, ngoài sự cố gắng hết mình của bản thân, em còn nhận được nhiều sự động viên, khích lệ từ gia đình, thầy cô và bạn bè.

Em xin chân thành cảm ơn các thầy cô của Trường đại học Công Nghệ Thông Tin & Truyền Thông Thái Nguyên đã truyền đạt nhiều kinh nghiệm và kiến thức quý báu cho em trong suốt quá trình học tập tại trường. Đặc biệt em xin tỏ lòng biết ơn sâu sắc tới Thầy ***ThS. Lê Hoàng Hiệp*** – giảng viên Bộ môn Mạng & An toàn thông tin, Khoa Công nghệ thông tin đã tận tình giúp đỡ em trong suốt quá trình thực hiện đồ án tốt nghiệp này.

Thái Nguyên , tháng 2 năm 2022

Sinh viên thực hiện

Hoàng Trung Dũng

LỜI CAM ĐOAN

Tôi cam đoan đồ án tốt nghiệp này là do bản thân tự nghiên cứu và thực hiện theo sự hướng dẫn khoa học của ***ThS. Lê Hoàng Hiệp.***

Tôi xin hoàn toàn chịu trách nhiệm về tính pháp lý trong quá trình nghiên cứu khoa học của đồ án tốt nghiệp này.

Thái Nguyên, Tháng 02, Năm 2022

Sinh viên

Hoàng Trung Dũng

CHƯƠNG I. GIỚI THIỆU VỀ THẾ HỆ TƯỜNG LỬA MỚI ĐẠI DIỆN FIREWALL PALOALTO VÀ FIREWALL FORTIGATE

1. GIỚI THIỆU CHUNG

1.1. Firewall thế mới là gì & đưa ra 2 đại diện cho firewall thế hệ mới

NGFW (Next-generation Firewall) là công nghệ tường lửa thế hệ thứ ba, dựa trên phần cứng hoặc phần mềm, có khả năng phát hiện và ngăn chặn các cuộc tấn công tinh vi bằng cách thực thi chính sách bảo mật ở mức độ ứng dụng, giao thức và cổng.

Ngoài các chức năng của tường lửa truyền thống hỗ trợ:

- Kiểm tra trạng thái lưu lượng mạng bằng cách giám sát trạng thái các kết nối đang hoạt động để xác định các gói tin được phép.
- Xác định lưu lượng được phép truy cập hoặc từ chối dựa trên trạng thái kết nối, cổng, và giao thức.
- Sử dụng các quy tắc (Rules) và chính sách quản trị ứng dụng để xác định loại lưu lượng mạng được phép và không được phép đi qua

NGFW kết hợp các chức năng tường lửa truyền thống với các tính năng của thiết bị mạng như tường lửa ứng dụng, IPS, kiểm tra lưu lượng mã hóa TLS/SSL, lọc trang web, chất lượng dịch vụ (QoS)/quản lý băng thông, kiểm tra chống virus, và tích hợp quản lý LDAP, RADIUS, và Active Directory,...

Một số chức năng phổ biến trên các sản phẩm NGFW:

- **Hỗ trợ các tính năng của tường lửa tiêu chuẩn**: bao gồm các chức năng tường lửa như kiểm tra trạng thái giao thức/cổng, Network Address Translation (NAT) và mạng riêng ảo (VPN),...
- **Nhận dạng và lọc lưu lượng dựa trên các ứng dụng cụ thể**: ngăn chặn các ứng dụng độc hại và hoạt động từ việc sử dụng cổng non-standard để tránh tường lửa. Một NGFW sẽ đóng vai trò kiểm soát lưu lượng, kiểm tra lưu lượng gửi, nhận và nội dung của gói tin để ngăn chặn các cuộc tấn công ứng dụng diễn ra trên các lớp 4-7 của mô hình OSI.
- **Kiểm tra SSL và SSH**: NGFW có thể kiểm tra lưu lượng mã hóa SSL và SSH, cho phép giải mã lưu lượng của ứng dụng được phép, kiểm tra các chính sách khác, và sau đó tái mã hóa lưu lượng. Điều này cung cấp bảo vệ hệ thống mạng đối với các ứng dụng độc hại và các hoạt động xâm nhập bằng cách sử dụng mã hóa để tránh tường lửa.
- **Chức năng ngăn chặn xâm nhập**: IPS, cung cấp kiểm tra "sâu" lưu lượng, phát hiện và phòng ngừa xâm nhập.
- **Tích hợp Directory:** hầu hết các NGFW hỗ trợ Active Directory, LDAP, quản lý các ứng dụng dựa trên người dùng có thẩm quyền và các nhóm người dùng.
- **Lọc mã độc**: ngăn chặn virus, trang web, các gói tin và các ứng dụng độc hại.

