

Όγιάαός ΙΎού Όçäåöþñĩõ êáé Ôåß÷ĩò Ðñĩóôáóßàò óôĩ 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 \$

Ôĩ FreeBSD áβιάέ Υία éáôĩ÷õñùĩΥĩĩ àìðñééÛ óγìáĩēĩ ôĩõ FreeBSD Foundation.
ÐñēēΥò áðù óéò ēΥìáéò ð õñÛóáéò ïé ïðĩßàð ÷ ñçóéìĩðñēĩγìóáé áðù ôĩõò éáóáóéäåóáóðΥò ð ôĩõò
ðñēçðΥò ôĩõò áéá íá áéáēñßñĩôĩ óá ðñĩùũĩóá ôĩõò éåùññĩγìóáé àìðñééÛ óγìáĩēá. ¼ðĩò áóðΥò
àìðáíßæñĩóáé óá áðù òĩ éåßìáñĩ éáé áéá ùóáð áðù áóðΥò àìùñßæáé ç ììÛáá ÁíÛððõçò ôĩõ FreeBSD ùóé
åßìáé ðééáìĩ íá áβìáé àìðñééÛ óγìáĩēá, éá ååßðå Υία áðù óá óγìáĩēá: “TM” ð “®”.

Áðù òĩ Ûñēñĩ ðåñéåñÛóáé ðùð ìðñåßðå íá ñðēĩßóåðå Υία ôåß÷ĩò ðñĩóðáóßàð (firewall) ÷ ñçóéìĩðñēĩγìóáð
ìéá PPP óγìááç ìΎúò òçäåöþñĩõ óôĩ FreeBSD ìå òĩ IPFW. Ðéĩ óðæäēñēĩΥία, ðåñéåñÛóáé çç ñγēìéçç áìùð
ôåß÷ĩò ðñĩóðáóßàð óá ìéá óγìááç ìΎúò òçäåöþñĩõ ðñĩ Õ÷áé äñĩáíēēð IP áéåγēðñĩç. Áðù òĩ éåßìáñĩ åáí
áç÷ñēåßðáé ìå òĩ ðùð éå ñðēĩßóåðå ççí áñ÷ēēð óáð óγìááç ìΎúò PPP. Áéá ðåñéóóùðåñåð ðççññĩõñßàð
ó÷åðéēÛ ìå ðéð ñðēĩßóåðò ìéáð óγìááç ìΎúò PPP ååßðå çç óåßåå ãñðéåáð ppp(8).

1 Ðññēĩñĩò

Áðù òĩ éåßìáñĩ ðåñéåñÛóáé ççí áéååééáóßá ðñĩ ÷ñåéÛæåóáé áéá íá ñðēĩßóåðå Υία ôåß÷ĩò ðñĩóðáóßàð óôĩ
FreeBSD ùðáí ç IP áéåγēðñĩç åßìáóáé äñĩáíēēÛ áðù òĩ ISP óáð. Ðåñññēĩ ðñĩ Õ÷÷ ðñĩóðåðóáé íá ēÛù áðù òĩ
éåßìáñĩ ùóĩ òĩ äñĩáðñĩ ðéĩ ðēðñåð éáé óùóðù, åßóðå äððñùóåäðñē íá óðåßåðå ðéð äéññēðóáéð, óá ó÷ñēéá ð ðéð
ðññòÛóáéð óáð óçç áéåγēðñĩç òñĩ óðåññåðΥá: <marcs@draenor.org>.

2 ÐåñÛìåðññēé ôñõ ððñĩá

Áéá íá ìðñΥóåðå íá ÷ ñçóéìĩðñēĩγìóáð òĩ IPFW, ðñΥðåé íá áìóùìåðóåðå ççí ó÷åðéēð ððñòðññēĩç óôĩ ððñĩá óáð.
Áéá ðåñéóóùðåñåð ðççññĩõñßàð ó÷åðéēÛ ìå çç ìåðåðððéçç òñõ ððñĩá, ååßðå òĩ òñĩá ñðēĩßóåðò òñõ ððñĩá óôĩ
Åå÷åññåēĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éå ðñΥðåé íá
ðññéçΥóåðå ðéð ðåñåéÛð ðççññåð òñõ ñðēĩßóåðò òñõ ððñĩá óáð áéá íá áñåñåðñēĩγìóáð ççí ððñòðññēĩç áéá òĩ
IPFW:

```
options IPFIREWALL
```

Άίᾱñᾱīðīēāß òī ēþäēēá òâß÷ìðð Ññíóðáóßáð òīð ððñÞíá.

