

Re: Routing for a Virtual Server in Checkpoint

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-09/msg00279.html>

- *From:* "Jean-François Gobin" <jf-no-spam-for-me@xxxxxxxxxxx>
 - *Date:* Sun, 17 Sep 2006 11:31:56 +0200
-

Hello there,

In fact it depends if you're doing prenat or postnat. One of them doesn't require routes at all, but beware ... you may need to review your entire rulebase (prenat is doing the NAT or de-NAT on the input interface ...postnat on the output interface). That's what they call "client side natting" or "server side natting".

Also, don't forget that manual natting exits at the first match, when automatic nat can do two rules (source and destination).

The routes you have to insert in the OS are only to determine "to which interface should this packet be sent". Quite logical if you think that the address in question may be connected to the outside interface or even to no interface (case of a "pure virtual network").

"Automatic ARP" is there only to ensure that the NAT address can be resolved to a physical (ie ethernet) address. Without that, you'll have to insert proxy ("permanent public" in term of BSD) arp for each nat (static or hide) you can have ... or insert host routes in your outside router.

The best thing to do is to play a bit with prenat, postnat and stuff like that. Only with that you can decide if you go for it or not.

Regards,
Jean-Francois

"Greg Hennessy" <me@xxxxxxxxxxx> a écrit dans le message de news:
r10qg295ag5gr3c13vu2fsjpdu5chkvlg@xxxxxxxxxxx

On Sun, 17 Sep 2006 07:05:04 +0000 (UTC),
larstr@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx wrote:

Will <westes-usc@xxxxxxxxxxxxxxxxxxx> wrote:

Re: Routing for a Virtual Server in Checkpoint

With newer versions of Checkpoint you can also use "client side natting" to avoid the need for such manual routing.

You still need it on some NGX platforms when working with manual nat rules & VIPs on different subnets.

greg

--

Wühle täglich in der Scheisse,
und niemand weiss, wie ich heisse.
Es gibt nur einen, der mich kennt,
und mich bei meinem Namen nennt.