Ordinador firewall-router de la xarxa interna (2009)

Aquesta pàgina conté la descripció del firewall-router instal·lat l'any 2009, i, excepte el preàmbul, el contingut és còpia del que hi havia a router_firewall amb el títol original: **Encaminador/Tallafocs (Router/Firewall)**

El motiu de copiar aquesta pàgina aquí, quan estic a punt de substituir l'ordinador, és que vull tenir un registre històric dels canvis fets a la configuració de la xarxa del Servei de RMN.

Preàmbul

A finals de 2008 vàrem decidir substituir el firewall-router original, que alhora funcionava també com a servidor de dades, per dos ordinadors: un funcionaria exclusivament com a firewall-router de la xarxa interna, i l'altre faria de servidor del servei i allotjaria els serveis d'Internet del SeRMN.

L'ordinador substituït l'any 2009 era un Tulip Vision Line amb un processador Intel Pentium a 166 MHz que havíem fet servir com a servidor de dades des de 2006. Pel nou firewall-router varem decidir aprofitar un dels ordinadors Hewlett Packard NetServer E60 500 que havien arribat amb els espectròmetres DPX-250 i que havíem decidit substituir per un de més potent. El NetServer E60 500 tenia un processador Intel Pentium III a 500 MHz que ens va semblar tenia unes prestacions suficients per funcionar com a tallafocs.

Pel servidor vàrem optar per comprar un HP Proliant ML110 G5 i instal·lar-ho a la xarxa interna del servei, protegit pel tallafocs. Al nou ordinador es va destinar principalment a funcionar com a servidor de dades (ProFTPD), portal de reserves (Bumblebee), i blog del servei (WordPress).

Descripció

L'ordinador que s'encarrega actualment [NOTA: estem a l'any 2009] de connectar la xarxa interna del SeRMN amb la xarxa de la UAB ja és força obsolet i cada dia està més a prop del seu final. A sobre, no només fa d'encaminador (*router*) entre ambdues xarxes, sinó que també fa de servidor de dades i gestiona l'accés restringit als espectròmetres, alhora que incorpora un senzill tallafocs (*firewall*). Per evitar haver de córrer el dia que finalment peti, he decidit substituir-lo per dos ordinadors, un dedicat específicament a fer d'encaminador/tallafocs i un altre que funcionarà com a servidor web, wiki, etcétera, alhora que també donarà accés a les dades als espectròmetres mentre no es posa en marxa un servidor NAS dedicat.

Com a tallafocs tinc previst fer servir un dels ordinadors Hewlett Packard NetServer E60 500 substituïts als espectròmetres DPX-250, i deixar el segon com a reserva i font de peces de recanvi. L'ordinador que es faci servir caldrà actualitzar-lo:

- ampliar la memòria RAM fins al màxim possible fent servir la memòria de l'ordinador de reserva. Si cal, comprar a Misco mòduls de memòria compatibles.
- ~~doble CPU, fer servir la CPU del segon ordinador~~ m0n0wall no és multiprocessador.
- retirar el lector de disquets. S'ha desconnectat i desactivat a la BIOS, però no s'ha tret.
- retirar el lector de CD/ROM. S'ha desconnectat i desactivat a la BIOS, però no s'ha tret.
- retirar la targeta SCSI
- retirar el disc dur. S'ha tret el disc SCSI i s'ha muntat un disc IDE fins que es pugui substituir per un lector IDE de targetes CF.
- instal·lar una targeta Ethernet amb capacitat 1000 Mbps per la LAN. Per ara no cal, ja ho decidirem en funció del tràfic de xarxa quan es posi en funcionament en condicions reals.
- instal·lar un adaptador *IDE/Targeta CF* i comprar una targeta de 256MB o més,
  - http://www.mioferta.com/catalogo/10323_10333-Adaptador_IDE_a_CFATA_Flash
  - http://www.6deal.com/es/lot-of-5pcs-dual-cf2x-compact-flash-to-ideata-adapterconverter.html
  - http://tenda.initron.com/product_info.php?cPath=462_474&products_id=6393
  - http://tenda.initron.com/product_info.php?cPath=462_473&products_id=1197
- ~~instal·lar una targeta de ports USB~~
- altres millores?

Algunes d'aquestes modificacions no són necessàries per les primeres proves i es poden fer posteriorment, un cop ja estigui en marxa.

