

2010

NANOSOFT., jsc

Minh Thang

NANO-FWBCA

GIẢI PHÁP TƯỜNG LỬA

--- Sản phẩm “độc quyền phân phối” từ Bộ công an ---

[TÀI LIỆU GIỚI THIỆU]

Giải pháp tường lửa(NANO-FWBCA) phục vụ trong ngành giáo dục nhằm phòng tránh virus, ngăn chặn những đợt tấn công từ bên ngoài, lọc bỏ những trang web độc... mang lại phương thức khai thác thông tin trên mạng an toàn hiệu quả với nội dung hoàn toàn được kiểm soát.

NỘI DUNG

- **Giới thiệu tổng quan**
- **Các chức năng của NANO-FWBCA**
- **Quản trị bước tường lửa**
- **Quản trị hệ thống**
- **Các tiện ích**

NANOSOFT

I. Giới thiệu tổng quan

Bức tường lửa (Firewall) là công cụ bảo vệ an ninh mạng máy tính chống truy nhập trái phép từ mạng bên ngoài (mạng không tin cậy) vào mạng bên trong (mạng tin cậy). Firewall là công cụ cần thiết cho mọi cơ quan, tổ chức có mạng tham gia vào mạng diện rộng hay mạng internet. Mục tiêu nghiên cứu xây dựng hệ thống tường lửa là nhằm chủ động nắm bắt công cụ bảo vệ an ninh an toàn mạng máy tính trong thời đại mà nhu cầu sử dụng công nghệ thông tin đang phát triển mạnh, công nghệ mạng máy tính ngày càng cao, tránh phụ thuộc vào công nghệ và các sản phẩm ngoại nhập, đồng thời giảm thiểu đầu tư kinh phí khi mở rộng các điểm nút bảo vệ mạng.

Hệ thống tường lửa FWBCA đã được chạy thử nghiệm tại Trung tâm Công nghệ kỹ thuật máy tính và Chiến thuật nghiệp vụ. Những kết quả thử nghiệm cho thấy hệ thống đã đảm lọc và ngăn chặn được mọi yêu cầu kết nối trên các cổng dịch vụ hiện hành, lưu các nhật ký giúp người quản trị phát hiện các dấu hiệu truy nhập trái phép để từ đó có biện pháp kỹ thuật ngăn chặn hoặc biện pháp khác kịp thời. Hệ thống không đòi hỏi cấu hình phần cứng cao, được chạy trên hệ điều hành Linux nên có tính ổn định cao. Hơn nữa, Hệ thống FWBCA cho phép quản trị từ xa qua giao diện web, có giao diện tiếng Việt thân thiện nên dễ quản trị.

Hy vọng rằng hệ thống tường lửa FWBCA sẽ đáp ứng được yêu cầu bảo vệ an ninh mạng máy tính cho từng đơn vị cụ thể. Chúng tôi rất mong nhận được sự góp ý để nhóm nghiên cứu phát triển hệ thống hoàn thiện hơn nữa, đáp ứng công tác bảo vệ an ninh an toàn mạng máy tính tốt hơn trong tình hình mới.

II. Các chức năng của NANO-FWBCA

- Bảo vệ chống truy nhập trái phép vào mạng nội bộ từ mạng bên ngoài (như Internet)
- Ngăn chặn mọi dấu hiệu quét thăm dò và tấn công hệ thống mạng nội bộ
- Lọc virus xâm nhập từ mạng Internet
- Kiểm soát và che dấu mọi địa chỉ IP của mạng nội bộ khi kết nối qua hệ thống tường lửa FWBCA
- Kiểm soát và ghi nhận mọi trạng thái kết nối các dịch vụ: web, thư điện tử, truyền tệp,...
- Cho phép người dùng mạng bên trong kết nối với mạng bên ngoài để tra cứu, tìm kiếm thông tin và khai thác CSDL một cách trong suốt
- Khả năng phục vụ 50 đến 100 máy kết nối cùng một lúc

