

Firewalls: iptables

Pablo Suau Pérez (aka Siew)

Marzo 2002

Contenido

- Introducción
 - Seguridad y Linux
 - ¿Necesita un usuario normal un sistema seguro?
 - Mecanismos de seguridad
 - Firewalls (cortafuegos)
- Alternativas de firewalls en Linux

Contenido

- Iptables
 - ¿Qué es iptables?
 - ¿Qué es ipchains?
 - ¿Qué necesito para usarlo?
 - Fundamentos de iptables
 - Tablas
 - Cadenas
 - Uso básico de la tabla filter
 - La tabla nat. ¿La necesita un usuario normal?

Contenido

- Diferencias iptables – ipchains
- Interfaces gráficas
 - Aplicaciones tradicionales
 - Aplicaciones web
 - phpIPtables



INTRODUCCIÓN

Seguridad y Linux

- Necesidad de asegurar los datos incrementa debido al auge de
 - Informática
 - Redes de ordenadores
- Linux → Amplia cota de mercado de servidores
→ no debe permanecer ajeno

¿Necesita un usuario normal un sistema seguro?

- Siempre que red privada conectada a red pública
- Incluso usuarios individuales
- Especialmente: DSL y cable-modems
- Rastrear Ips al azar
 - Eliminar/espiar archivos
 - Troyanos → Base para ataques de denegación de servicio

Mecanismos de Seguridad

- Linux dispone de gran cantidad de Software de seguridad
- Incluyendo al propio Sistema Operativo
- No solo asegurar propio sistema → puede asegurar otros sistemas y redes
- Principales mecanismos
 - Seguridad en el propio sistema operativo
 - Firewalls
 - Sistemas de detección de intrusos
 - Software de auditoría sobre equipos
 - Criptografía

Firewalls

- Sistema para el establecimiento de la política de acceso entre dos redes
 - Hardware (firewall dedicado)
 - Software
- Propiedades
 - Todo tráfico pasa a través de él
 - Solo tráfico autorizado por las políticas de acceso puede traspasarlo
 - Resistente a la penetración

Alternativas de Firewalls

- La mayoría de las soluciones basadas en iptables
- Otras posibilidades:
 - Linux Routing Project
(<http://master-www.linuxrouter.org:8080/>)
 - Micro-distribución Linux
 - Centrada en redes
 - Cabe en un floppy
 - Sinus Firewall
(<http://www.ifi.unizh.ch/ikm/SINUS/firewall/>)
 - Reglas dinámicas
 - Logging intensivo, alertas, etc...

Alternativas de Firewalls

- Snort (<http://www.snort.org>)
 - Puede actuar como
 - Sniffer
 - Packet Logger
 - **Network Intrusion Detection Mode** (mediante reglas dinámicas)
- SmoothWall (<http://www.smoothwall.org/gpl/home/>)
 - Sistema operativo para convertir Pcs en routers
 - Dedicados (sustitución de routers hardware)
 - Seguros



IPTABLES

¿Qué es iptables?

- Desarrollado por el proyecto **netfilter/iptables**
 - <http://netfilter.samba.org>
 - Paul 'Rusty' Rusell
- Subsistema de firewall para núcleos 2.4.x y 2.5.x
- Pensado como sustituto de los sistemas *ipchains* e *ipfwadm*
- Dos partes
 - La mayor parte está contenida en el núcleo estándar
 - Comandos del espacio de usuario

¿Qué es iptables?

- Características principales
 - Filtrado de paquetes
 - Por protocolo, puerto, ip...
 - Por estado de los paquetes (connection tracking)
 - Network Address Translation (NAT)
 - Infraestructura flexible y extensible
 - Capacidad de añadir funcionalidades mediante parches

¿Qué es ipchains?

