

## Help with IPFW + NATD + Passive FTP

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2004-11/3129.html>

---

*From:* James A. Coulter ([jacoulter\\_at\\_jacoulter.net](mailto:jacoulter_at_jacoulter.net))

*Date:* 11/28/04

Date: Sun, 28 Nov 2004 09:42:51 -0600

To: Freebsd-Questions <[freebsd-questions@freebsd.org](mailto:freebsd-questions@freebsd.org)>

Hoping someone can provide a solution to the following problem:

I am using a FBSD 4.10 box as a gateway/router/firewall between a cable modem and my home lan and its been working great for several months. All machines behind my firewall are able to connect to the outside world for http, e-mail, ping, ssh, and active ftp transfers

Last night I installed FBSD 4.10 on a box behind the firewall. The installation went fine, but when I attempted to install some packages via the FBSD ports collection I ran into the known problem establishing passive FTP connections through IPFW with NATD enabled. I am able to establish ftp connections, but when the client switches to passive mode the connection hangs. So I am unable to use the ports collection or cvsup on the FBSD box behind the firewall

I have been googling for several hours and found lots of references, but all the solutions I have found appear to be about allowing passive FTP connections on the box running IPFW and NATD (which my ruleset already allows - no problems using ports or cvsup from the gateway/router/firewall). I've tried several different configurations in the IPFW ruleset, but so far no luck.

Here is my IPFW ruleset and my rc.conf. Hoping someone can point out the error of my ways.

TIA,

Jim

```
#!/bin/sh
```

```
##### Start of IPFW rules file #####
```

```
# Flush out the list before we begin.
```

```
ipfw -q -f flush
```

```
# Set rules command prefix
```

```
cmd="ipfw -q add"
```

## freebsd-questions: Help with IPFW + NATD + Passive FTP

```
skip="skipto 800"
pif="dc1" # public interface name of Nic card
        # facing the public internet

#####
# No restrictions on Inside Lan Interface for private network
# Change xl0 to your Lan Nic card interface name
#####
$cmd 005 allow all from any to any via dc0

#####
# No restrictions on Loopback Interface
#####
$cmd 010 allow all from any to any via lo0

#####
# check if packet is inbound and nat address if it is
#####
$cmd 014 divert natd ip from any to any in via $pif

#####
# Allow the packet through if it has previous been added to the
# the "dynamic" rules table by a allow keep-state statement.
#####
$cmd 015 check-state

#####
# Interface facing Public internet (Outbound Section)
# Interrogate session start requests originating from behind the
# firewall on the private network or from this gateway server
# destine for the public internet.
#####

# Allow out access to my ISP's Domain name server.
# x.x.x.x must be the IP address of your ISP's DNS
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
$cmd 020 $skip udp from any to 193.0.14.129 53 out via $pif keep-state
$cmd 021 $skip udp from any to 68.1.18.25 53 out via $pif keep-state
$cmd 022 $skip udp from any to 68.10.16.30 53 out via $pif keep-state
$cmd 023 $skip udp from any to 68.105.161.20 53 out via $pif keep-state
$cmd 024 $skip tcp from any to 193.0.14.129 53 out via $pif setup
keep-state
$cmd 025 $skip tcp from any to 68.1.18.25 53 out via $pif setup
keep-state
$cmd 026 $skip tcp from any to 68.10.16.30 53 out via $pif setup
keep-state
$cmd 027 $skip tcp from any to 68.105.161.20 53 out via $pif setup
keep-state
# Allow out access to my ISP's DHCP server for cable/DSL configurations.
$cmd 030 $skip udp from any to 172.19.17.22 67 out via $pif keep-state
```

## freebsd-questions: Help with IPFW + NATD + Passive FTP

```
# Allow out non-secure standard www function
$cmd 040 $skip tcp from any to any 80 out via $pif setup keep-state

# Allow out secure www function https over TLS SSL
$cmd 050 $skip tcp from any to any 443 out via $pif setup keep-state

# Allow out send & get email function
$cmd 060 $skip tcp from any to any 25 out via $pif setup keep-state
$cmd 061 $skip tcp from any to any 110 out via $pif setup keep-state

# Allow out FBSD (make install & CVSUP) functions
# Basically give user root "GOD" privileges.
$cmd 070 $skip tcp from me to any out via $pif setup keep-state uid root
$cmd 071 $skip tcp from me to any out via $pif setup keep-state uid
jacoulter

# Tried this to allow passive ftp from behind firewall - didn't work
#$cmd 073 $skip tcp from any to any out via $pif setup keep-state uid root
#$cmd 074 $skip tcp from any to any out via $pif setup keep-state uid
jacoulter

# Allow out ping
$cmd 080 $skip icmp from any to any out via $pif keep-state

# Allow out Time
$cmd 090 $skip tcp from any to any 37 out via $pif setup keep-state

# Allow out nntp news (IE: news groups)
$cmd 100 $skip tcp from any to any 119 out via $pif setup keep-state

# Allow out FTP
$cmd 104 $skip tcp from any to any 20 out via $pif setup keep-state
$cmd 105 $skip tcp from any to any 21 out via $pif setup keep-state
$cmd 106 $skip tcp from any to any 1024-65000 out via $pif setup
keep-state

# Allow out FTP rules from
http://lantech.geekvenue.net/chucktips/jason/chuck/1023340076/index.html
# Didn't work
#$cmd 107 add pass log tcp from any 1024-65535 to any 49152-65535
#$cmd 108 add pass log tcp from any to any 21 in recv $pif setup
keep-state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
$cmd 110 $skip tcp from any to any 22 out via $pif setup keep-state

# Allow out whois
$cmd 120 $skip tcp from any to any 43 out via $pif setup keep-state
```