Όçíäßùóç: Ἀððü òī ēâßíáīī ēâùñâß üðē Ý÷âðâ ääēáðáððÞóáē òçí Ýēäīóç 5.X òīð FreeBSD Þ íēá ðēī ðñüðóðáðç. Áí ÷ñçóēīðīēâßðâ òçí Ýēäīóç 4.X, ðüðâ ēá ðñÝðâē íá áíᾱñᾱīðīēÞóâðâ òçí äðēēīäÞ IPFW2 ἑáé íá äēáâÜðâðâ òç óâēßäâ äīÞēäēáð ipfw(8) äēá ðññéóóüðâñâð ðēçñīðīñßâð ó÷âðēēÜ íâ òçí äðēēīäÞ IPFW2. ÑñíóÝíðâ ēäēáßðâñâ òī ðīÞíá *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFIREWALL_VERBOSE
```

ὈðÝēíäē óá íçýíáðá äēá óá ēáðÜēēçēá ðäēÝóá òòī log òīð óðóðÞíáðīð.

```
options IPFIREWALL_VERBOSE_LIMIT=500
```

ÄÜæäē ēÜðīēī üñēī óðēð öīñÝð ðīð ēÜðīēá äāññáðÞ ēá ēáðáññÜðâðäē. ϑóé ìðññâðâ íá ēáðáññÜðâðâ óá íçýíáðá áðü òī òâß÷ìð Ññíóðáóßáð ÷ùñßð òīī ēßíäðīī íá äâīßóíðí óá äñ÷âßá ēáðáññáðÞð òīð óðóðÞíáðüð óáð áí äâ÷ðâßðâ ēÜðīēá äðßēáóç. Òī üñēī 500 íçíðìÜðüí áßíäē íēá äñēâðÜ ēīäēēÞ ðēīÞ, äēēÜ ìðññâðâ íá ðñíóáññüóðâ áððÞ òçí ðēīÞ áíÜēīäâ íâ ðēð áðäēðÞóáēð òīð äēēýý óáð äēēðýīð.

