

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 ÷ñçóéïïðïéýíôáé áðü ôïõò êåôåóéåõåóôÝò P ôïõò
ðùèçöÝò ôïõò æéá íá æéåéñßíïõí òá ðñïúùíôá ôïõò èåùñïýíôáé áìðïñéêÜ óýíâïï
åìöåíßæïïôáé óå áôôü ôï êåßìåïï êéá æéá úôåò áðü áôôÝò áïùñßæåé ç lïÜää ÁíÜðôôïçò ôï FreeBSD üöé
åßíáé ðéèáíüí íá åßíáé áìðïñéêÜ óýíâïï, éá äåßôå 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 ôôåéññéïÝíá, ðåñéãñÜöåé ôç ñýèïéôç åñüð
ôåß÷ïò ðñïóôåóßáò óå ieá óýíâåôç ïÝóù ôçëåöþíï ðïõ Ý÷åé äôïáïéêP IP æéåýèôïç. Áôôü ôï êåßìåïï äåí
áó÷ïëåßôåé iå ôï ðùò èá ñôèìßöåôå ôçí áñ÷éêP óåò óýíâåôç ïÝóù PPP. Äéá ðåñéóóùôåñåò ðëçñïïñßåò
ð÷åôéêÜ la ôéò ñôèìßöåéò ieáò óýíâåôçò ïÝóù PPP äåßôå ôç ôåëßää åïÞèåéåò ppp(8).

1 Ðñüëïïò

Áôôü ôï êåßìåïï ðåñéãñÜöåé ôçí æéåééåôå ðïõ ÷ñâéÜæåôåé æéá íá ñôèìßöåôå Ýá ôåß÷ïò ðñïóôåóßáò ôïï
FreeBSD üðáí ç IP æéåýèôïç åßíåôåé äôïáïéêÜ áðü ôï ISP óåò. Ðáñüëï ðïõ Ý÷ù ðñïóðåèÞóåé íá êÜñu áôôü ôï
êåßìåïï üöí ôï äôïáôüí ðéï ðëÞñåò êéá óùóôü, åßöôå åôôñüöåâéïé íá ôôåßëåôå ôéò äéïñßöåéò, ôá ó÷üëéá P ôéò
ðñïóðÜôåéò óåò ôôç æéåýèôïç ôïõ ôôäññåöÝá: <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 ðåñéóóùôåñåò ðëçñïïñßåò ó÷åôéêÜ la ôç iåôåâæþöôéôç ôïõ ðôñÞíá, äåßôå ôï òïÞíá ñôèìßöåñüí ôïõ ðôñÞíá ôïï
Åå ÷åéñßäéï (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 åíåñäïðïéÞóåôå ôçí ðôïóðÞñéïç æéá ôï
IPFW:

Óýíäåóç ÌÝóù Ôçëåöþüïõ êáé Ôåß÷ïò Ðñiöôáóþáò óôï FreeBSD

options IPFIREWALL

Åíåñäiðiéåß ôiī êþäéêá ôåß÷iõò ðñiöôáóßáò ôiõ ðõñþíá.

ÓcīlāBūóç: Áôðû ôî êâBíâlïí èåùñâB ûöô Ý-âôðâ åâéâôáôòPôáé ôçí Ýéäïöç 5.X ôîð FreeBSD P íéá ðéï ðññüöðâôç. Áí ÷ñçöéïí ðïéâBðâ ôçí Ýéäïöç 4.X, ôùöôå éå ðñYðâéå íå åíñâñïöíéPôáôå ôçí åðéëïäP *IPFW2* êâé íå åéâåâÜðâôå ôç ðåéBðâ åíPèäéåò ipfw(8) åéå ðâñéóöùôñâñô ðëçñïöññBðâó ô: åðééêÜ íå ôçí åðéëïäP *IPFW2*. ÐññïöYñôå éæéâBðâñâ ôî òiPíá *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFIREWALL_VERBOSE
```

ÓóÝéíåé óá ìçíýìáôá ãéá óá êáôÜëëçëá ðáêÝôá óöi log ôïõ óõóôÞìáöiò.

