Masquerading Made Simple HOWTO

Tác giả:

	John Tapsell	<tapselj0@cs.man.ac.uk>
	Thomas Spellman	<thomasNO@SPAMresonancePLEASE.org>
	Matthias Grimm	<DeadBull@gmx.net>
Biên dịch:	**Nguyễn Hồng Thái**	<nhthai2005@gmail.com>

Nội dung:

1. Giới thiệu:
2. Tóm tắt:
3. Những điều cần thiết sâu hơn đối với version
4. Các chỉ dẫn sau khi cài đặt:

1. Giới thiệu:

Masquerading cho phép người dùng từ mạng LAN truy cập ra bên ngoài internet

---

2. Tóm tắt:

Giả sử:

Card nối ra internet là eth0 với địa chỉ IP là 123.12.23.43
Card nối với mạng LAN bên trong là eth1

```
$> modprobe ipt_MASQUERADE # Gọi module để hỗ trợ masquerade
$> iptables -F; iptables -t nat -F; iptables -t mangle -F
$> iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 123.12.23.43
$> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Đối với việc kết nối dial-up:

```
$> modprobe ipt_MASQUERADE #
$> iptables -F; iptables -t nat -F; iptables -t mangle -F
$> iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
$> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Thực hiện bảo mật nó:

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$> iptables -A INPUT -m state --state NEW -i ! eth0 -j ACCEPT
$> iptables -P INPUT DROP   #chỉ có 2 điều kiện đầu là cho qua
$> iptables -A FORWARD -i eth0 -o eth0 -j REJECT
```

Đối với việc kết nối dial-up:(với eth0 là card mạng nối với LAN bên trong):

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$> iptables -A INPUT -m state --state NEW -i ! ppp0 -j ACCEPT
$> iptables -P INPUT DROP   #only if the first two are succesful
$> iptables -A FORWARD -i ppp0 -o ppp0 -j REJECT
```

Cho hiện thị các luật mà iptables đã thiết lập: "**iptables -t nat -L**"

---

3. Những điều cần thiết sâu hơn đối với version

Biên dịch với kernel: (dùng kernel 2.4 trở lên)
Bạn cần hỗ trợ dưới đây trong kernel:

- Những options mạng như:
  - Lọc gói mạng (CONFIG_NETFILTER)
- Những option mạng để cấu hình Netfilter:

- Thực hiện kết nối: (CONFIG_IP_NF_CONNTRACK)
- Hỗi trợ giao thức FTP (CONFIG_IP_NF_FTP)
- Hỗ trợ iptables (CONFIG_IP_NF_IPTABLES)
- Hỗi trợ kiểm tra trạng thái kết nối (CONFIG_IP_NF_MATCH_STATE)
- Lọc gói: (CONFIG_IP_NF_FILTER)
  - Hỗ trợ REJECT target: (CONFIG_IP_NF_TARGET_REJECT)
- NAT đầy đủ: (CONFIG_IP_NF_NAT)
  - Hỗ trợ MASQUERADE target (CONFIG_IP_NF_TARGET_MASQUERADE)
  - Hỗ trợ REDIRECT target (CONFIG_IP_NF_TARGET_REDIRECT)
- Packet mangling (CONFIG_IP_NF_MANGLE)
- Hỗi trợ LOG target (CONFIG_IP_NF_TARGET_LOG)

Ban đầu, nếu những modules iptables và masq không được biên dịch vào kernel và không được cài đặt, nhưng vẫn tồn tại dưới dạng các module, chúng ta cần cài thêm chúng. Nếu bạn gọi ipt_MASQUERADE tức là nó sẽ tải lên load ip_tables, ip_conntrack and iptable_nat.

```
$> modprobe ipt_MASQERADE
```

Bây giờ, hoặc mạng intranet của bạn cỡ lớn hoặc bạn muốn thử thực hiện với 2 hoặc 3 máy tới mạng internet, điều đó không khác nhau cho lắm.

Bây giờ, ta sẽ xóa các luật mà iptables hiện đang có:

```
$> iptables -F; iptables -t nat -F; iptables -t mangle –F
```

Nếu bạn bị lỗi nói rằng không tìm thấy iptatables, thì bạn hãy tìm nó và cài thêm. Nếu nó nói rằng không có bảng 'nat', thì hãy biên dịch kernel lại với hỗ trợ nat. Nếu nó bảo rằng không có 'mangle', đừng lo lắng về nó, nó không cần thiết cho việc MASQUERADING của mình đâu. Nếu nó bảo rằng iptables không tương thích với kernel của bạn thì hãy tìm kernel 2.4 trở lên và biên dịch nó với hỗ trợ iptables.

