

## Re: ipfw forward bug?

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2005-12/msg00129.html>

---

- *From:* "mitrohin a.s." <swp@xxxxxxxxxx>
  - *Date:* Tue, 27 Dec 2005 11:23:22 +0600
- 

On Tue, Dec 27, 2005 at 02:38:18AM +0600, mitrohin a.s. wrote:

> helo.

>

> i have strange problem with forward rule.

>

> isp1 +-----+

> <-----[fxp0:x.x.x.1/24] router\_1 [re0:10.200.1.1/24]-----+

> | [xl2:10.4.2.1/24]----+ |

> +-----+ ||

> +-----+ ||

> | host\_1 [10.4.2.121/24]-----+ |

> +-----+ |

> |

> isp2 +-----+ |

> <-----[xl2:172.16.42.2/24] router\_2 [re0:10.200.1.2/24]-----+

> +-----+

>

> router\_1 propagate defaultroute via fxp0 (isp1) for local network.

> router\_2 have link via xl2 to isp2 and defaultroute to 10.200.1.1.

> i want to lead external traffic of host\_1 via isp2, but have got

> trouble.

>

>

> router\_2 ipfw rules:

>

> root@main# ipfw -c show

> 00100 321246 89176165 allow via lo0

> 00200 40 2000 deny { src-ip 127.0.0.0/8 or dst-ip 127.0.0.0/8 }

> 00400 7226 231262 allow dst-ip 224.0.0.0/4

> 00500 354153 88470867 allow src-ip 10.0.0.0/8 dst-ip 10.0.0.0/8

> 00600 0 0 check-state

>

> 00700 65 5460 skipto 50000 log proto icmp dst-ip 10.4.2.121 in keep-state

> 00800 0 0 skipto 50000 log proto icmp dst-ip 10.4.2.121 out keep-state

> 00900 0 0 skipto 50000 log proto icmp src-ip 10.4.2.121 in keep-state

> 01000 0 0 skipto 50000 log proto icmp src-ip 10.4.2.121 out keep-state

>

> 01800 133396 44504758 allow

>



## Re: ipfw forward bug?

```
>  
> send-pr?
```

and more interesting things here...

router\_2 ipfw rules:

```
table 1 – internal networks  
root@main# ipfw table 1 list  
10.0.0.0/8 0  
83.246.130.168/32 0  
83.246.136.144/28 0  
172.16.0.0/12 0  
192.168.0.0/16 0
```

```
table 2 – hosts routed via isp2  
1 – allow make connection to external world self  
root@main# ipfw table 2 list  
10.1.3.23/32 1  
10.1.3.68/32 1  
10.1.3.69/32 1  
10.1.3.87/32 0  
10.1.3.100/32 1  
10.1.3.199/32 1  
10.1.3.200/32 1  
10.4.2.121/32 0  
this is transit hosts for router_2 and traverse chain "in" of rules.
```

```
root@main# ipfw -c show  
allow via lo0  
deny { src-ip 127.0.0.0/8 or dst-ip 127.0.0.0/8 }  
allow dst-ip 224.0.0.0/4  
allow src-ip table(1) dst-ip table(1)  
check-state  
skipto 50000 proto icmp dst-ip table(2) in keep-state  
skipto 50000 src-ip table(2,1) in keep-state  
skipto 50000 proto tcp dst-ip 10.1.3.87 dst-port 21,25,80,110,143 in keep-state  
skipto 50000 proto tcp dst-ip 10.4.2.121 dst-port 80,443 in keep-state  
deny dst-ip table(2) in  
allow  
fwd 172.16.42.1 src-ip table(2) in  
allow  
deny ip from any to any
```

this is work for host 10.1.3.83 but not work for host 10.4.2.121.  
i dont see difference between 10.1.3.87 and 10.4.2.121. may be  
defaultroute overlap route with 10.4.2.121 only.

```
root@main# uname -a  
FreeBSD main.uni-altai.ru 6.0-RC1 FreeBSD 6.0-RC1 #0: Sun Oct 16 19:37:36 OMSST 2005  
swp@xxxxxxxxxxxxxxxxxxx:/usr/obj/usr/src/sys/ea_kernel i386
```

Re: ipfw forward bug?

Re: ipfw forward bug?

sorry for my terrible english.

/swp

---

freebsd-net@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxxxx"

---

• **References:**

◆ ***ipfw forward bug?***

◇ *From:* mitrohin a.s.

- Prev by Date: ***Re: Router on 6.0-stable fails to route tcp packets due to NAT?? malfunction***
- Next by Date: ***Re: Router on 6.0-stable fails to route tcp packets due to NAT?? malfunction***
- Previous by thread: ***ipfw forward bug?***
- Index(es):
  - ◆ ***Date***
  - ◆ ***Thread***