```
options IPFIREWALL_VERBOSE_LIMIT=500
```

ÂUæåé êÜðiéí üñéí óóéó öiñÝò ðiø êÜðiéá áâñáñåòP èá éâôáñäñUòâðåáé. òóé iðinâðßôð íá éâôáñäñUòâðåôð óâ íçýíâðåó áðü òi ôâß ÷iø ðññöôáðßáð ÷ùñßò ðiñ ëbñâðñí íá áâìßöiði ðá áñ ÷âßá éâôáññåòPò òiñ óôôðPìâðüò óâð áí áâ ÷âðßôð êÜðiéá âðßèåóç. Òi üñéí 500 íçíði Üòùí áâñáé ieá áñêåðÜ ëïâééP ôéiP, áëëÜ iðinâðßôð íá ðññöáññüóâðå áðôðP ôçí ôéiP áíÜeïäa ìå ðéð áðâéôðPòâðò ðiñ äééiy óâð äéêðyïò.

options IPDIVERT

Åíåññíðíéåß ôá *divert* sockets, ðíö èá äiýìå áññüôåñá ôé êÜíiñí.

ĐññéäéäiöiBíçóç: ìüëeo ôåéëåéþòåôå là ôéo ñòëèlBíðåéò êáé ôçí iàôåñäéþòôéóç ôïõ ðññíÞia óåò lçí èÜÍåôå åðåíåééBíçóç! Áí èÜÍåôå åðåíåééBíçóç óå åðôü ôï ôçìlåBí iòññåB íá êéåéäüèåBòå åðYùu áðü ôï óýôðçìÜ óåò. Đññååé íá åðñéïYíåôå iÝ: ñe íá ååééåôáôåèïý ié êáÍüíåò ôïõ ôåB÷ iõò ðññóåôåBåò êáé íá åíçìlåñùèïý üéá óå ò-åðééÜ áñ-åßá ñòëèlBíðåñü.

3 ÁeëááÝò óôï /etc/rc.conf áéá íá öiñôþíåôáé ôï ôåß÷iò ðñiöôáóßáò

Áéá íá áíâññïðíéåßôáé òï ôâß : ïò ðñïóðåóßåò êåðÜ òçí áåêëßíçöç òïò ñðóðßìáòïò êåé áéá íá ïñßóåðå òï áñ : áßï íå ôïòð êåíüíåò òïò ôâß : ïò ðñïóðåóßåò, ðñÝðåé íá áíçìåñßóåðå òï áñ : /etc/rc.conf. ÁðëÜ ðñïóðÝóåð ôéò ðåññåéÜòù ãññïÝò:

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

Áéá ðåñéóóüôðåñåò ðëçñïöñßåò ó÷åôééÜ íà ôç óçìáóßåò êáèåíéÜò áðü áôôÝò ôéò ãñáííÝò, ñßîòå ìéá ìáôéÜ óóïi /etc/default/rc.conf êáé áéáâÜôóâ ðçí man óåëßää rc.conf(5)

4 Áíåñäïöéþóôå ôçí ÁíóùìáôùìÝíç ìåôÜöñáóç Äéåöèýíóùí ôïõ PPP

Ãéá íá áðéôñ Ýóâóå óå Üééá iç÷ áíPiâóå ôiõ áéêôýïõ óåò íá óófâäÝíiöáé iå ôiï Ýìù êüöii lÝóù ôiõ FreeBSD, ÷ñçóëiïðiéþíôå òiù ùò “ðýéç”, éá ðñÝðåé íá áíâñäðiéþoâóå ôçí áíóùâóùí Ýíç iåôÜöñáóç áéâðeýíóâùí ôiõ PPP (NAT). Æá íá ábíráé áðóü, ðñiñöéÝóâóå ôiõ ãñ÷ábí /etc/rc.conf ôeò ðáññâéÜóù ãñâíí Ýó:

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

Óðóc ðe Ýðóc óið ðñiððæ _ðcð_ _ðyí_ ðaðcð ðñ Ýððæ íá að Úððæða ói ümíða ócð óyíðaððPð óáð, uððuð ói Ý ÷aðða aðiðeçðaðyðæ óðói áñ-ðaðBð /etc/ppp/ppp.conf.

5 Íé êáíüíåò ôïõ firewall

Ôi iuññ ðiññ áðññ Ýíåé óþþñá áßíáé íá iñþþñiñðlá ôiñðð êáññiñðá ôiñð firewall. Ié êáññiñðá ôiñðð iñðiñðñ ðåññéññ Üöiñðlá áðþp áßíáé áññéåðÜ êáéiñß áéá ôiñðð ðåññéóóüðåññiñðó ÷ñþþðåñð iñðð dialup óýññåóç, áéëÜ iýðá ðiññ ÷ñðåññééiñß áßíáé, iýðá áßíáé áðññáðñ íá óáññéññ Üæñðiñ iñð ðeð áññ Üäññåñð üeññ ðuñ ÷ñþþðóþp dialup. Iññiñý, üññò, íá ÷ñþþðéññýiñðiñ ñò Ýíå êáëü ðåññÜäññéññ iñðiñðóåññiñðó ðiññ IPFW êáé áßíáé ó ÷ñðåññéÜ áýññéiññ íá ðiññ ðiññóáññiñðóåññ ðoñðeð áéëÜ ðoñð óáó áññ Üäññåñð.

Áð að -þvítörlað ülluðó iá ðóðu áðáðéé Yðó að - Yðó áðuð öððáéðöý ðáð - ðvítörlodáðbáð. Já eððáéðöðu ðáð - ðvítörlodáðbáð áððáññáyáé éðaó' að - þrí êððeá óyíðaðc. Ið aéá - aéñéðöðbó ðiðññab yððóðñá ía ðvítörlé Yðóáé eáðuðið aéá ía áððéðn Yðóáé iðuññ óððáéðené Yðiðo ðoðiä Yðóáéð ía ðáññiðið aððu ði ðáð - ðvítörlodáðbáð. C ðeé ðoðiçééði Yðic óáðéñ Ü ðuññ eáðuññið óá Yðia eððáéðöðu ðáð - ðvítörlé: ðñpðá ié eáðuññið ðið aððéðn Yðiði iññéé Yðó ðoðiä Yðóáéð, eáé ðYðið ié eáðuññið ðið aððáññáyíði iðiðeáðaþðiða ðueéç óyíðaðc. C eëðáéðp ðbóñ aððu aððu ðáðiáü üððe ðñpðá aððæða ðiðð aððáññáyíði ðið aððéðn Yðiði ðññ Uðaáða ía ðáññiðið eáá yððóðñá üðða óá ðueéç aððáññáyíði ðiðð.

Áò ãïvýå ôbñá Ýíá ðánÜäåéãjá ôåß÷iøò ðñjöôáóßåò jå áñêåôÜ åðåçcäciáôéêÜ ó÷üééå.

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

