

Re: iptables using MASQUERADE and static IPs

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-05/0493.html>

From: gary (nospam_at_nospam.org)

Date: 05/29/03

Date: Thu, 29 May 2003 05:16:06 GMT

Hi Mike,

I used those commands to generate:

```
# Generated by iptables-save v1.2.6a on Mon Mar 10 17:49:15 2003
*nat
:PREROUTING ACCEPT [13115:2159862]
:POSTROUTING ACCEPT [190:39712]
:OUTPUT ACCEPT [537:91219]
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Mon Mar 10 17:49:15 2003
# Generated by iptables-save v1.2.6a on Mon Mar 10 17:49:15 2003
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [96:9625]
-A INPUT -s ! 192.168.1.0/255.255.255.0 -i eth1 -j LOG
-A INPUT -s ! 192.168.1.0/255.255.255.0 -i eth1 -j DROP
-A INPUT -s 192.168.1.0/255.255.255.0 -i ! eth1 -j DROP
-A INPUT -s 127.0.0.0/255.0.0.0 -i ! lo -j DROP
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i eth0 -p ! icmp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.1.0/255.255.255.0 -i eth1 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -j DROP
COMMIT
# Completed on Mon Mar 10 17:49:15 2003
```

mikepb@hoplite.org wrote:

> *In comp.security.firewalls G. Artim <gartim@attbi.com> wrote:*

>

>>Hi,

>

comp.security.misc: Re: iptables using MASQUERADE and static IPs

```
>
>>I'm currently just using my Redhat 9.x box as a router/firewall with
>>Masquerading turned on. I have 2 interface (eth0/eth1). My iptables
>>looks like so:
>
>
>>echo 0 > /proc/sys/net/ipv4/ip_forward
>># flush rules
>>/sbin/iptables -F INPUT
>>/sbin/iptables -F OUTPUT
>>/sbin/iptables -F FORWARD
>># Set default policies
>>/sbin/iptables -P INPUT DROP
>>/sbin/iptables -P OUTPUT ACCEPT
>>/sbin/iptables -P FORWARD ACCEPT
>># IP spoofing
>>/sbin/iptables -A INPUT -j LOG -i eth1 \! -s 192.168.1.0/24
>>/sbin/iptables -A INPUT -j DROP -i eth1 \! -s 192.168.1.0/24
>># IP Spoofing: deny address from outside with our addresses
>>/sbin/iptables -A INPUT -j DROP \! -i eth1 -s 192.168.1.0/24
>>/sbin/iptables -A INPUT -j DROP -i \! lo -s 127.0.0.0/255.0.0.0
>>/sbin/iptables -A INPUT -j ACCEPT -i lo
>># setup for ssh and http
>>/sbin/iptables -A INPUT -j ACCEPT -p tcp -i eth0 --dport ssh
>>/sbin/iptables -A INPUT -j ACCEPT -p tcp -i eth0 --dport http
>>#
>>/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -i eth0 -p
>>\! icmp -j ACCEPT
>># allow all local connetions from eth1
>>/sbin/iptables -A INPUT -j ACCEPT -p all -i eth1 -s 192.168.1.0/24
>># setup Masquerqading
>>/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
>># DROP any internet/new connections
>>/sbin/iptables -A INPUT -m state --state NEW -i eth0 -j DROP
>># turn on ip forwarding
>>echo 1 > /proc/sys/net/ipv4/ip_forward
>
>
>>My question: If I wanted to add static IPs for a machine on my lan what
>>would be the best/clearest implementation?
>
>
>>My goal: To have 2 machines with static IPs, either mapped to reserved
>> address like 192.168.1.1 and 192.168.1.2 or just have the static IPs go
>>to the static IPs thru the router, and have a bank of Nat address for
>>none server like machines (windoze). Will I need a 3rd nic if I do
>>static ip to static ip (ie a real ip addresses like 12.110.5.25 to ditto)?
>
>
>>Thanks for any suggestions/help,
>>Gary
```

```
>
>
> Is the above a script or the /etc/sysconfig/iptables file?
>
> my /etc/sysconfig/iptables file looks like this:
>
> # Generated by iptables-save v1.2.5 on Mon May 19 20:24:16 2003
> *mangle
> :PREROUTING ACCEPT [22016807:4205582825]
> :INPUT ACCEPT [9749925:2007269194]
> :FORWARD ACCEPT [12263504:2197747784]
> :OUTPUT ACCEPT [10500728:8717240927]
> :POSTROUTING ACCEPT [22786272:10920059103]
> COMMIT
> # Completed on Mon May 19 20:24:16 2003
> # Generated by iptables-save v1.2.5 on Mon May 19 20:24:16 2003
> *nat
> :PREROUTING ACCEPT [348141:21775482]
> :POSTROUTING ACCEPT [30890:2825689]
> :OUTPUT ACCEPT [140201:11849687]
> -A PREROUTING -d 24.242.137.28 -i eth1 -p tcp -m tcp --dport 135:139 -j DROP
> -A PREROUTING -d 24.242.137.29 -i eth1 -p tcp -m tcp --dport 135:139 -j DROP
> -A PREROUTING -d 24.242.137.28 -i eth1 -p udp -m udp --dport 135:139 -j DROP
> -A PREROUTING -d 24.242.137.29 -i eth1 -p udp -m udp --dport 135:139 -j DROP
> -A POSTROUTING -o eth1 -j MASQUERADE
> COMMIT
> # Completed on Mon May 19 20:24:16 2003
> # Generated by iptables-save v1.2.5 on Mon May 19 20:24:16 2003
> *filter
> :INPUT ACCEPT [5292:481501]
> :FORWARD ACCEPT [0:0]
> :OUTPUT ACCEPT [5103:508271]
> :advdrop - [0:0]
> :adverts - [0:0]
> :blkdrop - [0:0]
> :blocked - [0:0]
> :ext_in - [0:0]
> :ext_out - [0:0]
> :icmpmsg - [0:0]
> :localonly - [0:0]
> :logaccept - [0:0]
> :logdrop - [0:0]
> :rfc1918 - [0:0]
> :rfcdrop - [0:0]
> :webblock - [0:0]
> -A INPUT -i lo -j ACCEPT
> -A INPUT -i eth0 -j ACCEPT
> -A INPUT -d 24.242.137.26 -i eth1 -j ext_in
> -A INPUT -p icmp -j icmpmsg
> -A INPUT -p tcp -m tcp --dport 137:139 -j DROP
> -A INPUT -p udp -m udp --dport 137:139 -j DROP
```

comp.security.misc: Re: iptables using MASQUERADE and static IPs

> *-A INPUT -j logdrop*
>
> *The rest is snipped. Notice this file is mostly comments and argument*
> *strings to iptables, not the iptables command itself.*
>
> --
> *Michael P. Brininstool mikepb@hoplite.org*
> *"The American Republic will endure, until politicians realize they can*
> *bribe the people with their own money." -- Alexis de Tocqueville*