



NỀN TẢNG AN NINH TÍCH HỢP CỦA PALO ALTO NETWORKS

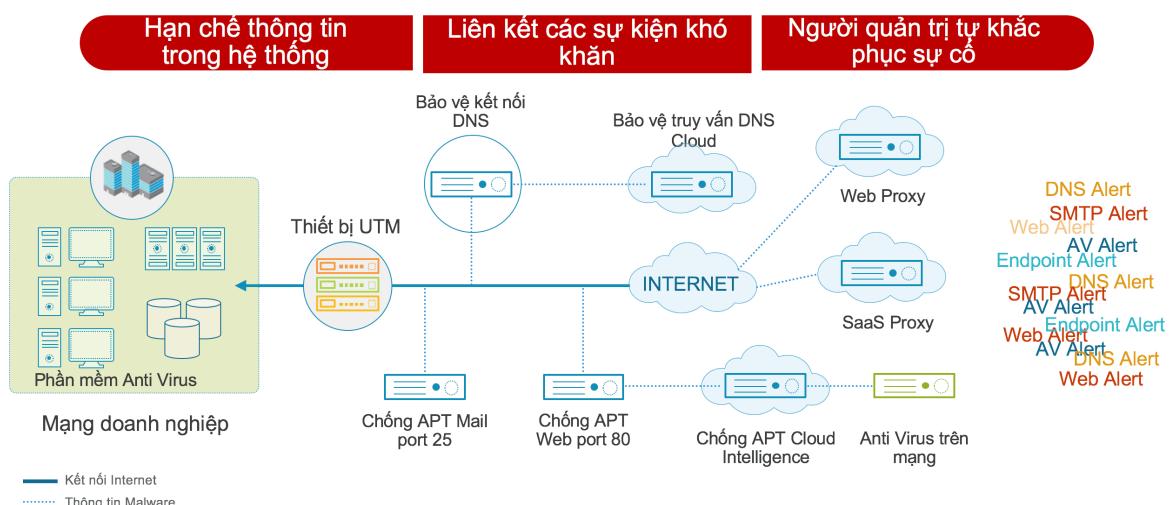
Hiep Nguyen
CCIE, CISSP
Solution Consultant

Mục lục

| | | |
|------------|--|-----------|
| 1 | Tổ chức vận hành các giải pháp an ninh thông tin truyền thống | 3 |
| 2 | Giải pháp tập trung ngăn chặn và phản ứng tự động..... | 4 |
| 3 | Hệ thống an ninh thông tin tích hợp của Palo Alto Networks | 6 |
| 3.1 | Tường lửa thế hệ mới – NGFW | 6 |
| 3.1.1 | Sử dụng các ứng dụng trên mạng một cách an toàn..... | 6 |
| 3.1.2 | Tập trung ngăn chặn các hình thức tấn công..... | 9 |
| 3.2 | Hệ thống phân tích sự kiện và phản ứng – WildFire..... | 17 |
| 3.3 | Hệ thống chống khai thác lỗ hổng và thực thi mã độc – Traps | 19 |
| 3.3.1 | Giải pháp truyền thông..... | 19 |
| 3.3.2 | Các dạng tấn công máy trạm phổ biến | 20 |
| 3.3.3 | Các chức năng của giải pháp Palo Alto Traps | 21 |

1 Tổ chức vận hành các giải pháp an ninh thông tin truyền thống

Trong thiết kế về bảo mật cho hệ thống thông tin, có nhiều giải pháp khác nhau được triển khai từ an ninh mạng, đến máy chủ, máy trạm, an ninh cho các phần mềm, ứng dụng cụ thể. Mỗi giải pháp giám sát, phòng vệ được phục vụ cho một mục đích riêng. Ở mức an ninh cửa ngõ mạng ở các vùng Internet và WAN, giải pháp Firewall dùng để kiểm soát dữ liệu ở lớp 4, AV để quét dấu hiệu mã độc của file truyền trên mạng, IPS để chống xâm nhập khai thác lỗ hổng qua giao thức mạng, APT Web & Mail để phân tích dấu hiệu qua giao thức... Mỗi giải pháp này thường tạo ra nhiều sự kiện cảnh báo khác nhau và không có phương thức liên kết, phản ứng với tấn công phù hợp.



Theo đó, việc trang bị nhiều điểm giám sát thông tin khác nhau nhưng không có đủ giải pháp và nhân sự để phân tích, phản ứng với sự cố sẽ làm thông tin nhận được không có tính liên kết, các sự kiện không được kết nối với nhau để mô tả lại cả cuộc tấn công, cũng như người quản trị cần tự khắc phục sự cố trên nhiều điểm khác nhau.

Do tính chất phức tạp, nguy hại và đổi mới liên tục của các hình thức tấn công hiện nay, việc đầu tư, triển khai cho đến sử dụng, vận hành các giải pháp an ninh thông tin yêu cầu nhiều nguồn lực về con người và chi phí để liên kết các sự kiện tấn công ở nhiều mức, từ hệ thống mạng đến máy trạm, từ dữ liệu lớp 4 đến lớp 7, cũng như để xử lý các sự cố an ninh khi xảy ra.

Theo đó, hướng tiếp cận về an ninh thông tin là cần triển khai những hệ thống có khả năng tự động hóa trong ngăn chặn tấn công cao. Các giải pháp này cho phép người quản

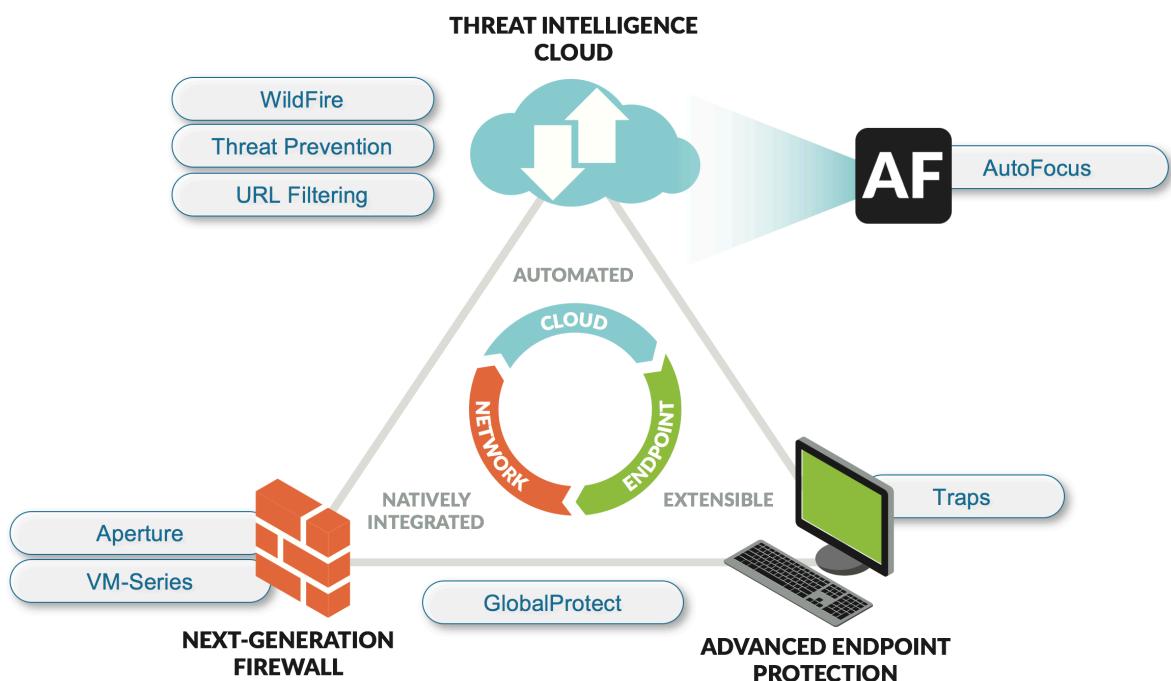
trị an ninh thông tin có thêm công cụ để ngăn chặn hiệu quả những tấn công phức tạp, hạn chế việc phân tích quá nhiều sự kiện cũng như tinh chỉnh chính sách.