- Khả năng mở rộng ứng dụng của sản phẩm phần mềm tường lửa FWBCA:
 - Thiết lập kết nối ảo giữa hai mạng LAN (VLAN) nằm xa nhau về khoảng cách thông qua hai hệ thống tường lửa FWBCA
 - Bảo vệ đường truyền giữa hai Gateway có cài đặt phần mềm FWBCA bằng kỹ thuật mạng riêng ảo (VPN), cho phép thay đổi thuật toán mã hoá và khoá bảo mật
 - Bảo vệ hội nghị truyền hình (Video Conferencing)
 - Sử dụng tính năng định hướng lại gói tin (REDIRECT) để thực hiện chiến thuật tin học trên mạng
- **Đặc biệt:** Tích hợp bộ lọc trang web đen (website có nội dung không mong muốn) với số lượng trang web ngăn chặn hiện có trên 1.000.000 website...

III. Quản trị bước tường lửa

- Mô hình và nguyên lý hoạt động
- Thiết lập cấu hình mạng
- Thiết lập cấu hình hệ thống tường lửa
- Thao tác với hệ thống luật
- Nhật ký hệ thống tường lửa

a. Mô hình và nguyên lý hoạt động

Trong các mô hình trên, Mạng bên ngoài thường được hiểu là mạng không tin cậy như: mạng diện rộng, mạng internet; Mạng nội bộ là mạng mà ta cần bảo vệ; Vùng DMZ là vùng chỉ chứa các máy chủ phục vụ; eth0,eth1,eth2 là các giao tiếp mạng của máy mà hệ thống tường lửa FWBCA cài đặt lên. Chú ý: trong các mô hình 1,2 thì Mạng bên trong (hay vùng DMZ) phải chọn Gateway ngầm định là địa chỉ IP của eth1 (hay eth2 với DMZ).

Mô hình 1: Thường được dùng cho các mạng nhỏ như: các phòng, ban trong đơn vị;

Mô hình 2: Dùng cho các nhu cầu lớn hơn như: các cục, vụ;

Mô hình 3: Được dùng cho các đơn vị có nhu cầu đảm bảo an ninh an toàn mạng ở mức cao. Trong mô hình 3, kẻ tấn công chỉ có thể phá vỡ hệ thống tường lửa bên ngoài, nhưng không thể vào được mạng bên trong cần bảo vệ.

Nguyên lý hoạt động:

Trước hết ta cần hiểu về cách thức tổ chức của hệ thống tường lửa FWBCA. Hệ thống tường lửa FWBCA được tổ chức theo các hướng lưu thông của các gói tin, tức là ứng với mỗi hướng ta tổ chức một bảng các

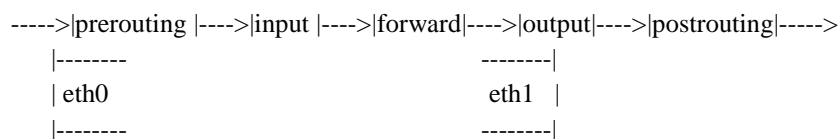
luật tương ứng với đặc điểm hoạt động của nó. Có ba hướng lưu thông cơ bản là: hướng gói tin đi vào (Input), hướng đi ra (Output) và hướng chuyển tiếp (Forward). Trong mỗi hướng này có các chính sách (Policy) và tập các luật (Rule).

Hệ thống tường lửa FWBCA này hoạt động cơ bản dựa trên nguyên lý của bộ lọc gói tin (Packet Filtering). Tức là nó dựa vào những thông tin nằm trong phần HEADER của gói tin để đưa ra những quyết định mà chính sách và hệ thống luật của ta đã định. Như ta đã biết, thông tin truyền trên mạng đều dưới dạng các gói tin. Mỗi gói tin này được chia làm 2 phần cơ bản là: phần đầu (HEADER) và phần dữ liệu (DATA). Phần DATA chứa dữ liệu cần chuyển đi, còn phần HEADER chứa các thông tin cho biết nguồn gốc, nơi đến, và một vài thông tin khác. Các thông tin mà hệ thống tường lửa FWBCA cần là trong phần HEADER của gói tin. Cụ thể các thông tin cần cơ bản bao gồm:

