TĂNG CƯỜNG AN NINH MẠNG BẰNG THIẾT BỊ TƯỜNG LỬA THẾ HỆ MỚI PALO ALTO

NGUYỄN DUY BÌNH,
DƯƠNG THỊ THANH TÚ,
HOÀNG SỸ LONG

THEO CÁC BẢNG ĐÁNH GIÁ, XẾP HẠNG CỦA CÁC TỔ CHỨC UY TÍN TRÊN THẾ GIỚI, VIỆT NAM ĐƯỢC XẾP HẠNG ĐÁNH GIÁ RẤT THẤP VỀ AN NINH MẠNG VÀ LUÔN LÀ MIẾNG ĐẤT MÀU MỠ CHO TỘI PHẠM CÔNG NGHỆ CAO. DO TẠI VIỆT NAM, VIỆC BẢO MẬT TRONG MẠNG CHƯA THỰC SỰ ĐƯỢC CHÚ TRỌNG HAY CŨNG CÓ THỂ DO CÁCH THỰC HIỆN CHƯA ĐÚNG, DẪN ĐẾN RẤT NHIỀU LỖ HỔNG CÓ THỂ BỊ TẤN CÔNG MỘT CÁCH DỄ DÀNG. AN NINH MẠNG LÀ MỘT VẤN ĐỀ CẤP THIẾT. TĂNG CƯỜNG AN NINH MẠNG BẰNG THIẾT BỊ TƯỜNG LỬA THẾ HỆ MỚI PALO ALTO NETWORK - MỘT TRONG CÁC GIẢI PHÁP ĐÁP ỨNG ĐƯỢC ĐẦY ĐỦ CÁC YÊU CẦU KHẮT KHE CỦA HỆ THỐNG VÀ HIỆN ĐANG ĐƯỢC TRIỂN KHAI RẤT HIỆU QUẢ TRONG CÁC HỆ THỐNG MẠNG MÁY TRÊN THẾ GIỚI. ĐÂY LÀ MỘT GIẢI PHÁP TƯỜNG LỬA THẾ HỆ MỚI MÀ VIỆT NAM CÓ THỂ TRIỂN KHAI ĐỂ ĐẢM BẢO AN NINH MẠNG.

Giới thiệu chung

Những năm gần đây, tình hình bảo mật mạng máy tính đã trở nên nóng bỏng hơn bao giờ hết khi hàng loạt các vụ tấn công, những lỗ hổng bảo mật được phát hiện hoặc bị lợi dụng tấn công. Theo Arthur Wong - Giám đốc điều hành của SecurityFocus - trung bình một tuần, phát hiện ra hơn 30 lỗ hổng bảo mật mới. Theo điều tra của SecurityFocus trong số 10.000 khách hàng của hãng có cài đặt phần mềm phát hiện xâm nhập trái phép thì trung bình mỗi khách hàng phải chịu 129 cuộc thăm dò, xâm

nhập. Những phần mềm web server như IIS của Microsoft là mục tiêu phổ biến nhất của các cuộc tấn công.

Trước tình hình đó, việc bảo vệ an toàn thông tin cho một hệ thống trước nguy cơ bị tấn công từ bên ngoài khi kết nối vào Internet là một vấn đề cấp bách. Sử dụng Firewall để bảo vệ mạng nội bộ, tránh sự tấn công từ bên ngoài là một giải pháp hữu hiệu, đảm bảo được các yếu tố: an toàn cho sự hoạt động của toàn bộ hệ thống mạng, bảo mật cao trên nhiều phương diện, khả năng kiểm soát cao, mềm dẻo và dễ sử dụng, trong suốt với người sử dụng và cuối cùng là đảm bảo được kiến trúc mở. Trong bảo mật hệ thống hiện nay, mô hình bảo mật với Firewall là mô hình chính yếu được sử dụng phổ biến trên toàn cầu. Tuy nhiên, nó vẫn gặp phải một số nhược điểm như:

- Firewall truyền thống không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Nó chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

- Firewall truyền thống không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó, chẳng hạn như những cuộc tấn công từ bên trong.