```
options IPDIVERT
```

Άίᾱñᾱīðīēāß óá *divert* sockets, ðīð ēá äīýíâ äññüðâñâ ðē ēÜññí.

Ññíäēäīðīßçóç: ìüēðð ðäēäēððáðâ íâ ðēð ñðēìßðäēð ἑáé òçí ìððäâēððððēóç òīð ððñÞíá óáð *íçí ēÜíäðâ äðáíäēēßíçóç!* Áí ēÜíäðâ äðáíäēēßíçóç óá áððü òī óçíäßí ìðññâß íá ēēäēäüēâßðâ áðÝíü áðü òī óýóðçìÜ óáð. ÑñÝðâē íá ðññēíÝíðâ ìÝ÷ñē íá ääēáðáðáēíýí íē ēáíüíäð ðīð òâß÷ìðð Ññíóðáóßáð ἑáé íá áíçíᾱññüēíýí üēá óá ó÷âðēēÜ äñ÷âßá ñðēìßðâñí.

3 ἈēēáñÝò òòī /etc/rc.conf ἑáé íá öīññÞíáðäē òī òâß÷ìð ðñíóðáóßáð

Ἄēá íá áíᾱñᾱīðīēāßðäē òī òâß÷ìð Ññíóðáóßáð ēáðÜ òçí äēēßíçóç òīð óðóðÞíáðīð ἑáé ἑáé íá ññßóâðâ òī äñ÷âßí íâ òīðð ēáíñíäð òīð òâß÷ìðð ðñíóðáóßáð, ðñÝðâē íá áíçíᾱññóðâð òī äñ÷âßí /etc/rc.conf. ἈðēÜ ðñíóēÝóðâ ðēð ðññäēÜðü äñññÝð:

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

Ἄēá ðññéóóüðâñâð ðēçññīññßâð ó÷âðēēÜ íâ òç óçíáóßáð ēäēäīēÜð áðü áððÝð ðēð äñññÝð, ñßíðâ íēá íáðēÜ óòī /etc/defaults/rc.conf ἑáé äēáâÜðâð òçí man óâēßäâ rc.conf(5)

4 ĀíāñāĩōĩēPóoā ôcí ĀíóuìáôuìYíc ĩăôÜöñáóc Äéáõëýíóăuì ôĩö PPP

Ἄεά ἰά ἀδεὼν Ὑρᾶοᾶ ὁᾶ Ὑεᾶ ἰç ÷ αἰ Πῖαᾶ ὁῖο ἀεεὶ ὧῖο ὁᾶ ἰά ὁῖᾶ Ὑῖῖοᾶῖ ἰᾶ ὁῖᾶ Ὑῖῖοῖ ἰ Ὑῖῖοῖ ὁῖο FreeBSD, ÷ ἡç ὁῖῖοῖ ἰ ὁῖῖοῖ ὁᾶ ὁῖ ὐò “ðýç”, ἐᾶ ὁῖ Ὑῖᾶῖ ἰᾶ ἰᾶ ἰᾶ ἡῖῖοῖ ὁῖῖοῖ ὁç ἰᾶ ὁῖῖοῖ ἰᾶ Ὑῖç ἰᾶ ὁῖ Ὑῖᾶῖ ἰᾶ ὁῖ Ὑῖᾶῖ ὁῖο PPP (NAT). Ἄεά ἰᾶ ἰᾶ ἰᾶ ἰᾶ ὁῖ, ὁῖῖοῖ Ὑῖᾶῖ ὁῖῖοῖ ἰᾶ ÷ ἰᾶ /etc/rc.conf ὁῖᾶ ὁῖᾶ ὁῖᾶ ὁῖᾶ ἰᾶ ὁῖᾶ Ὑῖᾶῖ:

```
ppp_enable="YES"
ppp_mode="auto"
ppp_nat="YES"
ppp_profile="ᄀᄁᄂᄃᄄᄅᄆᄇᄈᄉᄊᄋᄌᄍᄎᄏᄐᄑᄒᄓᄔᄕᄖᄗᄘᄙᄚᄛᄜᄝᄞᄟᄠᄡᄢᄣᄤᄥᄦᄧᄨᄩᄪᄫᄬᄭᄮᄯᄰᄱᄲᄳᄴᄵᄶᄷᄸᄹᄺᄻᄼᄽᄾᄿᅀᅁᅂᅃᅄᅅᅆᅇᅈᅉᅊᅋᅌᅍᅎᅏᅐᅑᅒᅓᅔᅕᅖᅗᅘᅙᅚᅛᅜᅝᅞᅟᅠᅡᅢᅣᅤᅥᅦᅧᅨᅩᅪᅫᅬᅭᅮᅯᅰᅱᅲᅳᅴᅵᅶᅷᅸᅹᆀᆁᆂᆃᆄᆅᆆᆇᆈᆉᆊᆋᆌᆍᆎᆏᆐᆑᆒᆓᆔᆕᆖᆗᆘᆙᆚᆛᆜᆝᆞᆟᆠᆡᆢᆣᆤᆥᆦᆧᆨᆩᆪᆫᆬᆭᆮᆯᆰᆱᆲᆳᆴᆵᆶᆷᆸᆹᆺᆻᆼᆽᆾᆿᇀᇁᇂᇃᇄᇅᇆᇇᇈᇉᇊᇋᇌᇍᇎᇏᇐᇑᇒᇓᇔᇕᇖᇗᇘᇙᇚᇛᇜᇝᇞᇟᇠᇡᇢᇣᇤᇥᇦᇧᇨᇩᇪᇫᇬᇭᇮᇯᇰᇱᇲᇳᇴᇵᇶᇷᇸᇹሀሁሂሃሄህሆሇለሉሊላልሎሏሐሑሒሓሔሕሖሗመሙሚማሜምሞሟሠሡሢሣሤሦሧረሩሪራሬርሮሯሰሱሲሳሴስሶሷሸሹፀፁፂፃፄፅፆፇፈፉፊፋፌፍፎፏፐፑፒፓፔፕፖፘፙፚ፛፜፝፞፟፠፡።፣፤፥፦፧፨፩፪፫፬፭፮፯፰፱፲፳፴፵፶፷፸፹ᏀᏁᏂᏃᏄᏅᏆᏇᏈᏉᏊᏋᏌᏍᏎᏏᏐᏑᏒᏓᏔᏕᏖᏗᏘᏙᏚᏛᏜᏝᏞᏟᏠᏡᏢᏣᏤᏥᏦᏧᏨᏩᏪᏫᏬᏭᏮᏯᏰᏱᏲᏳᏴᏵ᏶᏷ᏸᏹ᐀ᐁᐂᐃᐄᐅᐆᐇᐈᐉᐊᐋᐌᐍᐎᐏᐐᐑᐒᐓᐔᐕᐖᐗᐘᐙᐚᐛᐜᐝᐞᐟᐠᐡᐢᐣᐤᐥᐦᐧᐨᐩᐪᐫᐬᐭᐮᐯᐰᐱᐲᐳᐴᐵᐶᐷᐸᐹᑀᑁᑂᑃᑄᑅᑆᑇᑈᑉᑊᑋᑌᑍᑎᑏᑐᑑᑒᑓᑔᑕᑖᑗᑘᑙᑚᑛᑜᑝᑞᑟᑠᑡᑢᑣᑤᑥᑦᑧᑨᑩᑪᑫᑬᑭᑮᑯᑰᑱᑲᑳᑴᑵᑶᑷᑸᑹᒀᒁᒂᒃᒄᒅᒆᒇᒈᒉᒊᒋᒌᒍᒎᒏᒐᒑᒒᒓᒔᒕᒖᒗᒘᒙᒚᒛᒜᒝᒞᒟᒠᒡᒢᒣᒤᒥᒦᒧᒨᒩᒪᒫᒫᒭᒮᒯᒰᒱᒲᒳᒴᒵᒶᒷᒸᒹᓀᓁᓂᓃᓄᓅᓆᓇᓈᓉᓊᓋᓌᓍᓎᓏᓐᓑᓒᓓᓔᓕᓖᓗᓘᓙᓚᓛᓜᓝᓞᓟᓠᓡᓢᓣᓤᓥᓦᓧᓨᓩᓪᓫᓬᓭᓮᓯᓰᓱᓲᓳᓴᓵᓶᓷᓸᓹᔀᔁᔂᔃᔄᔅᔆᔇᔈᔉᔊᔋᔌᔍᔎᔏᔐᔑᔒᔓᔔᔕᔖᔗᔘᔙᔚᔛᔜᔝᔞᔟᔠᔡᔢᔣᔤᔥᔦᔧᔨᔩᔪᔫᔬᔭᔮᔯᔰᔱᔲᔳᔴᔵᔶᔷᔸᔹᕀᕁᕂᕃᕄᕅᕆᕇᕈᕉᕊᕋᕌᕍᕎᕏᕐᕑᕒᕓᕔᕕᕖᕗᕘᕙᕚᕛᕜᕝᕞᕟᕠᕡᕢᕣᕤᕥᕦᕧᕨᕩᕪᕫᕬᕭᕮᕯᕰᕱᕲᕳᕴᕵᕶᕷᕸᕹᖀᖁᖂᖃᖄᖅᖆᖇᖈᖉᖊᖋᖌᖍᖎᖏᖐᖑᖒᖓᖔᖕᖖᖗᖘᖙᖚᖛᖜᖝᖞᖟᖠᖡᖢᖣᖤᖥᖦᖧᖨᖩᖪᖫᖬᖭᖮᖯᖰᖱᖲᖳᖴᖵᖶᖷᖸᖹᗀᗁᗂᗃᗄᗅᗆᗇᗈᗉᗊᗋᗌᗍᗎᗏᗐᗑᗒᗓᗔᗕᗖᗗᗘᗙᗚᗛᗜᗝᗞᗟᗠᗡᗢᗣᗤᗥᗦᗧᗨᗩᗪᗫᗬᗭᗮᗯᗰᗱᗲᗳᗴᗵᗶᗷᗸᗹᘀᘁᘂᘃᘄᘅᘆᘇᘈᘉᘊᘋᘌᘍᘎᘏᘐᘑᘒᘓᘔᘕᘖᘗᘘᘙᘚᘛᘜᘝᘞᘟᘠᘡᘢᘣᘤᘥᘦᘧᘨᘩᘪᘫᘬᘭᘮᘯᘰᘱᘲᘳᘴᘵᘶᘷᘸᘹᙀᙁᙂᙃᙄᙅᙆᙇᙈᙉᙊᙋᙌᙍᙎᙏᙐᙑᙒᙓᙔᙕᙖᙗᙘᙙᙚᙛᙜᙝᙞᙟᙠᙡᙢᙣᙤᙥᙦᙧᙨᙩᙪᙫᙬ᙭᙮ᙯᙰᙱᙲᙳᙴᙵᙶᙷᙸᙹ ᚁᚂᚃᚄᚅᚆᚇᚈᚉᚊᚋᚌᚍᚎᚏᚐᚑᚒᚓᚔᚕᚖᚗᚘᚙᚚ᚛᚜᚝᚞᚟ᚠᚡᚢᚣᚤᚥᚦᚧᚨᚩᚪᚫᚬᚭᚮᚯᚰᚱᚲᚳᚴᚵᚶᚷᚸᚹᛀᛁᛂᛃᛄᛅᛆᛇᛈᛉᛊᛋᛌᛍᛎᛏᛐᛑᛒᛓᛔᛕᛖᛗᛘᛙᛚᛛᛜᛝᛞᛟᛠᛡᛢᛣᛤᛥᛦᛧᛨᛩᛪ᛫᛬᛭ᛮᛯᛰᛱᛲᛳᛴᛵᛶᛷᛸ᛹ᜀᜁᜂᜃᜄᜅᜆᜇᜈᜉᜊᜋᜌᜍᜎᜏᜐᜑᜒᜓ᜔᜕᜖᜗᜘᜙᜚᜛᜜᜝᜞ᜟᜠᜡᜢᜣᜤᜥᜦᜧᜨᜩᜪᜫᜬᜭᜮᜯᜰᜱᜲᜳ᜴᜵᜶᜷᜸᜹ᝀᝁᝂᝃᝄᝅᝆᝇᝈᝉᝊᝋᝌᝍᝎᝏᝐᝑᝒᝓ᝔᝕᝖᝗᝘᝙᝚᝛᝜᝝᝞᝟ᝠᝡᝢᝣᝤᝥᝦᝧᝨᝩᝪᝫᝬ᝭ᝮᝯᝰ᝱ᝲᝳ᝴᝵᝶᝷᝸᝹កខគឃងចឆជឈញដឋឌឍណតថទធនបផពភមយរលវឝឞសហឡអឣឤឥឦឧឨឩឪឫឬឭឮឯឰឱឲឳ឴឵ាិីឹ᠀᠁᠂᠃᠄᠅᠆᠇᠈᠉᠊᠋᠌᠍᠎᠏᠐᠑᠒᠓᠔᠕᠖᠗᠘᠙᠚᠛᠜᠝᠞᠟ᠠᠡᠢᠣᠤᠥᠦᠧᠨᠩᠪᠫᠬᠭᠮᠯᠰᠱᠲᠳᠴᠵᠶᠷᠸᠹᡀᡁᡂᡃᡄᡅᡆᡇᡈᡉᡊᡋᡌ
