

Re: IPFILTER_DEFAULT_BLOCK & No route to host

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2003-09/0845.html>

From: Justin (justin_at_othius.com)

Date: 09/30/03

Date: Tue, 30 Sep 2003 11:09:39 -0400 (EDT)

To: Dag-Erling Smørgrav <des@des.no>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Tue, 30 Sep 2003, Dag-Erling [iso-8859-1] Smørgrav wrote:

> *echelon* <e_chelon@yahoo.com> writes:

>> *However, I use the following rules for the internal network interface (xl1)*

>>

>> *# Group 9000 (internal network interface)*

>> *block return-rst in log quick on xl1 proto tcp from any to 192.168.x.x/32 port = 23 group 9000*

>> *block return-rst in log quick on xl1 proto tcp from any to 192.168.x.x/32 port = 21 group 9000*

>> *pass in quick on xl1 all group 9000*

>>

>> *With these rules, I believe I should able to ping and SSH the*

>> *freebsd box from my internal network no matter the option*

>> *IPFILTER_DEFAULT_BLOCK is set or not.*

>

> *You're only letting traffic *in*. You're not letting anything *out*.*

> *TCP, like love, is a two-way street.*

And if you want to keep it that way from a connection, rather than packet, point of view, use the "keep state" option on your pass in rule.

--Justin

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.3 (FreeBSD)

iD8DBQE/eZy5dYQBw9Ox1VgRAkU/AJwNwMUIP5A+H/+T0+jkh1y1CSncjQCgrn9

n6nmL3eMWM7NgW2pp6DhkCs=

=LOX9

-----END PGP SIGNATURE-----

freebsd-stable@freebsd.org mailing list

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

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

Re: IPFILTER_DEFAULT_BLOCK & No route to host