Óýíäåóç ÌÝóù Ôçëåöþíïõ êáé Ôåß÷ïò Ðñïóôáóßáò óôï FreeBSD

Marc Silver

marcs@draenor.org

$FreeBSD: doc/el_GR.ISO8859-7/articles/dialup-firewall/article.sgml,v 1.20 2008/12/08 03:10:51 keramida Exp $

Áõôü ôï Üñèñï ðáñÝ÷åé ðùò ìðïñåßôå íá ñõèìßóåôå Ýíá ôåß÷ïò ðñïóôáóßáò (firewall) ÷ñçóéìïðïéþíôáò ìéá PPP óýíäåóç ìÝóù ôçëåöþíïõ óôï FreeBSD ìå ôï IPFW. Ðéï óõãêåêñéìÝíá, ðáñÝ÷åôáé ç ñýèìéóç åíüò ôåß÷ïõò ðñïóôáóßáò óå ìéá óýíäåóç ìÝóù ôçëåöþíïõ ðïõ Ý÷åé äõíáìéêÞ IP äéåýèõíóç. Áõôü ôï êåßìåíï äåí áó÷ïëåßôáé ìå ôï ðùò èá ñõèìßóåôå ôçí áñ÷éêÞ óáò óýíäåóç ìÝóù PPP. Ãéá ðåñéóóüôåñåò ðëçñïöïñßåò ó÷åôéêÜ ìå ôéò ñõèìßóåéò ìéáò óýíäåóçò ìÝóù PPP äåßôå ôç óåëßäá âïÞèåéáò ppp(8).

1 Ðñüëïãïò

Áõôü ôï êåßìåíï ðáñÝ÷åé ôçí äéáäéêáóßá ðïõ ÷ñåéÜæåôáé ãéá íá ñõèìßóåôå Ýíá ôåß÷ïò ðñïóôáóßáò óôï FreeBSD üôáí ç IP äéåýèõíóç äßíåôáé äõíáìéêÜ áðü ôïí ISP óáò. Ðáñüëï ðïõ Ý÷ù ðñïóðáèÞóåé íá êÜíù áõôü ôï êåßìåíï üóï ôï äõíáôüí ðéï ðëÞñåò êáé óùóôü, åßóôå åõðñüóäåêôïé íá óôåßëåôå ôéò äéïñèþóåéò, ôá ó÷üëéá Þ ôéò ðñïôÜóåéò óáò óôç äéåýèõíóç ôïõ óõããñáöÝá: <`marcs@draenor.org`>.

2 ÐáñÜìåôñïé ôïõ ðõñÞíá

Ãéá íá ìðïñÝóåôå íá ÷ñçóéìïðïéÞóåôå ôï IPFW, ðñÝðåé íá åíóùìáôþóåôå ôçí ó÷åôéêÞ õðïóôÞñéîç óôïí ðõñÞíá óáò. Ãéá ðåñéóóüôåñåò ðëçñïöïñßåò ó÷åôéêÜ ìå ôç ìåôáãëþôôéóç ôïõ ðõñÞíá, äåßôå ôï ôìÞìá ñõèìßóåùí ôïõ ðõñÞíá óôï Åã÷åéñßäéï (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Èá ðñÝðåé íá ðñïóèÝóåôå ôéò ðáñáêÜôù åðéëïãÝò óôéò ñõèìßóåéò ôïõ ðõñÞíá óáò ãéá íá åíåñãïðïéÞóåôå ôçí õðïóôÞñéîç ãéá ôï IPFW:

```
options IPFIREWALL
```

Åíåñãïðïéåß ôïí êþäéêá ôåß÷ïõò ðñïóôáóßáò ôïõ ðõñÞíá.

> **Óçìåßùóç:** Áõôü ôï êåßìåíï èåùñåß üôé Ý÷åôå åãêáôáóôÞóåé ôçí Ýêäïóç 5.X ôïõ FreeBSD Þ ìéá ðéï ðñüóöáôç. Áí ÷ñçóéìïðïéåßôå ôçí Ýêäïóç 4.X, ôüôå èá ðñÝðåé íá åíåñãïðïéÞóåôå ôçí åðéëïãÞ *IPFW2* êáé íá äéáâÜóåôå ôç óåëßäá âïÞèåéáò ipfw(8) ãéá ðåñéóóüôåñåò ðëçñïöïñßåò ó÷åôéêÜ ìå ôçí åðéëïãÞ IPFW2. ÐñïóÝîôå éäéáßôåñá ôï ôìÞìá *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFIREWALL_VERBOSE
```

ÓôÝëíåé ôá ìçíýìáôá ãéá ôá êáôÜëëçëá ðáêÝôá óôï log ôïõ óõóôÞìáôïò.

