

# 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 \$

Ôï FreeBSD åßíáé Ýá êáôï ÷õñùìÝíï áìðïñéêü óýíâïï òï FreeBSD Foundation.  
ÐïëëÝò áðü ôéò ëÝíâéò P õñÜöåéò ie iðïßåò ÷ñçóéïïðïíýíôáé áðü ôïõò êáôáóéåõåóôÝò P ôïõò  
ðùèçöÝò ôïõò æéá íá æéâéñßíïõí òá ðñïúùíôá ôïõò èáùñïýíôáé áìðïñéêÜ óýíâïï  
âìöäíßæïïôáé óå áôôü ôï êåßìâïï êéá æéá úôåò áðü áôôÝò áïùñßæåé ç lïÜää ÁíÜðôôïçò ôï FreeBSD üôé  
åßíáé ðéèáíüí íá åßíáé áìðïñéêÜ óýíâïï, éá äâßôå Ýá áðü ôá óýíâïï: “™” P “®”.

Áôôü ôï Üñèñï ðåñéãñÜöåé ðùò iðïñåßôå íá ñôèìßöåôå Ýá ôåß÷ïò ðñïóôåóßáò (firewall) ÷ñçóéïïðïéþíôå  
ieá PPP óýíâåôç ïÝóù ôçëåöþíïõ ôï FreeBSD la òï IPFW. Ðéï ôôâéññéïÝíá, ðåñéãñÜöåé ôç ñýèïéôç åñüô  
ôåß÷ïò ðñïóôåóßáò óå ieá óýíâåôç ïÝóù ôçëåöþíï ðïõ Ý÷åé äôïâïéêP IP æéâýèôïç. Áôôü ôï êåßìâïï äâï  
áô÷ïëåßôåé iâ ôï ðùò èá ñôèìßöåôå ôçí áñ÷éêP óåò óýíâåôç ïÝóù PPP. Äéá ðåñéóóùôâñåò ðëçñïïñßåò  
ô÷åôéêÜ la ôéò ñôèìßöåéò ieáò óýíâåôçò ïÝóù PPP äâßôå ôç ôåëßää åïÞèåéåò ppp(8).

## 1 Ðñüëïïò

Áôôü ôï êåßìâïï ðåñéãñÜöåé ôçí æéâééåôå ðïõ ÷ñâéÜæåôåé æéá íá ñôèìßöåôå Ýá ôåß÷ïò ðñïóôåóßáò ôïï  
FreeBSD üôáí ç IP æéâýèôïç åßíåôåé äôïâïéêÜ áðü ôï ISP óåò. Ðáñüëï ðïõ Ý÷ù ðñïóðåèÞóåé íá êÜñu áôôü ôï  
êåßìâïï üöï ôï äôïâñåò íéï ðëÞñåò êéá óùóôü, åßöôå åôôñüöäâéïé íá ôôåßëåôå ôéò äéïñßöåéò, ôá ó÷üëéá P ôéò  
ðñïóðÜôåéò óåò ôôç æéâýèôïç ôïõ ôôâññåòÝá: <marcs@draenor.org>.

## 2 ÐáñÜìåôñïé ôïï ðôñÞíá

Äéá íá iðïñÝåôå íá ÷ñçóéïïðïéÞóåôå ôï IPFW, ðñÝðåé íá åíóñùåðþóåôå ôçí ó÷åôéêP ðôïóðÞñéïç ôôïï ðôñÞíá óåò.  
Äéá ðåñéóóùôâñåò ðëçñïïñßåò ó÷åôéêÜ la ôç iâôâéëþöôéôç ôïõ ðôñÞíá, äâßôå ôï òïÞíá ñôèìßöåñüí ôïõ ðôñÞíá ôïï  
Åâ ÷åéñßäéï ([http://www.FreeBSD.org/doc/el\\_GR.ISO8859-7/books/handbook/kernelconfig.html](http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html)). Èá ðñÝðåé íá  
ðñïóðÝåôå ôéò ðáñáêÜò ãðéëïäÝò óôéò ñôèìßöåéò ôïõ ðôñÞíá óåò æéá íá åíâñäïðïéÞóåôå ôçí ðôïóðÞñéïç æéá ôï  
IPFW:

options IPFIREWALL

Âlâññïðíéåß ôíí êþæéêá ôåß÷ïò ðñïóðáóþáò ôíò ððñþíá.

