

troubles defining firewall policies

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2003-07/0750.html>

From: Strider Alex Hunter (*stwolf_at_andinanet.net*)

Date: 07/26/03

To: <redhat-list@redhat.com>

Date: Sat, 26 Jul 2003 00:58:42 -0500

Hello there,

First, thank you for the answers of my previous post. For any strange reason my modem won't connect using the v.90 protocol nor i'll reach faster rates than 31,200 bps (accurate connection string: CONNECT 31200 BPS/LAPM/V34/V42bis) but i believe that i have to play with the modem strings harder.. the problem is that i've set the correct init strings to connect @ 46,666 + bps and using V.90 according to the manufacturer's manual and i can't achieve that under linux, something that i could do using Win 2K / XP. For the one who asked about the phone jack and/or line.. Yes, i'm using the same RJ-11 jack and phone line. In any case, thank you for your answers, now here is my new question:

i've got problems trying to configure my linux as a firewall via IPCHAINS and i don't know why everything gets blocked when i am just restricting high ports (7000 - 65535).

I use RH 7.3 and my eth0 interfase is part of the class C network 192.168.1.0 The IP of the linux machine is 192.168.1.4 and we share a 56K connection via modem (ppp0) using squid and some IP masquerade rules to allow external POP3 and SMTP connections. All of the other computers use the linux machine as their gateways so all the network traffic is held by it.

Let's suppose that i want:

- 1) Grant incoming connections (input chains) for every IP of my network to access every service of my linux machine, no exceptions.
- 2) Filter out incoming connections from foreign addresses that try to use ports equal or higher than 7000. (i do not use the port 8080 for HTTP / Proxy purposes)
- 3) Masquerade Ips of my network that want to use the ports 110 (POP3), 21 (FTP) and 25 (SMTP)
- 4) allow outgoing traffic from Ips of my network (from any port to any port)
- 5) restrict outgoing traffic from foreign addresses wanting to use ports > 7000

RedHat: troubles defining firewall policies

According to these rules, i've created the following rules:

```
Ipchains -P input REJECT
Ipchains -P output REJECT
Ipchains -A input -s 192.168.1.0/24 -j ACCEPT
Ipchains -A input -s ! 192.168.1.0/24 --destination-port 0:7000 -p tcp
-j ACCEPT
Ipchains -A input -s ! 192.168.1.0/24 --destination-port 0:7000 -p udp
-j ACCEPT
Ipchains -A input -s ! 192.168.1.0/24 -p icmp -j ACCEPT
Ipchains -A forward -s 192.168.1.0/24 --destination-port 110 -j MASQ
Ipchains -A forward -s 192.168.1.0/24 --destination-port 21 -j MASQ
Ipchains -A forward -s 192.168.1.0/24 --destination-port 25 -j MASQ
Ipchains -A output -s 192.168.1.0/24 -j ACCEPT
Ipchains -A output -s ! 192.168.1.0/24 -p tcp --destination-port 0:7000
-j ACCEPT
Ipchains -A output -s ! 192.168.1.0/24 -p udp --destination-port 0:7000
-j ACCEPT
Ipchains -A output -s ! 192.168.1.0/24 -p icmp -j ACCEPT
```

When i try the above settings, everything gets blocked... External SMTP, DNS queries, MS Messenger connections, even web surfing (having squid as http proxy of course) why? Are my firewall policies bad conceived? Have i used the wrong reasoning to create them? Are they correct but the physical implementation is wrong? Please help.

I also tried the other way, ACCEPTing every input and output connection but using 7001:65535 as --destination-port and -j REJECT as the jump policy but i got mixed results... I could use HTTP, check external POP3 accounts and send messages using the ISP's external SMTP server but DNS queries were still blocked... MSN Messenger uses low ports, above 1000 but below 5000, i am allowing ingoing and outgoing traffic for foreign connections and it simply won't connect, why? Same happens with yahoo messenger.. I use squid as http proxy for these instant messaging programs... Am i probably checking which ports outgoing connections are trying to use?

Is there any application out there (graphical or not) that could accurately tell me FOR SURE which servers:ports are trying to connect to which Ips:ports of my network? (and the other way too, which Ips:ports from my network want access either to my linux PC's server:ports or any foreign address:ports) Netstat is kinda basic and is not as accurate as i want it to be, unless i am using it the wrong way.

Thank you in advance,

Paul D Fabre.

--

redhat-list mailing list
unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>