2 Giải pháp tập trung ngăn chặn và phản ứng tự động

Để đối phó với các cuộc tấn công diện rộng hoặc tấn công có chủ đích đang phát triển và thay đổi liên tục hiện nay, việc các thiết bị bảo mật chỉ phát hiện ra một phần và không có cơ chế để bảo vệ sẽ dẫn đến những thiệt hại đáng kể do không tìm ra được điểm cần ngăn chặn, cũng như không đủ nguồn lực để ngăn chặn triệt để.

Do vậy, giải pháp tiếp cận của Palo Alto Networks là thay vì khách hàng đầu tư nhiều vào từng giải pháp đơn lẻ và phát triển đội ngũ nhân sự mạnh để vận hành hệ thống; thì có thể tập trung vào các điểm quan trọng nhất của hệ thống là Network và Endpoint kết hợp với hệ thống phân tích động thông minh để **tự động ngăn chặn** các cuộc tấn công qua ứng dụng mạng và tấn công mã độc.

Với tư tưởng thiết kế dạng Ngăn chặn, các tính năng của sản phẩm luôn tập trung vào việc bảo vệ, ngăn chặn tự động cho hệ thống nhiều nhất có thể mà không cần sự can thiệp nhiều từ đội ngũ vận hành hệ thống CNTT.



Giải pháp bao gồm 3 thành phần:

- **Next-Gen Firewall:** là thiết bị được thiết kế với hệ điều hành Firewall cho phép nhận biết và ngăn chặn sâu ở mức ứng dụng, thay vì chỉ theo giao thức và cổng như truyền thông. Bên cạnh đó, trong luồng xử lý của Firewall, gói tin sẽ được kiểm soát qua các engine về lọc malware inline, spyware, C&C, chặn khai thác lỗ hổng, lọc web, chặn file, chặn nội dung. Các engine này hướng vào tính năng ngăn chặn hiệu quả, do đó đều được thiết kế dạng mở gói tin một lần, lọc qua hết các engine, phân tích và chặn theo dạng luồng (thay vì phải lưu lại nội dung để đánh giá), giúp cho năng lực hệ thống khi bật toàn bộ tính năng an toàn luôn được ổn định.
- **Endpoint Protection:** là giải pháp ngăn chặn các loại tấn công xâm nhập lỗ hổng phần mềm cũng như ngăn chặn mã độc thực thi dưới dạng file hoặc script trên máy trạm. Giải pháp Endpoint được thực thi không dùng signature, không quét máy, và luôn kết nối với Threat Intelligence và Firewall để xử lý tự động các sự cố an ninh mạng khi xảy ra ở bất cứ điểm nào trong hệ thống.
- **Threat Intelligence:** là trung tâm làm hai chức năng chính bao gồm chức năng phân tích động các đường link, tập tin và gửi ngay thông tin để ngăn chặn trên Firewall, Endpoint khi phát hiện bất thường trong các đường link và tập tin vừa phân tích. Bên cạnh đó, đây cũng là nơi Palo Alto Networks thu thập thông tin về các sự kiện an ninh thông tin trên thế giới, viết các mẫu ngăn chặn mã độc, URL xấu, các domain và IP C&C, các lỗ hổng bảo mật để cập nhật cho thiết bị liên tục để bảo vệ hệ thống hiệu quả.

Ba thành phần này luôn làm việc chặt chẽ với nhau theo rất nhiều kịch bản để ngăn chặn tự động. Một số kịch bản phổ biến trong phản ứng tự động với tấn công bao gồm:

- Kịch bản 1: Người dùng tải file từ Internet về, file được truyền qua Firewall. Firewall xác định đây là file lạ, không có trong danh mục mẫu mã độc cũng như engine Anti Virus không phát hiện được cấu trúc mã độc theo signature, **Firewall** sẽ tự upload file này lên **Threat Intelligence** để phân tích động. Sau khi phân tích động và phát hiện bất thường trong hành vi, Threat Intelligence xác định mẫu này là mã độc, có các hành vi như gọi ra các máy chủ C&C và rà quét mạng LAN, Threat Intelligence sẽ viết signature để chặn các máy chủ C&C cũng như



cập nhật hash của file này trên database và cập nhật cho **Firewall**, **Endpoint** trong vòng 5 phút để chặn các hành động của mã độc này khi được thực thi.

- Kịch bản 2: Khi file được tải về thuộc loại zero-day mà **Firewall** chưa biết, file được thực thi trên **Endpoint**, cơ chế ngăn chặn không dùng signature mà dựa trên giám sát các kỹ thuật khai thác lỗ hổng và kỹ thuật thực thi của mã độc sẽ giúp Endpoint có thể ngăn chặn zero-day. Malware hoặc exploit này sẽ được cập nhật ngay lên **Threat Intelligence** và **Firewall** để file sẽ bị chặn ngay khi có người dùng khác cũng tải về, đồng thời các signature để chặn kết nối mạng của mã độc này ra bên ngoài cũng sẽ có sẵn trên Firewall.

3 Hệ thống an ninh thông tin tích hợp của Palo Alto Networks

3.1 Tường lửa thế hệ mới – NGFW

3.1.1 Sử dụng các ứng dụng trên mạng một cách an toàn

Tính năng kiểm soát ứng dụng

Tính năng quan trọng đầu tiên của hệ thống tường lửa thế hệ mới là có thể giúp cho cơ quan, tổ chức có thể sử dụng các ứng dụng trên mạng một cách an toàn. Ứng dụng ở đây bao gồm truy cập Web, Email, ứng dụng văn phòng, ứng dụng chat, ứng dụng gọi điện, ứng dụng quản trị nghiệp vụ...

Theo cách truyền thống, các ứng dụng được định nghĩa trên Firewall dưới dạng giao thức và port (Web là TCP cổng 80/443). Tuy nhiên hiện nay có rất nhiều kết nối trái phép, hoặc kết nối điều khiển của mã độc cũng được gửi qua cổng TCP 80 để đi qua được Firewall, tấn công trực tiếp người dùng. Cách tấn công này cũng rất phổ biến với nhiều giao thức và port phổ biến khác như TCP 23, 25, 443, 3389, 5060... Đây là các cổng luôn phải mở vì là các cổng cơ bản cho ứng dụng của người dùng cần truy cập hàng ngày.

Do vậy, điểm quan trọng nhất của giải pháp NGFW là cần nhận diện được từng loại ứng dụng chạy bên trên giao thức truyền thông. Để từ đó, bảng chính sách của Firewall sẽ bao gồm danh sách các ứng dụng được cho phép, còn lại sẽ chặn tất cả, để đảm bảo người dùng vẫn được truy cập các dịch vụ cần thiết, nhưng sẽ hạn chế được đáng kể các tấn công trên mạng.



| Name | Tags | Type | Source | | | Destination | | | Rule Usage | | | Application | Service | Action |
|-------------------|------|-----------|----------|---------|------|--------------|------------|---------|------------|---------------------|---------------------|--------------------------|---------------------|--------|
| | | | Zone | Address | User | HTTP Profile | Zone | Address | Hit Count | Last Hit | First Hit | | | |
| 1 web traffic | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 102510 | 2017-10-16 11:19:26 | 2017-10-10 10:46:11 | http-audio | service-https | Allow |
| 2 update | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 0 | - | - | traps | traps | Allow |
| 3 control traffic | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 56363 | 2017-10-16 11:19:25 | 2017-10-10 10:46:10 | apple-push-notifications | application-defined | Allow |
| 4 vpn | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 1467 | 2017-10-16 11:12:19 | 2017-10-12 23:15:32 | ciscovpn | any | Allow |
| 5 IM | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 5281 | 2017-10-16 11:09:12 | 2017-10-10 21:17:49 | aim-base | facetime | allow |
| 6 social | none | universal | Trust-L3 | any | any | any | Untrust-L3 | any | 3918 | 2017-10-16 11:12:14 | 2017-10-10 21:17:30 | apple-maps | facebook | Allow |

Filter by first tag in rule
Rule Order Alphabetical

Trên đây là bảng Policy của Palo Alto Networks Firewall, tất cả được định nghĩa theo các ứng dụng được chạy trên mạng, và mặc định sẽ chặn hết các ứng dụng không được phép. Mỗi ứng dụng như gmail, skype, viber, zalo, youtube... đều được nhận diện theo signature, mặc dù cùng dùng TCP cổng 443.

