**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**BỘ MÔN KỸ THUẬT MÁY TÍNH**

---------------o0o---------------

**A picture containing food

Description automatically generated**

**BÁO CÁO BÀI TẬP LỚN MÔN HỌC**

**NHẬP MÔN AN TOÀN THÔNG TIN**

**ĐỀ TÀI:**

**Bảo mật hệ thống, bảo mật mạng. Các**

**chính sách, các chuẩn trong hệ điều hành**

**Windows**

**GVHD: PGS. Nguyễn Linh Giang**

**SVTH: Nguyễn Văn Tựu - 20173462**

**Trịnh Đình Hiếu - 20173109**

**Nguyễn Sĩ Vũ - 20173469**

**Vũ Ngọc Trường - 20173426**

**MỤC LỤC**

[1. GIỚI THIỆU 2](#_Toc42433984)

[1.1 Giới thiệu chung 2](#_Toc42433985)

[1.2 Nhiệm vụ đề tài 2](#_Toc42433986)

[2. NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS 3](#_Toc42433987)

[2.1 TỔNG QUAN VỀ AN NINH MẠNG 3](#_Toc42433988)

[2.2 CÁC MỐI ĐE DỌA THƯỜNG GẶP 5](#_Toc42433989)

[2.3 CƠ CHẾ XÁC THỰC: QUẢN LÝ QUYỀN TRUY VÀ QUẢN LÝ DANH TÍNH 8](#_Toc42433990)

[2.4 TỔNG QUAN VỀ FIREWALL 12](#_Toc42433991)

[2.5 SỬ DỤNG FIREWALL 14](#_Toc42433992)

[2.6 WINDOWS DEFENDER 20](#_Toc42433993)

[2.7 CÁC CHÍNH SÁCH BẢO MẬT TRÊN WINDOWS 22](#_Toc42433994)

[3. KẾT LUẬN 24](#_Toc42433995)

[4. DEMO: TẠO TƯỜNG LỬA BẰNG PHẦN MỀM SMOOTHWALL 25](#_Toc42433996)

# GIỚI THIỆU

## Giới thiệu chung

Hệ điều hành Windows là hệ điều hành phổ biến nhất trên thế giới. Cũng vì sự phổ biến đó mà các vấn đề bảo mật trên các phiên bản hệ điều hành Windows rất được quan tâm và chú ý. Qua từng năm hệ thống bảo vệ trên hệ điều hành Windows ngày càng được cải tiến và nâng cấp nhưng vẫn không tránh khỏi những sai sót trong quá trình vận hành.

Hiện nay, vấn đề về an toàn trên máy tính ngày càng được coi trọng. Bất cứ chương trình nào muốn thực hiện một cách ổn định và hiệu quả đều phải có một hệ thống bảo mật. Cũng giống như vậy hệ điều hành muốn vận hành tốt cũng phải có hệ thống bảo vệ, hệ thống bảo vệ trở thành một thành phần quan trọng quyết định đến sự phổ biến của hệ điều hành đó.

Đối với hệ điều hành Windows, qua từng bước phát triển hệ điều hành càng ngày được nâng cấp đòi hỏi hệ thống bảo vệ phải được nâng cấp theo nhằm đảm bảo tính ổn định cho hệ điều hành và đối mặt với những nguy cơ về an ninh mạng. Sự nỗ lực nghiên cứu về bảo mật của các kỹ sư tại Microsoft đã được đền đáp xứng đáng qua từng phiên bản Windows.

## Nhiệm vụ đề tài

+Trong đề tài này, chúng ta sẽ nghiên cứu và tìm hiểu một cách chi tiết nhất về hệ thống bảo vệ trong hệ điều hành Windows qua các nội dung:

-Nội dung 1: Tổng quan về an ninh mạng, các mối đe dọa

-Nội dung 2: Cơ chế xác thực, quản lý quyền truy và quản lý danh tính (cơ chế xác thực người dùng)

-Nội dung 3: Tổng quan về Firewall, sử dụng Firewall

-Nội dung 4:Windows Defender

-Nội dung 5: Các chính sách trong Windows

# NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS

## TỔNG QUAN VỀ AN NINH MẠNG

* + 1. BẢO MẬT CHO MÁY TÍNH

Trong bối cảnh công nghệ thông tin ngày càng một phát triển hiện nay giúp cho sự kết nối giữa tất cả mọi người với nhau trở nên dễ dàng qua các thiết bị công nghệ, đặc biệt đó là máy tính. Kéo theo sự phát triển đó là nguy cơ mất an toàn thông tin, bảo mật dữ liệu. Hệ thống bảo vệ của Windows đã và đang hoàn thiện nhằm đáp ứng nhu cầu bảo mật cho người sử dụng

* + 1. CÁC HÌNH THỨC TẤN CÔNG TRÊN MẠNG

1, Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò tìm tên ng­ười sử dụng và mật khẩu.

2, Nghe trộm trên mạng

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên, mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa card giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

3, Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

4, Vô hiệu các chức năng của hệ thống

Đây là kiểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

Ví dụ sử dụng lệnh ping với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

5, Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

6, Tấn công mật khẩu (Password attack)

Đối với các cuộc tấn công mật khẩu, các hacker sẽ cố gắng "phá" mật khẩu được lưu trữ trên cơ sở dữ liệu tài khoản hệ thống mạng hoặc mật khẩu bảo vệ các tập tin.

Các cuộc tấn công mật khẩu bao gồm 3 loại chính: các cuộc tấn công dạng từ điển (dictionary attack), brute-force attack và hybrid attack.