- Reescritura de:
 - Código de Linux Ipv4 Firewalling
 - Ipfwadm, que a su vez es una reescritura del código BSD de ipfw
- Necesario para administrar filtro de paquetes
- Núcleos 2.1.102 y superiores
- Núcleos anteriores → parche
- Parte en el núcleo y parte como comandos de usuario
- <http://netfilter.samba.org/ipchains>

¿Qué necesito para usarlo?

- Instalación requiere compilación del núcleo (<http://www.linuxdoc.org/HowTo/kernel-HOWTO.html>)
- Fuentes de la parte usuario (<http://netfilter.samba.org>)
→ última versión 1.2.5
- Comandos de usuario
 - iptables
 - iptables-save
 - Iptables-restore

Fundamentos de Iptables

- Comando básico (inserción de reglas):
 - *Iptables [tabla] <comando> <filtro> <objetivo/acción>*
- Jerarquía:
 - Tablas → Cadenas → Reglas

Tablas

- Tres tablas:
 - filter
 - Filtrado de paquetes (firewall)
 - nat
 - Usada para Network Address Translation
 - mangling
 - Modificación de paquetes y sus cabeceras (TTL, TOS, ...)

Cadenas

- Tabla filter
 - FORWARD: para paquetes
 - No generados localmente
 - No destinados a nuestra máquina
 - INPUT: paquetes destinados a nuestra máquina (el propio firewall)
 - OUTPUT: paquetes generados localmente
 - Cadenas definibles por el usuario (sustituyen una acción DROP – ACCEPT – REJECT)

La tabla filter

- Construcción de reglas
 - `Iptables [tabla] <comando> <filtro> <objetivo/salto>`
 - En el caso de la tabla filter:
 - No hace falta indicar tabla (filter por defecto)
 - Comando
 - `-A` cadena \rightarrow Insertar al final
 - `-D` cadena \rightarrow Borrar
 - `-R` cadena num \rightarrow Reemplazar
 - `-I` cadena num \rightarrow Insertar
 - `-L` \rightarrow Listar
 - `-F` \rightarrow Limpiar
 - `-N` cadena \rightarrow Crear cadena
 - `-X` \rightarrow Eliminar cadena
 - `-P` \rightarrow Cambiar política

La tabla filter

- Filtro: especificación de qué paquetes se verán afectados por la regla
 - Genéricos
 - -p protocolo
 - -s dirección IP fuente
 - -d dirección IP destino
 - -i interfaz de entrada
 - -o interfaz de salida
 - TCP
 - --sport puerto origen
 - --dport puerto destino
 - -tcp-flags
 - UDP
 - --sport y --dport
 - ICMP
 - --icmp-type -> tipo de paquete icmp (echo-reply, echo request...) -> identificados por valor o nombre

La tabla filter

- Objetivo/Salto: Qué hacer con el paquete (parámetro -j)
 - ACCEPT
 - DROP
 - REJECT
 - LOG
 - Cadena definida por el usuario
- Orden de las reglas importante
 - Paquete entra en cadena correspondiente
 - Se manejará según el objetivo indicado por la primera regla con la que se pueda emparejar
 - Si no se empareja con ninguna regla -> Política por defecto de la cadena

La tabla filter

Algunos ejemplos:

```
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

```
iptables -A INPUT -s 62.81.31.3 -p tcp -m tcp --dport 110 -j  
REJECT
```

```
iptables -A OUTPUT -p icmp --icmp-type 0 -j DROP
```

```
iptables -A OUTPUT -p tcp -j LOG --log-prefix "Conexion TCP  
en salida: "
```

La tabla NAT

- -t nat
- Cadenas
 - PREROUTING
 - POSTROUTING
 - OUTPUT
- Objetivos
 - SNAT
 - DNAT
 - MASQUERADE

La tabla NAT

Algunos ejemplos:

```
-A PREROUTING -s 80.115.112.12 -j DNAT --to-destination  
192.168.0.1
```

```
-A POSTROUTING -d 192.168.0.3 -j SNAT --to-source 80.81.115.12
```

```
-A POSTROUTING -d 115.112.13.12 -j MASQUERADE
```

Diferencias iptables – ipchains

- Nombres de las cadenas
 - Ipchains: minúsculas
 - Iptables: mayúsculas
- Parámetro `-i`
 - Ipchains: interfaz (para cualquier cadena)
 - Iptables: interfaz de entrada, solo funciona con INPUT y FORWARD

Diferencias iptables – ipchains

- Puertos TCP–UDP
 - Ipchains: tal cual
 - Iptables: deben ser introducidos con las opciones *--source-port/-sport* y *--destination-port/-dport*, despues de *-p tcp* o *-p udp*
- Denegación de acceso
 - Ipchains: DENY
 - Iptables: DROP

Diferencias iptables – ipchains

- Características adicionales de iptables:
 - Se puede poner a cero una regla simple mientras trabaja
 - Poniendo a cero las cadenas predefinidas también se limpian los contadores de políticas
 - REJECT y LOG son ahora acciones extendidas, lo que significa que se encuentran en módulos distintos del núcleo
 - *insmod ipt_REJECT*
 - *insmod ipt_LOG*
 - Los nombres de las cadenas pueden tener hasta 16 caracteres
 - MASQ y REDIRECT ya no son acciones. Existe la tabla NAT para ello



INTERFACES GRÁFICAS

Aplicaciones tradicionales

- Scripts
 - FWM – Linux based Firewall Managment script (<http://jason.ihde.org/fwm.html>)
 - GIPTables (<http://www.giptables.org>)
 - Levy (<http://muse.linuxmafia.org/levy/>)
 - MonMotha's Firewall (<http://monmotha.mplug.org/firewall/index.php>)

Aplicaciones tradicionales

- Front-ends para consola
 - Ipmenu (<http://users.pandora.be/stes/ipmenu.html>)
 - EasyTables (<http://freshmeat.net/projects/easytables/>)
- Front-ends para entorno gráfico
 - Alfandega (<http://alfandega.sourceforge.net/>)
 - Knetfilter (<http://expansa.sns.it:8080/knetfilter/>)
 - Firewall Builder (<http://www.fwbuilder.org>)

Aplicaciones Web

- Módulo para Webmin
(<http://www.niemueller.de/webmin/modules/iptables/>)
- PHP Firewall Generator
(<http://phpfwgen.sourceforge.net/>)
- PhpIPtables (<http://www.alu.ua.es/p/psp4/>)

PhpIPTables


- Interfaz para iptables escrita en php