**Óçìåßùóç:** Áôôü ôí êåßìåíí èåùñåß üôé Ý÷åôå áâåêåðåóðþóåé ôçí Ýéäíöç 5.X ôíò FreeBSD ¶ ìéá ðéï ðñüööåôç. Áí ÷ñçóéïðíéåßòå ôçí Ýéäíöç 4.X, öüôå èá ðñïÝðåé íá álâññïðíéþóåðå ôçí åðééïäþ /IPFW2 éáé íá åéååÜðåðå ôç óåëßåå áíþéåéåò ipfw(8) áéá ðâñéöðüðåñåò ðëçñïðíñþåò ó÷åðééÜ íá ôçí åðééïäþ /IPFW2. ÐñïóÝîòå éæéåðåñá ôí ðíþíá *USING IPFW2 IN FreeBSD-STABLE*.

options IPFIREWALL\_VERBOSE

ÓôÝéíáé ôá ìçíýíåôá ãéá ôá êåðÜëëçëá ðáéÝóá ôðí log ôíò óðóðþíáðïò.

options IPFIREWALL\_VERBOSE\_LIMIT=500

ÂÜæåé êÜðíéï üñéï ôðéï ðíñÝò ðíø êÜðíéå áâåññåðþ èá êåðåññÜðåðåé, ôóé ðñïñåßòå íá êåðåññÜðåðå ôá ìçíýíåôá áðü ôí ôåß÷ïò ðñïóðåðåðå ÷ùñþò ôíí êþíåðñí íá áâìßòïðí ôá áñ÷åßá êåðåññåðþ ðí ðñïóðåðüð ôåð áí áâ÷åðåðå ðÜðíéå åðþèåóç. Ôí üñéï 500 ìçíðiÜòùí áâíáé íéá áñâåðÜ ëëæéþ ôéïþ, áëëÜ ðñïñåßòå íá ðñïóðñüöåðå ôðôþ ôçí ôéïþ áíÜëëå íá ôéð áðåéðþóåéò ôíò áééiy ôåð áééöyï.

options IPDIVERT

Âlâññïðíéåß ôá *divert* sockets, ðíò èá ãïýíå áññüöåñá ôé êÜíïðí.

**Ðñïåéäïðíßçóç:** ïüééò ôâéåéþóåðå íá ôéò ñôèïßóåéò êåé ôçí íâðåññþóöéç ôíò ððñþíá ôáò ìçí êÜíåðå åðáíåéêßíçóç! Áí êÜíåðå åðáíåéêßíçóç ôá áôôü ôí òçìåßí ðñïñåß íá êéåéåññåðþ åðÝù áðü ôí óýóðçïÜ ôåð. ÐñÝðåé íá ðâñéïÝåðå íÝ÷ñé íá áâåéåðåðåèïý íé êáíúíåò ôíò ôåß÷ïò ðñïóðåðå ðéé íá áíçìåññéïý üëá ôá ó÷åðééÜ áñ÷åßá ñôèïßóåùí.

