

weird queue keep-state behavior

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-02/0013.html>

From: Mikhail (*vip3r_at_inbox.ru*)

Date: 02/15/05

To: freebsd-security@freebsd.org

Date: Tue, 15 Feb 2005 20:08:47 +0300

I'm just one of those weirdos, who wanna make a powerfull queues shaper (not QoS but near) with ipfw2 on their freebsd 4.x-stable.

My server is using frequently used configuration with NAT+FW ADSL router with one external ip on external network interface (we're using ADSL modem in bringe mode).

I've configured single pipe, configured queues to use that pipe, add queues with different weights distinct on destination ports.

<skipped rules for lo0, antispoof rules, couple of counts>

//i'm doing nat with that rules:

```
03400 divert 8668 ip from { 192.168.132.0/24,192.168.10.0/24,172.16.1.0/24,10.10.10.0/24 or me } to any out via bfe0
```

```
03600 divert 8668 ip from any to me in via bfe0
```

<antispoof rules, icmp restricts, internal interface allow, allow incuming keep-state connections to services>

//here are defined queues

```
09600 queue 1 udp from me to any dst-port 53,123 out via bfe0 keep-state
```

```
09800 queue 2 tcp from any 1024-65535 to any out via bfe0 iptos lowdelay iplen 32-68 established
```

```
10000 queue 2 tcp from any 1024-65535 to any out via bfe0 iptos lowdelay established
```

```
10200 queue 2 tcp from any 1024-65535 to any out via bfe0 iptos lowdelay setup keep-state
```

```
10400 queue 3 tcp from any 1024-65535 to any dst-port 22,194,5190,23 out via bfe0 iplen 32-68 established
```

```
10600 queue 3 tcp from any 1024-65535 to any dst-port 22,194,5190,23 out via bfe0 established
```

```
10800 queue 3 tcp from any 1024-65535 to any dst-port 22,194,5190,23 out via bfe0 setup keep-state
```

```
11000 queue 4 tcp from any 1024-65535 to any dst-port 21,80,8080,443,8101,8081 out via bfe0 iplen 32-68 established
```

```
11200 queue 4 tcp from any 1024-65535 to any dst-port 21,80,8080,443,8101,8081 out via bfe0 established
```

```
11400 queue 4 tcp from any 1024-65535 to any dst-port 21,80,8080,443,8101,8081 out via bfe0 setup keep-state
```

```
11600 queue 5 tcp from any 1024-65535 to any out via bfe0 iplen 32-68 established
```

```
11800 queue 5 tcp from any 1024-65535 to any out via bfe0 established
```

```
12000 queue 5 tcp from any 1024-65535 to any out via bfe0 setup keep-state
```

```
12200 queue 6 udp from any 1024-65535 to any out via bfe0 keep-state
```

```
12400 allow tcp from any to 192.168.132.0/24,192.168.10.0/24,172.16.1.0/24,10.10.10.0/24 in via bfe0 established
```

FreeBSD-Security: weird queue keep-state behavior

//last rule is for weird packets that natd is pushing to the stack

When client is downloading file via passive ftp from nat'ed internal network he has
\${ADSL_INBOUND_SPEED} speed (55KByte/s)

Here is the problem:

When i ssh'ing to server and starting the SAME connection with wget i'm having only 14KByte/s.

Hitting many times "ipfw show" i've discovered that in the first case counters of 12000 rule are incrementing slowly and counters of rule 12400 are incrementing very fast. In the second case only counters of rule number 12000 are incrementing relative to the first case fast.

So here is the question:

Should I remove "keep-state" statement and use stateless firewall with adding "esablished" rules or this is bug (that tracking state of data flow in queue in both directions is bad, because in that case we limiting speed of inbound connection and outbound too (last is desired)).

Thanks beforehand.

PS: I can post here my rc.firewall on demand or exec what you want me to exec.

freebsd-security@freebsd.org mailing list

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

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