Cuộc tấn công dạng từ điển sử dụng danh sách các tập tin chứa các mật khẩu tiềm năng.

7, Một số kiểu tấn công mạng khác

- Tấn công nội bộ (Insider attack)

- Các cuộc tấn công của không tặc

-Buffer overflow (lỗi tràn bộ đệm)

-….

## CÁC MỐI ĐE DỌA THƯỜNG GẶP

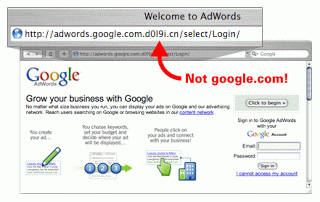
* + 1. Phishing

a, Khái niệm

Phishing là việc xây dựng những hệ thống lừa đảo nhằm đánh cắp các thông tin nhạy cảm, như tên đăng nhập, mật khẩu hay thông tin về các loại thẻ tín dụng của người dùng. Phishing xuất hiện như một thực thể đáng tin cậy, một trang thông tin điện tử, eBay, Paypal, gmail, hay các ngân hàng trực tuyến là những mục tiêu hướng đến của hình thức tấn công này. Phishing thường được thực hiện qua email, những tin nhắn nhanh và thường tập trung vào hướng lừa người dùng nhập các thông tin vào một form hay click vào một đường dẫn của website lừa đảo.

b, Những kỹ thuật của phishing

-Đường dẫn giả mạo: bằng việc tạo ra một cửa sổ có giao diện y hệt và đường dẫn gần giống trang web thật, người dùng dễ dàng nhập vào những thông tin cá nhân quan trọng



- Các phishers – kẻ thực hiện tấn công phishing, đã sử dụng các hình ảnh thay thế cho các dữ liệu text thông thường làm khó khăn hơn cho các “anti-phishing” có thể lọc và phát hiện những dữ liệu text thường có trong các email lừa đảo.

c, Cách nhận biết, phòng tránh

-Không bao nghĩ rằng một email là hợp lệ chỉ dựa trên địa chỉ của người gửi – chúng hoàn toàn có thể làm giả mạo.

-Một ngân hàng, tổ thức tin cậy như Paypal sẽ không bao giờ yêu cầu bạn nhập tên và mật khẩu trong một email paypal.

-Một Email từ một tổ chức tin cậy sẽ không bao giờ chứa các file đính kèm hoặc phần mềm.

-Click vào một đường dẫn trong email là cách để bọn lừa đảo lấy được tài khoản của bạn

* + 1. Trojan

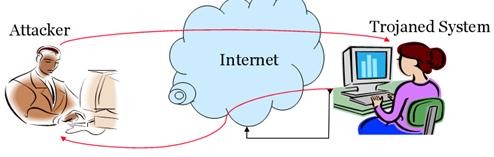
a, Khái niệm

Theo truyền thuyết, người Hy Lạp đã giành chiến thắng trong cuộc chiến thành Troy bằng cách ẩn trong một con ngựa khổng lồ bằng gỗ rỗng lẻn vào thành Troy kiên cố. Trong thế giới máy tính ngày nay, một Trojan horse được định nghĩa là một “chương trình độc hại ngụy trang như một cái gì đó được cho là lành tính“. Ví dụ, bạn tải về những chương trình đơn giản như một bộ phim hay tập tin âm nhạc, nhưng khi bạn click vào nó, bạn có thể mở ra một chương trình nguy hiểm xóa đĩa cứng của bạn, gửi số thẻ tín dụng và mật khẩu của bạn với một người lạ, hoặc cho phép người lạ chiếm quyền điều khiển máy tính của bạn hay trở thành một phần tử trong mạng botnet để góp phần vào một cuộc tấn công DDoS.

Nếu máy tính của nạn bị nhiễm Trojans, một kẻ tấn công cũng có thể truy cập và điều khiển toàn bộ máy tính của nạn nhân và chúng có thể sử dụng vào nhiều mục đích khác nhau.

b, Mục tiêu

Khá giống với Phishing, mục tiêu của Trojan cũng là ăn cắp thông tin người dùng nhưng can thiệp mạnh mẽ hơn dữ liệu người dùng thay vì chỉ lấy được tài khoản và mật khẩu



* + 1. Spyware

a, Khái niệm

Spyware hay phần mềm gián điệp là thuật ngữ thường được sử dụng để chỉ các phần mềm thực hiện hành vi nhất định như quảng cáo, thu thập thông tin người dùng hoặc thay đổi cấu hình máy tính của bạn, nói chung là không có sự đồng thuận của người dùng.

b, Cách khắc phục

Đây là tên một số phần mềm bạn có thể sử dụng để gỡ bỏ hoàn toàn phần mềm gián điệp:

Spyware Hunter

Malwarebytes

ADWCleaner

JunkWare Removal Tool

HitMan Pro

Hay các phần mềm diệt virus: Bit Defender, Bkav Pro, Kaspersky …

## 2.3 CƠ CHẾ XÁC THỰC: QUẢN LÝ QUYỀN TRUY VÀ QUẢN LÝ DANH TÍNH

2.3.1 HỆ THỐNG AAA

1, AUTHENTICATION

-Authentication là định danh, chỉ quá trình định danh một tài khoản đang vào hệ thống là người đó chứ không phải là người khác.

-Bước xác thực này thường thông qua form đăng nhập tài khoản mật khẩu vào hệ thống. Cũng có thể sử dụng một số phương pháp xác thực như Sinh học (vân tay, tròng mắt, khuôn mặt,..) và Khóa (public & private).