- <http://www.alu.ua.es/p/psp4/>
- Manejo básico de tablas
 - Filter
 - Nat
- Objetivos
 - Administración remota
 - Facilidad de uso
 - Persistencia de las reglas

PhpIPTables

phpIPTables 0.92 - Konqueror

Dirección Editar Ver Ir Marcadores Herramientas Opciones Ventana Ayuda

Dirección <http://localhost/phpIPTables/>



PHPIPTABLES
0.92

Se está utilizando iptables v1.2.5

Opciones de filtro	Opciones de NAT
Mostrar reglas actuales	Mostrar reglas actuales
Borrar todas las reglas	Borrar todas las reglas
Borrar una regla concreta	Borrar una regla concreta
Borrar reglas de una cadena	Borrar reglas de una cadena
Borrar cadenas definidas por el usuario	Borrar cadenas definidas por el usuario
Crear nueva cadena	Crear nueva regla NAT
Crear una nueva regla tcp/udp	Crear una nueva cadena
Crear una nueva regla ICMP	
Crear nuevas reglas para forwarding	
Cambiar la política de una cadena	Cambiar la política de una cadena
Cambiar orden de reglas	Cambiar orden de reglas
Modificar una regla	Modificar una regla

Opciones de configuración

- [Guardar reglas en /etc/iptables.rules](#)
- [Restaurar reglas de /etc/iptables.rules](#)

(Para cambiar el archivo donde se almacenarán las reglas, edite 'config.inc')

Carga completada

2002-03-08

PhpIPtables: crear regla

phpIPtables: insertar regla tcp/udp - Konqueror

Dirección Editar Ver Ir Marcadores Herramientas Opciones Ventana Ayuda

Dirección <http://localhost/phpIPtables/crearRegla.php>

Interfaz

Tipo de interfaz

- Entrada
- Salida

Protocolo

IP fuente
(ip1.ip2.ip3.ip4[/mask])

IP destino
(ip1.ip2.ip3.ip4[/mask])

Puerto fuente

Puerto destino

Acción

Estado

Flags TCP
(No se tendrán en cuenta si el protocolo seleccionado es UDP.
Si se selecciona algún primer parámetro, será obligado marcar un segundo parámetro)

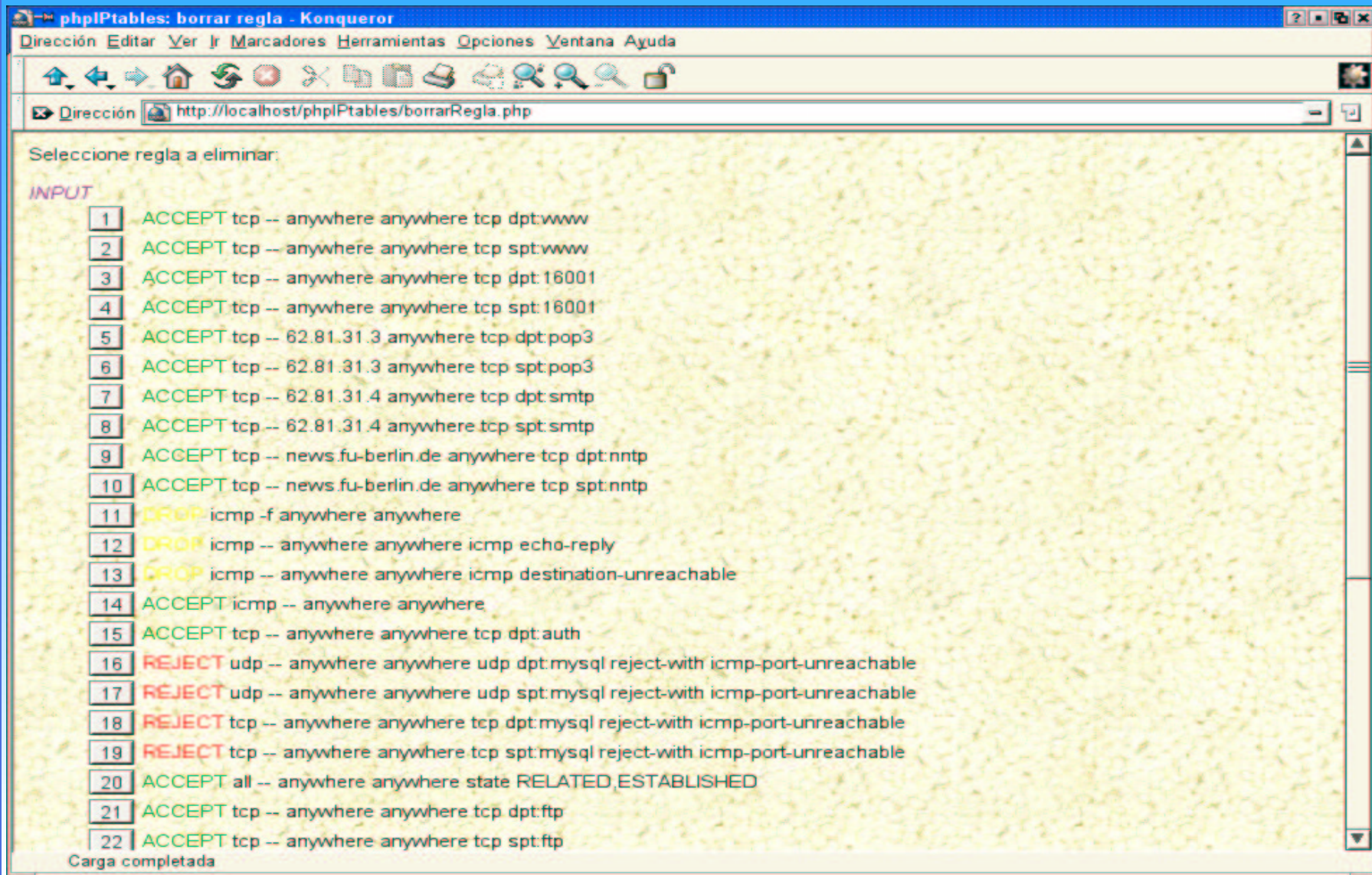
Primer parámetro: flags que deben estar desactivados	Segundo parámetro: flag que debe estar activado
<input type="checkbox"/> SYN	<input type="checkbox"/> SYN
<input type="checkbox"/> ACK	<input type="checkbox"/> ACK
<input type="checkbox"/> FIN	<input type="checkbox"/> FIN
<input type="checkbox"/> RST	<input type="checkbox"/> RST
