

# **Tài liệu quản trị FIREWALL BUILDER**

1	Chỉ dẫn .....	4
1.1	Chỉ dẫn Firewall Builder.....	4
1.2	Tổng quan về các đặc điểm của Firewall Builder.....	4
2	Các gói cài đặt .....	5
3	Giao diện đồ họa của Firewall Builder - GUI.....	6
3.1	Cửa sổ chính.....	6
3.2	Các tùy chọn GUI.....	7
3.2.1	Phần chung/Các đường dẫn (General/Paths).....	7
3.2.2	Phần mạng (Network).....	7
3.2.3	Giao diện người dùng (GUI).....	8
3.2.4	GUI/Object Tooltips.....	8
3.2.5	GUI/Behavior.....	8
3.2.6	GUI/Tree View.....	8
4	Cây đối tượng.....	10
4.1	Cấu trúc cây chuẩn.....	10
4.2	Tạo các đối tượng. ....	11
4.3	Chỉ dẫn và sắp xếp đối tượng.....	12
5	Làm việc với các đối tượng.....	14
5.1	Các thuộc tính chung.....	14
5.2	Đối tượng Host.....	14
5.2.1	Tạo các đối tượng Host.....	15
5.2.2	Sắp xếp một đối tượng mới.....	16
5.3	Interface của Host.....	18
5.4	Đối tượng Address.....	20
5.5	Đối tượng Physical Address.....	21
5.6	Đối tượng Network.....	23
5.7	Đối tượng Address Range. ....	24
5.8	Nhóm (Group) của các đối tượng.....	24
5.9	Đối tượng Firewall.....	25
6	Khám phá mạng: Cách để tạo một đối tượng nhanh.....	30
6.1	Đọc file /etc/hosts.....	31
6.2	Nhập DNS zone.....	32
6.3	Khám phá mạng .....	35
7	Làm việc với các dịch vụ .....	38
7.1	Dịch vụ IP.....	38
7.2	Dịch vụ ICMP .....	39
7.3	Dịch vụ TCP.....	40
7.4	Dịch vụ UDP .....	43
7.5	Dịch vụ Tùy biến .....	44
8	Chính sách Firewall .....	46
8.1	Chính sách và luật.....	46
8.1.1	Hành động.....	47
8.1.2	Định hướng.....	48
8.1.3	Global Firewall Policy .....	48

8.1.4 Interface Policy .....	49
8.2 Network Address Translation Rules .....	49
8.2.1 Luật NAT cơ bản.....	49
8.2.2 Chuyển đổi địa chỉ nguồn.....	50
8.3 Sửa chính sách firewall và luật NAT .....	52
8.3.1 Thêm và gỡ bỏ luật firewall.....	52
8.3.2 Thêm, bớt và sửa các đối tượng trong chính sách và luật NAT .....	53
8.3.3 Thay đổi hành động của luật .....	53
8.3.4 Thay đổi hướng của luật.....	54
8.3.5 Thay đổi tùy chọn và ghi nhật ký.....	54
8.4 Hỗ trợ cho các thành phần luật và đặc tính của các loại Firewall .....	55
8.5 Sử dụng đối tượng với đa địa chỉ trong chính sách và luật NAT .....	55
9 Các ví dụ về luật chính sách.....	56
9.1 Mở một dịch vụ trong khi khóa hết mọi thứ còn lại.....	56
9.2 Những đối tượng có thể đối lẫn nhau và những đối tượng không thể đối lẫn.....	56
9.3 Sử dụng các nhóm.....	56
9.4 Những dịch vụ chạy trong firewall.....	56
9.5 Khóa các kiểu gói không mong muốn.....	56
9.6 Luật antispoofing.....	57
9.7 Bảo vệ local host.....	58
9.8 Sử dụng hành động ‘Reject’ để khóa một giao thức nào đó.....	58
9.9 Sử dụng phủ định trong các luật chính sách.....	58
10 Các ví dụ về luật NAT.....	58
10.1 Cung cấp kết nối Internet cho các máy trạm ẩn đằng sau firewall.....	58
10.2 Server ẩn sau firewall sử dụng địa chỉ private.....	60
10.3 Server ẩn sau firewall sử dụng địa chỉ ảo để truy cập.....	60
10.4 Server ẩn sau firewall với port mapping.....	60
10.5 DNAT trên cùng mạng.....	60
10.6 Các luật không NAT.....	61
10.7 Lái traffic.....	61
11 Một số thao tác thường dùng.....	61
11.1 Thêm một đối tượng vào chính sách hiện tại.....	61
11.1.1 Thêm 1 host / 1 server (1 địa chỉ).....	61
11.1.2 Thêm một dải địa chỉ / một dải mạng mới.....	65
11.1.3 Thêm một dịch vụ mới.....	66
11.2 Thêm đối tượng vào luật hiện tại.....	68
11.2.1 Thêm một cổng dịch vụ vào nhóm dịch vụ sẵn có (ví dụ Internal Services).....	68