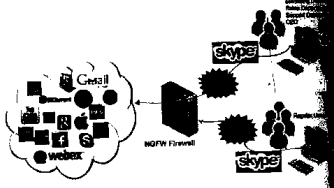
- Firewall truyền thống không thể chống lại các cuộc tấn công bởi virus, mã độc…

- Firewall truyền thống (stateful inspection firewall) chỉ nhận diện và kiểm soát được thông lượng với giao thức và cổng dịch vụ nhưng không nhận diện được ứng dụng, đặc biệt là các ứng dụng web sử dụng chung giao thức HTTP và cổng dịch vụ 80.

Với những hạn chế nêu trên của mô hình bảo mật firewall truyền thống, cùng với đó là sự phát triển mạnh mẽ và không ngừng của các kỹ thuật tấn công, yêu cầu cần phải có một mô hình bảo mật được nâng cấp, tối ưu và "thông minh" hơn nữa để đảm bảo an toàn cho hệ thống trước những mối hiểm hoạ. Giải pháp tường lửa thế hệ mới ra đời.

Mô hình bảo mật tường lửa thế hệ mới

Tường lửa thế hệ mới (Hình 1), là thiết bị tường lửa dựa trên xác thực người dùng, xác thực dựa trên ứng dụng hay nội dung. Với cơ chế này, người quản trị dễ dàng nhận dạng các ứng dụng, nội dung trong luồng dữ liệu với các mức độ nguy cơ đe dọa xuất phát từ người sử dụng nào.



Hình 1: Mô hình tường lửa thế hệ mới

Firewall thế hệ mới có rất nhiều các đặc tính cho phép nhà quản trị mạng có khả năng kiểm soát toàn diện hệ thống mạng của mình và khắc phục được những nhược điểm của Firewall truyền thống:

- Nhận dạng những ứng dụng trong hệ thống mà không phụ thuộc vào cổng hay giao thức mạng theo cách của firewall truyền thống, điều này giúp nhận diện chính xác cũng như bắt chặt các ứng dụng thông minh có khả năng chuyển đổi port hay giao thức mạng để hoạt động, nhằm tránh sự kiểm soát của các hệ thống bảo mật.

- Cho phép triển khai các chính sách dựa trên nhận dạng người dùng hoặc nhóm người dùng mà không chỉ kiểm tra địa chỉ IP của mạng theo cách làm truyền thống.

- Tích hợp công nghệ phòng chống tấn công để bảo vệ hệ thống ở chế độ thời gian thực, chống lại các cuộc tấn công và những phần mềm nguy hại khác nhúng vào những ứng dụng cũng như lỗ hổng về bảo mật của các ứng dụng hay hệ điều hành trong hệ thống.

- Cung cấp giao diện thân thiện trong việc quản lý và vận hành, giúp việc quản lý các chính sách

vệ cho hệ thống được đơn giản hơn bao giờ hết, cũng như cho phép tùy biến xuất các báo cáo trực quan chi tiết gắn kết giữa người dùng với ứng dụng và các mối nguy cơ tiềm tàng giúp nhà quản trị có được cái nhìn bao quát và giúp đưa ra quyết định được nhanh chóng và kịp thời hơn.

- Được xây dựng kiến trúc đa luồng xử lý đồng thời giúp hiệu năng tổng thể của hệ thống được đảm bảo lên đến hàng gigabit trên giấy, đảm bảo độ trễ là thấp nhất ngay cả khi kích hoạt tất cả các tính năng hoạt động, chạy hết công suất.

Rất nhiều hãng trên thế giới đã đưa ra các giải pháp tường lửa thế hệ mới của riêng mình. Có thể điểm qua một số giải pháp nổi bật hiện nay:

- Giải pháp UTM: với tính năng chính là cho phép qua, chặn lại và ghi lại hoạt động, một số loại có thêm chứ năng QoS hay kiểm soát băng thông bị giới hạn chức năng cho một số ứng dụng đặc biệt mà không phải cho mọi ứng dụng.

- Giải pháp tường lửa thế hệ mới của Cisco: Được tích hợp tính năng kiểm soát ứng dụng, hệ thống phòng chống xâm nhập thế hệ mới cùng với giải pháp phòng chống malware tiên tiến từ sourcefire.