```

Όδες εΥος οιο δῆλῖοββ_ος_όγύῖααόςο δῆΥῖαε ῖα ἁῦεαοἶ οἰ ὑῖῖἁ ὅςο ὅγύῖααόςο οαό, ὑδουο οἰ Υ÷ἁοἶ ἁῖεεεἶἁῖοἶ
 ὁῖἱ ἁῖ÷ἁῖ / etc/ppp/ppp.conf.

5 ĩé êáíüíãò ôĩõ firewall

Òi iun òrò aḡn Ýíáé ḡpná áβíáé íá iñβóíoiá òíòò éafúíáð òíò firewall. Íé éafúíáð òíòò íðíβòð ðáñéáñÜóíoiá áap áβíáé áñéáñÜ éáfíβ áéá òíòò ðáñéóóuðáñíòð ÷ ñPóðáð íá dialup óýíááóc, áééÜ íýðá òðí ÷ ñáñóééíβ áβíáé, íýðá áβíáé áðíáðuí íá ðáéñéÜæíóí íá óéð áíÜáéáð uéuí òuí ÷ ñçóðíí dialup. Ìðñíýí, uíuð, íá ÷ ñçóéíáyóíóí uð Ýíá éáéu ðáñÜáééáíá ñóéíβóáuí òíò IPFW éáé áβíáé ó÷ áðééÜ ávéíéí íá òíòò ðñíóáñíuóáðá óéðð áééÝð óáð áíÜáéáð.

Ἄν ἀν÷Βοιῶτα υἱὸν τὰ οὐρ ἀαοεῖΥδ ἀν÷Υδ ἀφὺδ ἐεᾶεοῖρ οἶβ÷τῶδ θνιῶδαοβᾶδ. τὰ ἐεᾶεοῦ οἶβ÷τῶδ θνιῶδαοβᾶδ
 ἀδαῖνᾱγᾱε εᾶδ' ἀν÷Πῖ εὔεᾶ οὔγᾱαῶς. Ἰ αἷα÷αἷνεοῶδῶδ ἰθῖνᾱβ γῶδᾱᾱ τὰ θνιῶεΥῶε εᾱφῖτᾱδ αἷα τὰ ἀδεὼνΥῶε ἰυτῖ
 οἶαεᾱεἷεΥῖτᾱδ οὔγᾱΥῶαδ τὰ θᾱνῖΥῖτᾱ ἀδῦ οἱ οἶβ÷τῶδ θνιῶδαοβᾶδ. Ç δει οὔτσεοῖΥῖτς οᾱεἷῶ οἱ εᾱφῖτῖ οᾱ Υῖτᾱ
 ἐεᾶεοῦ οἶβ÷τῶδ ᾱβῖᾱε: θηῶα ἰε εᾱφῖτᾱδ θῖο ἀδεὼνΥῶτῖοἱ ἰᾱεεῖΥδ οὔγᾱΥῶαδ, εᾱε οὔεῖο ἰε εᾱφῖτᾱδ θῖο ἀδαῖνᾱγῖοἱ
 ἰθῖεᾱβῖοῖδᾱ ὕεες οὔγᾱαῶς. Ç εῖᾱεῖβ ὀβῶν ἀδῦ ἀοῶν ᾱβῖᾱε υἱε θηῶα ἀΥᾱεᾱδ οἱοδ εᾱφῖτᾱδ θῖο ἀδεὼνΥῶτῖοἱ θηῶᾱῖαδ
 τὰ θᾱνῖοἱοἱ εᾱε γῶδᾱᾱ υἷε οᾱ ὕεᾱ ἀδαῖνᾱγῖοῖε ἀοῶῖαδᾱ.

[illegible]

Áò àìvìà òpñá Ýía ðánÜäæëià òàß÷iõð ðñiíóôáoßáò ià áñêáoÜ äðáicãciáoééÜ 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
```

