Bloquear Facebook (acceso vía HTTPS)

Guillermo GARCIA – Esc. 4-185
garcia.guillermo@outlook.com

Desde Administrador de Servicios

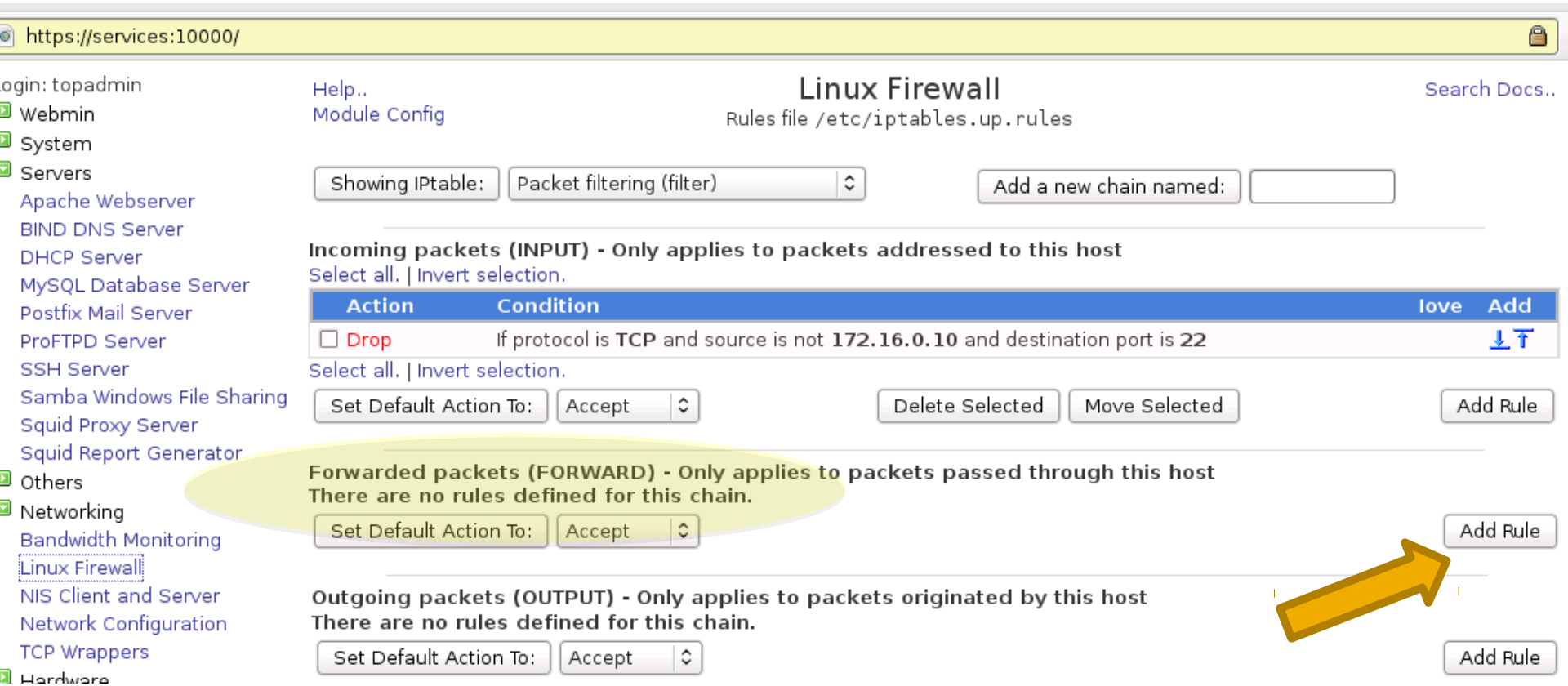
- Ingresar al Administrador de Servicios (desde el ícono en el escritorio del Servidor, o de forma remota: https://services:10000
- Poner usuario y contraseña
- En el menu (izquierda) ir a:
- Networking → Linux Firewall
  (en Español: Red → Cortafuego de Linux)

Administrador de Servicios

Agregar la regla (Forward)

- Vemos varias secciones. La primer sección es "Incoming packets (INPUT)" o en Español: "Paquetes Entrantes". En esta sólo hay una regla del tipo DROP. No tocaremos nada.
- Trabajaremos en la segunda sección: "Forwarded packets (FORWARD)" o "Paquetes Reenviados"
- Crearemos una nueva regla (Rule) desde el botón que está a la derecha: "Add Rule"

Agregar la regla (Forward)



Regla

Que es lo que hay que modificar:
(Sólo modificar lo que aparece a continuación, nada más)

- Rule Comment: comentario que describa la regla

  (Ej: "Agregado por Guillermo el 02/10/12 para bloquear Face por HTTPS")
- Action to take (acción a tomar): **DROP** (descartar)
- Destination address or network: **11.22.33.44/99**

  [Aquí va algún rango de IP de Facebook. Ver lista siguiente]
- Network Protocol: **Equals** (Igual) - **TCP**
- Destination TCP or UDP port (Puerto TCP o UDP de destino):

