

Re: ipfw rules vs routes to localhost?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2003-05/0109.html>

From: Crist J. Clark (crist.clark_at_attbi.com)

Date: 05/28/03

Date: Wed, 28 May 2003 14:03:59 -0700

To: Paul Chvostek <paul@it.ca>

On Wed, May 28, 2003 at 12:51:54AM -0400, Paul Chvostek wrote:

>

> *I'm considering:*

>

> *ipfw add N deny ip from a.b.c.d to any*

>

> *vs.*

>

> *route add -host a.b.c.d localhost*

>

> *I need to block traffic to a number of IP addresses. I thought I'd use*

> *ipfw to avoid things like UDP DNS lookups that might come in and take up*

> *resources while my system tried to respond, but it's been suggested on*

> *another list that setting routes to localhost will use less resources.*

> *Ideally, I'd like to be able to block a few tens of thousands of IPs.*

>

> *What's the scoop?*

Someone is assuming the old rule for blocking traffic on a (Cisco) router applies to the FreeBSD stack. It doesn't necessarily apply.

First off, blocking it in ipfw rules is obviously more efficient if you are running ipfw(8) already.

If you wouldn't be otherwise running ipfw(8) at all, there *may* be some gain. Packets blocked by ipfw(8) get dropped very early in ip_input(), which is good, but *all* packets have to go through ipfw(8), and we usually assume the majority of packets are "good" ones. So, the second case, adding the route, doesn't add much overhead to the processing of good packets, but does greatly increase the resources used before you toss out bad ones. You may end up using fewer resources if there are only a few bad ones relative to the good.

IMHO, if this machine is a firewall, use the right tool for firewalling, ipfw(8). Are you short on resources in the first place? If you are really pushing this machine's routing capabilities to its

freebsd-net: Re: ipfw rules vs routes to localhost?

max, you might be in need of an OS and hardware designed solely for routing. Tinkering with ipfw(8) versus blackhole routes probably is not the way to solve the problem.

--

Crist J. Clark		cjclark@alum.mit.edu
		cjclark@jhu.edu
http://people.freebsd.org/~cjc/		cjc@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"