Guia rápida de Newnat

Guía rápida de Newnat

Christian Conejero > christian@debian−potato.com.ar Versión: 1, Abril 2003

Contenido

1 Introducción

Bienvenido, gentil lector

Está a punto de sumergirse en el fascinante (y a veces horrendo) mundo del NEWNAT (N.A.T. = Network Address Translation), y esto es una guía más o menos precisa para el núcleo 2.4.16 de Linux.

En Linux 2.4.X, se ha introducido una infraestructura para trastear con los paquetes, llamada «netfilter». Hay una capa por encima que proporciona NAT, completamente rescrita con respecto a anteriores núcleos.

Sarge (Testing), pero es totalmente válido para otras versiones de Debian, incluso para otras distribuciones de Linux.

2. ¿Dónde está el sitio Web oficial y la lista?

Sitios oficial:

http://www.netfilter.org (Iptables y Newnat)

La lista oficial de correo de netfilter está en el servidor de listas de Samba: http://lists.samba.org/

3 ¿Que es Network Address Translation?

Normalmente, los paquetes viajan en una red desde su origen (por ejemplo su ordenador) a su destino (como por ejemplo www.kernel.org) a través de varios enlaces diferentes: unos 19 desde donde yo estoy en Australia (esto lo dice Rusty, claro). Ninguno de estos enlaces altera realmente el paquete: simplemente lo envían un paso adelante.

Si uno de estos enlaces hiciera NAT, podría alterar el origen o destino del paquete según pasa a través suyo. Como puede imaginar, ésta no es la función para la que se diseñó el sistema, y por tanto NAT es siempre un tanto enrevesado. Normalmente, el enlace que esté haciendo NAT recordará cómo jugueteó con el paquete, para hacer la acción inversa con el paquete de respuesta, de manera que todo funciona como se esperaba.

3.1 ¿Que es H.323?

El estándar H.323 proporciona la base para la transmisión de voz, datos y vídeo sobre redes no orientadas a conexión y que no ofrecen un grado de calidad del servicio, como son las basadas en IP, de manera tal que las aplicaciones y productos puedan ínter operar, permitiendo la comunicación entre los usuarios sin que éstos se preocupen por la compatibilidad de sus sistemas. La LAN sobre la que los terminales H.323 se comunican puede ser un simple segmento o un anillo, o múltiples segmentos con una topología compleja, lo que puede resultar en un grado variable de rendimiento.

H.323 fija los estándares para la comunicación de voz y vídeo sobre redes de área local, con cualquier protocolo que por su propia naturaleza presentan una gran latencia y no garantizan una determinada calidad del servicio (QoS). Para la conferencia de datos se apoya en la norma T.120, con lo que en conjunto soporta las aplicaciones multimedia. Los terminales y equipos conforme a H.323 pueden tratar voz en tiempo real, datos y vídeo.

El estándar contempla el control de la llamada, gestión de la información y ancho de banda para una comunicación punto a punto y multipunto, dentro de la LAN, así como define interfaces entre la LAN y otras redes externas, como puede ser la RDSI. Es una parte de una serie de especificaciones para videoconferencia sobre distintos tipos de redes, que incluyen desde la H.320 a la H.324, estas dos válidas para RTB (Red Telefónica Básica) y RTC (Red Telefónica Conmutada), respectivamente.

H.323 establece los estándares para la compresión y descompresión de audio y vídeo, asegurando que los equipos de distintos fabricantes se entiendan. Así, los usuarios no se tienen que preocupar de cómo el equipo receptor actúe, siempre y cuando cumpla este estándar. La gestión del ancho de banda disponible para evitar que la LAN se colapse con la comunicación de audio y vídeo, por ejemplo, limitando el número de conexiones simultáneas, también está contemplada en el estándar.

La norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica.