<input type="checkbox"/> URG	<input type="checkbox"/> URG
<input type="checkbox"/> PSH	<input type="checkbox"/> PSH
	<input type="checkbox"/> ALL

NOTA: Los campos vacíos serán interpretados como 'cualquiera'

[\[VOLVER\]](#)

Carga completada

PhpIPtables: borrar regla



The screenshot shows a web browser window titled "phpIPtables: borrar regla - Konqueror". The address bar displays "http://localhost/phpIPtables/borrarRegla.php". The main content area has a yellow background and contains the text "Seleccione regla a eliminar:" followed by a list of 22 numbered rules. The rules are as follows:

- 1 ACCEPT tcp -- anywhere anywhere tcp dpt:www
- 2 ACCEPT tcp -- anywhere anywhere tcp spt:www
- 3 ACCEPT tcp -- anywhere anywhere tcp dpt:16001
- 4 ACCEPT tcp -- anywhere anywhere tcp spt:16001
- 5 ACCEPT tcp -- 62.81.31.3 anywhere tcp dpt:pop3
- 6 ACCEPT tcp -- 62.81.31.3 anywhere tcp spt:pop3
- 7 ACCEPT tcp -- 62.81.31.4 anywhere tcp dpt:smtp
- 8 ACCEPT tcp -- 62.81.31.4 anywhere tcp spt:smtp
- 9 ACCEPT tcp -- news.fu-berlin.de anywhere tcp dpt:nntp
- 10 ACCEPT tcp -- news.fu-berlin.de anywhere tcp spt:nntp
- 11 DROP icmp -f anywhere anywhere
- 12 DROP icmp -- anywhere anywhere icmp echo-reply
- 13 DROP icmp -- anywhere anywhere icmp destination-unreachable
- 14 ACCEPT icmp -- anywhere anywhere
- 15 ACCEPT tcp -- anywhere anywhere tcp dpt:auth
- 16 REJECT udp -- anywhere anywhere udp dpt:mysql reject-with icmp-port-unreachable
- 17 REJECT udp -- anywhere anywhere udp spt:mysql reject-with icmp-port-unreachable
- 18 REJECT tcp -- anywhere anywhere tcp dpt:mysql reject-with icmp-port-unreachable
- 19 REJECT tcp -- anywhere anywhere tcp spt:mysql reject-with icmp-port-unreachable
- 20 ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
- 21 ACCEPT tcp -- anywhere anywhere tcp dpt:ftp
- 22 ACCEPT tcp -- anywhere anywhere tcp spt:ftp

At the bottom of the page, it says "Carga completada".

PhpIPTables

- Características adicionales (no incluidas en línea de comandos)
 - Cambio de orden de las reglas
 - Modificación de reglas
 - Creación de reglas forward
 - Almacenamiento/recuperación de reglas