Giải pháp Firewall hiện nay được thiết kế với tính năng kiểm soát theo ứng dụng được tích hợp mặc định vào luồng xử lý dữ liệu do vậy luôn được chú trọng ưu tiên cũng như tối ưu năng lực xử lý. Thông lượng của Palo Alto Firewall được đo có sẵn tính năng App-ID này. Bất kể loại dữ liệu nào đi qua Firewall cũng được xử lý với App signature trước, sau đó mới kiểm tra qua các luật truy cập và kiểm soát khác. Tính năng này khi được tích hợp mặc định và trước tất cả các luật khác sẽ đảm bảo hiệu năng và người quản trị có thể sử dụng hoàn toàn Application cho các luật chặn, mở, giảm thiểu hầu hết rủi ro so với việc sử dụng giao thức kết hợp với port truyền thống.



Người dùng



Ứng dụng



Nội dung

Tính năng kiểm soát theo người dùng

Tính năng quan trọng thứ hai của NGFW là quản lý được theo người dùng. Người dùng nội bộ đều được quản lý bằng Microsoft AD hoặc LDAP, do vậy, Firewall cần có khả năng làm chính sách, quản lý, giám sát, ghi log theo thông tin user ID của Active Directory, thay vì dùng địa chỉ IP.

Tính năng này giúp người quản trị không phụ thuộc vào địa chỉ IP cố định, đồng thời giúp việc viết chính sách, giám sát thuận tiện và tường minh hơn. Khi triển khai, bảng policy trên Firewall sẽ thay vì đặt địa chỉ IP nguồn, thì trường thông tin nguồn sẽ là tên đăng nhập của người dùng, hoặc theo nhóm trên LDAP. Chức năng User-ID giúp cho việc triển khai chính sách truy cập hoàn toàn theo nhóm người dùng. Đồng thời khi xem log truy cập, tất cả sự kiện sẽ được gắn với người dùng cụ thể, không chỉ là địa chỉ IP.

Hệ thống Firewall tích hợp sẵn khả năng đọc log WMI trên Active Directory để xây dựng nhanh bảng ánh xạ giữa người dùng với địa chỉ IP, mà không cần có agent ngoài để xử lý việc này, giúp giảm tải trên mạng cũng như giảm điểm quản trị cho đội ngũ vận hành.

Tính năng kiểm soát nội dung

Firewall ở các cửa ngõ mạng Internet cần có khả năng kiểm soát được nội dung trong các bản tin gửi nhận để đảm bảo tuân thủ chính sách. Nội dung cần kiểm soát bao gồm loại file truyền qua mạng, nội dung văn bản, nội dung file tài liệu, nội dung người dùng đăng/gửi qua web mail, mạng xã hội.

Palo Alto Firewall có khả năng kiểm soát sâu về nội dung của file cũng như nội dung text gửi/nhận qua các ứng dụng. Chính sách kiểm soát ứng dụng cũng được tích hợp sẵn như một chức năng trong luồng dữ liệu. Theo đó, người quản trị có thể bật kiểm soát nội dung trong cùng một chính sách truy cập. Chức năng này cũng được thực hiện theo dạng stream based và không cần phải lưu lại nội dung để xử lý, không làm giảm hiệu năng của thiết bị.

Bên cạnh đó, hiện nay có rất nhiều cách để truyền nội dung qua mạng và thông qua nhiều ứng dụng, do vậy các giải pháp Firewall với khả năng kiểm soát ứng dụng mặc định sẽ cho phép giám sát dữ liệu truyền trên từng ứng dụng khác nhau, không chỉ dựa

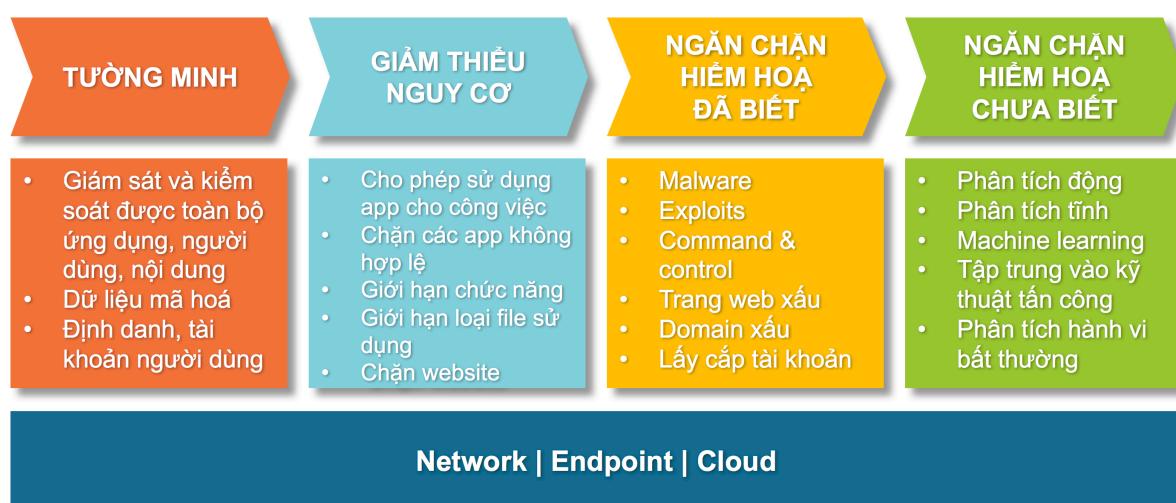


trên HTTP, HTTPS hay FTP thông thường. Firewall có thể ngăn chặn truyền nhận file trên nhiều ứng dụng khác nhau như gmail, google docs, google photo, facebook chat, evernote, 4shared, github, megaupload... Tính năng này giúp cho việc kiểm soát sẽ được thực hiện chi tiết hơn (có ứng dụng cần kiểm soát, có ứng dụng không cần), và chính xác hơn vì đọc nội dung của ứng dụng sẽ không bị nhầm lẫn hay bỏ sót hoặc thậm chí không nhận diện được nội dung như khi đọc theo giao thức thông thường.

3.1.2 Tập trung ngăn chặn các hình thức tấn công

Palo Alto Networks phát triển các tính năng ngăn chặn chuyên sâu trên Firewall để giám sát tường minh hệ thống, giảm thiểu các hiểm họa từ nhiều hướng, ngăn chặn các tấn công đã biết cũng như tấn công chưa biết hay có chủ đích.

Các tính năng này chia làm 4 nội dung chính:



3.1.2.1 Tường minh

Để bảo vệ và ngăn chặn hiệu quả, Firewall cung cấp khả năng nhận diện được toàn bộ ứng dụng, người dùng cũng như nội dung được truyền qua mạng. Các thông tin này sẽ dùng để làm chính sách, nhận biết và ngăn chặn tấn công, kiểm soát dữ liệu và hỗ trợ cho các chức năng phân tích sâu hơn của Firewall.

Một vấn đề đặt ra là hiện nay hầu hết các dữ liệu truyền qua mạng của là dữ liệu mã hoá, do đó nếu không giải mã dữ liệu, Firewall sẽ chỉ nhìn thấy thông tin header của bản tin SSL và các chức năng sẽ kiểm soát sâu sẽ không thực hiện được.