- Địa chỉ IP máy gửi
- Địa chỉ IP máy nhận
- Cổng dịch vụ máy gửi
- Cổng dịch vụ máy nhận
- Giao thức sử dụng (hay dịch vụ)

FWBCA dựa vào các thông tin đó để xử lý gói tin. Nguyên tắc hoạt động như sau:

Giả sử ta xét gói tin đi từ mạng ngoài vào: khi gói tin đến giao tiếp mạng eth0, FWBCA sử dụng hướng input để kiểm tra, nếu gói tin được phép đi vào (vào máy FWBCA qua eth0) thì nó sẽ cho vào. Sau đó nó sử dụng hướng forward để chuyển tiếp đến giao tiếp mạng eth1 (hoặc eth2). Tiếp đó nó sử dụng hướng output để kiểm tra lần cuối gói tin trước khi đi vào mạng trong qua eth1 (hoặc qua eth2). Trường hợp ngược lại gói tin đi từ mạng trong ra ngoài: gói tin đến eth1 (hoặc eth2), FWBCA dùng bảng luật của input để xem xét, nếu được phép nó sẽ cho gói tin đi vào máy FWBCA. Tiếp đó dùng bảng luật của forward để chuyển gói tin đến eth0 (nếu từ mạng nội bộ đi ra thì thường qua đây gói tin sẽ được đóng gói lại và lấy địa chỉ IP là của card eth0). Và cuối cùng trước khi ra mạng ngoài, gói tin phải qua kiểm tra bởi bảng luật của output. Để hình dung rõ hơn ta có mô hình sau:



<----|postrouting|<----|output|<----|forward|<----|input |<----|prerouting |<---->

Như thế tại mỗi card mạng có bốn bảng luật. Trong đó bảng luật prerouting dùng để thay đổi địa chỉ IP đích của gói tin, bảng luật postrouting dùng để thay đổi địa chỉ IP nguồn của gói tin. Còn hai bảng luật là input và output dùng để kiểm soát gói tin. Và cuối cùng để chuyển tiếp giữa hai card mạng ta dùng bảng luật forward. Như vậy các luật của ta sẽ chủ yếu đặt tại hai bảng luật input và output để kiểm soát - tức là cho phép hay cấm - các dịch vụ lưu thông qua hệ thống tường lửa.

Trong mỗi bảng luật trên khi gói tin đến thì các luật được xử lý tuần tự - tức là luật nào tạo trước thì gói tin sẽ phải đối mặt trước. Nếu luật 1 không phù hợp thì luật 2 được gọi để xử lý gói tin, nếu luật 2 không phù hợp thì luật 3 được gọi,... cứ như thế cho đến khi có luật phù hợp. Trong trường hợp không có luật nào phù hợp thì chính sách (Policy) của hướng sẽ được sử dụng. Như vậy chính sách sẽ là giải pháp cuối cùng để xử lý gói tin.

Trong hệ thống tường lửa FWBCA, chính sách (Policy) ngầm định của các hướng là DENY (từ chối) - tức là nếu không có luật nào phù hợp thì có nghĩa gói tin đó sẽ không được phép đi qua. Do vậy ta sẽ thiết lập các luật theo nguyên tắc “mở dần” - tức là nếu muốn cho phép gói tin nào thì ta tạo và thiết lập luật cho phép gói tin đó.

b. Thiết lập cấu hình mạng

Phát triển bởi Nhóm An ninh an toàn thông tin - P4-E15-TC6-BCA
Điện thoại: 069-47831 - Địa chỉ: 280B, Lạc Long Quân, Hà Nội

