

Re: divert , ipfw question

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2004-09/0382.html>

From: Nickolay A. Kritsky (*nkritsky_at_star-sw.com*)

Date: 09/28/04

Date: Tue, 28 Sep 2004 14:23:56 +0400

To: Zrelli Saber Ben Mohamed <zrelli@jaist.ac.jp>

Hello Zrelli,

the rule 65000 allow ip from any to any stops processing of a packet,
so it will never reach diverting rule 65100.

see man ipfw about rule-processing

Tuesday, September 28, 2004, 2:08:36 PM, Zrelli Saber Ben Mohamed wrote:

ZSBM> Hi ,

ZSBM> I'm interested in the "divert" mechanism and want to try it out ,
ZSBM> so I recompiled the kernel (FreeBSD 5.2.1-RELEASE #0) after adding the
ZSBM> IPDIVERT option and then added the needed lines in the rc.conf file,
ZSBM> after that , I set up ipfw to divert packets to some port
ZSBM> here is my ipfw rule set .

ZSBM> 00100 allow ip from any to any via lo0
ZSBM> 00200 deny ip from any to 127.0.0.0/8
ZSBM> 00300 deny ip from 127.0.0.0/8 to any
ZSBM> 65000 allow ip from any to any
ZSBM> 65100 divert 5000 ip from any 22 to me <----- the divert rule
ZSBM> 65535 deny ip from any to any

ZSBM> then, I wanted to monitor the diverted traffic using tcpdump :

ZSBM> \$ tcpdump port 5000

ZSBM> when I do a telnet connection to the port 22 from a remote host , I was
ZSBM> expecting that tcpdump will display packets diverted to the port 5000 by
ZSBM> ipfw.

ZSBM> The remote host I use shows that it connects to port 22 and the ipfw
ZSBM> divert rule seems not to work.

ZSBM> I can set another rule to block the traffic in the port 22 , and it works.

ZSBM> only the divert rule seems to fail.

ZSBM> I wrote some piece of code using divert socket to read packets from the

freebsd-hackers: Re: divert , ipfw question

ZSBM> divert port , but no result ...

ZSBM> I think I'm missing something ,

ZSBM> so please enlighten my mind ...

ZSBM> Many Thanks

ZSBM> --

ZSBM> Saber

--

Best regards,
; Nikolay A. Kritsky
; SysAdmin STAR Software LLC
; mailto:nkritsky@star-sw.com

freebsd-hackers@freebsd.org mailing list

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

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@freebsd.org"

freebsd-net@freebsd.org mailing list

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

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