Do vậy, Firewall cần có khả năng giải mã SSL theo chiều người dùng nội bộ kết nối ra ngoài và theo chiều từ ngoài truy cập máy chủ ứng dụng của cơ quan, tổ chức. Hệ thống Palo Alto Firewall tích hợp sẵn khả năng giải mã SSL mạnh, với thiết kế phần cứng sử dụng chip FPGA cho các chức năng khác nhau. Với chiều người dùng nội bộ kết nối ra ngoài, Firewall đứng ở giữa luồng dữ liệu, hoạt động với chức năng SSL Forward Proxy. Với chiều kết nối từ ngoài vào máy chủ ứng dụng (Web, Mail...), Firewall sẽ có private key của server và giải mã được luồng dữ liệu truy vấn đến server mà không cần chặn giữa phiên kết nối.

3.1.2.2 Giảm thiểu nguy cơ

Các nguy cơ có thể đến từ người dùng truy cập các trang Web lạ, các file được truyền qua mạng, được đính kèm trong email, được gửi thông qua các chương trình chat, hoặc trong mạng có sẵn mã độc đang kết nối ra các máy chủ điều khiển ở ngoài để lấy cắp dữ liệu...

Firewall sẽ ngăn chặn các nguồn tấn công để giảm thiểu nguy cơ cho hệ thống, các tính năng này bao gồm:

- Lọc Web: Firewall và Threat Intelligence sẽ định nghĩa danh mục các trang web, sau đó tự động phân loại URL vào các danh mục này. Người quản trị có thể định nghĩa các danh mục được phép và không được phép truy nhập, để hạn chế truy cập vào các trang web có rủi ro cao cũng như các trang web lạ không biết. Bên cạnh đó, Tính năng lọc nội dung của Firewall có khả năng đọc được đường link gửi trong nội dung email và so sánh với cơ sở dữ liệu URL filtering. Bên cạnh

đó, các đường link không nằm trong danh mục đã biết sẽ được gửi lên chạy ở sandbox để phân tích nội dung và đưa ra phân loại, sau đó cập nhật signature ngăn chặn nếu đường link này xấu để đảm bảo an toàn cho người dùng khỏi tấn công phising và tấn công mã độc.

| URL Filtering Profile | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|----------|-------------|----------|-------|--------------|-------|-------|-------|---------------------|-------|----------|-------|----------------------|-------|---------------------|-------|----------------------------|-------|---------------------------|-------|-----|----|
| <input type="text"/> Name Strict filtering <input type="text"/> Description | | | | | | | | | | | | | | | | | | | | | | | |
| | <input type="button"/> Categories <input type="button"/> Overrides <input type="button"/> URL Filtering Settings <input type="button"/> User Credential Detection <input type="button"/> HTTP Header Insertion | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Category</th> <th>Site Access</th> </tr> </thead> <tbody> <tr><td>abortion</td><td>allow</td></tr> <tr><td>abused-drugs</td><td>block</td></tr> <tr><td>adult</td><td>block</td></tr> <tr><td>alcohol-and-tobacco</td><td>allow</td></tr> <tr><td>auctions</td><td>allow</td></tr> <tr><td>business-and-economy</td><td>allow</td></tr> <tr><td>command-and-control</td><td>allow</td></tr> <tr><td>computer-and-internet-info</td><td>allow</td></tr> <tr><td>content-delivery-networks</td><td>allow</td></tr> <tr><td>...</td><td>..</td></tr> </tbody> </table> <small>* indicates a custom URL category, + indicates external dynamic list</small> | | Category | Site Access | abortion | allow | abused-drugs | block | adult | block | alcohol-and-tobacco | allow | auctions | allow | business-and-economy | allow | command-and-control | allow | computer-and-internet-info | allow | content-delivery-networks | allow | ... | .. |
| Category | Site Access | | | | | | | | | | | | | | | | | | | | | | |
| abortion | allow | | | | | | | | | | | | | | | | | | | | | | |
| abused-drugs | block | | | | | | | | | | | | | | | | | | | | | | |
| adult | block | | | | | | | | | | | | | | | | | | | | | | |
| alcohol-and-tobacco | allow | | | | | | | | | | | | | | | | | | | | | | |
| auctions | allow | | | | | | | | | | | | | | | | | | | | | | |
| business-and-economy | allow | | | | | | | | | | | | | | | | | | | | | | |
| command-and-control | allow | | | | | | | | | | | | | | | | | | | | | | |
| computer-and-internet-info | allow | | | | | | | | | | | | | | | | | | | | | | |
| content-delivery-networks | allow | | | | | | | | | | | | | | | | | | | | | | |
| ... | .. | | | | | | | | | | | | | | | | | | | | | | |

- Giới hạn chức năng của ứng dụng: các ứng dụng web hiện nay có rất nhiều chức năng khác nhau. Ví dụ facebook sẽ có tính năng duyệt nội dung, tính năng chat, tính năng đăng bài, tính năng đăng ảnh, tính năng gửi tài liệu... Palo Alto Firewall có thể cho phép người dùng truy cập facebook nhưng chặn các tính năng gửi nhận file để giảm nguy cơ bị tấn công mã độc qua mạng xã hội. Các tính năng này tương tự như với google (gmail, google drive, google doc...) hay các ứng dụng khác trên Internet, Palo Alto Firewall hỗ trợ người quản trị kiểm soát chặt chẽ từng chức năng một.

| | | | | | |
|---|--|---|---|--|---|
| <input type="checkbox"/> facebook <input type="checkbox"/> <input type="checkbox"/> facebook-apps <input type="checkbox"/> <input type="checkbox"/> facebook-base <input type="checkbox"/> <input type="checkbox"/> facebook-chat <input type="checkbox"/> <input type="checkbox"/> facebook-code <input type="checkbox"/> <input type="checkbox"/> facebook-file-sharing <input type="checkbox"/> <input type="checkbox"/> facebook-mail <input type="checkbox"/> <input type="checkbox"/> facebook-posting <input type="checkbox"/> <input type="checkbox"/> facebook-rooms <input type="checkbox"/> <input type="checkbox"/> facebook-social-plugin <input type="checkbox"/> <input type="checkbox"/> facebook-video <input type="checkbox"/> <input type="checkbox"/> facebook-voice | collaboration collaboration collaboration collaboration collaboration general-internet collaboration collaboration collaboration collaboration collaboration media collaboration | social-networking social-networking instant-messaging social-networking file-sharing email social-networking social-networking social-networking photo-video voip-video | 4 4 3 1 4 3 4 2 3 4 1 | browser-based browser-based browser-based browser-based browser-based browser-based browser-based browser-based browser-based browser-based peer-to-peer | tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/80,443 tcp/443 |
|---|--|---|---|--|---|

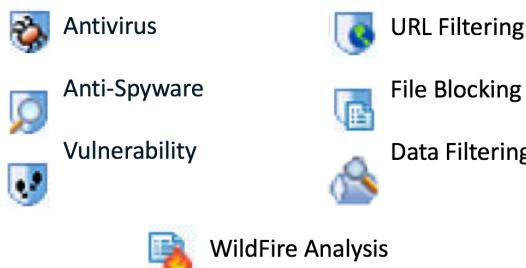
- Firewall có thể ngăn chặn truyền nhận file trên nhiều ứng dụng khác nhau như gmail, google docs, google photo, facebook chat, evernote, 4shared, github, megaupload... Hiện nay có rất nhiều cách để truyền nội dung qua mạng và thông qua nhiều ứng dụng, do vậy các giải pháp Firewall với khả năng kiểm soát ứng

dụng mặc định sẽ cho phép giám sát dữ liệu truyền trên từng ứng dụng khác nhau, không chỉ dựa trên HTTP, HTTPS hay FTP thông thường. Tính năng này giúp cho việc kiểm soát sẽ được thực hiện chi tiết hơn (có ứng dụng cần kiểm soát, có ứng dụng không cần), và chính xác hơn vì đọc nội dung của ứng dụng sẽ không bị nhầm lẫn hay bỏ sót hoặc thậm chí không nhận diện được nội dung như khi đọc theo giao thức thông thường.