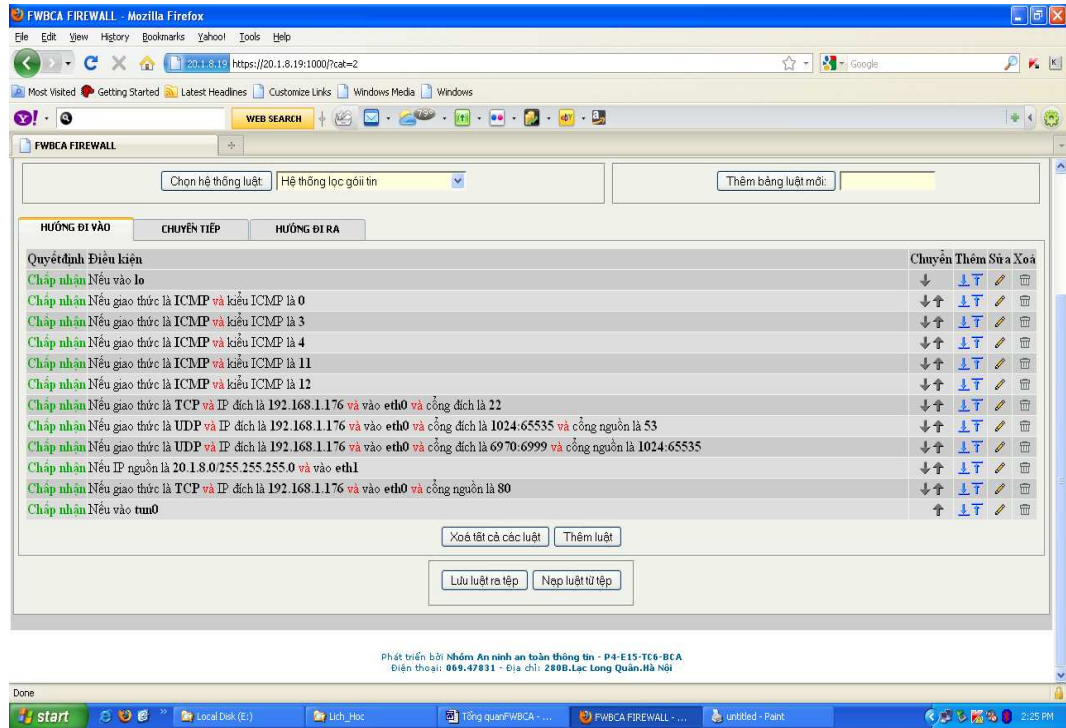
Chú ý: Các thao tác ở phần này chỉ thực hiện nếu bạn là người quản trị mạng. Khi thay đổi địa chỉ IP giao tiếp mạng trong (eth1) khác lớp địa chỉ mạng nội bộ đang dùng thì có thể kết nối hiện tại sẽ bị ngắt, khi đó cần thay đổi địa chỉ mạng trong cho phù hợp với lớp địa chỉ mới (cùng lớp với eth1) và đăng nhập lại.

Thiết lập cấu hình mạng gồm các thao tác: Thiết lập địa chỉ IP giao tiếp mạng, Bảng định tuyến, Thiết lập DNS, Thiết lập định danh máy. Trong các thao tác này, thiết lập địa chỉ IP và DNS là hai thao tác cần thiết. Thiết lập địa chỉ IP giao tiếp mạng: thông thường địa chỉ IP đã được thiết lập sẵn phù hợp với mạng hoạt động nên thao tác này chỉ dùng khi ta chuyển mạng hay định lại địa chỉ IP cho toàn mạng. Ta không nên thay đổi "thủ", vì quá trình thay đổi có thể sẽ làm ta không thể vào được hệ thống tường lửa nữa.

