Cómo configurar Iptables para bloquear servicios indeseables. V. 1.0.1

Actualizado el Domingo 05/05/2002, 18:30:05 GMT -0600.

Joel Barrios Dueñas
jbarrios arroba linuxparatodos punto net
http://www.linuxparatodos.net/

Usted puede contribuir financiando la elaboración de más documentos como éste haciendo aportaciones voluntarias y anónimas en:
Bital, Banco Internacional, S.A. (México)
Cuenta: 4007112287, Sucursal 0643
A nombre de: Joel Barrios Dueñas.

Introducción.

Bloquear servicios indeseables en una LAN es vital, especialmente cuando, como en la mayoría de los casos, el abuso en el consumo del valioso ancho de banda consecuente en el detrimento de los servicios que son verdaderamente importantes.

Justificantes.

Servicios como los utilizados para compartir archivos, principalmente música, además de fomentar la piratería, y comprometer indirectamente a la empresa en dicha actividad, son los que representan el mayor consumo de ancho de

banda.

Otros servicios, como los utilizados para mensajería instantánea, contribuyen, aunque en menor grado, también contribuyen a este detrimento. Representan también un riesgo de seguridad para los mismos usuarios debido a la proliferación de gusanos, troyanos y virus, hecho que puede llegar a comprometer datos e información confidencial y estratégica de la empresa.

Procedimientos

Las siguientes constituyen las reglas necesarias para añadir en el guión del muro contrafuegos a fin de bloquear los servicios indeseables.

Compartición de archivos.

```
# Red de Audio Galaxy
/sbin/iptables -A FORWARD -d 64.245.58.0/23 -j REJECT

# GNUtella, Bearshare y ToadNode
/sbin/iptables -A FORWARD -p TCP --dport 6346 -j REJECT

# eDonkey
/sbin/iptables -A FORWARD -p tcp --dport 4661:4662 -j REJECT
/sbin/iptables -A FORWARD -p udp --dport 4665 -j REJECT

# Puertos y redes de Kazaa y Morpheus
/sbin/iptables -A FORWARD --dport 1214 -j REJECT
/sbin/iptables -A FORWARD -d 213.248.112.0/24 -j REJECT
/sbin/iptables -A FORWARD -d 206.142.53.0/24 -j REJECT

# Red de Napigator
/sbin/iptables -A FORWARD -d 209.25.178.0/24 -j REJECT

# Red de Napster
/sbin/iptables -A FORWARD -d 64.124.41.0/24 -j REJECT

# Redes de WinMX
/sbin/iptables -A FORWARD -d 209.61.186.0/24 -j REJECT
/sbin/iptables -A FORWARD -d 64.49.201.0/24 -j REJECT

# Red de IMesh
```

```
/sbin/iptables -A FORWARD -d 216.35.208.0/24 -j REJECT
```

Mensajería instantánea.

```
# AIM e ICQ
/sbin/iptables -A FORWARD --dport 9898 -j REJECT
/sbin/iptables -A FORWARD --dport 5190:5193 -j REJECT
/sbin/iptables -A FORWARD -d login.oscar.aol.com -j REJECT
/sbin/iptables -A FORWARD -d login.icq.com -j REJECT

# Jabber
/sbin/iptables -A FORWARD --dport 5222:5223 -j REJECT

# MSN Messenger
/sbin/iptables -A FORWARD -p TCP --dport 1863 -j REJECT
/sbin/iptables -A FORWARD -d 64.4.13.0/24 -j REJECT

# Yahoo! Messenger
/sbin/iptables -A FORWARD -p TCP --dport 5000:5010 -j REJECT
/sbin/iptables -A FORWARD -d cs.yahoo.com -j REJECT
/sbin/iptables -A FORWARD -b scsa.yahoo.com -j REJECT
```