Sau đó, nếu bạn có một địa chỉ ip tĩnh (tức là card mạng không dùng DHCP dịch vụ cấp ip động)

```
$> iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 123.12.23.43
```

Còn nếu là ip động (tức là một modem) thì bạn phải làm như sau:

```
$> iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Khi mà kernel bảo là 'Okey' thì bạn sẽ thực hiện cho các các có thể đi qua giữa 2 card mạng (forwarding packets):

```
$> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Một lần nữa, bạn hãy kiểm kiểm tra tất cả các công việc này, chỉ cho phép masquerading từ mạng nội bộ mà không muốn cho phép những người trên internet làm điều gì. Thì trước hết, cho phép bất kỳ kết nối nào tồn tại hoặc có mối liên hệ (chẳng hạn như kết nối ftp server sẽ trả về bạn):

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Nếu điều này bị một lỗi nào đó, thì sau đó bạn sẽ không kiểm tra được kết nối và như vậy bạn phải mắc công biên dịch lại kernel. Sau đó, bạn cho phép các kết nối mới chỉ từ mạng intranet của bạn (tức mạng cục bộ). Bằng cách thay ppp0 vào eth0 hoặc là một thiết bị kết nối đến mạng bên ngoài.

```
$> iptables -A INPUT -m state --state NEW -i ! ppp0 -j ACCEPT
```

Và bây giờ ta thực hiện từ chối tất cả mọi thứ:

```
$> iptables -P INPUT DROP   #chỉ thực hiện khi 2 luật trên thành công
```

Nếu hoặc một trong 2 luật ban đâu bị lỗi, thì sau đó ta thực hiện luật cuối cùng là thực hiện mặc định là cho phép "**iptables -P INPUT ACCEPT**".

---

4. Các chỉ dẫn sau khi cài đặt:

Và nó có thể làm việc ngày bây giờ. Nhưng đừng quên là:

- Cài đặt tất cả clients trong mạng cục bộ trỏ tới địa chỉ IP nội bộ Linux như một gateway. Trong windows ta click chuột phải vào neighbourhood của mạng, chọn properties, chọn gateway sau đó đổi địa chỉ gateway của nó thành địa chỉ của máy Linux (máy dùng làm gateway).
- Cài đặt tất cả các clients để sử dụng được proxy HTTP của ISP nếu chúng có một, thì sử dụng một proxy trong suốt (transparent proxy) (Chú ý – Tôi có nghe nói những bài báo các về thực hiện proxy trong suốt thì rất chậm trong những mạng lớn), hoặc chạy squid trên máy dùng làm gateway linux của bạn. (Điều này là một chọn lựa, nhưng có thể tham khảo từ những mạng cỡ lớn)
- Phải đảm bảo chỉ ra được một DNS khi cài đặt cho các clients của bạn. Hoặc là bạn sẽ mắc phải các lỗi trên clients nó nói rằng 'cannot resolve address' … Nếu DNS thường làm việc nhưng không chịu làm việc nữa sau khi cài đặt masquerading, thì nguyên nhân là do nhà cung cấp dịch vụ internet (ISP) hoặc là DHCP Server không trả về cho bạn những gì mà địa chỉ DNS có.
- Bây giờ, bạn nên bắt đầu thực hiện bảo mật nó! Trước tiên tắt forwarding trong trường hợp tổng quát:"**iptables -P FORWARD DROP**", và sau đó học cáh sử dụng iptables và `/etc/hosts.allow` và `/etc/hosts.deny` để bảo mật hệ thống của bạn. Chú ý - Đừng thử luật iptables hiện có đến khi bạn thực hiện masquerading. Bạn phải cho phép mỗi gói thông qua những gì mà bạn muốn nếu bạn sẽ cài đặt luật cuối cùng để từ chối thì thực hiện "**iptables -P FORWARD ACCEPT**")

  Cho phép thông qua bất kỳ dịch vụ nào mà bạn muốn internet để xem. Ví dụ : cho phép truy cập web server của bạn thì thực hiện như sau:

```
$> iptables -A INPUT --protocol tcp --dport 80 -j ACCEPT
$> iptables -A INPUT --protocol tcp --dport 443 -j ACCEPT
```

  Để cho phép đi đúng port đến 113:

```
$> iptables -A INPUT --protocol tcp --dport 113 -j ACCEPT
```

  Để kiểm tra nó:
  Thử kết nối từ một client tới web sử dụng một IP. IP của Google là 216.239.33.100 và bạn có thể lấy được một reply từ nó tức là "**ping 216.239.33.100**" "**lynx 216.239.33.100**".
- Thử một kết nối ra ngoài bằng tên chẳng hạn"**ping google.com**" "**lynx google.com**" hoặc từ Internet Explorer / netscape. Trong đó, eth0 là card internet bên ngoài còn 123.12.23.43 là địa chỉ bên ngoài của máy.