

Configuración del servicio: iptables

2.1 Descripción

Iptables es la aplicación encargada de gestionar de entre otros el firewall de linux y todo lo relativo al enrutamiento de paquetes y red. Mientras no se añada ningún sistema de filtrado adicional a la arquitectura actual, es recomendable éste sistema de filtrados.

Para ello se ajustará la configuración de las reglas de filtrado iptables con las siguientes características:

Desde la propia máquina se puedan acceder a todos sus servicios (correo, servidor x ...)

Desde los routers de entrada, permitir únicamente el acceso a los puertos que se correspondan con los servicios ofrecidos (http/80, 21/ftp ...)

Desde la LAN (192.168.1.0/24, con la excepción del rango de routers) permitir el acceso a los servicios de ssh, web y webmin.

No permitir el resto de conexiones

1. Actuaciones

Para activar las iptables y que se arranquen de forma automática al iniciar la máquina será necesario crear el siguiente archivo:

```
/etc/sysconfig/iptables
```

2. Configuración

Se deben modificar las reglas de filtrado, teniendo en cuenta los siguientes aspectos:

Desde la propia máquina se pueden acceder a todos sus servicios (correo, servidor x, ...)

```
-A INPUT -i lo -j ACCEPT  
-A OUTPUT -o lo -j ACCEPT
```

Permite la salida de todos los paquetes por la interfície loopback, asi como la entrada a la máquina de todos los paquetes que lleguen por la interfície loopback

Permitir nuevos accesos remotos desde la LAN y routers (.19) a los puertos ssh (22), ftp(20:21), ftp pasivo (50000:60000) y http (80)

```
-A INPUT -p tcp -m state -m tcp --dport 20 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 21 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 22 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 80 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 50000:60000 --state NEW -j
ACCEPT
```

Permite recibir las respuestas de los DNS configurados en /etc/resolv.conf

```
-A INPUT -p 50 -j ACCEPT
-A INPUT -p 51 -j ACCEPT
```

Permite la respuesta del Multicast DNS

```
-A INPUT -p udp -d 224.0.0.251 --dport 5353 -j ACCEPT
```

Impide el acceso a cualquier puerto tcp desde los routers

```
-A INPUT -s 192.168.1.1:9 -j REJECT --reject-with icmp-host-prohibited
```

Desde la propia LAN (192.168.1.0/24, con la excepción del rango de routers) permitir el acceso a los servicios de webmin, mysql y https

```
-A INPUT -p tcp -m state -m tcp --dport 443 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 6714 --state NEW -j ACCEPT
-A INPUT -p tcp -m state -m tcp --dport 3306 --state NEW -j ACCEPT
```

Permite el acceso a los puertos 6714 (webmin), 3306 (mysql) y 443 (https) desde cualquier IP dentro de la red local (previamente a este punto están las reglas que impiden el acceso a estos puertos desde los routers)

A revisión: ping (icmp)

```
-A INPUT -p icmp --icmp-type any -j ACCEPT
```

Permitir el trafico ya establecido.

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Prohibir otros.

```
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

Rechazan el resto de peticiones tanto TCP como UDP

Es muy importante el orden con el que se aplican las reglas.

Es recomendable aplicar las reglas progresivamente directamente con el comando *iptables*. por ejemplo para la primera regla mencionada anteriormente batíamos

```
iptables -A INPUT -i lo -j ACCEPT
```

De esta forma iremos aplicando progresivamente las reglas de filtrado. Una vez terminadas de aplicar todas y comprobando que este es realmente el resultado que deseamos conseguir, utilizaremos el comando *iptables-save* o *service iptables save* para generar el archivo `/etc/sysconfig/iptables` necesario para que se carguen automáticamente las reglas al inicial el servidor.

```
service iptables save
```

Reinicio y aplicación de las nuevas reglas

Para que las nuevas configuraciones estén activas se requerirá el reinicio del servicio, que recogerá la información del archivote configuración y aplicará las nuevas reglas en este momento.

```
service iptables restart
```

Nota: Se incluye en archivo de configuración *complete* para *iptables* ubicados es `/etc/sysconfig/iptables` en los anexos de esta misma unidad

Referencias

Para ampliar información consulta las siguientes referencias:

<http://www.netfilter.org/>

<http://www.multicastdns.org/>

¿Que es iddover.net?

Iddover Hosting es una iniciativa española en el sector de servidores dedicados. Nace en contraposición de los servicios actuales de hosting . Pretende ofrecer un hosting de alta calidad gestionable a través de un potente panel propio que se adecua a los requisitos de seguridad y que proporciona al cliente potentes herramientas al alcance de un solo click

Desde 69€ dispondrás de un servidor dedicado administrado auditado con todas las medidas de seguridad ya aplicadas.

<http://www.iddover.net>