# Các yêu cầu về chức năng của hệ thống Firewall Internet và Partner

## Yêu cầu chung

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… 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.

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 hoá 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.

## Các yêu cầu về tính năng đối với hệ thống Firewall cho Internet và Partner

### Chính sách sử dụng của ngân hàng đã định nghĩa đầy đủ các loại ứng dụng/dịch vụ được sử dụng trên mạng. Firewall cần hỗ trợ thực thi chính sách này, cho phép người dùng ngân hàng sử dụng các ứng dụng an toàn, hạn chế rủi ro bị tấn công qua các giao thức TCP/UDP với port phổ biến.

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. Theo đó, 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 nội bộ đều được quản lý bằng Microsoft AD, 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. Yêu cầu Firewall tự tích hợp với AD, không cần cài đặt agent ngoài.

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. 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.

### Firewall cửa ngõ mạng Internet và Partner 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.

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.

### 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.

### Firewall cần 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 của ngân hàng, 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 cần 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 toản bộ file cũng như không cần lưu file để phân tích, giúp đảm bảo hiệu năng và hiệu quả hoạt động.

### Firewall có thể thực hiện inline scan virus dựa trên nội dung binary của file chứ không dùng cơ chế so sánh hash SHA-256, do hash rất dễ thay đổi và bị bỏ qua khi gặp hash mới.

Tính năng kiểm tra mã độc với engine AV và tính năng lọc nội dung trên Firewall đều được thực hiện theo dạng stream based, luồng thông tin đi qua theo thời gian thực. Quan trọng hơn, Firewall có thể chặn inline các file này mà không cần đợi phân tích, xử lý bằng các hệ thống ngoài, giúp tăng hiệu quả ngăn chặn.

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 thay đổi, Firewall sẽ phải cho file đi qua sau đó đợi phân tích rồi đưa ra cảnh báo.

### Engine AntiVirus trên Firewall cần 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.

### Đối với các file truyền trên hệ thống thuộc loại chưa biết, Firewall cần có sẵn tính năng gửi file để chạy trên sandbox, và khi xác định file là mã độc, hệ thống threat intelligence sẽ tự tạo được signature để cập nhật tức thì cho Firewall ngăn chặn các URL, IP, Application, Protocol mà mã độc sử dụng.

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… Điểm quan trọng của là hệ thống sandbox sau khi phân tích xong, sẽ cần viết signature mới cập nhật ngay cho Firewall (trong vòng 5p) để chặn các kết nối, hoặc chặn mẫu mã độc vừa phát hiện.

### Firewall hỗ trợ gửi tự động nhiều chuẩn file đến hệ thống sandbox bao gồm file exe, pdf, office, flash, apk, MacOS file.

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.

### Hiện nay hầu hết các dữ liệu truyền qua mạng của ngân hàng đều là dữ liệu mã hoá, 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 ngân hàng.

Hệ thống 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 server của ngân hàng, 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.

### Firewall ở vùng Internet và Partner chạy ở chế độ Layer 3, với nhiều Router và đường truyền ra ngoài, do đó cần có sẵn tính năng Policy based routing/forwarding để cấu hình định tuyến ra nhiều đường truyền. Tính năng này cần có trên giao diện quản trị đồ hoạ local của thiết bị, không cần dùng dòng lệnh.

Tính năng Policy Based Forwarding được tích hợp sẵn trên giao diện đồ hoạ local của thiết bị. Người quản trị có thể cấu hình định tuyến theo từng ứng dụng, từng IP nguồn. Firewall còn có thể kiểm tra trạng thái của IP đích khi thực hiện định tuyến để đảm bảo các điều kiện đường truyền up/down khác nhau khi vận hành.

### Firewall ở vùng Internet cần có sẵn tính năng VPN, để dễ triển khai cho các máy trạm kết nối từ xa với mục đích quản trị, chia sẻ dữ liệu.

Tính năng SSL và IPSec VPN có sẵn trên Firewall và không cần trang bị license riêng cho tính năng này.

### Một số dịch vụ quan trọng của ngân hàng 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 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.

### 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. Firewall Internet cần có khả năng ngăn chặn người dùng đăng nhập username và password công ty lên các website phising.

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.

### 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.