3.1.2.3 Ngăn chặn các hiểm họa đã biết

Hiểm họa đã biết bao gồm các loại mã độc, các hạ tầng C&C, các phương thức kết nối, các lỗ hổng bảo mật đã được xác định. Đối với các hiểm họa đã biết, Firewall được cập nhật thường xuyên các signature để ngăn chặn hiệu quả ngay sau khi đã có các sự kiện diễn ra trên thế giới cũng như sau khi đội phân tích thông tin ở Threat Intelligence tìm ra.

| Policies > Security | | | | | | | | | | | | |
|---------------------|-----------|--------|---------|-------------|-------------|---------|-------------|---------|--------|---------|---------|--|
| Name | Type | Source | | Destination | | Address | Application | Service | Action | Profile | Options | |
| | | Zone | Addr... | User | Zone | | | | | | | |
| 1 Server-Access | universal | | any | any | | any | | | | | | |
| 2 allow outbound | universal | | any | any | | any | any | any | | | | |
| 3 allow NTP | universal | | any | any | | any | | | | none | | |
| 4 intrazone-default | Intrazone | any | any | any | (intrazone) | any | any | any | | none | none | |
| 5 interzone-default | interzone | any | any | any | any | any | any | any | | none | none | |



Các tính năng ngăn chặn hiểm họa đã biết được Firewall ngăn chặn qua 4 module chức năng chính: Anti Virus, Anti Spyware, Vulnerability Protection và Chống phising.

Anti Virus:

Firewall có khả năng giám sát và ngăn chặn các bản tin, tập tin nguy hại dùng để tấn công được truyền từ mạng ngoài vào mạng nội bộ, bao gồm cả mã độc đã biết và chưa biết. Firewall có thể thiết lập chính sách đọc và kiểm soát nội dung theo cả chiều từ trong gửi ra cũng như từ ngoài vào. Nội dung này sẽ được xử lý qua engine AV theo stream based và xử lý nội bộ trên Firewall, không cần gửi ra ngoài, không cần lưu lại file hay so sánh mẫu. Bên cạnh engine AV, nội dung

sẽ được kiểm soát qua cả chức năng lọc nội dung. Với mã độc chưa biết, Firewall sẽ tự gửi mẫu lên hệ thống sandbox để phân tích tĩnh, phân tích động và cập nhật signature cho Firewall.

Tính năng anti virus có thể được bật mặc định trên tất cả các rule của Firewall. Theo đó, Firewall cần chặn virus xâm nhập theo cách stream based, không cần tải toàn bộ file cũng như không cần lưu file để phân tích, giúp đảm bảo hiệu năng và hiệu quả hoạt động.

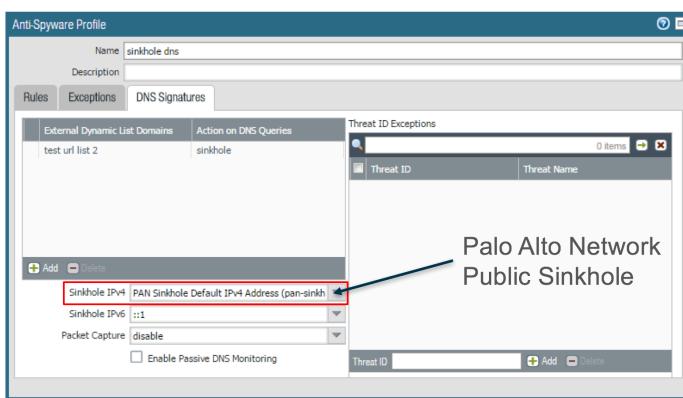
| Decoder | Action | WildFire Action |
|---------|--|----------------------|
| ftp | default (reset-both) | default (reset-both) |
| http | default (reset-both) | default (reset-both) |
| imap | default (alert) | default (alert) |
| pop3 | default (alert) | default (alert) |
| smb | default (reset-both) | default (reset-both) |
| smtp | default (alert) default (alert) allow alert drop reset-client reset-server reset-both | default (alert) |

Cơ chế này sẽ hiệu quả hơn và nhanh hơn so với việc chỉ so sánh hash của file với cloud, do hash có thể thay đổi nhanh chóng. Và khi hash SHA-256 thay đổi, Firewall sẽ phải cho file đi qua sau đó đợi phân tích rồi đưa ra cảnh báo.

Palo Alto sử dụng Engine AntiVirus trên Firewall của chính hãng, để đảm bảo hoạt động tích hợp với hệ điều hành và luồng xử lý dữ liệu của Firewall, cũng như cập nhật trực tiếp từ nguồn của chính hãng. Tính năng AV nếu sử dụng engine của các hãng thứ 3 thì khi tích hợp vào luồng xử lý của Firewall sẽ giống như một module độc lập trong UTM. Kiến trúc phần mềm này sẽ giống như xử lý trên hai hệ thống riêng biệt, gói tin cần xử lý nhiều lần. Thiết kế tối ưu hơn là sử dụng engine AV tích hợp sẵn trong luồng xử lý dữ liệu, và các cập nhật cũng được nhận từ một nguồn duy nhất.

Anti Spyware:

Anti Spyware Là tính năng ngăn chặn các tấn công C&C và lấy cắp dữ liệu. Các cuộc tấn công mã độc hiện nay thường dùng mã độc thực thi trên máy trạm, sau đó mã độc sẽ mở kênh kết nối về máy chủ điều khiển Command & Control (C&C) để nhận lệnh thực thi, để tải thêm mã độc mới, để điều khiển làm các tác vụ phức tạp hơn hoặc để gửi dữ liệu ra bên ngoài. Hầu hết các tấn công thế hệ mới ngày nay đều có sự tham gia điều khiển từ C&C để tăng độ hiệu quả khi thực thi.



Engine Anti Spyware có bộ signature được cập nhật liên tục với danh sách địa chỉ IP, domain C&C và các payload điều khiển để Firewall ngăn chặn được các tấn công mã độc sử dụng C&C. Các cuộc tấn công này thường sử dụng giao thức gọi về C&C được kèm trong nội dung các giao thức phổ biến như HTTP, DNS để đi qua Firewall, do đó, Engine Anti Spyware sẽ giúp ngăn chặn hiệu quả. Đồng thời, cơ chế chặn C&C theo domain kèm theo khả năng dự đoán domain động sẽ nhanh và triệt để hơn là sử dụng hoàn toàn payload như một số giải pháp truyền thống.

Trong module Anti Spyware, người quản trị còn có thể định nghĩa cho Firewall đọc nội dung bản tin DNS (bản tin mã độc dùng để hỏi IP của máy chủ C&C dựa trên tên miền để tránh blacklist IP). Khi đọc nội dung DNS, nếu tên miền được hỏi nằm trong danh mục, Firewall sẽ chặn bản tin DNS này, và trả lời lại cho mã độc một địa chỉ IP không có thật, hoặc trả về địa chỉ IP của máy chủ thu thập dữ liệu phục vụ cho việc điều tra, phân tích hành vi mã độc. Người quản trị cũng có

thể tự cập nhật thêm danh sách các tên miền mã độc sử dụng dựa trên các thông tin từ các tổ chức phân tích sự kiện trên thế giới.