-Mật khẩu (password, pin) hay Sinh học đã quá quen thuộc với chúng ta và đã áp dụng trên hầu hết thiết bị công nghệ. Riêng Khóa (public & private) thường chỉ áp dụng cho hệ thống quản trị sever.

2, AUTHORIZATION

Sau quá trình định danh thì cần phải phân quyền cho người sử dụng hệ thống. Có 2 thành phần hoạt động giúp phân quyền hiệu quả:

-Phân quyền theo nhóm (Role-based authorization): người dùng được phân thành các nhóm có đặc điểm chung giống nhau và chỉ được cấp phát quyền đáp ứng nhu cầu của nhóm đó

VD: nhóm Students không được cấp quyền truy cập Database chứa điểm kiểm tra

-Phân quyền theo cá nhân (Object-based authorization): phân quyền cho từng cá nhân riêng biệt

VD: thầy dạy Kiến trúc máy tính chỉ được phép lên điểm cho môn Kiến trúc máy tính chứ không được quyền can thiệp vào môn học khác

3, ACCOUNTING

-Là quá trình kiểm tra và ghi log. Một số hoạt động hay toàn bộ hoạt động của người dùng trên hệ thống.

-Việc ghi log có hai tác dụng là đánh giá, theo dõi hoạt động của thành viên (nhân viên…) trên hệ thống và điều tra khi có sự cố mất mác, sai lệch, rò rĩ thông tin mà không rõ nguyên nhân.

2.3.2 Network Authentication Systems

- Network Authentication Systems là Hệ thống xác thực mạng

- Để xác thực một người dùng trong mạng và chắc chắn người dùng được phép, người sử dụng cần cung cấp 2 mẫu thông tin : identification và proof of identity. Trong hầu hết các mạng, người dùng được nhận diện qua chính tài khoản email của mình.

- Theo truyền thống, mật khẩu được sử dụng để chứng minh danh tính của người dùng. Người dùng biết mật khẩu thì có thể truy cập được quyền của mình. Nhưng dùng mật khẩu khó tránh những rủi ro nhất định, như người khác có thể biết mật khẩu của bạn, bạn có thể bị hack mật khẩu,… nên đã tạo ra những phương thức hiệu quả hơn mật khẩu. Đó là nhận diện người dùng thông qua một mật khẩu gửi qua SMS với số điện thoại đăng ký trước, dùng vân tay của người dùng ( khá là hạn chế khi chưa có quá nhiều thiết bị trang bị cảm biến vân tay),…

2.3.3 Storing User Credentials (Lưu trữ giấy chứng nhận người dùng)

- Các mô hình chứng thực phân cấp đòi hỏi tài nguyên mạng để duy trì một danh sách user và các thông tin của user. Qua đó người dùng có thể xác thực việc sử dụng các tài nguyên mạng, nó sẽ trở thành không thể quản lý trên mạng với hơn một máy chủ. Trong các mạng Windows, mỗi máy chủ duy trì một danh sách những người dùng địa phương(local users) mà có thể được sử dụng để thực hiềnj một mô hình chứng thực phân cấp.

- Mô hình chứng thực tập trung cho phép quản lý đơn giản đáng kể trong các mạng lớn hơn, tiện hơn cho Help desk quản lý mật khẩu. Trong mô hình tập trung, tài nguyên mạng dựa vào một cơ quan trung tâm để xác định user. Chứng thực tập trung là cần thiết trong môi trường mà người dùng truy cậ vào tất cả các tài nguyên mạng với một bộ các thông tin, một tình hình lý tưởng được gọi là Single sign-on. Trong các mạng Windows, chứng thực tập trung được cung cấp bởi Active Directory. Các mạng lớn hơn có thể sử dụng nhiều doamin, với việc trusts để user trong domain này truy cập tài nguyên của domain khác.

2.3.3 Authentication Features of Windows Server 2003

Windows Server 2003 cung cấp phương pháp xác thực mạnh mẽ và linh hoạt có thể được cấu hình để đáp ứng nhu cầu của các tổ chức từ doanh nghiệp nhỏ cho đến doanh nghiệp tầm cỡ. Tính năng xác thực chính của Windows Server 2003 bao gồm:

-Trung tâm quản lý các tài khoản người dùng: (Central administration of user accounts) Các dịch vụ Active Directory cho phép người dùng đăng nhập vào máy tính trong một môi trường multidomain, multiforest bằng cách sử dụng một yếu tố xác thực (single-factor authentication) hoặc các loại đa chứng thực(multifactor authentication)

-Môi trường đăng nhập một lần (Single sign-on environmentn): Khi người dùng được chứng thực trong một doamin đó, qua đó loại bỏ sự xác thực không cần thiết khi người dùng truy cập tài nguyên khác nhau. Khi công nghệ ngày được sử dụng với người dùng Windows XP, người dùng có thể truy cập tài nguyên trong các lĩnh vực khác bằng cách cung cấp mật khẩu một lần và lưu trữ các mật khẩu như một hàn tài khoản người dùng trong doanmin.

-Máy tính và các tài khoản dịch vụ(Computer and service accounts):

Ngoài cho người dùng, máy tính và các tài khoản dịch vụ cũng được xác thực với hệ thống.

-Đa hỗ trợ(Multifactor support): Windows Server 2003 natively hỗ trợ thẻ thông minh và một loạt cơ chế xác thực khác.