  Equals (Igual) - Port(s) (Puerto): **443**
- Bajar hasta el final y apretar el botón "**Create**" (Crear)

Login: topadmin
Webmin
System
Servers
Apache Webserver
BIND DNS Server
DHCP Server
MySQL Database Server
Postfix Mail Server
ProFTPD Server
SSH Server
Samba Windows File Sharing
Squid Proxy Server
Squid Report Generator
Others
Networking
Bandwidth Monitoring
Linux Firewall
NIS Client and Server
Network Configuration
TCP Wrappers
Hardware
Un-used Modules
Search:
View Module's Logs
System Information
Logout

Module Index

Edit Rule

Chain and action details

Part of chain Forwarded packets (FORWARD) - Only applies to packets passed through this host

Rule comment

Action to take ○ Do nothing ○ Accept ◉ Drop ○ Reject ○ Userspace
○ Exit chain ○ Log packet ○ Run chain

Reject with ICMP type ◉ Default ○ Type icmp-net-unreachable

The action selected above will only be carried out if **all** the conditions below are met.

Condition details

Source address or network	<Ignored>					
Destination address or network	Equals	65.201.208.24/29				
Incoming interface	<Ignored>	eth0				
Outgoing interface	<Ignored>	eth0				
Fragmentation	◉ Ignored ○ Is fragmented ○ Is not fragmented					
Network protocol	Equals	TCP				
Source TCP or UDP port	<Ignored>	◉ Port(s)		○ Port range		to
Destination TCP or UDP port	Equals	◉ Port(s)	443	○ Port range		to
Source and destination port(s)	<Ignored>					
TCP flags set	<Ignored>	☐ SYN ☐ ACK ☐ FIN ☐ RST ☐ URG ☐ PSH out of ☐ SYN ☐ ACK ☐ FIN ☐ RST ☐ URG ☐ PSH				
TCP option number is set	<Ignored>					
ICMP packet type	<Ignored>	any				
Ethernet address	<Ignored>					
Packet flow rate	<Ignored>	/ second				
Packet burst rate	<Ignored>					

Rangos de IP de Facebook (Local)

- 65.201.208.24/29
- 65.204.104.128/28
- 66.92.180.48/28
- 66.93.78.176/29
- 66.199.37.136/29
- 66.220.144.0/20
- 67.200.105.48/30
- 69.63.176.0/20
- 69.171.224.0/19
- 74.119.76.0/22
- 173.252.64.0/18
- 204.15.20.0/22

Copiar cada rango de IP como aparece en cada punto, sin modificarlo, en el campo “Destination Address” del punto anterior

Login: topadmin
Webmin
System
Servers
Apache Webserver
BIND DNS Server
DHCP Server
MySQL Database Server
Postfix Mail Server
ProFTPD Server
SSH Server
Samba Windows File Sharing
Squid Proxy Server
Squid Report Generator
Others
Networking
Bandwidth Monitoring
Linux Firewall
NIS Client and Server
Network Configuration
TCP Wrappers
Hardware
Un-used Modules
Search:
View Module's Logs
System Information
Logout

Help..
Module Config

Linux Firewall

Rules file /etc/iptables.up.rules

Search Docs..

Showing IPtable: Packet filtering (filter) Add a new chain named:

Incoming packets (INPUT) - Only applies to packets addressed to this host

Select all. | Invert selection.

Action	Condition	Move	Add
Drop	If protocol is **TCP** and source is not **172.16.0.10** and destination port is **22**		

Select all. | Invert selection.

Set Default Action To: Accept Delete Selected Move Selected Add Rule

Forwarded packets (FORWARD) - Only applies to packets passed through this host

Select all. | Invert selection.

Action	Condition	Move	Add
Drop	If protocol is **TCP** and destination is **65.201.208.24/29** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **65.204.104.128/28** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **66.92.180.48/28** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **66.93.78.176/29** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **66.199.37.136/29** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **66.220.144.0/20** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **67.200.105.48/30** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **69.63.176.0/20** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **69.171.224.0/19** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **74.119.76.0/22** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **173.252.64.0/18** and destination port is **443**		
Drop	If protocol is **TCP** and destination is **204.15.20.0/22** and destination port is **443**		

Select all. | Invert selection.

Set Default Action To: Accept Delete Selected Move Selected Add Rule

Outgoing packets (OUTPUT) - Only applies to packets originated by this host

There are no rules defined for this chain.

Set Default Action To: Accept Add Rule

Apply Configuration — Click this button to make the firewall configuration listed above active. Any firewall rules currently in effect will be flushed and replaced

Revert Configuration — Click this button to reset the configuration listed above to the one that is currently active.

Finalizar y usar reglas nuevas

- Al terminar de cargar todas las reglas, ir al final de la pantalla principal y apretamor el botón: "**Apply configuration**" (Aplicar configuración)

- Esperar unos momentos y hacer pruebas de si funciona facebook por puerto seguro (443): https:\\www.facebook.com

- Para bloquear páginas 'comunes' utilizar DansGuardian (ver alguno de los instructivos)