Chúng ta có thể thấy rằng ở thời điểm hiện tại có rất nhiều hãng đã có và triển khai cũng như có các dòng firewall thế hệ mới kể đến như Fortinet, Paloalto, Sophos, Checkpoin, Cisco, Huawai,Juniper. Nhưng ở trong bài báo cáo này em xin chọn ra hai hãng firewall tiêu biểu nhất đó là Fortinet và Paloalto để so sánh và đưa ra lựa chọn phù hợp nhất cho công ty Bảo Thắng tại sao lại lựa chọn hai hãng firewall này bởi vì dựa trên kinh phí và cũng do một phần là ở trên hệ thống máy của em không đủ khả năng để có thể thử nghiệm và đưa ra so sánh công bằng nhất và cũng bởi vì hai hãng Paloalto và Fortinet cũng là hai hãng chiếm thị phần lớn firewall thế hệ mới nên em quyết định đưa ra hai đề cử như trên.

1.2. Giới thiệu về Firewall Paloalto :

Palo Alto Networks là tường lửa thế hệ tiếp theo được triển khai tại nhiều điểm trong doanh nghiệp. Với khả năng hiển thị và kiểm soát lưu lượng mạng dựa trên các ứng dụng, người sử dụng, và nội dung, chúng tôi quản lý các ứng dụng một cách an toàn, ngăn chặn các mối đe dọa, và đơn giản hóa cơ sở hạ tầng

1.2.1. Các ưu điểm có thể kể đến như sau :

- Nền tảng vận hành bảo mật với **tường lửa Palo Alto Networks** cho phép bạn tự động hóa nhận dạng và thực thi mối đe dọa trên đám mây, mạng và điểm cuối của bạn.
- Giảm các bề mặt tấn công và ngăn chặn các mối đe dọa bằng cách bật ứng dụng một cách an toàn
- Cung cấp chính sách tự động, thời gian thực cho mọi môi trường
- Mở rộng bảo vệ cho các công nghệ mới và mạng ảo
- Sử dụng một hệ sinh thái chia sẻ mối đe dọa tình báo rộng lớn

1.2.2. Các tính năng có thể kể đến như sau :

- Tính năng nhận dạng người dùng UserID:

Tích hợp với Microsoft Active Directory kết nối địa chỉ IP với người dùng, nhóm cho phép phòng IT kiểm soát ứng dụng, nội dung dựa trên thông tin nhân viên được lưu trong Active Directory. User-ID cho phép nhà quản trị kết hợp thông tin người dùng với ứng dụng, tạo policy, log dữ liệu và báo cáo. Với kiến trúc phần cứng được thiết kế riêng biệt, firewall thế hệ mới Palo Alto mang lại sự tường minh và khả năng kiểm soát hoạt động mạng của người dùng.

- Tính năng kiểm soát và ngăn chặn các mối đe doạ bằng ContentID:

` Một engine quét dựa trên luồng dữ liệu (stream-based engine) giúp kiểm soát các dữ liệu mã hóa mà không làm giảm hiệu suất của hệ thống. Tích hợp tính năng Threat Prevention vào firewall với các tính năng: dò tìm và chặn viruses, spyware, worms và lỗ hổng ứng dụng, kiểm soát việc truyền file hay thông tin nhạy cảm ra khỏi hệ thống, thực hiện scan ngay khi packet đầu tiên đến.

- Tính năng lọc web bằng URL Filtering:

Các tính năng lọc của Palo Alto hiệu quả hơn rất nhiều so với các tính năng lọc của Firewall truyền thống. Bao gồm: lọc file theo chủng loại, giải nén file nén để nhận dạng các file bên trong, nhận dạng đến cả nội dung bên trong file…Palo Alto còn tích hợp cơ sở dữ liệu với hơn 20 triệu URL với trên 76 categories vào trong firewall cho phép kiểm soát việc truy cập web của người dùng ngăn chặn người dùng truy cập vào các trang web chứa mã độc, virus hoặc các trang web không phù với các chính sách của công ty.

- Truy cập ứng dụng một cách an toàn với App-ID:

Sử dụng 4 cơ chế phân loại dữ liệu khác nhau, App-ID™ nhận dạng chính xác các ứng dụng nào thực sự đang chạy trên hạ tầng mạng mà không phụ thuộc vào ứng dụng đó đang chạy trên cổng dịch vụ gì, giao thức nào, hay đã được mã hóa SSL hay không. Nhờ đó giúp người quản trị có thể tạo những chính sách toàn diện để quản lí việc sử dụng ứng dụng và traffic inbound và outbound để gia tăng sự bảo mật của hệ thống hạ tầng mạng.

App-ID cho phép bạn hiểu và kiểm soát các ứng dụng và chức năng của chúng, chẳng hạn như truyền phát video so với trò chuyện, tải lên so với tải xuống, chia sẻ màn hình so với điều khiển thiết bị từ xa, v.v.