Cuando se origina una llamada telefónica sobre Internet, los dos terminales deben negociar cual de los dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Una cuestión importante es, como se ha dicho, que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

La comunicación bajo H.323 contempla las señales de audio y vídeo. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo el estándar T.120 que permite la

compartición de aplicaciones en conferencias punto a punto y multipunto. Una característica de la telefonía sobre una LAN o Internet es que se permite la información de vídeo sobre la de audio (videoconferencia), formateada de acuerdo con el estándar H.261 o H.263, formando parte de la carga útil del paquete RTP. Dado que se envían sólo los cambios entre cuadros resulta muy sensible a la pérdida de paquetes, lo que da origen a la distorsión de la imagen recibida.

3.2 Razones para usar NEWNAT

La razón es muy simple esta guía esta armada para personas que necesitan implementar H323 o RTP.

Les dejo un links para que puedan profundizar en el tema.

http://greco.dit.upm.es/~david/TAR/trabajos2002/01−SIP−%20Diego−Acosta.pdf

Pido mil disculpas a aquellas personas que buscan en esta guía encontrar información de cómo poder implementar NAT, teniendo en cuenta que nos vamos a saltear muchos pasos obvios de Iptables.

Acá les dejo un link muy bueno que los pone al tanto de que es NAT y Iptables

http://www.insflug.org/COMOs/NAT−COMO/NAT−COMO.html

3.3 Puesta al día rápida con respecto a los núcleos 2.0 y 2.2

Lo siento por aquellos que todavía estén aturdidos por la transición desde 2.0 (ipfwadm) a 2.2 (ipchains). Hay buenas y malas noticias.

Primero, puede seguir usando ipchains o ipfwadm como antes. Para hacerlo, necesita cargar los módulos del núcleo «ipchains.o» o «ipfwadm.o» que encontrará en la última distribución de netfilter. Son mutuamente exclusivos (está advertido), y no deberían combinarse con ningún otro módulo de netfilter.

Una vez haya instalado uno de estos módulos puede utilizar ipchains e ipfwadm con normalidad, excepto por las siguientes diferencias:

- Establecer los tiempos límite (time out) con ipchains −M −S o ipfwadm −M −s no hace nada. Como los límites de tiempo con la nueva infraestructura NAT son más grandes, no debería haber problema.
- Los campos init_seq, delta y previous_delta en la lista ampliada de enmascaramiento (verbose masquerade listing) siempre son 0.
- Listar los contadores y ponerlos a cero al mismo tiempo «−Z −L» ya no funciona: los contadores no se pondrán a cero.

4 Ingredientes J

Kernel 2.4.16 (www.kernel.org)

iptables 1.2.6 a –5 (IP packet filter administration tools for 2.4.4+ kernels)

newnat5−and−helpers−2.4.16.patch.gz (http://roeder.goe.net/~koepi/newnat.html)

4.1 Howto

http://www.insflug.org/COMOs/NAT−COMO/NAT−COMO.html

http://www.collaborium.org/onsite/benin/docs/services/NETFILTER_RELATED/netfilter−extensions/netfilter−extens

http://www.linuxguruz.com/iptables/howto/2.4routing.html#toc18

http://iptables−tutorial.frozentux.net/

http://www.adj.idv.tw/server/linux_nat.htm

http://www.study−area.org/linux/system/linux_kernel.htm

http://www.kfki.hu/~kadlec/sw/netfilter/

http://www.tsmservices.com/masq/

http://www.iana.org/assignments/port−numbers

http://www.practicallynetworked.com/sharing/app_port_list.htm

5 Instalación

1) Bajamos el kernel y lo guardamos en **cd /usr/src/**

2) Descomprimimos el kernel **/usr/src/# tar Ixvf linux−2.4.16.tar.gz**

3) Entramos a la carpeta **cd /usr/src/linux**

4) aplicamos el patch de NEWNAT **gzip −cd newnat5−and−helpers−2.4.16.patch.gz | patch −p1 –E**

5) Nos fijamos si estamos en la carpeta del kernel **pwd**

6) A compilar **make menuconfig**

7) Y para los que no saben como compilar un kernel les dejo unos links muy buenos
http://www.zonasiete.org/docs/locales/kernel_mini_howto/
http://grulla.hispalinux.es/articles/kernel.pdf
http://www.linuxfocus.org/Castellano/July2001/article209.shtml
http://documentos.glo.org.mx/?HOWTO=mini−quickcam