- Thiết lập địa chỉ IP giao tiếp mạng: thông thường địa chỉ IP đã được thiết lập sẵn phù hợp với mạng hoạt động nên thao tác này chỉ dùng khi ta chuyển mạng hay định lại địa chỉ IP cho toàn mạng. Ta không nên thay đổi "thủ", vì quá trình thay đổi có thể sẽ làm ta không thể vào được hệ thống tường lửa nữa. Trong trường hợp cần thay đổi, nhấn chọn tên giao tiếp muốn sửa, sau khi nhập các thông số cần thiết nhấn nút “Ghi và kích hoạt” để xác nhận các thay đổi. Chú ý: đối với card eth1 nối với giao tiếp mạng trong, nếu thay đổi địa chỉ IP của nó sang lớp khác với lớp cũ thì kết nối hiện tại sẽ bị ngắt, trường hợp này ta phải thay đổi lại địa chỉ IP mạng trong phù hợp và đăng nhập lại.
- Bảng Routing và Gateway: thông thường máy FWBCA đứng sau một Router mặc định, vì vậy ta không cần phải lập bảng định tuyến nữa. Vì luôn có sẵn gateway đến router mặc định rồi.
- Máy trạm DNS: thiết lập máy giải nghĩa tên miền cho máy FWBCA. Thông thường máy chủ DNS giống với máy DNS của mạng nội bộ.

Các địa chỉ máy: Trường hợp không có (hoặc không thiết lập) máy chủ DNS, ta có thể tự định nghĩa để ánh xạ tên và địa chỉ IP trong chức năng này. Ta chọn “Thêm mới”, sau đó nhập địa chỉ IP và các tên ánh xạ của nó (Một địa chỉ IP có thể có nhiều tên).

c. Thiết lập cấu hình hệ thống tường lửa



Chức năng này nhằm tạo ra một hệ thống luật ngầm định. Sau khi tạo, hệ thống luật này sẽ hoạt động ngay, vì vậy nếu các thông số nhập sai thì có thể bạn sẽ không nhận được kết quả mong muốn. Thông thường ta nên chấp nhận các tham số mặc định. Nếu muốn cho phép dịch vụ chia sẻ tệp tin (share) hay tìm tên máy trên hệ điều hành Windows thì chọn cho phép dịch vụ Netbios. Tuy nhiên một khuyến cáo là không nên cho phép dịch vụ Netbios, vì nó luôn tạo ra các lỗ hổng làm mất tính an toàn của hệ thống mạng cần bảo vệ.

d. Thao tác với hệ thống luật

Để tạo (hoặc sửa) một luật mới, ta chọn biểu tượng mũi tên (hay cây bút) tùy theo vị trí cần đặt luật. Các thông tin cần cho một luật có thể gồm: 1-Quyết định; 2-Địa chỉ IP nguồn, 3-Địa chỉ IP đích; 4-Giao tiếp mạng; 5-Giao thức; 6-Cổng dịch vụ nguồn; 7-Cổng dịch vụ đích. Các lựa chọn này (có thể tất cả hoặc 1 trong số đó) để xác định điều kiện xử lý gói tin, tức nếu gói tin nào thoả mãn các điều kiện ấy nó sẽ có "Quyết định" rõ ràng. Còn để xóa luật, chỉ đơn giản nhấn chọn biểu tượng "thùng rác". Và tất nhiên sau khi thay đổi ta cần nhấn nút "Lưu các thay đổi" để lưu lại mọi thao tác đã làm. Cần lưu ý:

- Khi chọn cổng nguồn hoặc đích thì phải chọn giao thức là TCP hoặc UDP
- Chọn kiểu ICMP thì phải chọn giao thức là ICMP
- Một số cổng dịch vụ thông dụng: 20,21-FTP; 22-SSH; 23-Telnet; 25-SMTP; 53-DNS; 80-HTTP; 110-POP3; 135-RPC; 137,138,139-Netbios; 143-IMAP4; 443-HTTPs...

