pfSense - Feature #1136

Add logic to automatically avoid route-to for static route networks

12/27/2010 10:11 AM - Jim Pingle

Status:	New		**Start date:**	12/27/2010
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:	Rules / NAT		**Estimated time:**	0.00 hour
Target version:				

Description

If pfSense is in use as an intermediate router (multiple networks on LAN and WAN directly connected or reachable by directly connected routers with static routes), this scenario is broken on upgrade.

We add reply-to on the WAN rules now, even for networks that are "local". It can be disabled on a per-rule basis but on upgraded configurations routing will be broken until every relevant rule is edited and has that box checked.

We may need a bit more logic when applying reply-to on an interface's rules, skipping it automatically for rules that refer to directly reachable networks. If not overall, at least in upgrade code.

History

#1 - 12/27/2010 12:32 PM - Jim Pingle

Note that this was hit when someone upgraded from a 1.2-RELEASE box. 1.2.2/1.2.3 had a global reply-to disable checkbox, which doesn't seem to exist on 2.0.

It would still make sense to automatically skip/disable reply-to for local networks when possible.

#2 - 12/27/2010 12:47 PM - Chris Buechler

We already automatically bypass reply-to for directly connected subnets via a kernel patch, have since 1.2.3 (at least). The only diff from 1.2.3 is the missing checkbox to disable reply-to globally, which will be a regression on upgrade for some installs. Restoring that will resolve this.

#3 - 12/27/2010 01:15 PM - Jim Pingle

Seth's router was hitting reply-to for a network reachable via static route, so there may still be a bug then.

#4 - 12/27/2010 01:28 PM - Chris Buechler

Oh, there is no handling of networks reachable via routers other than the gateway on that interface. Just have to disable reply-to in that case.

#5 - 12/27/2010 01:38 PM - Jim Pingle

- Tracker changed from Bug to Feature

- Subject changed from Intermediate router scenario broken on upgrade to 2.0 due to reply-to to Add logic to automatically avoid route-to for static route networks

- Target version changed from 2.0 to 2.1

- Affected Version changed from 2.0 to All

Yeah after looking it over some more and in light of it coming from 1.2-RELEASE I've changed the description a bit. It might be nice to automatically detect and avoid this in the future but as long as the behavior is consistent with 1.2.x. The missing global reply-to disable is a regression for sure, I'll open another ticket for that and push this off as a nice-to-have feature for 2.1.

#6 - 10/20/2012 09:32 AM - Chris Buechler

- Target version deleted (2.1)