### 3 ÁééåãÝò óðí /etc/rc.conf ãéá íá öiñþíåðåé ôí ôåß÷ïò ðñïóðåðå

Ãéá íá álâññïðíéåðåé ôí ôåß÷ïò ðñïóðåðå ðéé íá ôçí áâéëßíçóç ôíò ððóðþíáðïò êåé ãéá íá ïñþóåðå ôí áñ÷åßí íá ôíò ðñïñåðå ðéé ôåß÷ïò ðñïóðåðå, ðñÝðåé íá áíçìåñþóåðå ôí áñ÷åßí /etc/rc.conf. ÁðéÜ ðñïóðÝóåð ôéð ðáññéÜòù áññíìÝò:

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

Ãéá ðâñéöðüðåñåò ðëçñïðíñþåò ó÷åðééÜ íá ôçí áâéëßíçóç ôíò ððóðþíáðïò êåé ãééåðÜò áðü áðôÝò ôéð áññáñìÝò, ñþîðå ìéá íáðéÜ ôðí /etc/default/rc.conf êéé åééåÜðåðå ôçí man óâëßää rc.conf(5)

## 4 ÁíáññïðíéÞóôå ôçí ÁíóùìáôùìÝíç ìåôÜöñáóç Äéåõèýíóåùí ôiõ PPP

Áéá íá åðéóñÝøåôå óå Üëëá iç÷áÍpiáôå ôiõ äéêóýiõ óåò íá óðíäÝiiðáé íå ôií Ýîù êüöií iÝóù ôiõ FreeBSD, ÷ñçóéiïðíéþíðå ôiù ùò “ðýéç”, éá ðñÝðåé íá áíáññïðíéÞóôå ôçí áíóùìáôùìÝíç ìåôÜöñáóç äéåõèýíóåùí ôiõ PPP (NAT). Áéá íá áßíáé áðôú, ðñiöèÝóôå óõi áñ÷åßí /etc/rc.conf ôéò ðáññéÜòù áññíiÝò:

```
ppp_enable="YES"
ppp_mode="auto"
ppp_nat="YES"
ppp_profile="/etc/ppp/option_ipfw.conf"
```

Óôç èÝóç ôiõ ðñiöþë\_ôçò\_óýíäåóçò ðñÝðåé íá áÜëåôå ôi üññíá ôçò óýíäåóÞò óåò, üðùò ôi Ý÷åôå áðièçêåýóåé óõi áñ÷åßí /etc/ppp.conf.

## 5 Íé êáíüíåò ôiõ firewall

Ôi üññí ðiõ áðiñÝíáé ôþñá áßíáé íá íñßöriðiå ôiõò êáíüíåò ôiõ firewall. Íé êáíüíåò ôiõò iðiþiõò ðåññéññÜöriðiå áäþ áßíáé áñéåðÜ éáéiñ áéá ôiõò ðåññéóñüðåññiõò ÷ñÞóðåò ið dialup óýíäåóç, áééÜ iýðå ôði÷ññúðééiñ áßíáé, iýðå áßíáé áðiññúñ íá ðåññéññÜæiñi ìå ôéò áíÜäéåò üëñí ðñiöðí ÷ñçóéþí dialup. Iðiññíy, üñùò, íá ÷ñçóéiñáýóiõi ùò Ýíá êáëü ðáññÜäåéäñá ññðéñþóåùí ôiõ IPFW êáé áßíáé ó÷åðééÜ áýéññí íá ôiõò ðñiñóáññüðåôå óóéò áééÝò óåò áíÜäéåò.