# 1 Chỉ dẫn

## 1.1 Chỉ dẫn Firewall Builder

Một trong những việc quan trọng nhất khi cài đặt và cấu hình một firewall là phải xây dựng được chính sách rõ ràng và chuẩn xác cho firewall đó. Firewall Builder là một công cụ có thể giúp bạn quản lý chính sách an ninh của firewall chính xác và hiệu quả mà không cần phải học về giao diện dòng lệnh để điều khiển mà một vài Firewall thương mại vẫn phải làm.

Bạn không phải nghĩ về những số cổng khó hiểu, giao diện firewall và các lựa chọn các luật thuộc về interface nào.

Thay vì đó bạn tạo ra một tập hợp các đối tượng mô tả firewall của bạn, máy chủ, phân mạng con, và bạn chỉ cần kéo và thả các đối tượng là thành các luật.

Bạn có thể sử dụng một số lượng lớn các đối tượng chuẩn được định nghĩa sẵn, mô tả nhiều giao thức và dịch vụ chuẩn. Ngay sau khi chính sách được tạo trên giao diện đồ họa quản lý (GUI), bạn có thể biên dịch nó và cài nó lên firewall của bạn.

## 1.2 Tổng quan về các đặc điểm của Firewall Builder.

Hơn một trăm đối tượng được định nghĩa trước cho các giao thức và dịch vụ phổ dụng. Khả năng tự tạo các đối tượng theo giao thức IP, ICMP, TCP, UDP hoặc các dịch vụ ứng dụng khác.

Khả năng tự tạo các đối tượng theo các hosts, networks và dải địa chỉ IP.

Có đầy đủ tính năng và công cụ giúp bạn thực hiện các chính sách firewall và thi hành các chính sách chuẩn cho các mạng chuẩn mà sau đó vẫn có thể mở rộng cũng như chỉnh sửa lại bằng tay.

Công cụ khám phá mạng tự động tạo nhiều đối tượng.