Vulnerability Protection:

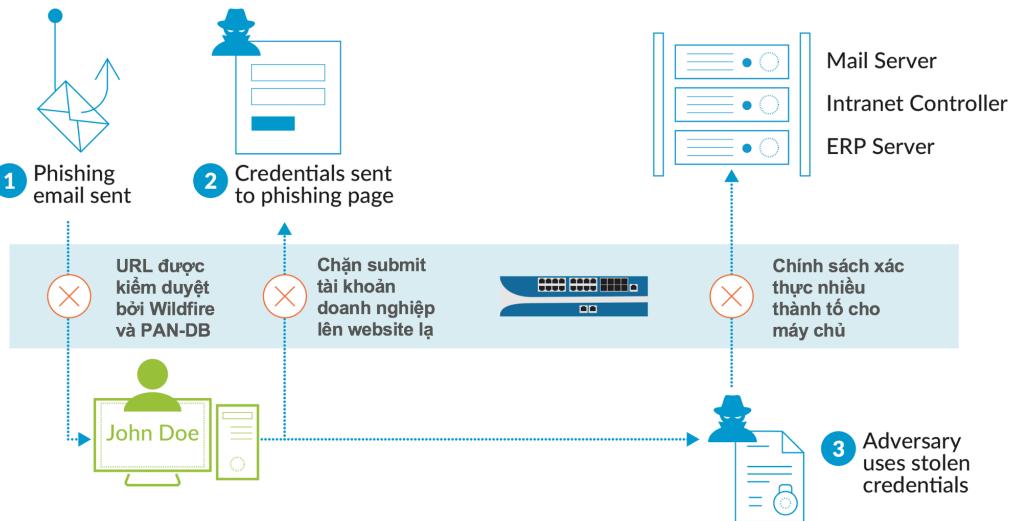
Một hình thức tấn công phổ biến nhưng rất hiệu quả là tấn công vào các lỗ hổng hệ thống. Sau khi khai thác thành công lỗ hổng của hệ điều hành và của phần mềm, hacker có thể chạy các câu lệnh điều khiển từ xa, cũng như đẩy mã độc vào hệ thống để thực hiện các tấn công chuyên sâu hơn.

Vulnerability protection là tính năng Firewall sử dụng IPS engine để ngăn chặn các tấn công khai thác lỗ hổng trên giao thức mạng, hoặc lỗ hổng của hệ điều hành, của phần mềm để tấn công từ ngoài. Khi hacker thực hiện khai thác lỗ hổng, trong nội dung của bản tin gửi đến máy nạn nhân sẽ có payload dùng để làm tràn bộ đệm, một chuỗi ký tự để tấn công vào logic của phần mềm hoặc rất nhiều kỹ thuật tương tự. Firewall sẽ bảo vệ khỏi các tấn công này thông qua vulnerability signature để payload không được gửi qua cũng như ngăn chặn sớm các bất thường trong kết nối mạng.

Chống phising lấy cắp tài khoản

Hình thức tấn công phising đánh lừa người dùng đăng nhập tài khoản công ty lên các trang web giả mạo không chỉ ảnh hưởng đến từng người dùng mà còn có nguy cơ thất thoát dữ liệu của doanh nghiệp khi hacker có được tài khoản đăng nhập. Palo Alto Firewall có khả năng ngăn chặn người dùng đăng nhập username và password công ty lên các website phising.

Giải pháp chống lấy cắp tài khoản nhiều lớp



Firewall với khả năng lọc web và nhận diện nội dung có thể thiết lập chính sách để cho phép hoặc chặn người dùng nhập username và password công ty lên các website không được phép. Tính năng này được bật sẵn đi kèm với mỗi URL category. Theo đó, người quản trị có thể kiểm soát chống gửi username, password lên các nhóm URL có sẵn, hoặc tạo danh sách các URL được phép, còn lại sẽ chặn hết để giảm thiểu rủi ro tối đa cho các trường hợp phising lấy tài khoản.

Bên cạnh đó, phục thức tấn công phising và tấn công mã độc qua đường link gửi trong nội dung email rất phổ biến. Firewall cần có khả năng lọc được đường link gửi trong nội dung email thông qua các danh mục URL và chạy URL trên sandbox.

Tính năng lọc nội dung của Firewall có khả năng đọc được đường link gửi trong nội dung email và so sánh với cơ sở dữ liệu URL filtering. Bên cạnh đó, các đường link không nằm trong danh mục đã biết sẽ được gửi lên chạy ở sandbox để phân tích nội dung và đưa ra phân loại, sau đó cập nhật signature ngăn chặn nếu đường link này xấu để đảm bảo an toàn cho người dùng khỏi tấn công phising và tấn công mã độc.

Bắt buộc phiên kết nối phải qua xác thực nhiều thành tố

Một số dịch vụ quan trọng của yêu cầu xác thực nhiều thành tố, theo đó Firewall phải có khả năng làm chính sách bắt buộc người dùng phải qua xác thực nhiều

thành tố trước khi truy cập. Tính năng này cũng giúp ngăn chặn xâm nhập trái phép của hacker khi có được username và password đăng nhập.

Hiện nay, có nhiều ứng dụng khi chưa tích hợp sẵn xác thực hai thành tố. Để bảo vệ xâm nhập vào những máy chủ ứng dụng này khỏi mã độc, hacker có thông tin tài khoản đăng nhập hoặc những người dùng trái phép, Firewall có khả năng thiết lập chính sách xác thực nhiều thành tố ở mức network. Theo đó, phiên truy cập đến máy chủ ứng dụng cần bảo vệ sẽ được kiểm tra qua Authentication policy trước. Nếu chính sách xác thực yêu cầu xác thực nhiều thành tố, Firewall sẽ dẫn phiên truy cập đó qua nhiều bước xác thực, dùng username/password trên web, sau đó đến soft/hard token... rồi mới mở kết nối vào ứng dụng.

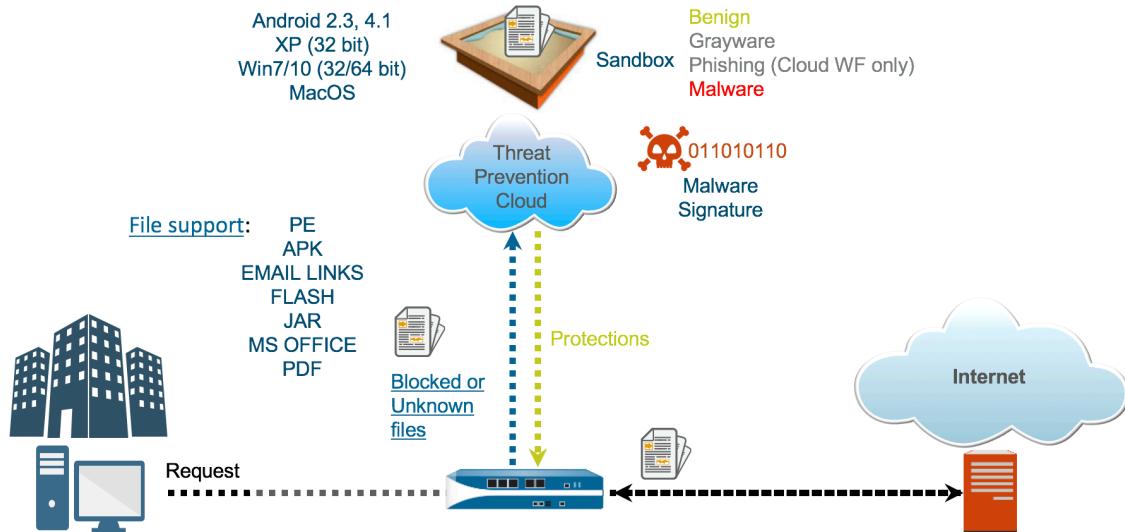
3.2 Hệ thống phân tích sự kiện và phản ứng – WildFire

Trong mô hình ngăn chặn tự động của Palo Alto Networks, bên cạnh Firewall thì một thành phần rất quan trọng để đảm bảo sự hiệu quả chính là hệ thống phân tích sự kiện và phản ứng WildFire.

Hiện nay hầu hết các cuộc tấn công nguy hiểm, được đầu tư và có quy mô phức tạp đều là tấn công có chủ đích, hay nói cách khác, đều là các cuộc tấn công chưa được biết đến trước đó. Do vậy cơ chế bảo vệ dựa trên phân tích tĩnh hoặc dùng signature trên Firewall sẽ không đầy đủ và chính xác hoàn toàn nếu thiếu trung tâm phân tích động các mẫu file, mẫu URL và cập nhật thông tin mới tức thì cho Firewall xử lý, ngăn chặn.