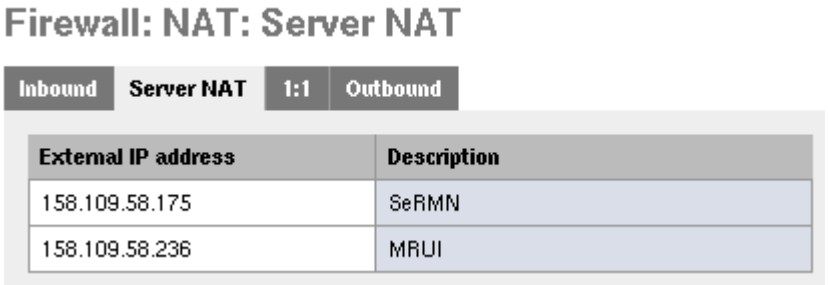
<note tip> M'he de baixar els manuals on-line del NetServer E60 disponibles al website d'Hewlett Packard. </note>

Instal·lació i configuració del M0n0wall

Instal·lació

Configuració

Definir les diferents adreces IP, que hi ha a la WAN.



Enllaços d'interès

- Especificacions i protocols

    - Tallafocs (Firewall)
    - Passarel·la (Gateway)
    - Encaminador (Router)

- Programari
    - m0n0wall
    - M0n0wall
    - pfSense
    - PfSense
    - untangle
    - Untangle

- Recomanacions i articles tècnics
    - Comparació de tallafocs
    - List of Linux router or firewall distributions

- Altres
    - No sé si serviria pel m0n0wall, però ferm is a tool to maintain complex firewalls, without having the trouble to rewrite the complex rules over and over again. ferm allows the entire firewall rule set to be stored in a separate file, and to be loaded with one command. The firewall configuration resembles structured programming-like language, which can contain levels and lists.

Configuració de xarxa dels servidors

El problema

Ahir (2009-01-29) per la tarda em vaig posar a esbrinar perquè les connexions als servidors virtuals de vegades semblen no funcionar i fins i tot arriben a exhaurir el temps de connexió sense respondre. Em va sorprendre veure que `ifconfig -a` no donava cap estadística de tràfic per *eth0* i que `netstat -rn` o `route` mostraven una ruta duplicada. Vaig sospitar que el problema tenia a veure amb això i una cerca al Google ho va confirmar.

A l'enllaç LinuxQuestions.org: Why can I not ping two networks? un usuari plantejava una situació semblant a la nostra. Té dues targetes de xarxa, totes dues amb adreces IP a la mateixa xarxa, *eth0* és *192.168.0.2* i *eth1* és *192.168.0.99*. Quan fa un `ping` a la segona IP, obté una resposta. Quan ho fa a la primera IP, la resposta és *unreachable*, però si indica que faci el ping a través d'*eth0* llavors sí que obté una resposta. El diagnòstic del problema és que té totes dues targetes assignades a la mateixa xarxa, i que de les dues rutes definides, Linux només fa servir la primera ruta vàlida que troba a la taula de rutes. La solució és que faci servir la màscara de xarxa per assignar un rang d'adreces (xarxa) diferent a cada interfície de forma que no hi hagi duplicitat de rutes a la taula de rutes.

Aquest és exactament el nostre cas, *eth0* té assignada la IP `192.168.0.20/255.255.255.0` i *eth1* la IP `192.168.0.21/255.255.255.0`, i la taula de rutes resultant és,

```
$ sudo route -n
Password:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
```

```
Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
default         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
default         192.168.1.1     0.0.0.0         UG    0      0        0 eth1
```

on es pot comprovar la duplicitat de rutes.

La solució

Per resoldre aquest problema, seguint les recomanacions de l'enllaç anterior, he decidit assignar les interfícies a xarxes separades, definint rangs dins de `192.168.0.x`, Per això he fet servir una calculadora d'adreces IP disponible a la Internet.