```
# 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.
iface="fxp0"
```

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

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

Óýíääöç ÌÝóù Ôçëäöþüõ êáé Ôåß÷iò Ðñïóôáóßáò óöi 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
```

6 ÅñùôÞóåéò

1. ÂéÝðù íçíýíáôá üððù limit 500 reached on entry 2800 êáé ìåðÜ áððü áððü ôi óýðôçíÜ ñiø óôâíáôÜâé íá êáðâáñÜðâé ôá ðáéÝðá ðiø åiðïäßæíîôáé áððü ôi ôâß÷iø ðññiöðâóßâò. Äiøëåýâé áêüìá ôi firewall ñiø;

Áððùn áððÜ òçíáßíâé ðùò Ý÷âé ÷iñçöéñiððíéçðâß ôi ñYâéööñi ñiñçí êáðâáññâöÞò (logging) åéá áððù ôiñ êáññüá. Í êáññüáò i ßæíiø åiâéíiøðâé íá åiøëåýâé, åeëÜ åaií èá óôÝëíâé ðéá íçíýíáôá ôiñ áñ÷âßí êáðâáññâöÞò ôiø õððôÞíâòiø ñY÷ñé íá íçâáißðâôá ðÜéé ïiðò ìåðñçöÝð. ðiññâßðâá íá íçâáißðâôá ôiøò ìåðñçöÝð ìå ôçí åiññëÞ

```
# ipfw resetlog
```