## freebsd-questions: Help with IPFW + NATD + Passive FTP

```
# Allow ntp time server
$cmd 130 $skip udp from any to any 123 out via $pif keep-state

#####
# Interface facing Public internet (Inbound Section)
# Interrogate packets originating from the public internet
# destined for this gateway server or the private network.
#####

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16 to any in via $pif #RFC 1918
private IP
$cmd 301 deny all from 172.16.0.0/12 to any in via $pif #RFC 1918
private IP
$cmd 302 deny all from 10.0.0.0/8 to any in via $pif #RFC 1918
private IP
$cmd 303 deny all from 127.0.0.0/8 to any in via $pif #loopback
$cmd 304 deny all from 0.0.0.0/8 to any in via $pif #loopback
$cmd 305 deny all from 169.254.0.0/16 to any in via $pif #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24 to any in via $pif #reserved for
doc's
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif #Sun cluster
$cmd 308 deny all from 224.0.0.0/3 to any in via $pif #Class D & E
multicast

# Deny ident
$cmd 315 deny tcp from any to any 113 in via $pif

# Deny all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
$cmd 320 deny tcp from any to any 137 in via $pif
$cmd 321 deny tcp from any to any 138 in via $pif
$cmd 322 deny tcp from any to any 139 in via $pif
$cmd 323 deny tcp from any to any 81 in via $pif

# Deny any late arriving packets
$cmd 330 deny all from any to any frag in via $pif

# Deny ACK packets that did not match the dynamic rule table
$cmd 332 deny tcp from any to any established in via $pif

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type.
# Only necessary for cable or DSL configurations.
# This rule is not needed for 'user ppp' type connection to
# the public internet. This is the same IP address you captured
# and used in the outbound section.
$cmd 360 allow udp from 172.19.17.22 to any 68 in via $pif keep-state
```

## freebsd-questions: Help with IPFW + NATD + Passive FTP

```
# Allow in standard www function because I have apache server
# $cmd 370 allow tcp from any to me 80 in via $pif setup limit src-addr 2
$cmd 375 allow tcp from any to me 8888 in via $pif setup limit src-addr 2

# Allow in secure FTP, Telnet, and SCP from public Internet
$cmd 380 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Allow TCP FTP control channel in & data channel out
# Added from www.freebsd-howto.com/HOWTO/Ipfw-Advanced-Supplement-HOWTO
# Attempting to get passive FTP to work
# Didn't work
# $cmd 381 allow tcp from any to any 21 in via $pif setup keep-state limit
src-addr 4
# $cmd 382 allow tcp from any 20 to any 1024-49151 out via $pif setup
keep-state limit src-addr 4

# Allow in any from jacoulter.net
# $cmd 385 allow tcp from 66.226.64.13 to me in via $pif setup limit
src-addr 2
# $cmd 385 allow tcp from www.jacoulter.net to me in via $pif setup limit
src-addr 2
$cmd 385 allow tcp from 66.226.64.13:20 to me in via $pif setup limit
src-addr 2

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID & PW are passed over public
# internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
# $cmd 390 allow tcp from any to me 23 in via $pif setup limit src-addr 2

# Reject & Log all unauthorized incoming connections from the public
internet
$cmd 500 deny log all from any to any in via $pif

# Reject & Log all unauthorized out going connections to the public internet
$cmd 550 deny log all from any to any out via $pif

# This is skipto location for outbound stateful rules
$cmd 800 divert natd ip from any to any out via $pif
$cmd 801 allow ip from any to any

# Everything else is denied by default
# deny and log all packets that fell through to see what they are
$cmd 999 deny log all from any to any

##### End of IPFW rules file #####

-----

# rc.conf
# -- sysinstall generated deltas -- # Sun Jul 4 10:40:48 2004
```

## freebsd-questions: Help with IPFW + NATD + Passive FTP

```
# Created: Sun Jul 4 10:40:48 2004
# Enable network daemons for user convenience.
# Please make all changes to this file, not to /etc/defaults/rc.conf.
# This file now contains just the overrides from /etc/defaults/rc.conf.
hostname="sara.mshome.net"
ifconfig_dc1="DHCP"
ifconfig_dc0="inet 192.168.1.1 netmask 255.255.255.0"
firewall_enable="YES"
firewall_script="/etc/ipfw.rules"
firewall_logging="YES"
kern_securelevel_enable="NO"
linux_enable="YES"
moused_enable="YES"
named_enable="YES"
nfs_client_enable="YES"
nfs_reserved_port_only="YES"
nfs_server_enable="YES"
sendmail_enable="NONE"
sshd_enable="YES"
usbd_enable="YES"
ntpd_enable="YES"
inetd_enable="YES"
gateway_enable="YES"
natd_enable="YES"
natd_interface="dc1"
natd_flags="-dynamic"
apache_enable="YES"

--
James A. Coulter
jacoulter@jacoulter.net
http://jacoulter.net

```

---

```
freebsd-questions@freebsd.org mailing list
http://lists.freebsd.org/mailman/listinfo/freebsd-questions
To unsubscribe, send any mail to "freebsd-questions-unsubscribe@freebsd.org"
```