```
options IPFIREWALL_VERBOSE_LIMIT=500
```

ÂÜæåé êÜðïéï üñéï óôéò öïñÝò ðïõ êÜðïéá åããñáöÞ èá êáôáãñÜöåôáé. ¸ôóé ìðïñåßôå íá êáôáãñÜöåôå ôá ìçíýìáôá áðü ôï ôåß÷ïò ðñïóôáóßáò ÷ùñßò ôïí êßíäõíï íá ãåìßóïõí ôá áñ÷åßá êáôáãñáöÞò ôïõ óõóôÞìáôüò óáò áí äå÷ôåßôå êÜðïéá åðßèåóç. Ôï üñéï *500* ìçíõìÜôùí åßíáé ìéá áñêåôÜ ëïãéêÞ ôéìÞ, áëëÜ ìðïñåßôå íá ðñïóáñìüóåôå áõôÞ ôçí ôéìÞ áíÜëïãá ìå ôéò áðáéôÞóåéò ôïõ äéêïý óáò äéêôýïõ.

```
options IPDIVERT
```

Åíåñãïðïéåß ôá *divert* sockets, ðïõ èá äïýìå áñãüôåñá ôé êÜíïõí.

> **Ðñïåéäïðïßçóç:** Ìüëéò ôåëåéþóåôå ìå ôéò ñõèìßóåéò êáé ôçí ìåôáãëþôôéóç ôïõ ðõñÞíá óáò *ìçí êÜíåôå åðáíåêêßíçóç!* Áí êÜíåôå åðáíåêêßíçóç óå áõôü ôï óçìåßï ìðïñåß íá êëåéäùèåßôå áðÝîù áðü ôï óýóôçìÜ óáò. ÐñÝðåé íá ðåñéìÝíåôå ìÝ÷ñé íá åãêáôáóôáèïýí ïé êáíüíåò ôïõ ôåß÷ïõò ðñïóôáóßáò êáé íá åíçìåñùèïýí üëá ôá ó÷åôéêÜ áñ÷åßá ñõèìßóåùí.

3 ÁëëáãÝò óôï `/etc/rc.conf` ãéá íá öïñôþíåôáé ôï ôåß÷ïò ðñïóôáóßáò

Ãéá íá åíåñãïðïéåßôáé ôï ôåß÷ïò ðñïóôáóßáò êáôÜ ôçí åêêßíçóç ôïõ óõóôÞìáôïò êáé ãéá íá ïñßóåôå ôï áñ÷åßï ìå ôïõò êáíüíåò ôïõ ôåß÷ïõò ðñïóôáóßáò, ðñÝðåé íá åíçìåñþóåôå ôï áñ÷åßï `/etc/rc.conf`. ÁðëÜ ðñïóèÝóôå ôéò ðáñáêÜôù ãñáììÝò:

```
firewall_enable="YES"
firewall_script="/etc/firewall/fwrules"
```

Ãéá ðåñéóóüôåñåò ðëçñïöïñßåò ó÷åôéêÜ ìå ôç óçìáóßá êáèåìéÜò áðü áõôÝò ôéò ãñáììÝò, ñßîôå ìéá ìáôéÜ óôï `/etc/defaults/rc.conf` êáé äéáâÜóôå ôçí man óåëßäá rc.conf(5)

4 ÅíåñãïðïéÞóôå ôçí ÅóùìáôùìÝíç ÌåôÜöñáóç Äéåõèýíóåùí ôïõ PPP

Ãéá íá åðéôñÝøåôå óå Üëëá ìç÷áíÞìáôá ôïõ äéêôýïõ óáò íá óõíäÝïíôáé ìå ôïí Ýîù êüóìï ìÝóù ôïõ FreeBSD, ÷ñçóéìïðïéþíôáò ôï ùò “ðýëç”, èá ðñÝðåé íá åíåñãïðïéÞóåôå ôçí åóùìáôùìÝíç ìåôÜöñáóç äéåõèýíóåùí ôïõ PPP (NAT). Ãéá íá ãßíåé áõôü, ðñïóèÝóôå óôï áñ÷åßï `/etc/rc.conf` ôéò ðáñáêÜôù ãñáììÝò:

```
ppp_enable="YES"
ppp_mode="auto"
ppp_nat="YES"
ppp_profile="ðñïößë_ôçò_óýíäåóçò"
```

Óôç èÝóç ôïõ `ðñïößë_ôçò_óýíäåóçò` ðñÝðåé íá âÜëåôå ôï üíïìá ôçò óýíäåóÞò óáò, üðùò ôï Ý÷åôå áðïèçêåýóåé óôï áñ÷åßï `/etc/ppp/ppp.conf`.

5 Ïé êáíüíåò ôïõ firewall

Ôï ìüíï ðïõ áðïìÝíåé ôþñá åßíáé íá ïñßóïõìå ôïõò êáíüíåò ôïõ firewall. Ïé êáíüíåò ôïõò ïðïßïõò ðåñéãñÜöïõìå åäþ åßíáé áñêåôÜ êáëïß ãéá ôïõò ðåñéóóüôåñïõò ÷ñÞóôåò ìå dialup óýíäåóç, áëëÜ ïýôå õðï÷ñåùôéêïß åßíáé, ïýôå åßíáé äõíáôüí íá ôáéñéÜæïõí ìå ôéò áíÜãêåò üëùí ôùí ÷ñçóôþí dialup. Ìðïñåßôå, üìùò, íá ÷ñçóéìåýóïõí ùò Ýíá êáëü ðáñÜäåéãìá ñõèìßóåùí ôïõ IPFW êáé åßíáé ó÷åôéêÜ åýêïëï íá ôïõò ðñïóáñìüóåôå óôéò äéêÝò óáò áíÜãêåò.

Áò áñ÷ßóïõìå üìùò ìå ôéò âáóéêÝò áñ÷Ýò åíüò êëåéóôïý ôåß÷ïõò ðñïóôáóßáò. ¿íá êëåéóôü ôåß÷ïò ðñïóôáóßáò áðáãïñåýåé êáô’ áñ÷Þí êÜèå óýíäåóç. Ï äéá÷åéñéóôÞò ìðïñåß ýóôåñá íá ðñïóèÝóåé êáíüíåò ãéá íá åðéôñÝøåé ìüíï óõãêåêñéìÝíåò óõíäÝóåéò íá ðåñíÜíå áðü ôï ôåß÷ïò ðñïóôáóßáò. Ç ðéï óõíçèéóìÝíç óåéñÜ ôùí êáíüíùí óå Ýíá êëåéóôü ôåß÷ïò åßíáé: ðñþôá ïé êáíüíåò ðïõ åðéôñÝðïõí ìåñéêÝò óõíäÝóåéò, êáé ôÝëïò ïé êáíüíåò ðïõ áðáãïñåýïõí ïðïéáäÞðïôå Üëëç óýíäåóç. Ç ëïãéêÞ ðßóù áðü áõôü åßíáé üôé ðñþôá âÜæåôå ôïõò êáíüíåò ðïõ åðéôñÝðïõí ðñÜãìáôá íá ðåñÜóïõí êáé ýóôåñá üëá ôá Üëëá áðáãïñåýïíôáé áõôüìáôá.

ÖôéÜîôå, ëïéðüí, Ýíá êáôÜëïãï óôïí ïðïßï èá áðïèçêåýïíôáé ïé êáíüíåò ôïõ ôåß÷ïõò ðñïóôáóßáò. Óå áõôü ôï Üñèñï ÷ñçóéìïðïéïýìå ùò ðáñÜäåéãìá ôïí êáôÜëïãï `/etc/firewall`. ÁëëÜîôå êáôÜëïãï ìÝóá óå áõôüí êáé äçìéïõñãÞóôå ôï áñ÷åßï `fwrules` ðïõ ôï üíïìÜ ôïõ åß÷áìå ãñÜøåé óôï `rc.conf`. Óçìåéþóôå ðùò ìðïñåßôå íá áëëÜîåôå ôï üíïìá ôïõ áñ÷åßïõ áõôïý óå üôé èÝëåôå. Áõôüò ï ïäçãüò äßíåé áõôü ôï üíïìá óáí ðáñÜäåéãìá êáé ìüíï.

Áò äïýìå ôþñá Ýíá ðáñÜäåéãìá ôåß÷ïõò ðñïóôáóßáò ìå áñêåôÜ åðåîçãçìáôéêÜ ó÷üëéá.