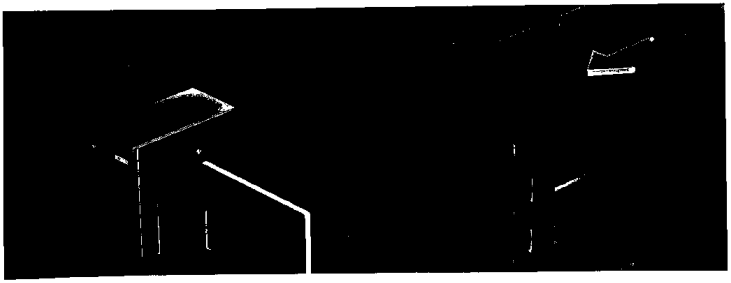
- Giải pháp tường lửa thế hệ mới Palo Alto: là thiết bị tường lửa thế hệ mới. Cung cấp một giải pháp toàn diện cho người quản trị cả về đảm bảo an ninh và quản lý hệ thống.

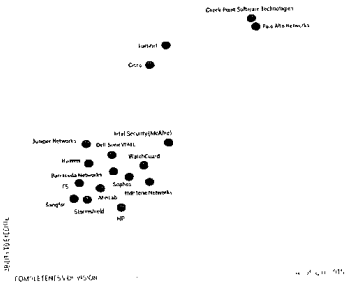
Ngoài ra còn có một số giải pháp khác như: tường lửa thế hệ mới của HP, Fortinet hay tường lửa thế hệ mới được cung cấp bởi Check point, Dell Sonic wall, Clavister, ... Trong số các giải pháp tường lửa thế hệ mới nêu trên, Palo Alto được đánh giá là một trong các giải pháp tường lửa thế hệ mới hàng đầu.

Giải pháp tường lửa thế hệ mới Palo Alto

Vùng Internet rất cần thiết cho việc kết nối ra ngoài cũng như các ứng dụng web công cộng. Đây là vùng rất nhạy cảm, dễ dàng bị tấn công, xâm nhập từ bên ngoài vào. Chính vì thế, đây cũng là vùng cần được bảo đảm an toàn, chống lại các nguy cơ từ bên ngoài vào vùng DMZ là vùng thường xuyên giao tiếp với Internet và cả những truy cập từ bên trong hệ thống ra. Do nguy cơ tấn công và những hiểm họa từ Internet là rất cao, vì vậy thiết bị tường lửa tại vùng này vô cùng quan trọng. Tường lửa thế hệ mới Palo Alto đặt tại phân vùng Internet, có khả năng nhận dạng, kiểm soát các ứng dụng, kiểm soát nội dung, môi trường hoạt động đa dạng, có khả năng phòng chống tấn công có chủ đích và thông lượng làm việc cao cũng như môi trường hoạt động đa dạng và hiển thị báo cáo linh hoạt, dễ dàng thiết lập chính sách.

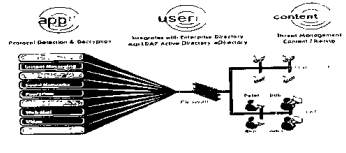
Theo như các bản đánh giá của Gartner hằng năm, Palo Alto luôn được đánh giá rất cao và bốn năm liên tiếp (từ 2011 đến 2015) đều nằm trong nhóm dẫn đầu (LEADERS) về xu thế công nghệ so với các "ông lớn" khác như: Cisco, Fortinet, Juniper... (Hình 2).





Hình 2. Biểu đồ đánh giá của Gartner năm 2015

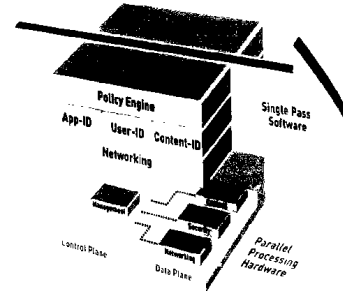
Palo Alto mang lại sự tường minh và khả năng kiểm soát ứng dụng, người dùng và nội dung với sự kết hợp sử dụng ba công nghệ nhận dạng tiên tiến App-ID, User-ID and Content-ID.