8) Acá les muestro para que puedan chaquear si el patch fue aplicado y lo pueden instalar como modulo o estático, la compilación queda a gusto de cada usuario y/o administrador.

```
1.       Networking options  --->

2.          [*] Network packet filtering (replaces ipchains)

3.          [*] TCP/IP networking

4.            IP: Netfilter Configuration  --->

5.             <M> Connection tracking (required for masq/NAT)

6.             <M>  FTP protocol support

7.             <M>  talk protocol support

8.             <M>  H.323 (netmeeting) support

9.             <M>  IRC protocol support
```

9) Al terminar de compilar ponemos **make dep && make clean && make bzImage && make modules && make modules_install**

10) Copiamos el archivo System.map (esta en /usr/src/linux/) y lo copiamos a la carpeta **/Boot** así **System.map−2.4.16** Ejemplo: **cp /usr/src/linux/System.map /boot/System.map−2.4.16**

11) Copiamos el archivo **bzImage** (esta en /usr/src/linux/ arch/i386/boot/) y lo copiamos a la carpeta **/Boot** así **bzImage** Ejemplo: **cp /usr/src/linux/arch/i386/boot/bzImage /boot/bzImage−2.4.16**

12) Chequeamos que estén los archivos **cd /boot** y **ls –l**

13) Acá declaramos los cambios en el **LILO** que se encuentre en **/etc/lilo.conf** lo editamos y ponemos lo siguiente

Descomentamos las 2 líneas de abajo

prompt

timeout=100

Acá es donde le decimos que kernel arrancar

default=linux−2416

Acá declaramos el nuevo núcleo

image=/boot/bzImage

label=Linux−2416

read−only

 # restricted

 # alias=1

Salvamos lo ingresado en el archivo lilo.conf y tipeamos el comando **lilo**

Ejemplo:

ns1:~# lilo

Added Linux

Added Linux−2416 *

Skipping /vmlinuz.old

Esto **Added Linux−2416 *** significa que lilo acepto los cambios

14) Ya esta hicimos todo, nos queda solo añadir las reglas de iptables para NEWNAT en nuestro SCRIPT de NAT, muestro ejemplos:

Ejemplo N 1

#! /bin/bash

EXTERNAL_IF=eth0

EXTERNAL_IP=64.116.229.30

PCA_HOST=192.168.1.4

$IPTABLES=/sbin/iptables

Mod='modprobe'

$Mod ip_tables

$Mod iptable_filter

$Mod ip_conntrack_h323

$Mod ip_nat_h323

logger −s "H323 Ports"

H323_PORTS="389 522 1503 1720 1731 8080"

for PORT in $H323_PORTS; do

$IPTABLES −t nat −A PREROUTING −i $EXTERNAL_IF −p tcp −d $EXTERNAL_IP \

−−dport $PORT −m state −−state NEW,ESTABLISHED,RELATED \

−j DNAT −−to−destination $PCA_HOST −v

```
done


logger −s "H323 Ports"
H323_PORTS="389 522 1503 1720 1731 8080"
for PORT in $H323_PORTS; do
$IPTABLES −t nat −A PREROUTING −i $EXTERNAL_IF −p udp −d $EXTERNAL_IP \
−−dport $PORT −m state −−state NEW,ESTABLISHED,RELATED \
−j DNAT −−to−destination $PCA_HOST −v
done
```

Ejemplo N 2

```
#! /bin/bash


$IP=/sbin/iptables
Mod='modprobe'


$Mod ip_tables
$Mod iptable_filter
$Mod ip_conntrack_h323
$Mod ip_nat_h323


# Esto es para las conexiones H.323 salientes.
$IP −A FORWARD −m state −−state RELATED,ESTABLISHED −j ACCEPT
$IP −A FORWARD −i eth0 −o eth1 −p tcp −−dport 1720 −−syn −j ACCEPT
# Esto permite que las llamadas vayan del exterior a una dirección interna
```