```
# Define the firewall command (as in /etc/rc.firewall) for easy
# reference.  Helps to make it easier to read.
fwcmd="/sbin/ipfw"

# Define our outside interface.  With userland-ppp this
# defaults to tun0.
oif="tun0"

# Define our inside interface.  This is usually your network
# card.  Be sure to change this to match your own network
# interface.
iif="fxp0"

# Force a flushing of the current rules before we reload.
$fwcmd -f flush

# Divert all packets through the tunnel interface.
```

```
$fwcmd add divert natd all from any to any via tun0

# Check the state of all packets.
$fwcmd add check-state

# Stop spoofing on the outside interface.
$fwcmd add deny ip from any to any in via $oif not verrevpath

# Allow all connections that we initiate, and keep their state,
# but deny established connections that don’t have a dynamic rule.
$fwcmd add allow ip from me to any out via $oif keep-state
$fwcmd add deny tcp from any to any established in via $oif

# Allow all connections within our network.
$fwcmd add allow ip from any to any via $iif

# Allow all local traffic.
$fwcmd add allow all from any to any via lo0
$fwcmd add deny all from any to 127.0.0.0/8
$fwcmd add deny ip from 127.0.0.0/8 to any

# Allow internet users to connect to the port 22 and 80.
# This example specifically allows connections to the sshd and a
# webserver.
$fwcmd add allow tcp from any to me dst-port 22,80 in via $oif setup keep-state

# Allow ICMP packets: remove type 8 if you don’t want your host
# to be pingable.
$fwcmd add allow icmp from any to any via $oif icmptypes 0,3,8,11,12

# Deny and log all the rest.
$fwcmd add deny log ip from any to any
```

Ôþñá Ý÷åôå Ýíá ïëïêëçñùìÝíï ôåß÷ïò ðñïóôáóßáò, ôï ïðïßï óõíäÝóåéò óôéò èýñåò 22 êáé 80 êáé êáôáãñÜöåé üëåò ôéò Üëëåò óõíäÝóåéò óôï áñ÷åßï êáôáãñáöÞò ôïõ óõóôÞìáôïò. ÐëÝïí åßóôå Ýôïéìïé ãéá åðáíåêêßíçóç. Ôï ôåß÷ïò ðñïóôáóßáò èá åíåñãïðïéçèåß áõôüìáôá êáé èá öïñôþóåé ôïõò êáíüíåò ðïõ ðñïóèÝóáôå. Áí äå ãßíåé áõôü Þ Ý÷åôå ïðïéáäÞðïôå ðñïâëÞìáôá, Þ áí Ý÷åôå êÜðïéåò ðñïôÜóåéò ãéá íá äéïñèùèåß áõôü ôï Üñèñï, åðéêïéíùíÞóôå ìáæß ìïõ ìå email.

6 ÅñùôÞóåéò

1. ÂëÝðù ìçíýìáôá üðùò “`limit 500 reached on entry 2800`” êáé ìåôÜ áðü áõôü ôï óýóôçìÜ ìïõ óôáìáôÜåé íá êáôáãñÜöåé ôá ðáêÝôá ðïõ åìðïäßæïíôáé áðü ôï ôåß÷ïò ðñïóôáóßáò. Äïõëåýåé áêüìá ôï firewall ìïõ;

Áõôü áðëÜ óçìáßíåé ðùò Ý÷åé ÷ñçóéìïðïéçèåß ôï ìÝãéóôï üñéï êáôáãñáöÞò (logging) ãéá áõôü ôïí êáíüíá. Ï êáíüíáò ï ßäéïò åîáêïëïõèåß íá äïõëåýåé, áëëÜ äåí èá óôÝëíåé ðéá ìçíýìáôá óôï áñ÷åßï êáôáãñáöÞò ôïõ óõóôÞìáôïò ìÝ÷ñé íá ìçäåíßóåôå ðÜëé ôïõò ìåôñçôÝò. Ìðïñåßôå íá ìçäåíßóåôå ôïõò ìåôñçôÝò ìå ôçí åíôïëÞ