Hình 3: Kết hợp các công nghệ tiên tiến nhất vào Palo Alto

Ba công nghệ nhận dạng này đã giúp giải quyết được rất nhiều nhược điểm của Firewall truyền thống. Sử dụng bốn 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. Content-ID như là một engine quét dựa trên luồng dữ liệu (stream-based engine) giúp phát hiện và chặn các mối hiểm họa và giới hạn việc chuyển một cách trái phép các tập tin dữ liệu, nội dung nhạy cảm. Và User-ID cho phép nhà quản trị kết hợp thông tin người dùng với ứng dụng, tạo policy, log dữ liệu và báo cáo. Hơn thế nữa, điều này đã giúp cho Palo Alto giải quyết được thách thức về mặt tích hợp và khả năng xử lý mà rất nhiều các NG-Firewall khác chưa giải quyết được.

Bên cạnh đó, Palo Alto được thiết kế với một phần cứng chuyên biệt tốc độ cao. Phần cứng của Palo Alto được thiết kế để xử lý các tác vụ một cách song song, mỗi tác vụ sẽ được xử lý riêng biệt bởi từng CPU. Palo Alto tách biệt Control Plane và Data Plane giúp nó có hiệu năng xử lý cực cao ngay cả khi chạy hàng loạt tác vụ nặng như nhận dạng ứng dụng, quét virus, bật chức năng IPS hay ngay cả khi giải mã SSL/SSH, và hơn thế là giúp nó chống chọi với các cuộc tấn công tốt hơn.



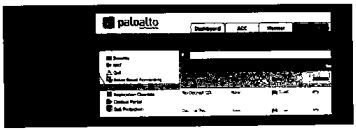
Hình 4. Kiến trúc phần cứng và phần mềm tiên tiến và mạnh mẽ của Palo Alto

Chính vì thế, giải pháp tường lửa thế hệ mới của Palo Alto cung cấp có một giải rộng các tính năng bảo mật, bao gồm:

Tính năng nhận dạng ứng dụng: dựa trên thông tin ứng dụng để xử lý, hỗ trợ nhận dạng người dùng

với việc hỗ trợ số lượng giao thức để nhận dạng người dùng, tích hợp sẵn tính năng nhận dạng người dùng trên thiết bị, không chỉ hỗ trợ lấy thông tin người dùng từ AD, Exchange, LDAP... mà còn từ syslog servers, các công cụ xác thực hay trực tiếp từ cửa sổ Captive Portal cho người dùng đăng nhập.

- Tính năng kiểm soát và ngăn chặn các mối đe dọa: 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 virus, 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.



Hình 5: Khả năng giải mã SSL của Palo Alto

- Tính năng lọc: 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 category vào trong firewall cho phép kiểm soát việc lọc URL bổ sung cho khả năng kiểm soát ứng dụng dựa trên các điều luật bảo vệ doanh nghiệp từ việc tuân thủ một số các tiêu chuẩn cũng như tăng năng suất làm việc và giảm các nguy cơ gây hại đến nguồn lực công ty.

Ngoài ra còn có một số tính năng khác được Palo Alto cung cấp như: chống tấn công APT, hiển thị báo cáo đa dạng với rất nhiều báo cáo dạng đồ thị, hoặc mẫu báo cáo tạo sẵn để người dùng có thể nhanh chóng tạo ra hay tùy biến khi cần.

Kết luận

Thiết bị tường lửa Palo Alto Next-Generation Firewall đặt tại phân vùng Internet cùng với kiến trúc tiên tiến và mạnh mẽ, kết hợp cùng phần cứng chuyên biệt tốc độ cao, đã cung cấp các tính năng bảo mật vượt trội, giúp khắc phục những nhược điểm của mô hình bảo mật firewall truyền thống và 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 hiện nay.

Tài liệu tham khảo:

1. Dell Sonic Wall, Next Generation Firewall, 2014.

2. Gartner, Magic Quadrant for Enterprise Network Firewalls, 2015.

3. Palo Alto Networks, 10-things-your-next-firewall-must-do, 2013.

4. Palo Alto Networks, Designing Networks With Palo Alto Networks Firewalls, 2012.

5. Palo Alto Networks, Palo Alto Networks Web Interface Reference Guide, April 2015.