No es necesario, si usted desea solamente hacer llamadas; no recibirlas

$IP −t nat −A PREROUTING −i eth0 −d 64.116.229.30 −p tcp −−dport 1720 −−syn −j DNAT −−to 192.168.1.4

$IP −A FORWARD −i eth0 −o eth1 −p tcp −−dport 1720 −−syn −j ACCEPT

15) Seguro que se pregunta como puede hacer si uso el programa ICQ, o si uso MSN o talvez jugar al Quake…….. miren esto:

5.1 Guía de puerto TCP/UDP

Mensajes & Conferencias

Active Worlds
IN TCP 3000
IN TCP 5670
IN TCP 7777
IN TCP 7000−7100

[0000]
Type=TCP
Translation=NORMAL
Port=5670

[0001]
Type=TCP
Translation=NORMAL
Port=7777

[0002]
Type=TCP
Translation=NORMAL
Port=7000−7100

[0003]
Type=TCP
Translation=NORMAL
Port=3000

AIM Talk
OUT TCP 4099
IN TCP 5190

Battlecom
IN UDP 2300 − 2400
IN TCP 2300 − 2400
IN UDP 47624
IN TCP 47624

Buddy Phone
(solamente comunicaciones. No FTP)
IN UDP 700 − 701

Calista IP phone
OUT TCP 5190
IN UDP 3000

CuSeeMe
OUT UDP 24032
IN UDP 1414 [usa H.323 protocolo si esta habilitado]
IN UDP 1424 [usa H.323 protocolo si esta habilitado]
IN TCP 1503
IN TCP 1720 [usa H.323 protocolo si esta habilitado]
IN UDP 1812 1813
IN TCP 7640
IN TCP 7642
IN UDP 7648
IN TCP 7648
IN TCP 7649 7649
IN UDP 24032
IN UDP 56800
OUT UDP 1414 [usa H.323 protocolo si esta habilitado]
OUT UDP 1424 [usa H.323 protocolo si esta habilitado]
OUT TCP 1503
OUT TCP 1720 [usa H.323 protocolo si esta habilitado]
OUT UDP 1812 1813
OUT TCP 7640
OUT TCP 7642
OUT UDP 7648
OUT TCP 7648
OUT TCP 7649
OUT UDP 56800

Delta Three PC to Phone
IN TCP 12053 [usa el protocolo del CuSeeMe si esta habilitado]
IN TCP 12083
IN UDP 12080
IN UDP 12120
IN UDP 12122
IN UDP 24150 − 24179

Dialpad
OUT TCP 7175
IN UDP 51200 51201
IN TCP 51210
IN TCP 1584 1585
OUT TCP 8680 8686

Dwyco Video Conferencing
IN UDP 12000 − 16090
IN TCP 1024 − 5000
IN TCP 6700 − 6702
IN TCP 6880

Go2Call
IN UDP 2090 2091
IN TCP 2090

H.323 compliant video player,
NetMeeting 2.0, 3.0, Intel Video Phone
(Llamadas en camino no es posible por que usa NetMeeting asignación de puertos automáticamente.)
OUT TCP 1720
IN UDP 1024 65534 [usa H.323 protocolo si esta habilitado]
OUT UDP 1024 65534 [usa H.323 protocolo si esta habilitado]
IN TCP 1024 1502 [usa H.323 protocolo si esta habilitado]
OUT TCP 1024 1502 [usa H.323 protocolo si esta habilitado]
IN TCP 1504 1730 [usa H.323 protocolo si esta habilitado]
OUT TCP 1504 1730 [usa H.323 protocolo si esta habilitado]
IN TCP 1732 65534 [usa H.323 protocolo si esta habilitado]
OUT TCP 1732 65534 [usa H.323 protocolo si esta habilitado]
OUT TCP 1503 1503
OUT TCP 1731 1731
IN TCP 1503 1503
IN TCP 1731 1731

Hotline Server
IN TCP 5500 − 5503
IN UDP 5499
Los puertos TCP habilitados son 5500 − 5503 (Esto es para los estándar 5500 puerto Hotline)

