

Re: src/etc/rc.firewall simple \${fw_pass} tcp from any to anyestablished

Re: src/etc/rc.firewall simple \${fw_pass} tcp from any to anyestablished

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2006-11/msg00029.html>

- *From:* Alexander Leidinger <Alexander@xxxxxxxxxxxxxx>
 - *Date:* Sat, 11 Nov 2006 21:32:55 +0100
-

Quoting "R. B. Riddick" <arne_woerner@xxxxxxxxxx> (from Sat, 11 Nov 2006 11:00:49 -0800 (PST)):

----- "Julian H. Stacey" <jhs@xxxxxxxxxxxxxxxxxx> wrote:

I tried adding
\${fwcmd} add pass tcp from any to any established
from src/etc/rc.firewall case - simple. Which solved it.
But I was scared, not understand what the established bit did, &
how easily an attacker might fake something, etc.
I found adding these tighter rules instead worked for me
\${fwcmd} tcp from any http to me established in via tun0
\${fwcmd} tcp from me to any http established out via tun0
Should I still be worrying about established ?

Hmm... I personally use "check-state" and "keep-state", so that it is not enough to fake the "established" flags, but the attacker had to know the ports, the IPs, control over routing in pub inet(?) and some little secrets in the TCP headers (I dont know exactly how it works):

```
add check-state
add pass icmp from any to any keep-state out xmit tun0
add pass tcp from any to any setup keep-state out xmit tun0
add pass udp from any to any domain keep-state out xmit tun0
```

These are the stats of the first 7 rules on my DSL line afer one day:

```
00100 6423992 376898110 allow ip from any to any via lo0
00200 0 0 deny ip from any to 127.0.0.0/8
00300 0 0 deny ip from 127.0.0.0/8 to any
20000 0 0 check-state
30000 10013 1047483 deny tcp from any to any established
30100 226 45640 deny ip from any to any not verrevpath in
30200 7 280 deny tcp from any to any tcpoptions !mss setup
```

Another nice rule (stats after one day):

```
30800 3149862 117471324 deny ip from any to 0.0.0.0/8,169.254.0.0/16,192.0.2.0/24,224.0.0.0/4,240.0.0.0/4
via tun0
```

Re: src/etc/rc.firewall simple \${fw_pass} tcp from any to anyestablished

Re: src/etc/rc.firewall simple \${fw_pass} tcp from any to anyestablished

Bye,
Alexander.

--

Committees have become so important nowadays that subcommittees have to be appointed to do the work.

<http://www.Leidinger.net> Alexander @ Leidinger.net: PGP ID = B0063FE7

<http://www.FreeBSD.org> netchild @ FreeBSD.org : PGP ID = 72077137

freebsd-security@xxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"