```
# ipfw resetlog
```

Åíáëëáêôéêþ, ìðïñåßôå íá áõîÞóåôå ôï üñéï êáôáãñáöÞò óôéò ñõèìßóåéò ôïõ ðõñÞíá óáò ìå ôçí åðéëïãÞ `IPFIREWALL_VERBOSE_LIMIT` üðùò ðåñéãñÜøáìå ðáñáðÜíù. Ìðïñåßôå íá áëëÜîåôå áõôü ôï üñéï (÷ùñßò íá ìåôáãëùôôßóåôå ðÜëé ôïí ðõñÞíá óáò êáé íá êÜíåôå reboot) ÷ñçóéìïðïéþíôáò ôçí sysctl(8) ôéìÞ net.inet.ip.fw.verbose_limit.

2. ÊÜðïéï ëÜèïò ðñÝðåé íá Ýãéíå. Áêïëïýèçóá ôéò åíôïëÝò êáôÜ ãñÜììá êáé ôþñá êëåéäþèçêá áðÝîù.

Áõôüò ï ïäçãüò õðïèÝôåé üôé ÷ñçóéìïðïéåßôå ôï *userland-ppp*, ãé áõôü êé ïé êáíüíåò ðïõ äßíïíôáé ÷ñçóéìïðïéïýí ôï `tun0` interface, ðïõ áíôéóôïé÷åß óôçí ðñþôç óýíäåóç ðïõ öôéÜ÷íåôáé ìå ôï ppp(8) (áëëéþò ãíùóôü êáé ùò *user-ppp*). Ç åðüìåíç óýíäåóç èá ÷ñçóéìïðïéÞóåé ôï `tun1`, ìåôÜ ôï `tun2` êáé ðÜåé ëÝãïíôáò.

Èá ðñÝðåé åðßóçò íá èõìÜóôå üôé ôï pppd(8) ÷ñçóéìïðïéåß ôï interface `ppp0`, ïðüôå áí îåêéíÞóåôå ôç óýíäåóÞ óáò ìå ôï pppd(8) èá ðñÝðåé íá áíôéêáôáóôÞóåôå ôï `tun0` ìå `ppp0`. ÐáñáêÜôù èá äåßîïõìå Ýíá åýêïëï ôñüðï íá áëëÜîåôå ôïõò êáíüíåò ôïõ firewall êáôÜëëçëá. Ïé áñ÷éêïß êáíüíåò óþæïíôáé óå Ýíá áñ÷åßï ìå üíïìá `fwrules_tun0`.

```
% cd /etc/firewall
  /etc/firewall% su
  Password:
  /etc/firewall# mv fwrules fwrules_tun0
  /etc/firewall# cat fwrules_tun0 | sed s/tun0/ppp0/g > fwrules
```

Ãéá íá êáôáëÜâåôå áí ÷ñçóéìïðïéåßôå ôï ppp(8) Þ ôï pppd(8) ìðïñåßôå íá åîåôÜóåôå ôçí Ýîïäï ôçò ifconfig(8) áöïý åíåñãïðïéçèåß ç óýíäåóÞ óáò. Ð.÷., ãéá ìéá óýíäåóç ðïõ åíåñãïðïéÞèçêå áðü ôï pppd(8) èá äåßôå êÜôé óáí áõôü (äåß÷íïíôáé ìüíï ïé ó÷åôéêÝò ãñáììÝò):

```
% ifconfig
  (skipped...)
  ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1524
          inet xxx.xxx.xxx.xxx --> xxx.xxx.xxx.xxx netmask 0xff000000
  (skipped...)
```

Áðü ôçí Üëëç, ãéá ìéá óýíäåóç ðïõ åíåñãïðïéÞèçêå ìå ôï ppp(8) (*user-ppp*) èÜ ðñåðå íá äåßôå êÜôé ðáñüìïéï ìå ôï ðáñáêÜôù:

```
% ifconfig
  (skipped...)
  ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
  (skipped...)
  tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1524
          (IPv6 stuff skipped...)
          inet xxx.xxx.xxx.xxx --> xxx.xxx.xxx.xxx netmask 0xffffff00
          Opened by PID xxxxx
  (skipped...)
```