Tạo bảng luật mới:

Ngâm định, hệ thống tường lửa có 3 bảng luật là input,output và forward. Các bảng luật này không thể xoá được. Để dễ dàng trong việc quản trị, chức năng này cho phép người quản trị tạo ra bảng luật mới, bảng luật này cũng có thể xoá được. Tuy nhiên cần lưu ý là tên bảng luật mới không được trùng với các bảng luật đã có. Các bảng luật được tạo ra có thể dùng làm "Quyết định" của một luật. Nó hoạt động như sau: giả sử ta có luật B và quyết định của nó là vào bảng luật TEST. Khi đó, nếu có gói tin phù hợp với các điều kiện của B thì gói tin đó sẽ phải so sánh tiếp với các điều kiện là các luật trong bảng luật TEST. Để dễ hình dung ta xem xét mô hình sau:

```
input          ---> TEST
1. Luật A      -----> 1. Luật T1
2. Luật B     -----> 2. Luật T2
3. Luật C
```

Khi một gói tin vào bảng luật input, thì luật A được gọi ra để xem xét, nếu luật A không phù hợp thì luật B được gọi ra. Trường hợp các điều kiện của B phù hợp và vì B có "quyết định" là TEST nên các gói tin "được chuyển" cho bảng luật TEST. Tiếp đó, luật T1 được gọi ra để xem xét, nếu T1 không phù hợp thì T2. Và nếu T2 cũng không phù hợp thì luật C được gọi ra để xử lý gói tin.

Như vậy, các bảng luật do người quản trị tạo ra sẽ rất thuận lợi khi ta muốn quản lý theo nhóm đối tượng, như: nhóm địa chỉ, nhóm dịch vụ,...

Các thao tác khác

1. *Lưu luật ra tệp*: Thao tác này cho phép người quản trị lưu toàn bộ hệ thống luật ra thành tệp tin. Chú ý: nếu trùng tên tệp tin thì nội dung mới sẽ thay thế nội dung cũ.
2. *Nạp luật từ tệp*: Dùng để nạp hệ thống luật từ tệp mà người quản trị đã lưu. Chú ý: là toàn bộ hệ thống luật hiện tại sẽ bị thay thế bởi hệ thống luật từ tệp này.

3. *Nạp luật ngầm định*: Nạp hệ thống luật ngầm định. Thông thường hệ thống luật này đã có sẵn hoặc được tạo ra khi thực hiện chức năng "Thiết lập" hệ thống tường lửa.