Όπná Ý÷áoá Ýía ðēēçñüíÝíí óåβ÷ìð ðñüóóáóβáo, òì ìðìβì óðíaÝóáéð óðéð èýñåð 22 éáé 80 éáé éáoáåñÜöåé üēåð óéð Üēēåð óðíaÝóáéð óôi åñ÷åβì éáoáåñåððò òìò óóóðßíåðìð. ÐēÝíí åβóðå Ýðìēñē áéå åðáíåēēßçóç. Ôì óåβ÷ìð ðñüóóáóβáo éå áíåñåñðēçēåß áóðüííåð éáé éå òñòðóåé òìò éåíüíåð ðìò ðñìóēÝóáóå. Áí åå åβíåé áóðü ð Ý÷áoå ððēååððìòå ðñíåçßåðå, ð áí Ý÷áoå èÜðēåð ðñìÜóáéð áéå íå áéññēñēåß áóðü òì Üñēñì, åðēēñēñìßóåå íåæß ììò íå email.

6 Åñüòßóåéò

1. ÅēÝðü ìçíýíåð üðüð limit 500 reached on entry 2800 éåé ìåðÜ áðü áóðü òì óýóóçìÜ ììò óåííåðÜåé íå éáoáåñÜöåé óå ðåÝóå ðìò åìðñåññíåðåé áðü òì óåβ÷ìð ðñüóóáóβáo. Åìçåýåé åéñüå òì firewall ììò;