WildFire được cung cấp dưới dạng Threat Intelligence/Prevention cloud hoặc một thiết bị đặt trong mạng. Wildfire bên cạnh việc định kỳ, thường xuyên cập nhật thông tin về các mẫu mã độc, các signature ngăn chặn virus, spyware, C&C, ngăn chặn tấn công lỗ hổng thì chức năng quan trọng của Wildfire trong hệ thống bảo vệ của Palo Alto Networks là phản ứng tự động với các hiểm họa chưa biết.

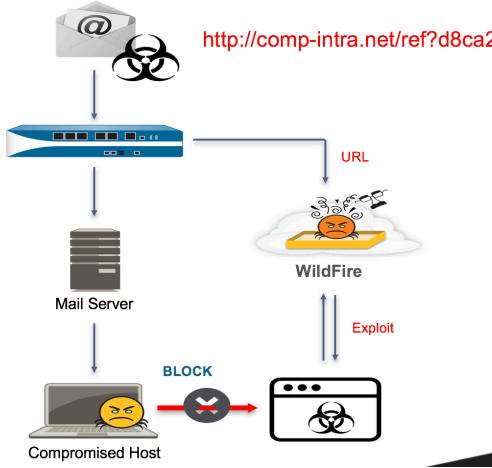




Khi Firewall nhận diện các file chưa xác định được, file sẽ được gửi lên sandbox để chạy thử qua các tính năng nhận diện cấu trúc file (phân tích tĩnh), chạy thử file và quan sát hoạt động trên hệ điều hành (phân tích động). Sau quá trình phân tích động, hệ thống sandbox sẽ biết được cơ chế hoạt động bao gồm việc thay đổi thông tin trong hệ điều hành, kết nối ra các máy chủ bên ngoài, truyền/nhận dữ liệu qua một số giao thức mạng... Nếu Wildfire xác định file là mã độc, hệ thống threat intelligence sẽ tự tạo được signature để cập nhật tức thì (trong vòng 5 phút) cho Firewall ngăn chặn các URL, IP, Application, Protocol mà mã độc sử dụng. Bên cạnh đó, hash SHA-256 của file này sẽ được cập nhật để sau đó không người dùng nào có thể tải được file này về máy trạm được nữa.

Bên cạnh các loại file mã độc truyền thống dạng exe, Firewall có khả năng gửi tự động đến hệ thống sandbox các loại file của hệ điều hành MacOS, Android và nhiều loại file khác như pdf, flash. Việc hỗ trợ nhiều chuẩn file sẽ giúp Firewall và hệ thống sandbox không bỏ sót những loại mã độc phổ biến khác được viết trên các hệ điều hành này.

Không chỉ đối với file, để ngăn chặn hiệu quả các cuộc tấn công mã độc, phising qua email, Palo Alto Firewall có thể tách được URL trong email gửi đến cho người dùng, gửi URL chạy thử trên WildFire để nhận diện nội dung URL. Nếu URL có chứa mã độc, WildFire sẽ báo cáo để Firewall ghi lại sự kiện người dùng nhận được email có chứa mã độc, đồng thời sẽ tạo signature để chặn URL này ngay sau khi phát hiện xong.



Ngoài ra, với tất cả các sự kiện đã được WildFire phân tích và đưa ra nhận định có phải mã độc hay không, người quản trị có thể vào truy vấn, xem báo cáo về hành vi, cũng như nếu người dùng có mẫu file nào muốn phân tích thì có thể tự upload lên giao diện quản lý của WildFire để phân tích thử, và ghi lại hash của file để sau này Firewall sẽ tự tra cứu khi có sự kiện liên quan đến file đó xảy ra.

| Received Time | Source | File / URL | Verdict |
|---------------------|--------------|---|---------|
| 2016-03-30 20:38:38 | 001901001577 | service.morphotak.com/content/software/Configuration%20Tool/Co | Benign |
| 2016-03-30 20:38:37 | 0003C104846 | imasdk.googleapis.com/flash/sdkloader/adapi_3.swf | Benign |
| 2016-03-30 20:38:37 | 0009C101289 | 200.242.37.2/os2pdf/usuarios/G166041/emitido/IMPRTELA_4837.pdf | Pending |
| 2016-03-30 20:38:36 | 0008C100647 | mail.uol.com.br/attachment?msg_id=MTA2NTU&ctype=PROJETO+GREMIO+ | Benign |

3.3 Hệ thống chống khai thác lỗ hổng và thực thi mã độc – Traps

3.3.1 Giải pháp truyền thống

Giải pháp bảo vệ trên máy trạm truyền thông bằng Anti-Virus thường tập trung vào xây dựng bộ signature về các mẫu Malware có sẵn (và được cập nhật thường xuyên từ trung tâm Threat Intelligence khi có mẫu mới). Bộ signature này được lưu local trên máy trạm của người dùng, và các phần mềm AV sẽ quét toàn bộ tập tin trên máy trạm, bao gồm cả tập tin đang lưu trên ổ cứng lẫn các tập tin đang chạy. Tiến trình này được thực hiện liên tục để ngăn chặn mã độc thực thi. Do vậy, nếu không được cập nhật mẫu từ trung tâm, các phần mềm Anti Virus sẽ không thể phát hiện mã độc, đặc biệt là các mã độc

chưa biết (zero-day hoặc các mã độc được viết riêng như APT). Và khi chạy thì phần mềm AV chiếm nhiều CPU và bộ nhớ trên máy trạm do cơ chế quét liên tục.

Theo đó, giải pháp chống khai thác lỗ hổng và chống thực thi mã độc của Palo Alto sẽ hoàn toàn sử dụng các kỹ thuật để ngăn chặn, chứ không dùng signature, do vậy cũng không phụ thuộc vào việc update mẫu từ trung tâm hay phải quét máy mới có thể ngăn chặn. Giải pháp này sẽ hiệu quả hơn với các tấn công dạng zero-day.

3.3.2 Các dạng tấn công máy trạm phổ biến

Có hai bước chính trong tấn công máy trạm:

- **Exploit:** khai thác lỗ hổng trên hệ điều hành hoặc các phần mềm trên hệ điều hành của máy nạn nhân. Sau khi khai thác thành công, hacker có thể triển khai rất nhiều loại payload để tạo backdoor kết nối về máy điều khiển hoặc chuẩn bị cho tấn công malware hoặc đơn giản là làm crash các tiến trình trên máy trạm.

Các máy trạm hiện nay chủ yếu đều được kết nối mạng nên tấn công exploit có thể thực thi qua giao thức mạng hoặc thực thi payload trực tiếp trên máy trạm của người dùng.

Hiện nay có rất nhiều loại exploit được viết sẵn, tập trung vào khoảng vài chục kỹ thuật exploit phổ biến (heap spray, dll hijack, buffer overrun, address space randomization, return oriented programming, shell code allocation...) để khai thác lỗ hổng về software logic, buffer overflow trên các phần mềm (từ trình duyệt, word, excel, PDF reader... đến các câu phần của hệ điều hành Windows, MacOS).

- **Malware:** là các đoạn mã độc có thể thực thi trên file chạy (exe, com...) hoặc script đính kèm vào các tập tin pdf, office, trình duyệt... Các mã độc này thực thi nhiệm vụ chính của cuộc tấn công như phá hoại, mã hoá dữ liệu tổng tiền, dò quét mạng, thu thập dữ liệu, gửi dữ liệu ra ngoài v.v..

Do hoàn toàn là đoạn mã được viết với rất nhiều mục đích khác nhau, hướng đến nhiều đối tượng khác nhau nên số lượng malware rất nhiều, liên tục có mẫu mới và không thể chặn hết triệt để nếu chỉ dùng signature biết trước hoặc so sánh hash với mẫu file trên cloud.