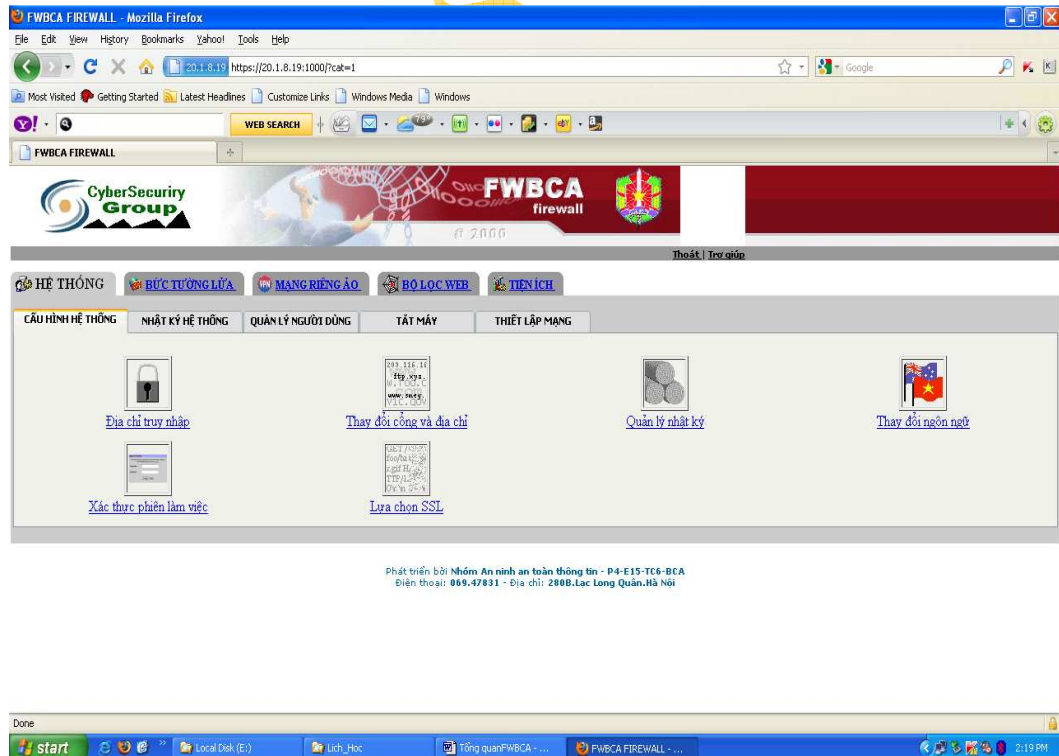
e. **Nhật ký hệ thống tường lửa**

Chức năng này cho phép người quản trị theo dõi các thông tin hay các dấu hiệu tấn công, để từ đó có các chính sách xử lý kịp thời. Nếu khi tạo một luật mà ta chọn chức năng nhật ký các gói tin phù hợp với luật đó thì gói tin phù hợp sẽ được nhật ký lại. Chức năng này cho phép lọc nhật ký theo nhiều điều kiện gồm: giao thức, địa chỉ IP nguồn-đích, cổng nguồn-đích.

IV. **Quản trị hệ thống**

- Cấu hình hệ thống
- Nhật ký hệ thống
- Quản trị người dùng

a. **Cấu hình hệ thống**



Cấu hình hệ thống cho phép người quản trị giới hạn địa chỉ truy nhập, thay đổi cổng và địa chỉ hoạt động của hệ thống quản trị tường lửa,

quản lý nhật ký, thay đổi giao diện người dùng, thay đổi ngôn ngữ hiển thị và chọn chế độ xác thực phiên làm việc.

- Địa chỉ truy nhập: ngầm định hệ thống cho phép tất cả các địa chỉ truy nhập. Tuy nhiên ta có thể giới hạn bằng cách chọn mục "Chỉ cho phép các địa chỉ trong danh sách" hoặc "Từ chối các địa chỉ trong danh sách", khi chọn một trong hai mục này ta phải nhập vào ô bên cạnh danh sách địa chỉ IP (hoặc tên máy) mà ta muốn cho phép hay hạn chế. Trong trường hợp nhập vào tên máy thì ta nên chọn mục "Giải nghĩa các tên máy" để ánh xạ tên máy và địa chỉ IP. Sau khi chọn xong cần nhấn nút "Ghi" để lưu lại mọi thay đổi.
- Thay đổi cổng và địa chỉ: chức năng này cho phép thay đổi cổng dịch vụ và địa chỉ IP mà hệ thống sẽ lắng nghe để nhận kết nối từ máy trạm. Ngầm định là lắng nghe trên mọi địa chỉ và cổng ngầm định là 10000. Nếu không có dịch vụ nào khác đã sử dụng cổng này thì ta không cần thiết phải thay đổi gì thêm.
- Quản lý nhật ký: lựa chọn có sử dụng nhật ký hay không, chọn modul cần nhật ký, thời gian tự động xoá nhật ký,... Thông thường ta nên chọn các mục sau:
 - Dừng nhật ký
 - Xoá nhật ký sau 168 giờ
 - Ghi nhật ký tất cả các modul
- Thay đổi ngôn ngữ: có hai ngôn ngữ hỗ trợ là Anh và Việt. Ngôn ngữ thể hiện ngầm định là tiếng Việt.
- Xác thực phiên làm việc: trong chức năng này ta nên chọn sau:
 - Dừng mật khẩu có timeout -> Ngăn chặn các máy có nhiều hơn 5 lần đăng nhập....
 - Dừng xác thực phiên -> Tự động đăng xuất sau 15 phút không tác động
 - Luôn yêu cầu tên đăng nhập và mật khẩu-> Đây là ba lựa chọn quan trọng để tránh việc truy nhập trái phép hoặc bị lộ mật khẩu đăng nhập. Các lựa chọn khác nên để mặc định.