Áò áñ÷ßóriðiå üñùò íå ôéò ááðééÝò áñ÷Ýò áñùò êéåéóôiy ôåß÷iõò ðñiñóðåóÞáò, já êéåéóôù ôåß÷iõ ðñiñóðåóÞáò áðåäññåýéé áéó’ áñ÷ßí éÜéå óýíäåóç. Í áéá÷åéñéóðò ðñiñåß ýðóðåñá íá ðñiñóéÝóåé êáíüíåò áéá íá áðéóñÝøåé iññí óðåññéññÜíåò óðiñäÝóåéò íá ðåññÜíåò áðü ôi ðåß÷iõ ðñiñóðåóÞáò. Ç ðéí õðíçééññÜíç ðåñññÜ ôùí êáíüñí óå Ýíá êéåéóôù ôåß÷iõ áßíáé: ðñþþåò ié êáíüíåò ðiõ áðéóñÝðiõò iññéñÝò óðiñäÝóåéò, éáé ôYëiõò ié êáíüíåò ðiõ áðåäññåýiõi iðiéññÜðiðå Üëëç óýíäåóç. Ç ëíñéññÜ ðþóù áðü áðôú áßíáé üüðé ðñþþåò áÜæåðå ôiõò êáíüíåò ðiõ áðéóñÝðiõò ðñÜäññåò íá ðåññÜóriñ êáé óýóðåñá üëñ áå Üëëá áðåäññåýíñðåé áðôññíåðå.

ÓðéÜñðå, eíéðñí, Ýíá êáðÜëiñi óðíi ðiþí ëá áðièçêåýíñðåé ié êáíüíåò ôiõ ôåß÷iõ ðñiñóðåóÞáò. Óå áðôú ôi Üññéññ ÷ñçóéiïðíéýiñ ùò ðáññÜäåéäñá ôií êáðÜëiñi /etc/firewall. ÁéëÜñðå êáðÜëiñi iÝóá óå áðôññí êáé áçìéiññÞóôå ôi áñ÷åßí fwrules ðiõ ôi üññíÜ ôiõ áß÷åíå áññÜøåé óõi rc.conf. Óçìåéþóå ðñù ðiðiññåðå íá áéëÜñðå ôi üññí åiõ áñ÷åßí ãðôñý óå üüðé èÝëåðå. Áðôñùò i räçññü ãßíáé áðôú ôi üññí óåí ðáññÜäåéäñá êáé iññí.

Áò aïýíå ôþñá Ýíá ðáññÜäåéäñá ôåß÷iõ ðñiñóðåóÞáò íå áñéåðÜ áðåñçäçìåóééÜ 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.
```

## Óýíååðç ÌÝóù Ôçëåöþñõ êáé Ôåþ÷ïò Ðñïóðåðáþáò óðî FreeBSD

```
$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÷åðå Áýá iæíçëçñùì Ýñõ ôðåþ÷ïò ðñïóðåðáþáò, ôí iðíþü óðñà Ýóåéò óðéò ëýñåò 22 êáé 80 êáé êáðåññÜðåé üðåò ðéò Üëéåò óðñà Ýóåéò óðíí áñ÷åßí êáðåññáþò ðø ôíø óðñóðþíáþò. ÐéÝíí åßóðå Ýðíéíé ãéá åðåíåêëþíçóç. Ôí ôðåþ÷ïò ðñïóðåðáþáò èá åíâññäðíéçèåß áðôñùåðá êáé èá óïñðþóåé ôíðò êáññüåðò ðíø ðñïóðéÝóåðå. Áí áå åðíáðé áðóðü Þ Ý÷åðå iðíéåðþðíø ðñïäðþíáðá, Þ áí Ý÷åðå êÜðíéåò ðñïðÜðåéò ãéá íá æéññëùèåß áðóðü ôí Üñèñí, åðééëíéñúÞóðå ìáæß iñò ìå

## 6 Åñùðþóåéò

1. ÅéÝðù içíýíåðå üðùò “limit 500 reached on entry 2800” êáé ìåðÜ áðü áðóðü ôí óýóðçìÜ ñò òðåíåðÜåé íá êáðåññÜðåé ôá ðáëÝðá ðíø åíðíäþæíñåé áðü ôí ôðåþ÷ïò ðñïóðåðáþáò. Äiðéäýåé åêüìá ôí firewall ñò;