-Kiểm toán (Auditing): Windows Server 2003 cho phép kiểm soát việc đăng nhập và truy cập tài nguyên của người dùng.

2.3.4 Giao thức xác thực người dùng challenge-response

-LAN Manager (LM): Được phát triển bởi IBM và Microsoft để sử dụng trong OS2 và windows cho Worrkgroups. Đây là hình thức kém an toàn của xác thực challenge-response vì nó là dễ bị kẻ tấn công nghe trộm, và máy chủ chứng thực người dùng phải lưu trữ các thông tin trong LMHash.

-NTLM: là hình thực nâng cấp của giao thức LM, giúp nâng cao tính bảo mật cho giao thức thông qua việc sử dụng mã hóa 56-bit (NTLM1) và 128-bit (NTLM2).

2.3.4 Giao thức xác thực người dùng Kerberos

-Là giao thức mặc định cho Windows Server 2003, Windows 2000 và Windows XP Professional.

-Hiệu quả: Khi một máy chủ cần xác thực một client, máy chủ Kerberos có thể xác nhận các thông tin của client mà không cần phải liên hệ với domain controller.

-Tự chứng thực (Mutual authentication) Ngoài việc chứng thực client đến server Kerberos cho hép máy chủ tự xác thực lẫn nhau.

-Ủy quyền chứng thực (Delegated authentication): Cho phép các dịch vụ để đóng vai client khi truy cập tài nguyên.

-Đơn giản hóa quản lý: Có thể sử dụng trust giữa các domain trong cùng môt forest và các domain kết nối với một forest

-Khả năng cộng tác: Kerberos được dựa trên tiêu chuẩn Internet Engineering Task Force (IETF) và do đó tuơng thích với IETF khác tuân theo lõi Kerberos

## TỔNG QUAN VỀ FIREWALL

2.4.1 Firewall là gì?

Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những traffic phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi traffic khác đều bị từ chối.

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một “người gác cổng” như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet. Thứ 2, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là Internet Protocol address (hay còn gọi là địa chỉ IP): Nếu không có firewall hỗ trợ, nó chẳng khác gì chuyện bạn bật tất cả đèn lên và mở rộng cửa để đón trộm vào.

Một firewall được cấu hình chính xác sẽ ngăn chặn điều này xảy ra và giúp máy tính “ẩn” một cách hiệu quả, cho phép người dùng thoải mái thưởng thức những gì thế giới trực tuyến mang lại. Firewall không giống chương trình diệt virus. Thay vào đó, nó làm việc cùng với những công cụ này nhằm đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến.

2.4.2 Firewall hoạt động như thế nào?

Công việc của một firewall khá khó khăn, bởi có rất nhiều dữ liệu hợp pháp cần được cấp phép cho ra hoặc vào máy tính kết nối mạng. Ví dụ, khi chúng ta truy cập vào trang web Quantrimang.com, đọc tin tức, tips công nghệ mới thì thông tin và dữ liệu của trang web cần được truyền từ và tới máy thông qua mạng để hoàn thành quá trình này.

Một firewall cần biết được sự khác biệt giữa lưu lượng hợp pháp như trên với những loại dữ liệu gây hại khác.

Firewall sử dụng rule hoặc ngoại lệ để làm việc với những kết nối tốt và loại bỏ những kết nối xấu. Nhìn chung, quá trình này được thực hiện ẩn, người dùng không thấy được hoặc không cần tương tác gì cả.

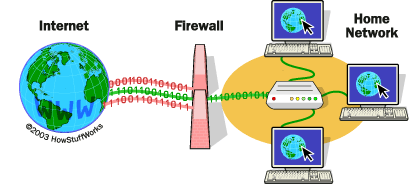
## SỬ DỤNG FIREWALL

* + 1. Chức năng

Internet Firewall (gọi tắt là Firewall) là một thành phần nằm giữa Intranet và Internet để kiểm soát việc lưu thông và truy cập giữa chúng với nhau bao gồm:

* Firewall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập bên trong, và cả những dịch vụ nào bên ngoài mà người bên trong được phép truy cập.
* Để firewall làm việc hiệu quả, tất cả trao đổi thông tin từ trong ra ngoài và ngược lại đều phải qua firewall.
* Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ mới được quyền thông qua firewall.

Sơ đồ minh họa chức năng của firewall :



Sơ đồ minh họa chức năng của firewall

* + 1. Cấu trúc

Firewall bao gồm:

* Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến(router) hoặc có chức năng router. (phần cứng)
* Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là hệ thống xác thực, cấp quyền, kế toán (AAA). (phần mềm)
  + 1. Các thành phần của Firewall

Một firewal chuẩn ba gồm một hay nhiều các thành phần sau đây:

* Bộ lọc packet
* Cổng ứng dụng
* Cổng mạch

Sau đây ta sẽ đi tìm hiểu từng thành phần một cách chi tiết và đầy đủ hơn

Thành phần thứ nhất: Bộ lọc gói tin ( Packet filtering router)

* Nguyên lý:

Firewall hoạt động chặt chẽ với giao thức liên mạng TCP/IP. Giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu theo thuật toán chia nhỏ các dữ liệu nhận được trên mạng thành các gói dữ liệu (data packets) rồi gán cho những gói này những địa chỉ để có thể nhận dạng, tái lập lại ở đích đến, do đó các loại firewall cũng liên quan tới các gói tin và địa chỉ của chúng.