- Lưu lượng được mã hoá an toàn mà không thoả hiệp quyền riêng tư với Decryption:

Người dùng dành hơn 80% thời gian cho các trang web và ứng dụng được mã hóa. Thật không may, những kẻ tấn công khai thác mã hóa để che giấu các mối đe dọa từ các thiết bị bảo mật. Tường lửa thế hệ tiếp theo của Palo Alto sử dụng giải mã dựa trên chính sách để cho phép các chuyên gia bảo mật giải mã lưu lượng độc hại nhằm mục đích ngăn chặn các mối đe dọa, nhưng vẫn bảo vệ quyền riêng tư của người dùng và hiệu suất có thể dự đoán được.

- Ngăn chặn các mối đe doạ chưa được biết đến với WildFire:

Palo Alto đã tạo ra môi trường phân tích WildFire, đây là nơi dùng để phân tích các mối nguy hai chưa biết đến mà các thiết bị tường lửa Palo Alto gửi về. Quy trình hoạt động của tính năng này diễn ra như sau.

Khi thiết bị tường lửa Palo Alto phát hiện một mẫu không xác định (tệp hoặc liên kết trong email), tường lửa sẽ tự động chuyển tiếp các mẫu này đến môi trường WildFire để thực hiện phân tích.

Dựa trên các thuộc tính, hành vi, hoạt động của các mẫu này trong quá trình phân tích và thực hiện trên môi trường WildFire, nó sẽ đưa ra kết luận các mẫu này có lành tình không hay là các mẫu chưa virus độc hại.

Nếu WildFire xác định các mẫu này là độc hại nó sẽ tạo signature cho các mẫu vừa xác định và thực hiện chia sẻ lên tất cả các thiết bị Palo Alto trên toàn cầu. Tất cả các quá trình từ gửi file, phân tích, xác định mẫu phân tích và chia sẻ toàn cầu đều được diễn ra trong thời gian thực.

- Kết nối các site hoặc kết nối từ xa với VPN:

Tường lửa Palo Alto Networks hỗ trợ các triển khai VPN sau:

VPN Site-to-Site: Hỗ trợ kết nối các site lại với nhau với bộ giao thức IPSec. Bộ giao thức này sẽ thiết lập một tunnel để kết nối 2 site lại với nhau giúp cho người dùng ở cả 2 site có thể trao đổi lưu lượng mạng với nhau và đặc biệt các lưu lượng mạng khi đi qua tunnel này đều được mã hóa để tránh việc bị tấn công mạng.

VPN Remote access: Đây là một giải pháp sử dụng phần mềm GlobalProtect để cho phép người dùng từ xa thiết lập kết nối đến nơi làm việc an toàn thông qua tường lửa. Giải pháp này sử dụng SSL và IPSec để thiết lập kết nối an toàn giữa người dùng và nơi làm việc.

1.3. Firewall fortigate:

Firewall UTM Fortinet đã đi tiên phong trong khái niệm Unified Threat Management (UTM) - hợp nhất nhiều chức năng bảo mật mạng thành một thiết bị duy nhất. UTM cung cấp cho các tổ chức lớn và nhỏ một cách hiệu quả và đơn giản để đối phó với cảnh quan an ninh phức tạp ngày càng phát triển.

Khi mà việc áp dụng rộng rãi các mạng lưới giữa các doanh nghiệp vừa và nhỏ, cùng với sự bùng nổ của các thiết bị di động và các ứng dụng, đã đẩy nhanh yêu cầu bổ sung an ninh mạng cho cả mạng nhỏ nhất. Các mối đe dọa từ tin tặc, các phần mềm độc hại phức tạp, botnet và các mối đe dọa liên tục hiện đại nhấn mạnh sự cần thiết phải triển khai và thực thi các kiểm soát an ninh.

1.3.3. Các ưu điểm có thể kể đến như sau :

- **Nền tảng phần cứng :**

  Nền tảng phần cứng độc quyền FortiASIC đem lại sự ổn định, tốc độ cao và đầy đủ các tính năng mà một hệ thống bảo mật thế hệ mới cần có.

- **Các chức năng tích hợp trên thiết bị :**

  Thiết bị tích hợp tính năng chống Virus, quét Virus ra thời gian thực qua các con đường thu điện tử (SMTP, POP3, IMAP) chuyển file, web mà không làm chậm tốc độ mạng.

- **Cơ quan chứng nhận đảm bảo an ninh :**

  Đã được chứng nhận bởi ICSA về Hệ thống quản lý tốt chống virus, Firewall, VPN. Khi phát hiện ra đường dẫn Virus có thể xóa, quét tự động, cách ly để xử lý, cảnh báo người dùng.

- **Chống spam thư rác :**

  Chống thư rác không liên quan đến các từ khóa mà doanh nghiệp cài đặt trong hệ thống.

- **Đảm bảo băng thông:**

  FortiOS phân biệt các loại dữ liệu khác nhau, thiết lập được các chính sách đảm bảo chống tắc nghẽn đồng thời ưu tiên cho các ứng dụng đòi hỏi thời gian đáp ứng cao như VoIP:

  - Hệ thống lọc những trang Web an toàn, giao diện đơn giản dễ sử dụng.
  - Hệ thống phát hiện, phòng ngừa truy cập trái phép.
  - Tính năng điều khiển ứng dụng