Óýíäåóç ÌÝóù Ôçëåöþüô êáé Ôåß÷iò Ðñiöóáóßáò óoï FreeBSD

ÁíáæéåêôéêÜ, iðiñåbhôá íá áóíÞróåôá ði üñëí éåðåáññåðPò óðéð ñðøèìßóåéð ðið ððñÞíá óåð íå ðíçí áðééïäP
IPFIREWALL_VERBOSE_LIMIT üðùò ðåñéäñÜøåíå ðåñåðÜíü. Iðiñåbhôá íá áéëÜíåðå áðoü ði üñëí (÷ùñßò íá
íåðåáñëùðòßóåôá ðÜéé ðið ððñÞíá óåð êáé íá êÜíåðå reboot) ÷ñçöéïðiéþíðå ðíçí sysctl(8) óéïP
net.inet.ip.fw.verbose_limit.

2. ÊÜÐIËI ËÜÈIÖ ÐÑÝÐÄÉ ÍÁ ÝÄÉÍÁ. ÁÆIËIÝÈCÓÁ ÐÖÐ ÅÍÐIËÝÐ ËÁ ËÅÐÜ ÆÑÜHÁ ËÁÉ ÐÞÑÁ ËËÄÆÍÞÈCÉÁ ÅÐÝIÙ.

Áðóöùò i iäçüüò öðíèÝðåâé üöé ÷ñçóéiiðiéâßôå öi userland-*ppp*, æé áðóöù éé ié éáúíüåò ðiò äßiiíöáé ÷ñçóéiiðiéiýí öi tun0 interface, ðiò áíðéóöié ÷åß ööçí ðñþôç öýíäåóç ðiò ööéÜ ÷iåðåé iå öi ppp(8) (áæééþò áíûööù êáé ùò user-*ppp*). Ç åðüìåíç öýíäåóç èá ÷ñçóéiiðiéiýóå öi tun1, iåðÜ öi tun2 êáé ðÜåé Ýäííöåò.

Èá ðñÝðåé áðþbóç ð íá èðiÜöôå üöé ði pppd(8) ÷ñçóéiiðiéåb ði interface ppp0, iðüöôå áí iâééíÞóåôå ðc óýiâåðP óåô iâ ði pppd(8) èá ðñÝðåé íá áíôééâåóôÞóåôå ði tun0 iâ ppp0. ÐáñáéÜöôù èá áâðiññiði Ýíá áyéiði ôñüði íá áeëÜiåôå ðiðò èáfuiåò ðiðò firewall êáðÜëeçéá. Íe áñ ÷eéñið áfuiåò óþæiññiðé óá Ýíá áñ ÷âði iâ uññiâ 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 êáðåéÜâåôå áí ÷ñçóëiiðíéåbôå ôi ppp(8) P ôi pppd(8) ïðïñâbôå íá åiâôÜóåôå ôçí Ýiïäi ôçò ifconfig(8) áöïý åfâñäiðíéçéåß ç óýíäåóP óåò. D. ÷., ãéá iéá óýíäåóç ðïõ åiâñäiðíéPèçéå áðü ôi pppd(8) éá åâbôå êÜôé óáí áðôü (ååß ÷iïôéæ iüñ ié ó ÷åöééÝò ãñâiìÝò):

```
% ifconfig
  (skipped...)
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1524
        inet xxxx.xxxx.xxxx.xxxx --> xxxx.xxxx.xxxx.xxxx netmask 0xffff000000
  (skipped...)
```

Áðú ðíçí Úëëç, áæá íéá óýfåâðóç ðíð áíññáïðíéÞèçéâ íà ðí ppp(8) (*user-ppp*) èÜ ðññåðå íá åâðßöå èÜðé ðáññüìíéí íà ðí ðáññáéÜðú:

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