Bộ lọc gói tin cho phép hay từ chối mỗi gói tin mà nó nhận được. Nó kiểm tra xem gói tin đó có hợp lệ hay không. Muốn làm được vậy thì cần có các thông tin của gói tin đó là:

~ Địa chỉ IP nơi xuất phát

~ Địa chỉ IP nơi nhận

~ Những thủ tục truyền tin

~ Cổng TCP/UDP nơi xuất phát

~ Cổng TCP/UDP nơi nhận

~ Dạng thông báo ICMP

~ Giao diện packet đến

~ Giao diện packet đi

Nếu packet thỏa mãn các yêu cầu thì sẽ được chuyển qua firewall. Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, firewall chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó mới được phép chạy trên hệ thống mạng cục bộ.

* Ưu điểm:

~ Đa số các firewall đều sử dụng bộ lọc packet. Chi phí thấp vì đã được bao gồm trong phần mềm của router.

~ Bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng

* Hạn chế:

Việc định nghĩa các chế độ lọc packet là một việc khá phức tạp, nó đòi hỏi người quản tị mạng cần có những hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header,và các giá trị cụ thể mà họ nhận trên môi trường. Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phực tạc, rất khó để quản lý và điều khiển.

Do làm việc dựa vào thông tin header của các packet, bộ lọc gói tin sẽ không kiểm soát đươc nội dung của gói tin. Nên các gói tin được thông qua vẫn có thể mang theo những hành động có ý đồ tấn công.

Thành phần thứ hai: Cổng ứng dụng (application-level gateway)

* Nguyên lý:

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service (dịch vụ đại diện). Proxy service là các bộ chương trình đặc biệt cài trên gateway cho từng ứng dụng. Người quản trị mạng không cài đặt chương trình proxy cho một ứng dụng nào đó , dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall.Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối các đặc điểm khác.

Một cổng ứng dụng thường được coi như một pháo đài (bastion host) bởi nó được thiết kế để chống lại sực tấn công bên ngoài. Các biện pháp giúp đảm bảo an ninh cho bastion host là :

~ Bastion host luôn chạy các version an toàn của các phần mềm hệ thống. Các version an toàn này được thiết kế để chống lại sự tấn công vào phần mềm hệ thống, cũng như đảm bả.o sự tích hợp firewall.

~ Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion. Thông thường chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user được cài đặt trên bastion host.

~ Bastion có thể yêu cầu nhiều mức độ xác thực khác nhau

~ Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa là tính cục bộ và tính thống nhất đói với máy chủ và bộ lệnh được nâng cao.

~ Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng thiết lập, tháo gỡ hay thay thế một proxy.

~ Mỗi proxy đều ghi lại nhật ký toàn bộ chi tiết về thông qua, kết nối. Nhật ký này giúp tìm dấu vết và ngăn chặn kẻ phá hoại.

* Ưu điểm:

~ Cho phép người quản trị mạng hoàn toàn điều khiển từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết địng những máy chủ nào có thể truy nhập được bởi các dịch vụ.

~ Cho phép nguời quản trị mạng hoàn toàn điều khiển những dịch vụ nào cho phép, bởi vì nếu không có proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khóa

~ Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy cập hệ thống.

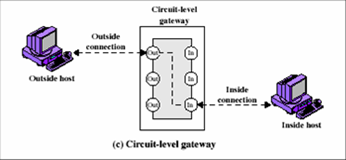
~ Cổng ứng dụng dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

* Hạn chế:

Yêu cầu các users biến đổi thao tác, hoặc thao tác phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh.

Thành phần thứ ba: Cổng vòng (circuit-Level Gateway)

* Circuit Level Gateway – cổng vòng – là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.
* Hình sau minh họa một hành động sử dụng kết nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống firewall nên nó che dấu thông tin về mạng nội bộ.



* Cổng vòng thường được sử dụng cho những kết nối ra ngoài. Ưu điểm lớn nhất là một Bastion host có thể được cấu hình như là một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy câp tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.
  + 1. Những hạn chế của firewall

Không cái gì là toàn diện cả, tuy Firewall cung cấp nhiều tính năng hữu ích để bảo vệ người dùng, song nó vẫn có những nhược điểm như:

+ Firewall không thể bảo vệ các mối nguy hiểm từ bên trong nội bộ. Tác hại thì khỏi cần nói các bạn cũng đã biết, nếu một ai trong công ty có ý đồ xấu, muốn phá hoại thì Firewall cũng đành bó tay.

+ Firewall không có đủ thông minh để có thể đọc và hiểu từng loại thông tin và tất nhiên là nó không thể biết được đâu là nội dung tốt và đâu là nội dung xấu. Mà đơn thuần Firewall chỉ hỗ trợ chúng ta ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

+ Firewall không thể ngăn chặn các cuộc tấn công nếu như cuộc tấn công đó không “đi qua” nó. Ví dụ cụ thể đó là Firewall không thể chống lại một cuộc tấn công từ một đường dialup, hoặc là sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp ra đĩa mềm.

+ Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số ứng dụng hay phần mềm.. được chuyển qua thư điện tử (ví dụ như Gmail, Yahoo mail…), nó có thể v­ượt qua Firewall vào trong mạng được bảo vệ.

+ Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu đ­ược chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu để có thể thoát khỏi khả năng kiểm soát của firewall. Tuy nhiên, chúng ta không thể phủ nhận một điều rằng Firewall vẫn là giải pháp hữu hiệu được áp dụng khá rộng rãi hiện nay.

## WINDOWS DEFENDER

* + 1. WINDOWS DEFENDER là gì?