Si ud. Cambia los puertos por defecto, después ud. Debe habilitar estos 3 puertos (también si elige el puerto 4000, después debe habilitar los puertos 4000 al 4003)

ICQ
En las preferencias del ICQ "Preferences & security", "Preferences" haga click en Connections, y en "I am behind a firewall or proxy" después un click en "Firewall Settings". Y seleccione "I don't have a SOCKS Proxy server on my firewall" y/o "I am using another Proxy server". Click en siguiente “Next”. Click en "Use the following TCP listen ports for incoming event" y seleccione puertos TCP desde 20000 al 20019 para el primer usuario, 20020 al 20039 para el segundo usuario, 20040 al 20059 para el tercero, etc.

OUT UDP 4000
IN TCP 20000 20019 (para el primer usuario)
OR
IN TCP 20000 20039 (para dos usuarios)
OR
IN TCP 20000 20059 (para tres usuario, etc.)

ICUII Client
OUT TCP 2019
IN TCP 2000 2038
IN TCP 2050 2051
IN TCP 2069
IN TCP 2085
IN TCP 3010 3030
OUT TCP 2000 2038
OUT TCP 2050 2051
OUT TCP 2069
OUT TCP 2085
OUT TCP 3010 3030

ICUII Client (Version 4.xx)
IN TCP 1024 − 5000
IN TCP 2000 − 2038
IN TCP 2050 − 2051
IN TCP 2069
IN TCP 2085
IN TCP 3010 − 3030
IN TCP 6700 − 6702
IN TCP 6880
IN UDP 12000 − 16090

Internet Phone
OUT UDP 22555

Ivisit
IN UDP 9943
IN UDP 56768

LIVvE
(Para mandar mensajes de Pager solamente)
IN UDP 8999

mIRC DCC / IRC DCC
[mIRC Proxy/Firewall Help page]
IN TCP 1024 − 5000

mIRC Chat
(El puerto usual del IRC es el 6667)
IN TCP 6660 − 6669

mIRC IDENT
IN UDP 113

MSN Messenger
NOTA: Apague cualquier programa personal de firewall como alguno de estos BlackIce, ZoneAlarm, etc.
Ports 6891−6900 habilitar para el intercambio de archivos,
Port 6901 es para la comunicaciones de voz.
IN TCP 6891 − 6900
IN TCP 1863
IN UDP 1863
IN UDP 5190
IN UDP 6901
IN TCP 6901

Net2Phone
OUT UDP 6801 al 6803
IN UDP 6801 al 6803
IN/OUT UDP/TCP 30000

Pal Talk
IN UDP 2090 [voz]
IN UDP 2091 [Control]
IN TCP 2090 [transferencia de archivos]
IN TCP 2091 [escucha de video]
IN TCP 2095 [transferencia de archivos – viejas versiones]
OUT TCP 5001 − 50015 [mensajes de texto]
OUT TCP 8200 − 8700 [Firewall / network mode group voice]
OUT UDP 8200 − 8700 [Firewall / network mode group voice]
OUT UDP 1025 − 2500

PhoneFree
IN UDP 1034 − 1035
IN UDP 9900 − 9901
IN TCP 1034 − 1035
IN TCP 2644
IN TCP 8000

Para llamada entrantes

8000 TCP Server access
1034 UDP Voice in/out
1035 TCP Voice in/out
2644 TCP Personal Communication Center
9900−9901 UDP.

Polycom ViaVideo H.323
IN TCP 3230 − 3235
IN UDP 3230 − 3235
NOTE: Ud. Necesita habilitar estos puertos para llamar a fuera.
También habilite en ViaVideo (en el H.323 QoS) 'que use puertos' 3230−3235 TCP y UDP