Áóðü áðēÜ óçíåñíåð ðüð Ý÷å ðñóéññðēçēåß òì ìÝåóòì ùñēñ éáoáåñåððò (logging) áéå áóðü òì éåíüíå. Ì éåíüíåð ì ðåñð áíåññññåß íå åìçåýåé, åēÜ ååñ éå óóÝñíå ðéå ìçíýíåð óôi åñ÷åβì éáoáåñåððò òìò óóóðßíåðìð ìÝ÷ñé íå ìçåññóåðå ðÜēé òìò ìåñçóÝð. Ìðñåßåå íå ìçåññóåðå òìò ìåñçóÝð ìå òçííññåð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òì ùñéì éáóáññáöðò óóέò ñòèìβóáέò òìò ðòñáíá óáo ìá òçì áðέέìáÐ IPFWALL_VERBOSE_LIMIT ùðòò ðáñέáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òì ùñéì (÷ ùñβò íá ìáðááèòóðβóáðá ðÛέέ òì ðòñáíá óáo éάέ íá èÛíáðá reboot) ÷ ñçóέììðìéáðáð òçì sysctl(8) óéìÐ net.inet.ip.fw.verbose_limit.

2. ÈÛðìéì èÛèò ðñÝðáé íá Ýáέíá. Áέèìéçóá óέò áíòèÝð éáoÛ ãñÛíá éάέ òþñá èéáέäþèçéá áðÝñ.

Áðóóò ì ìäçáùð òðìèÝðáé ùðé ÷ ñçóέììðìéáβóá òì *userland-ppp*, áé áðóó èé ìé éáfííáð ðìò áβñíóáé ÷ ñçóέììðìéíýì òì tun0 interface, ðìò áíóέóðìé÷ áβ óðçì ðñþòç óýíááóç ðìò óðέÛ÷ íáðáé ìá òì ppp(8) (áέέéðò áñóóó èάέ ùð *user-ppp*). Ç áðñíáç óýíááóç éá ÷ ñçóέììðìéíýóá òì tun1, ìáðÛ òì tun2 éάέ ðÛáé èÝáñíóáð.

Èá ðñÝðáé áðβóçò íá èòìÛóðá ùðé òì pppd(8) ÷ ñçóέììðìéáβ òì interface ppp0, ìðóðá áí ìáέέíáóáðá òç óýíááóÐ óáo ìá òì pppd(8) éá ðñÝðáé íá áíóέéáóóðβóáðá òì tun0 ìá ppp0. ÐáñáέÛóó èá ááβñíóìá Ýíá áýέèè ðñóðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éáoðÛέçéá. Ìé áñ÷έέìβ éáfííáð òþæííóáé óá Ýíá áñ÷áβ ìá ùññá 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
```

Άέά íá éáðáέÛááðá áí ÷ ñçóέììðìéáβóá òì ppp(8) Ð òì pppd(8) ìðññáβóá íá áñáðÛóáðá òçì Ýññáì òçò ifconfig(8) áóñý áñáñáñðìéçéáβ ç óýíááóÐ óáo. Ð.÷., áέά ìéá óýíááóç ðìò áñáñáñðìéçéçéá áðó òì pppd(8) éá ááβðá èÛóέ óáí áðóó (ááβ÷ñíóáé ìñì ìé ò÷áðέéÝð ãñáñìÝð):

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

Άðó òçì Ûέçç, áέά ìéá óýíááóç ðìò áñáñáñðìéçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá èÛóέ ðáñññéì ìá òì ðáñáέÛóó:

```
% 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 0xffffffff00
    Opened by PID xxxxx
(skipped...)
```