El resultat és una subxarxa `192.168.0.0/25` assignada a *eth0* amb el rang d'adreces `192.168.0.1-126`

```
Address:   192.168.0.1           11000000.10101000.00000000.0 0000001
Netmask:   255.255.255.128 = 25  11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   192.168.0.0/25        11000000.10101000.00000000.0 0000000 (Class
C)
Broadcast: 192.168.0.127         11000000.10101000.00000000.0 1111111
HostMin:   192.168.0.1           11000000.10101000.00000000.0 0000001
HostMax:   192.168.0.126         11000000.10101000.00000000.0 1111110
Hosts/Net: 126                   (Private Internet)
```

i una subxarxa `192.168.0.128/25` assignada a *eth1* amb el rang d'adreces `192.168.0.129-254`

```
Address:   192.168.0.128         11000000.10101000.00000000.1 0000000
Netmask:   255.255.255.128 = 25  11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   192.168.0.128/25      11000000.10101000.00000000.1 0000000 (Class
C)
Broadcast: 192.168.0.255         11000000.10101000.00000000.1 1111111
HostMin:   192.168.0.129         11000000.10101000.00000000.1 0000001
HostMax:   192.168.0.254         11000000.10101000.00000000.1 1111110
Hosts/Net: 126                   (Private Internet)
```

Això ens permetrà mantenir la configuració `192.168.0.1/24` de la interfície de LAN a l'encaminador,

```
Address:   192.168.0.1           11000000.10101000.00000000 .00000001
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000 .11111111
=>
Network:   192.168.0.0/24        11000000.10101000.00000000 .00000000 (Class
```

```
C)
Broadcast: 192.168.0.255         11000000.10101000.00000000 .11111111
HostMin:   192.168.0.1           11000000.10101000.00000000 .00000001
HostMax:   192.168.0.254         11000000.10101000.00000000 .11111110
Hosts/Net: 254                   (Private Internet)
```

Configuració final de xarxa de l'encaminador

Aquesta és la configuració de la WAN assignada pel servidor de DHCP a la MAC `00:0e:18:c2:16:e2`,

```
MAC:       00:0e:18:c2:16:e2
Hostname:  sermn.uab.es          (sermn.uab.cat)
Address:   158.109.58.175        10011110.01101101.00111010.1010 1111
Netmask:   255.255.255.240 = 28  11111111.11111111.11111111.1111 0000
Wildcard:  0.0.0.15              00000000.00000000.00000000.0000 1111
=>
Network:   158.109.58.160/28     10011110.01101101.00111010.1010 0000 (Class
B)
Broadcast: 158.109.58.175        10011110.01101101.00111010.1010 1111
HostMin:   158.109.58.161        10011110.01101101.00111010.1010 0001
HostMax:   158.109.58.174        10011110.01101101.00111010.1010 1110
Hosts/Net: 14
```

Aquesta MAC té assignada una segona adreça IP que correspon al hostname `oldmrui.uab.cat` (quan es faci el trasllat definitiu des de `sermn02.uab.cat`, el nom es canviarà a `mrui.uab.cat`),

```
MAC:       00:0e:18:c2:16:e2
Hostname:  mrui.uab.es           (mrui.uab.cat)
Address:   158.109.58.236        10011110.01101101.00111010.1110 1100
Netmask:   255.255.255.240 = 28  11111111.11111111.11111111.1111 0000
Wildcard:  0.0.0.15              00000000.00000000.00000000.0000 1111
=>
Network:   158.109.58.224/28     10011110.01101101.00111010.1110 0000 (Class
B)
Broadcast: 158.109.58.239        10011110.01101101.00111010.1110 1111
HostMin:   158.109.58.225        10011110.01101101.00111010.1110 0001
HostMax:   158.109.58.238        10011110.01101101.00111010.1110 1110
Hosts/Net: 14
```

Pel que fa a la LAN, aquesta és la configuració,

```
MAC:       00:50:04:e8:a5:30
Hostname:  sermn.sermn.net
Address:   192.168.1.1           11000000.10101000.00000001 .00000001
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000 .11111111
=>
Network:   192.168.1.0/24        11000000.10101000.00000001 .00000000 (Class
```

```
C)
Broadcast: 192.168.1.255         11000000.10101000.00000001 .11111111
HostMin:   192.168.1.1           11000000.10101000.00000001 .00000001
HostMax:   192.168.1.254         11000000.10101000.00000001 .11111110
Hosts/Net: 254                   (Private Internet)
```

He configurat l'opció *DNS Forwarder Overrides* del m0n0wall de forma que pels ordinadors a la LAN

- el hostname `sermn.uab.cat/es` es correspon amb la IP `192.168.1.2` (sermnserver.sermn.net), i
- el hostname `oldmrui.uab.cat/es` es correspon amb la IP `192.168.1.129` (mruiserver.sermn.net).

Configuració final dels virtual host

L'ordinador on es troben allotjats els servidors virtuals disposa de dues targetes ethernet assignades als servidors `sermnserver.sermn.net` i `mruiserver.sermn.net`.