b. Nhật ký hệ thống

Nhật ký hệ thống cho phép người quản trị xem lại các thao tác mà một người dùng đã thực hiện thao tác trên giao diện, đây không phải là nhật ký của bức tường lửa. Để xem nhật ký bạn chọn các điều kiện và nhấn nút "Xem", nếu phù hợp các lựa chọn thì kết quả sẽ hiện một bảng danh sách các thao tác đã thực hiện với modul nào cùng người dùng, địa chỉ IP và

ngày giờ thực hiện. Để chi tiết hơn, ta nhấn chọn lên kết ngay tên từng thao tác.

c. Quản trị người dùng

Trong giao diện này, cột "Người dùng" thể hiện danh sách người dùng đã tồn tại, cột "Các modul" là danh sách các modul mà người dùng tương ứng được sử dụng, có thể nhấn chọn tên modul để thay đổi quyền của người dùng đối với modul đó.

- Thay đổi người dùng đã tồn tại: ta chỉ việc nhấn vào người dùng muốn thay đổi trong danh sách ở cột "Người dùng". Trong mục này ta có thể thay đổi tên và mật khẩu đăng nhập của một người dùng đã tồn tại, hoặc thay đổi các lựa chọn. Chú ý: với người dùng mặc định "admin" thì không nên thay đổi gì mà nên để các lựa chọn là mặc định, vì đây là người dùng cần có quyền cao nhất để tạo ra các người dùng khác.
- Tạo người dùng mới: cần nhập tên đăng nhập và mật khẩu cho người dùng mới. Người dùng được tạo ra chỉ được phép thực hiện bởi các điều kiện mà người quản trị cao nhất cho phép. Thông thường ta chỉ cần chọn cho phép người mới này dùng các modul nào, còn các lựa chọn khác nên để mặc định. Sau khi chọn xong các điều kiện cần nhấn nút "Ghi" để lưu lại.

Chú ý: Người dùng mới không được trùng tên đăng nhập với các từ: admin, fwbca, và các tên đăng nhập đã có. Mật khẩu đăng nhập phải đặt tối thiểu 6 ký tự.

V. Các tiện ích

- Ping
- Trace route

a. Ping

Thực hiện chương trình Ping ngay trên giao diện web. Có thể ping theo địa chỉ IP hay tên máy.

b. Trace route

Tiện ích này thực hiện chương trình theo dấu gói tin ngay trên giao diện web cho phép ta biết được đường đi của gói tin từ máy này đến một máy đích cụ thể.

Tài liệu giới thiệu (NANO-FWBCA)

Mọi chi tiết xin liên hệ:

Nguyễn Minh Thắng – Phòng kinh doanh, hỗ trợ dự án

Mobile phone: [0985 224 229](tel:0985224229)

Support online: minhthang_sat@yahoo.com

Email: thangnm@nanosoft.vn

Đình Văn Định – Phụ trách kinh doanh

Mobile phone: [094 797 6660](tel:0947976660)

Support online: dvd_tin@yahoo.com

Email: dinhdv@nanosoft.vn

Nguyễn Văn Sự – Hỗ trợ kỹ thuật

Mobile phone: [0977 270 874](tel:0977270874)

Email: sunv@nanosoft.vn

CÔNG TY CỔ PHẦN CÔNG NGHỆ NANOSOFT

Trụ sở : Số 2C9B – Tô Hiệu – Cầu Giấy – Hà Nội

Văn phòng : Số 3 Ngõ 122 – Kim Giang – Đại Kim – Hoàng Mai – Hà Nội

Điện thoại : [04. 3 559 2799](tel:0435592799); [6 292 4093](tel:0435594093) – Fax: [04. 3 559 2799](tel:0435592799)

Email : info@nanosoft.vn – Website: www.nanosoft.vn

Chào trân trọng và rất hân hạnh được hợp tác!