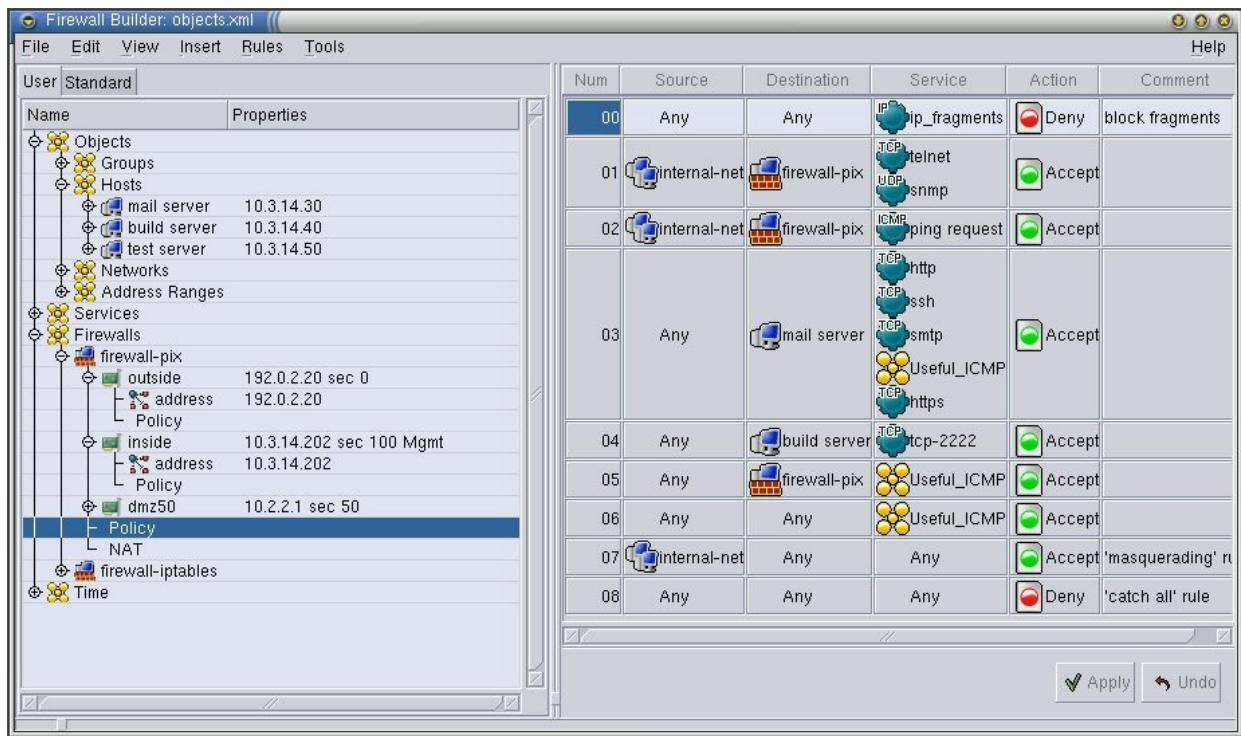
Từ định hướng đối tượng đến quản lý chính sách: bất cứ thay đổi tạo một đối tượng ngay lập tức nhận được phản hồi trong tất cả các luật chính sách của các firewall sử dụng đối tượng đó.

Khả năng chuyển chính sách thành một file cấu hình hoặc một script rồi cài nó lên một firewall chỉ với vài cái click chuột.

Giao diện đồ họa thuận tiện hỗ trợ vận hành cắt dán cho các chuỗi text và các đối tượng mạng và cho phép soạn thảo chính sách bằng cách kéo và thả.

Hỗ trợ một vài nền tảng firewall bao gồm Cisco PIX và Open Source như firewall iptables, ipfilter và pf.

Khả năng in ra một đối tượng riêng lẻ, một chính sách firewall hoặc xuất nó ra một file text hay file html.



**Hình 1-1. Ví dụ về chính sách của firewall**

## 2 Các gói cài đặt

Firewall Builder là một dự án mã nguồn mở. Mã nguồn cho thư viện API, GUI và các chính sách chính sách cho iptables, ipfilter và pf (packet filter) có thể download được từ trang web <http://www.fwbuilder.org>. Firewall Builder cho PIX là sản phẩm thương mại có licensed được cung cấp dưới dạng một gói nhĩ phân.

Có thể xem hướng dẫn cài đặt Firewall Builder trực tuyến tại trang web: <http://www.fwbuilder.org/Documents/Builder.html>, cũng như các tài liệu hướng dẫn xây dựng Firewall Builder từ mã nguồn. Firewall Builder có thể được dịch và làm việc với những hệ điều hành sau:

- Debian Linux
- Mandrake Linux
- RedHat Linux
- SuSE Linux
- FreeBSD
- Mac OS X
- Solaris

Tài liệu tại <http://www.fwbuilder.org/Documents/Builder.html> luôn được cập nhật thông tin về những phiên bản mới và những hệ điều hành đi kèm.