La configuració de `sermnserver.sermn.net` és la següent,

```
MAC:       00:e0:7d:84:df:07
Hostname:  sermnserver.sermn.net
Address:   192.168.1.2           11000000.10101000.00000001.0 0000010
Netmask:   255.255.255.128 = 25  11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   192.168.1.0/25        11000000.10101000.00000001.0 0000000 (Class
C)
Broadcast: 192.168.1.127         11000000.10101000.00000001.0 1111111
HostMin:   192.168.1.1           11000000.10101000.00000001.0 0000001
HostMax:   192.168.1.126         11000000.10101000.00000001.0 1111110
Hosts/Net: 126                   (Private Internet)
```

i la configuració de `mruiserver.sermn.net` és la següent,

```
MAC:       00:05:1c:0c:06:b1
Hostname:  mruiserver.sermn.net
Address:   192.168.1.129         11000000.10101000.00000001.1 0000001
Netmask:   255.255.255.128 = 25  11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   192.168.1.128/25      11000000.10101000.00000001.1 0000000 (Class
C)
Broadcast: 192.168.1.255         11000000.10101000.00000001.1 1111111
HostMin:   192.168.1.129         11000000.10101000.00000001.1 0000001
```

```
HostMax:   192.168.1.254         11000000.10101000.00000001.1 1111110
Hosts/Net: 126                   (Private Internet)
```

Taula de rutes

Un cop fets aquests canvis, la taula de rutes que resulta és la següent,

```
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.1.0     0.0.0.0         255.255.255.128 U     0      0        0 eth1
192.168.1.128   0.0.0.0         255.255.255.128 U     0      0        0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth1
```

una comanda alternativa és `ip route show`.

Resolució d'adreces IP a partir del hostname

El contingut del fitxer `/etc/hosts` s'ha completat amb les correspondències *hostname*-adreça IP de la xarxa local,

```
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
#
127.0.0.1 localhost localhost.localdomain
#
192.168.1.1 sermn.sermn.net
192.168.1.2 cie-58-175b.sermn.net cie-58-175b sermnserver.sermn.net
sermnserver
192.168.1.129 mruiserver.sermn.net mruiserver
```

I el fitxer `/etc/host.conf` s'ha modificat per indicar que a l'hora de resoldre adreces IP a partir d'un hostname primer s'ha de consultar el fitxer `/etc/hosts` i, si no es resol, el servidor de noms,

```
order hosts,bind
multi on
```

Finalment, aquesta és la configuració

```
# cat /etc/resolv.conf
search uab.es
```

```
nameserver 192.168.1.1
```

Local hostname

Addicionalment, aquests canvis fan que es pugui obtenir el nom del servidor, tan el nom principal i àlies,

```
# hostname -a
cie-58-175b  sermnserver.sermn.net  sermnserver
```

com el *FQDN (Fully Qualified Domain Name),*

```
# hostname -f
cie-58-175b.sermn.net
```

Bibliografia

- Linux Network Administrators Guide
- Linux Advanced Routing & Traffic Control. A must read on *iproute2* the (not so) new Linux routing framework, and the `ip` command that replaces `ifconfig`, `route` and similar old commands.
- ClarkConnect User Guide. It is a server/gateway software solution. Its documentation is quite complete and detailed.

Enllaços

- LinuxQuestions.org: Why can I not ping two networks?
- LinuxQuestions.org: Can't route/ping between networks
- The Perfect Server - Debian Lenny (Debian 5.0) [ISPConfig 2]. For instance, it is mentioned: *“replace allow-hotplug eth0 with auto eth0; otherwise restarting the network doesn't work, and we'd have to reboot the whole system”*.
- The Perfect Server - Debian Lenny (Debian 5.0) [ISPConfig 3]
- Rename Network Interface using Udev in Linux
- Debian Networking for Basic and Advanced Users
- Dual NIC config question.
- t1n1wall As m0n0wall decided to close it's doors, and no further development is planned, I have created a fork.
    - Error trying to mount FreeBSD/UFS partition from FreeNAS A partir de la segona resposta més votada vaig trobar la comanda correcta per muntar el sistema de fitxer de FreeBSD/m0n0wall creat a la targeta de memòria Compact Flash: `mount -t ufs -o ufstype=44bsd /dev/sdb5 /mnt/monowall/`
- SmallWall another m0n0wall followup project.