Roger Wilco
IN TCP 3782
IN UDP 3782
IN UDP 3783

Speak Freely
IN UDP 2074 − 2076

Yahoo Messenger Chat
IN TCP 5000 − 5001

Yahoo Messenger Phone
IN UDP 5055

Audio & Video

Camerades
IN TCP 2047 2048
IN UDP 2047 2048

GNUtella
IN TCP 6346
IN UDP 6346

IStreamVideo2HP
IN TCP 8076 − 8077
IN UDP 8076 − 8077

KaZaA
IN TCP 1214

Napster
OUT TCP 6699
IN TCP 6699

QuickTime 4 Server
IN TCP 6970
IN UDP 6970 − 7000

QuickTime 4 Client & RealAudio on Port 554
OUT TCP 554
IN UDP 6970 − 32000

RealAudio on Port 7070
OUT TCP 7070
IN UDP 6970 − 7170

ShoutCast Server
IN TCP 8000 − 8005

Games

Aliens vs. Predator
IN UDP 80
IN UDP 2300 − 2400
IN UDP 8000 − 8999

Anarchy Online (BETA)
IN TCP 7013
IN TCP 7500 − 7501
IN UDP 7013
IN UDP 7500 − 7501

Asheron's Call [support page] [mapping info]
OUT UDP 9000, 9004, 9008, 9012
IN UDP 9000, 9001, 9004, 9005, 9012, 9013
NOTE: Ud puede necesitar el MSN Game Zone y puertosDX.

Black and White
IN TCP 2611 − 2612
IN TCP 6667
IN UDP 6500
IN UDP 27900

Blizzard Battlenet
IN TCP/UDP 4000
IN TCP/UDP 6112

Bungie.net, Myth, Myth II Server
IN TCP 3453

Dark Reign 2
IN TCP 26214
IN UDP 26214

Delta Force (Cliente & Server)
OUT UDP 3568
IN TCP 3100 3999
OUT TCP 3100 3999
IN UDP 3100 3999
OUT UDP 3100 3999

Delta Force 2
IN UDP 3568
IN UDP 3569

Elite Force
IN UDP 26000
IN UDP 27500
IN UDP 27910
IN UDP 27960 al 27962

Everquest
Mire la pagina de ayuda Everquest para mas información.
IN TCP 1024 7000
IN UDP 1024 6000
Note: Puede tener abiertos este ultimo puerto del rango UDP F−16, Mig 29
IN UDP 3862
IN UDP 3863

F−22 Lightning 3
IN UDP 3875
IN UDP 4533
IN UDP 4534
IN UDP 4660 − 4670 (para VON)

F−22 Raptor
IN UDP 3874, 3875

Fighter Ace II
IN TCP 50000 − 50100
IN UDP 50000 − 50100

DX para jugar usar estos puertos:
IN TCP 47624
IN TCP 2300 − 2400
IN UDP 2300 − 2400

Half Life
IN UDP 6003
IN UDP 7002
IN UDP 27010
IN UDP 27015
IN UDP 27025

Half Life Server
IN UDP 27015

Heretic II Server
IN TCP 28910

Hexen II
Cada computadora con Hexen II debe usar diferente rango de puertos, empezando del 26900 y incrementando de 1.

IN UDP 26900 (Para un jugador)

KALI
Cada computadora con KALI debe usar diferente rango de puertos, empezando del 2213 y incrementando de 1.

IN UDP 2213 (Para un jugador)
IN UDP 6666

Kohan Immortal Sovereigns
IN UDP 3855
IN UDP 17437
IN TCP 3855
IN TCP 17437

Motorhead server
IN UDP 16000
IN TCP 16000
IN TCP 16010 − 16030
IN UDP 16010 − 16030

MSN Game Zone [support page] [DX support page]
IN TCP 6667
IN TCP 28800 − 29000

DX para jugar estos puertos:
IN TCP 47624
IN TCP 2300 − 2400
IN UDP 2300 − 2400

Need for Speed − Porche
IN UDP 9442

Need for Speed 3− Hot Pursuit
IN TCP 1030

Operation FlashPoint

TCP 47624 ~ 47624
TCP 2234 ~ 2234
TCP & UDP Ports 6073 ~ 6073

Outlaws
IN UDP 5310
IN TCP 5310

Quake2 (Cliente y Server)
IN UDP 27910

QuakeIII
Cada computadora con Quake III debe usar diferente rango de puertos, empezando del 27660 y incrementando de 1.