Firewall Builder có một vài gói cài như sau:

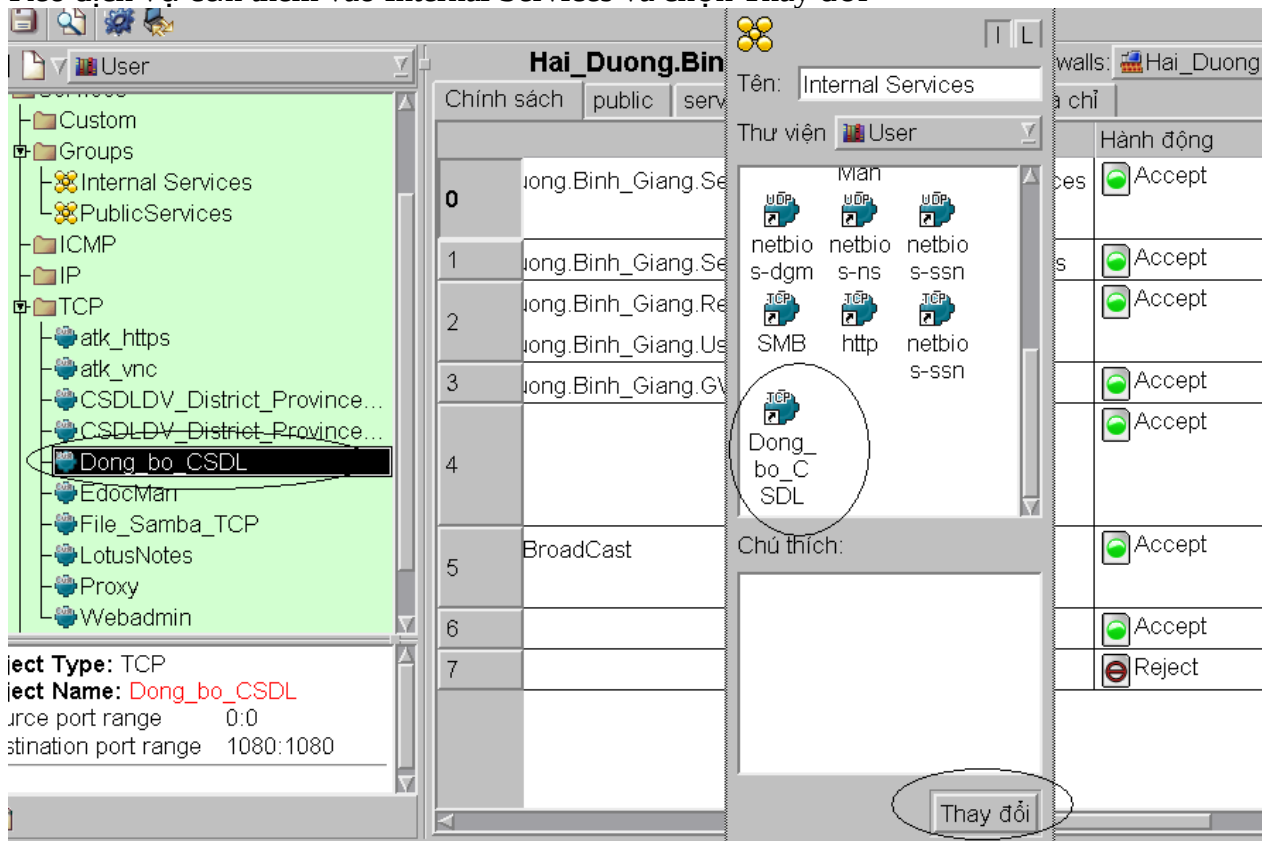
Thư viện API của Firewall Builder: gói libfwbuilder

Giao diện đồ họa của Firewall Builder: gói fwbuilder

Các phần của giao diện đồ họa và các trình biên dịch chính sách cho iptables: fwbuilder-ipt

Các phần của giao diện đồ họa và các trình biên dịch chính sách cho ipfilter: fwbuilder-ipf

Kéo dịch vụ cần thêm vào Internal Services và chọn Thay đổi



Dịch lại luật vào khởi động lại tường lửa