Windows Defender, trước đó là Microsoft AntiSpyware, là một sản phẩm phần mềm của Microsoft để phòng chống, gỡ bỏ và cô lập spyware trên Microsoft Windows. Nó có sẵn và được bật theo mặc định trong Windows Vista và Windows 7, và được tải miễn phí cho Windows XP và Windows Server 2003.

* + 1. Chức năng

I.Chức năng cơ bản

Windows Defender có chức năng quét hệ thống như các phần mềm miễn phí khác trên thị trường, và bao gồm một số tác tử bảo mật thời gian thực theo dõi sự thay đổi một vài khu vực chung của Windows có thể do bị nhiễm spyware. Nó cũng có khả năng gỡ các ứng dụng ActiveX đã được cài đặt. Ngoài ra việc tích hợp vào mạng SpyNet của Microsoft cho phép người dùng thông báo cho Microsoft những gì họ cho là spyware, và những ứng dụng hay trình điều khiển nào cho phép cài đặt trên hệ thống của họ.

II Chức năng nâng cao

1. Bảo vệ thời gian thực

Trong các tùy chọn của Windows Defender, người dùng có thể cấu hình các tùy chọn bảo vệ thời gian thực:

Auto Start - Theo dõi các chương trình cho phép chạy khi khởi động hệ thống

System Configuration (settings) - Theo dõi các thiết lập cảnh báo bảo mật trong Windows

Internet Explorer Add-ons - Theo dõi các chương trình tự động chạy khi mở Internet Explorer

Internet Explorer Configurations (settings) - Theo dõi cấu hình bảo mật trình duyệt

Internet Explorer Downloads - Theo dõi các tệp và chương trình được thiết kế cho Internet Explorer

Services and Drivers - Theo dõi các dịch vụ và trình điều khiển tương tác với Windows và các chương trình

Application Execution - Theo dõi các hành động của các chương trình khi đang chạy

Application Registration - Theo dõi các công cụ và tệp nơi mà các chương trình có thể đăng ký để chạy

Windows Add-ons - Theo dõi các chương trình phụ trợ cho Windows

1. Tích hợp với Internet Explorer

Có một sự tích hợp với Internet Explorer cho phép quét file sau khi tải để đề phòng nguy cơ tải về file độc hại. Cải tiến này giống với các trình anti-virus khác trên thị trường. Mặc dù không dùng kèm được với Firefox hoặc các trình duyệt khác, Windows Defender vẫn quét các tệp tải về như một phần của chức năng bảo vệ thời gian thực

1. Softwware Explorer

Mục Advanced Tools cho phép người dùng khám phá các nguy cơ tiềm ẩn với Software Explorers. Chúng hiển thị các chương trình tự chạy, chương trình đang chạy, chương trình kết nối mạng, và trình cung cấp Winsock (Winsock LSP). Trong mỗi khung Explorer, mỗi đối tượng được đánh giá "Biết", "Không biết" hay "Nguy cơ không mong muốn". Thể loại đầu tiên và cuối cùng cung cấp liên kết liên quan đến đối tượng được chọn, và thể loại thứ hai mời người dùng gửi ứng dụng tới SpyNet để chẩn đoán bởi các chuyên gia.

1. Chức năng chỉ định của Windows Vista

Windows Defender trong Windows Vista tự động chặn tất cả các ứng dụng tự chạy cần quyền quản trị (đây là cách đối xử nghi ngờ với các chương trình khởi động). Việc chặn này liên quan đến chức năng UAC (User Account Control) trong Windows Vista, và yêu cầu người dùng tự chạy chúng mỗi lần khi đăng nhập.

## CÁC CHÍNH SÁCH BẢO MẬT TRÊN WINDOWS

* + 1. Chính sách về tài khoản:

Các chính sách này được xác định trên các thiết bị; chúng ảnh hưởng đến cách tài khoản người dùng có thể tương tác với máy tính hoặc tên miền. Chính sách tài khoản bao gồm các loại chính sách sau:

**Chính sách mật khẩu:** Các chính sách này xác định cài đặt cho mật khẩu, chẳng hạn như thực thi và thời gian sống. Chính sách mật khẩu được sử dụng cho các tài khoản miền.

**Chính sách khóa tài khoản:** Các chính sách này xác định các điều kiện và thời gian mà tài khoản sẽ bị khóa khỏi hệ thống. Chính sách khóa tài khoản được sử dụng cho tên miền hoặc tài khoản người dùng cục bộ.

**Chính sách của Kerberos:** Các chính sách này được sử dụng cho tài khoản người dùng miền; họ xác định các cài đặt liên quan đến Kerberos, chẳng hạn như tuổi thọ vé và thực thi.

* + 1. Chính sách địa phương:

Các chính sách này áp dụng cho máy tính và bao gồm các loại cài đặt chính sách sau:

**Chính sách kiểm toán**: Chỉ định cài đặt bảo mật kiểm soát việc ghi nhật ký các sự kiện bảo mật vào Nhật ký bảo mật trên máy tính và chỉ định loại sự kiện bảo mật nào cần ghi (thành công, thất bại hoặc cả hai).

**Chuyển nhượng quyền người dùng:** Chỉ định người dùng hoặc nhóm có quyền đăng nhập hoặc đặc quyền trên thiết bị

**Tùy chọn bảo mật:** Chỉ định cài đặt bảo mật cho máy tính, chẳng hạn như tên Quản trị viên và Tài khoản khách; truy cập vào ổ đĩa mềm và ổ đĩa CD-ROM; lắp đặt trình điều khiển; nhắc nhở đăng nhập; và như thế.