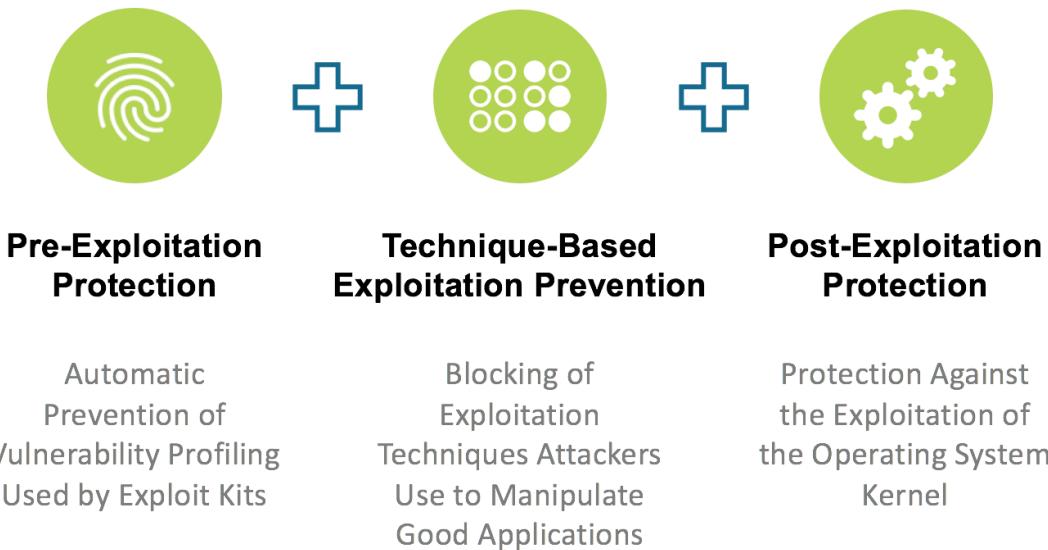
Malware thường được đẩy vào máy trạm sau khi máy đã bị exploit, hoặc có thể do người dùng bị lừa chạy các file mã độc ẩn danh được đính kèm vào email hoặc một chương trình phổ biến.

Các giải pháp AV hiện nay chủ yếu hướng vào dò quét Malware, bỏ sót nhiều kỹ thuật exploit nên tính hiệu quả cho các tấn công mới, chưa biết còn hạn chế.

Các tiếp cận của Palo Alto Traps là **Ngăn chặn**, có **gắn ngắt chặn** triệt để các cuộc tấn công mã độc ngay **từ bước exploit bằng nhiều kỹ thuật và chặn mã độc không dùng signature** có sẵn để tăng tính linh hoạt. Triết lý ngăn chặn tối đa giúp Traps tăng tính hiệu quả trong môi trường thật của rất nhiều mô hình khách hàng khác nhau, cũng như giảm thiểu thiệt hại của các cuộc tấn công mã độc thực tế.

3.3.3 Các chức năng của giải pháp Palo Alto Traps

3.3.3.1 Tính năng chống Exploit



Traps chống Exploit với 3 lớp kết hợp:

- Trước khi thực thi, các bộ Exploit kit của hacker sẽ dò quét (fingerprinting) đặc tính, lỗ hổng của phần mềm và hệ điều hành của máy nạn nhân. Cơ chế finger printing thường đẩy một số gói tin mẫu và xem phản ứng của phần mềm trên máy nạn nhân để xác định kỹ thuật exploit sẽ sử dụng để tấn công. Traps ngăn chặn các hoạt động này để bảo vệ người dùng trước khi thực sự bị exploit.

- Chống exploit đã biết hoặc chưa biết bằng việc ngăn chặn các kỹ thuật lập trình và can thiệp hệ điều hành của exploit kit. Hiện nay có đến vài nghìn exploit đã biết được viết và chia sẻ trên mạng (ví dụ bộ Metasploit), tuy nhiên hầu hết đều sử dụng khoảng vài chục kỹ thuật cơ bản trong can thiệp bộ nhớ, can thiệp file hệ thống, lấy dữ liệu trên vùng đệm... Traps tích hợp sẵn cơ chế chống các kỹ thuật exploit này, do đó, với các exploit đã biết và các exploit mới đều có thể ngăn chặn được dựa trên các kỹ thuật chung này.
- Ngoài kỹ thuật exploit vào phần mềm, rất nhiều exploit hiện nay hướng vào hệ điều hành để escalate privilege, chiếm quyền của process đang chạy... Traps cũng hỗ trợ chặn các loại kỹ thuật này để bảo vệ người dùng với các exploit thực thi sâu ở lớp kernel.

3.3.3.2 Tính năng chống Malware

| | | | |
|--|--|---|--|
|  |  |  |  |
| WildFire Threat Intelligence | Local Analysis (via Machine Learning) | WildFire Analysis | Malicious Process Control |
| Automatic Prevention of Previously-Seen Malware | Automatic Prevention of Unknown Malware | Rapid Detection & Prevention of Unknown Malware | Control Launching of Applications That Can Be Used for Malicious Purposes |

Bên cạnh chống Exploit là một bước hết sức quan trọng cũng như phổ biến trong tấn công mã độc, Traps cũng tập trung vào các kỹ thuật chống mã độc thực thi.

Cách tiếp cận của Traps là không dùng bộ AV Signature và disk scanning do cách này sẽ chỉ dùng được với các mẫu mã độc đã biết, cũng như làm tải máy trạm tăng lên nhiều do tốn CPU và RAM.

Traps cũng không dựa toàn bộ vào cloud như các giải pháp EDR do máy trạm không phải lúc nào cũng kết nối Internet, và EDR chỉ hướng vào việc phân tích, phát hiện rồi cô lập, còn Traps sẽ cố gắng ngăn chặn tối đa ngay từ đầu.

Traps chống mã độc với 4 kỹ thuật:

- Với mã độc đã biết trên thế giới: Để đạt hiệu quả nhanh chóng với các mã độc đã biết, Traps sử dụng hỗ trợ của cloud Threat Intelligence của Palo Alto trên Internet (hoặc dùng một thiết bị Threat Intelligence – WildFire đặt trong mạng). Traps sẽ check hash của các file thực thi với WildFire để so sánh và nhận diện mã độc đã biết.
- Tuy nhiên, nếu chỉ kiểm tra hash thì không hiệu quả do mã độc có thể được thay đổi rất nhiều dạng, mỗi dạng sẽ có hash khác nhau, đồng thời với mã độc chưa biết trước thì trên threat intelligence không có thông tin. Do vậy Traps kết hợp Local Analysis với AI để phân tích các kỹ thuật mã độc sử dụng trên hệ điều hành trực tiếp. Local Analysis không yêu cầu kết nối lên trung tâm, chạy nội bộ trên máy trạm và dùng để nhận diện các mã độc chưa biết dựa trên các kỹ thuật (hành vi) của mã độc thực hiện trên máy trạm.
- Bên cạnh local analysis trên máy trạm, Traps có thể gửi mẫu file chưa biết lên WildFire (Threat Intelligence) để chạy thử và kiểm tra. WildFire là một dạng sandbox nhưng được tích hợp thêm nhiều chức năng bao gồm:
 - o Dynamic Analysis: chạy trong môi trường sandbox với rất đa dạng hệ điều hành (windows XP, 7, 8, 10, MacOS).
 - o Bare-metal Analysis: chạy file trong môi trường máy vật lý phần cứng mà không dùng máy ảo, do rất nhiều loại mã độc hiện nay được viết với kỹ thuật chống sandbox máy ảo.
 - o Static Analysis: đọc mã dịch ngược để nhận diện mã độc.
 - o Thời gian thực hiện các tác vụ này và cập nhật policy cho Traps cũng như cập nhật signature cho NGFW Palo Alto mất khoảng 5 phút.
- Một dạng tấn công mã độc hiện nay rất phổ biến là dùng các phần mềm cơ bản như Internet Explorer, Word để tạo ra các child process và chạy PowerShell, hay các trình dịch code, từ đó thực thi một đoạn mã mà không bị phát hiện. Traps có thể tạo các chính sách chặn child process được thực thi thông qua blacklist, whitelist.