

Outgoing DNAT, incoming SNAT?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-11/0753.html

myopius_at_gmail.com

Date: 11/19/05

Date: 18 Nov 2005 17:06:43 -0800

I know it's possible to perform SNAT on outgoing packets and DNAT on incoming ones, for purposes of IP masquerading, but is it possible to perform DNAT on outgoing packets and SNAT on incoming packets that match specific IP addresses, or specific IP addresses and ports? If so, what do I need to do that, and how do I do it?

I have a client program which doesn't allow me to alter the IP/ports to which it connects, and seeing as I can't compile from source, this would allow me to connect to a different IP which is accessible and that in turn connects to the server through port forwarding.

Using iptables in Linux I can accomplish this easily with rules resembling:

```
iptables -t nat -A OUTPUT -p tcp -o eth0 -d 64.233.161.99 -dport 80 -j  
DNAT --to-destination 216.155.200.155  
iptables -t nat -A POSTROUTING -p tcp -s 216.155.200.155 -sport 80 -j  
SNAT --to-source 64.233.161.99
```

which is what I would type to make it so that whenever I tried to connect out to Google's web server, I would be connected to Altavista instead. (This is just an example, my client isn't a web client.)

Right now my connection to the internet is through the LAN, behind a router. I'm assigned an IP address over DHCP.

Thanks,
Matt