* + 1. Chỉnh sách Firewall:

Chỉ định cài đặt để bảo vệ thiết bị trên mạng của bạn bằng cách sử dụng tường lửa trạng thái cho phép bạn xác định lưu lượng truy cập mạng nào được phép đi qua giữa thiết bị của bạn và mạng.

* + 1. Chính sách quản lý danh sách mạng :

Chỉ định cài đặt mà bạn có thể sử dụng để định cấu hình các khía cạnh khác nhau về cách các mạng được liệt kê và hiển thị trên một thiết bị hoặc trên nhiều thiết bị.

* + 1. Chính sách khóa công khai:

Chỉ định cài đặt để kiểm soát Hệ thống tệp mã hóa, bảo vệ dữ liệu và mã hóa ổ đĩa BitLocker ngoài các đường dẫn chứng chỉ và cài đặt dịch vụ nhất định.

* + 1. Chính sách hạn chế phần mềm:

Chỉ định cài đặt để xác định phần mềm và kiểm soát khả năng chạy trên thiết bị, đơn vị tổ chức, tên miền hoặc trang web cục bộ của bạn.

* + 1. Chính sách kiểm soát ứng dụng :

Chỉ định cài đặt để kiểm soát người dùng hoặc nhóm nào có thể chạy các ứng dụng cụ thể trong tổ chức của bạn dựa trên danh tính duy nhất của tệp.

* + 1. Chính sách bảo mật IP trên máy tính cục bộ :

Chỉ định cài đặt để đảm bảo liên lạc riêng tư, an toàn qua mạng IP thông qua việc sử dụng các dịch vụ bảo mật mã hóa. IPsec thiết lập sự tin cậy và bảo mật từ một địa chỉ IP nguồn đến một địa chỉ IP đích.

* + 1. Cấu hình chính sách kiểm toán nâng cao:

Chỉ định cài đặt kiểm soát việc ghi nhật ký các sự kiện bảo mật vào nhật ký bảo mật trên thiết bị. Các cài đặt trong Cấu hình chính sách kiểm toán nâng cao cung cấp quyền kiểm soát tốt hơn đối với các hoạt động sẽ giám sát trái ngược với cài đặt Chính sách kiểm toán trong Chính sách cục bộ.

## 

# KẾT LUẬN

Sự nỗ lực nghiên cứu về bảo mật của các kỹ sư tại Microsoft đã được đền đáp xứng đáng qua từng phiên bản Windows

Hệ thống bảo vệ trên hệ điều hành Windows đã và đang làm tốt nhiệm vụ của mình, giúp máy tính được bảo vệ gần như tốt nhất.

Tuy vậy để đối mặt với ngày càng nhiều nguy cơ an ninh mạng, hệ thống bảo vệ cần được nâng cấp hơn nữa

Ngoài ra, hệ thống bảo vệ trong hệ điều hành Windows không thể giải quyết được vấn đề liên quan đến Virus và sự phát triển của Virus nên máy tính của bạn cần có những chương trình diệt Virus tốt và phù hợp

# DEMO: TẠO TƯỜNG LỬA BẰNG PHẦN MỀM SMOOTHWALL

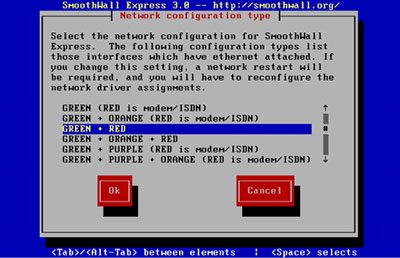
- Tải về tập tin ISO ứng dụng SWE , sau đó ghi ra đĩa.

- Khởi động lại hệ thống, chọn đĩa CD và chạy trình cài đặt, giúp bạn dọn dẹp ổ cứng “chào đón” SWE.

- Chế độ mặc định “Half- Open” cho phép thực hiện hầu hết các kết nối xuất hoạt động bình thường, trừ những kết nối tiềm ẩn nguy hiểm. Bạn có thể chọn chế độ “Open” để không giới hạn các kết nối xuất, hoặc chọn “Closed” để “khóa cửa”, chỉ cho phép những kết nối cụ thể nhất định được cấp phép.

Bạn sẽ cần cấu hình giao diện của mạng, giữa màu xanh, đỏ, cam hay tím.

Giao diện màu xanh cho thấy đây là một mạng LAN đáng tin cậy. Màu đỏ là mạng Internet tiềm ẩn nguy hiểm. Màu cam là hệ thống DMZ của bạn (một vùng nằm riêng lẻ so với LAN). Màu tím là hệ thống LAN không dây.



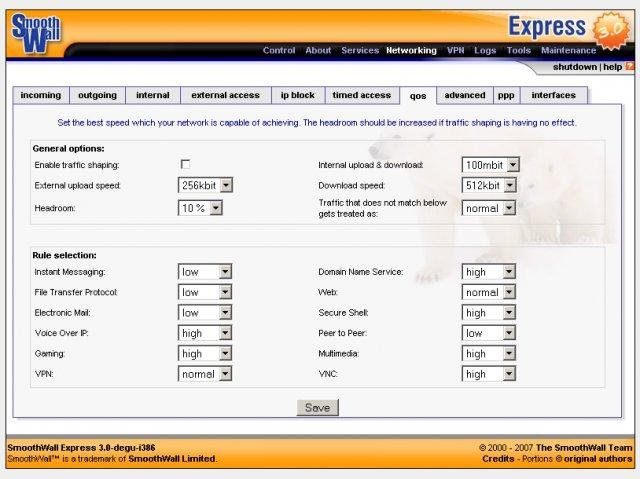
- Tiếp đến, bạn cần chọn card mạng nào sẽ chỉ định cho từng hốc. SmoothWall có thể tự động dò hầu hết các loại card. Bạn sẽ cần phải định rõ IP, hệ thống DNS và các thông số cài đặt Gateway.

