

El Día a Día del Administrador de Sistemas

ASUNTOS NAT

Si las LAN no usasen NAT (Traducción de Direcciones de Red), el espacio de direcciones IPv4 se habría agotado hace algunos años. A pesar de todo, es buena idea comprobar lo que llega a través de las conexiones NAT. **POR CHARLY KÜHNAST**

Desde un punto de vista global, las LAN son las incógnitas de Internet. Muchos equipos públicos son en realidad puertas de enlace tras las cuales podrían residir diversos ordenadores con direcciones IP privadas. La Traducción de Direcciones de Red se asegura de que los ordenadores sin una IP pública puedan acceder a Internet. Sin embargo, desde el punto de vista del administrador, NAT oculta la visión de la red. Por ello me alegra tener en mi caja de herramientas el programa Netstat-nat [1].

```

File Edit View Terminal Tabs Help
router:~ # netstat-nat -L -n
Proto Source Address          Destination Address      State
tcp    10.0.0.150:4416             10.0.0.254:4949         TIME_WAIT
tcp    10.0.0.214:46363           10.0.0.254:22           ESTABLISHED
tcp    10.0.0.214:51788           10.50.5.252:22          ESTABLISHED
tcp    10.0.0.254:4949            10.0.0.150:2829         ESTABLISHED
udp    10.0.0.150:514             10.0.0.254:514          UNREPLIED
udp    10.50.5.252:1031           194.77.253.129:53       ASSURED
router:~ #

```

Figura 1: Con `-L -n` se le indica a Netstat-nat que muestre las conexiones que no pasan por la puerta de enlace NAT.

Este pequeño programa escrito en C, disponible como *tar.gz*, RPM y formato Deb, muestra el estado de las conexiones NAT fisgando los datos de conexión que iptables escribe en `/proc/net/ip_conntrack*`.

SYSADMIN

Desperimetrización66

Vemos un nuevo concepto en materia de seguridad.

IPMI69

Una herramienta para monitorización remota de servidores.

Para Internet, la salida de Netstat-nat puede ser desordenada, pero hay una serie de opciones que hacen que la herramienta no muestre tanta información; por ejemplo, Netstat-nat soporta una clasificación básica basada en el tipo de protocolo usado. Tecleando

```
netstat-nat -p tcp
```

por ejemplo, oculta las conexiones UDP; con esto se restringe la salida a las conexiones TCP. También, estableciendo las opciones `-S` y `-D` se especifica si se desean ver las con-

exiones NAT de origen y de destino. Una NAT fuente (SNAT) convierte las direcciones internas, que normalmente están en la zona RFC 1918 como 192.168.0.0/16, a direcciones IP públicas válidas. Los routers DSL de las redes de las pequeñas empresas y de las casas particulares utilizan SNAT. Una NAT de destino (DNAT) funciona a la inversa.

Estableciendo los Hechos

Con el siguiente comando se averigua si un ordenador específico en la red enmascarada está actualmente

estableciendo una conexión por medio de la puerta de enlace NAT:

```
netstat-nat -s nombre
```

La variable *nombre* puede ser cualquier nombre de host o una dirección IP. También funciona en la otra dirección: estableciendo el parámetro `-d nombre` muestra los ordenadores que son los destinos de las direcciones NAT.

Pero, ¿qué hay de las conexiones que no pasan a través de la puerta de enlace NAT, como puede ser mi propia conexión SSH a la puerta de enlace?

Tecleando el siguiente comando se muestra la salida que aparece en la Figura 1:

```
netstat-nat -L -n
```

El parámetro `-n` evita la resolución de nombres tanto para el host como para el puerto. Aunque aún no están implementadas, sería útil indicarle a la herramienta que resuelva el nombre del host y del puerto. Añadiéndole `| cat -b` al comando, se le añade un número a cada línea de la salida, algo que puede ser útil cuando ésta es grande, de este modo nos podemos hacer una idea de cuantas páginas está compuesta la salida sin haberlas leído realmente.

RECURSOS

[1] Netstat-nat: <http://tweegy.demon.nl/projects/netstat-nat/>