Ud. También tiene que hacer estos cambios:

1. Click derecho en el icono de QIII
2. Elegir "Propiedades"
3. "C:\Program Files\Quake III Arena\quake3.exe"
4. Agregue el Quake III net_port en comandos y especifique el único puerto de comunicación en cada sistema (pc).
5. Click OK.
6. Repita esto si esta detrás de un firewall con NAT, estos son los puertos 27660,27661,27662

IN UDP 27660 (Para un jugador)

Rainbow Six (Cliente & Server)
OUT TCP 2346
IN TCP 2346

Rogue Spear
OUT TCP 2346
IN TCP 2346

Soldier of Fortune
IN UDP 28910 − 28915

Starcraft
IN UDP 6112

Starfleet Command
IN TCP 2300 − 2400
IN TCP 47624
IN UDP 2300 − 2400
IN UDP 47624

SWAT3
IN TCP 16639
IN UDP 16638

Ultima
IN TCP 5001−5010 Juego
IN TCP 7775−7777 Logueo
IN TCP 8888 Parche
IN TCP 8800−8900 UO Messenger
IN TCP 9999 Parche
IN TCP 7875 UOMonitor

Unreal Tournament server
IN UDP 7777 (puerto por defecto para jugar)
IN UDP 7778 (puerto server query)
IN UDP 7779 − 7781
IN UDP 27900

IN TCP 8080

Apprule courtesy of Quantus' World
OUT TCP 4000
IN TCP 4000
IN UDP 1140 1234
IN TCP 1140 1234
OUT UDP 1140 1234
OUT TCP 1140 1234

ZNES
IN UDP 7845

Common Servers

FTP Server en su LAN
IN TCP 21

POP3 Mail Server en su LAN
IN TCP 110

SMTP Mail server" en su LAN
IN TCP 25

TELNET Server en su LAN
IN TCP 23

WEB Server en su LAN
IN TCP 80

Other

BAYVPN
OUT UDP 500

CITRIX Metaframe / ICA cliente
IN TCP 1494
IN UDP 1604
IN TCP 1023 − 5000

CarbonCopy32 Coputadora en su LAN
IN TCP 1680
IN UDP 1023−1679

Deerfield MDaemon Email Server
IN TCP 3000
IN TCP 3001

Direct Connect
IN TCP 375 − 425

FW1VPN
OUT UDP 259

Laplink Host
IN TCP 1547

Lotus Notes Server
IN TCP 1352

NTP (Network Time Protocol)
OUT UDP 123
IN UDP 123

pcANYHWERE host en su LAN
IN TCP 5631
IN UDP 5632

RAdmin (Fama Tech)
IN TCP 4899

Remote Anything
IN TCP 3999 − 4000
IN UDP 3996 − 3998

Remotely AnyWhere
IN TCP 2000

Remotely Possible Server
IN TCP 799

Shiva VPN
OUT UDP 2233
IN UDP 2233

Timbuktu Pro
IN TCP 407

IN TCP 1417 − 1420
IN UDP 407
IN UDP 1417 − 1420

Virtual Network Computing (VNC)
IN TCP 5500
IN TCP 5800
IN TCP 5900

Windows 2000 Terminal Server
(porbablemente trabaje con NT Terminal services)
IN TCP 3389
IN UDP 3389

16) Instalamos iptables de Netfilter **apt−get install iptables 1.2.6 a –5**

17) Bueno esto es el fin ;−) espero que les allá servido toda la info que les acabo de dar tenga en cuenta que esta guía esta armada para un nivel medio o avanzado.

6 Agradecimientos y Comentario

Quiero agradecer a mi novia y familia que me apoya día a día, a las personas que trabajan codo a codo conmigo y especialmente a Sebastián Caballaro.

Y al resto del mundo que soportó mis enojos mientras aprendía sobre los horrores de NAT. y NEWNAT.

Todo el material fue buscado en libros, Web, Howto en Ingles y otros idiomas, solo trate de armar una guía de ayuda.

Saludos cordiales,

Christian Conejero