Ngoài ra, các thông số khác cũng cần được cấu hình là Web Proxy, ISDN, ADSL và DHCP.

Cuối cùng, bạn cần đặt mật khẩu cho các tài khoản root, quản trị bằng dòng lệnh và tài khoản quản trị qua giao diện web.

Mặc dù SWE đã có thể hoạt động trơn tru với tất cả các tính năng của ứng dụng, nhưng bạn còn có thể khám phá thêm những khả năng tiềm ẩn của nó thông qua một trang cấu hình bằng giao diện Web.

-Truy cập vào trang web của smoothwall <http://smoothwallgreenaddress:441/> và nhập mật khẩu trước đó đã cấu hình

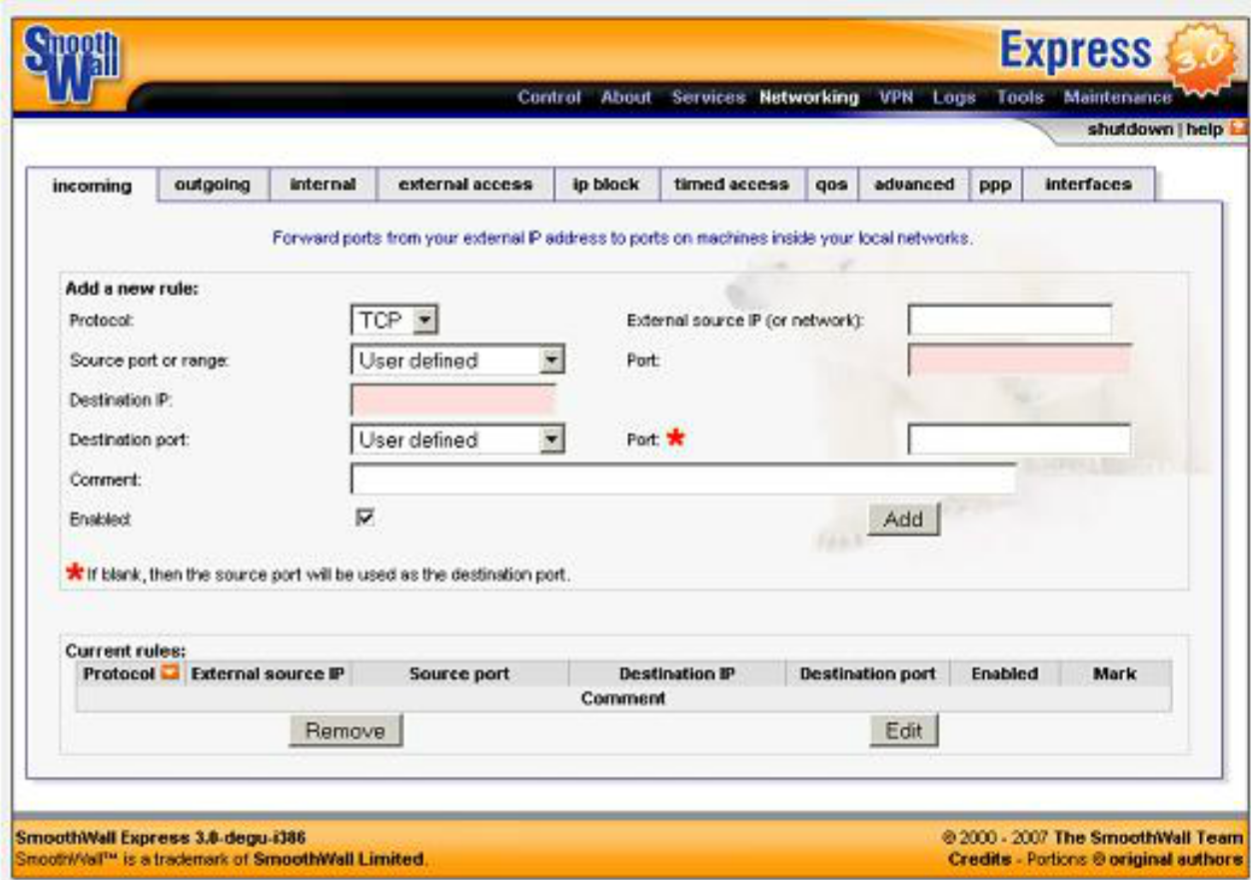


**-**  SmoothWall hỗ trợ hàng loạt tính năng, trong đó có: Proxy Servers, IDS, Logging, Traffic Graphs, DHCP, VPN, Dynamic DNS, Port Forwarding, Server Health and Access Control.

SWE cũng hỗ trợ bạn sao lưu hoặc phục hồi các thông số cấu hình trước đó. Một khi những hệ thống PC cũ gặp trục trặc, bạn có thể phục hồi một cách dễ dàng những thông số, cài đặt cũ.

**Một số cài đặt thông dụng trên Smoothwall:**

**a, Sử dụng Web Proxy**



**b, Cấu hình Im Proxy**



**c, Hiển thị Ip và ping và traceroute**