Áðóðü áðëÜ óçíáþíåé ðùò Ý÷åé ÷ñçóéíðíéçèåß ôí iÝãéóôí üñéí êáðåññáþò (logging) ãéá áðóðü ôíí êáññíá. Í êáññíá ñò ßæéò åíâéíéðøåß íá åíðíäýåé, áéëÜ ååí èá óðÝéíåé ðéá içíýíåðå óðíí áñ÷åßí êáðåññáþò ôíð ðñïóðþíáþò ñé íá içäåíþóåðå ðÜëé ôíðò ìåðñçòÝò. Íðíñåðå íá içäåíþóåðå ôíðò ìåðñçòÝò ìå ôçí åíðëÞ

```
# ipfw resetlog
```

ÂíáæéáêðééÜ, ìðïñåßôå íá áðîÞóåðå ði üñéi êáðáãñáöÞð óðéò ñðèìßôåéò ðiõ ððñÞíá óáð iå ôçí áðéëíäÞ  
IPFIREWALL\_VERBOSE\_LIMIT üðùò ðåñéanÜøåiå ðáñáðÜiù. Ìðïñåßôå íá áéëÜíåôå áðóü ði üñéi (÷ùñßò íá  
ìåðáãëùðôßôåðå ðÜëé ðiõ ððñÞíá óáð êáé íá êÜíåôå reboot) ÷ñçóéiiðíéþíðå ôçí sysctl(8) óéíÞ  
net.inet.ip.fw.verbose\_limit.

**2. ÊÜðíëi ëÜeëò ðñÝðåé íá Ýæéfå. Áéïëíyèçóá ôéò áíðiëÝò êáðÜ ãñÜíà êáé ôþñá êëåéäþèçéá áðÝiù.**

Áðóüò iäçüò ðiðiëÝóåé üðé ÷ñçóéiiðíéåßôå ði userland-ppp, áé áðóü êé ié êáíüiåò ðiõ äßííóåé ÷ñçóéiiðíëiÝí ði tun0 interface, ðiõ áíðéóöié÷åß ôçí ðñþðç óýíååóç ðiõ öðéÜ÷íåðåé iå ði ppp(8) (áéëéþò áñúóðü êáé ùò user-ppp). Ç åðüìåíç óýíååç èá ÷ñçóéiiðíëiÝóå ði tun1, iåðÜ ði tun2 êáé ðÜåé ëÝaiíðåò.

Èá ðñÝðåé áððóçð íá ðiðiÜóåü üðé ði pppd(8) ÷ñçóéiiðíéåß ði interface ppp0, iðüðå áí áâééÍÞóåðå ôç óýíååóÞ óáð iå ði pppd(8) èá ðñÝðåé íá áíðéêáðåðóÞóåðå ði tun0 iå ppp0. ÐáñáðÜòù èá áâßííðiå Ýíá áýíëi ôñüði íá áéëÜíåôå ðiòð  
êáíüiåò ðiði firewall êáðÜëëçéá. Íé áñ÷ééiþ êáíüiåò óþæíóåé óá Ýíá áñ÷åßi iå üñíñá 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 êáðáæéÜâåôå áí ÷ñçóéiiðíéåßôå ði ppp(8) Þ ði pppd(8) ðiðiñåßôå íá áâåðÜóåôå ôçí Ýííäi ôçò ifconfig(8) áöïý  
âíâñäiðíéçéåß ç óýíååóÞ óáð. Ð.÷., ãéá iéá óýíååóç ðiði áíâñäiðíéþèçéå áðü ði pppd(8) èá áâßôå êÜðé óáí áðóü  
(áâß÷ñííóåé iüñi ié ó÷åðééÝò ãñáñiÝò):

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

Áðü ôçí Üëëç, ãéá iéá óýíååóç ðiði áíâñäiðíéþèçéå iå ði ppp(8) (user-ppp) èÜ ðñåðå íá áâßôå êÜðé ðáñüñíëi iå ði  
ðáñáðÜòù:

```
% 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.netmask 0xffffffff
        Opened by PID xxxxx
(skipped...)
```