pfSense - Bug #2163

1:1 NAT Reflection helper rules do not cover static route subnets

02/03/2012 11:43 AM - Jim Pingle

Status:	Resolved	**Start date:**	02/03/2012
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	NAT Reflection	**Estimated time:**	0.00 hour
Target version:	2.1		
Plus Target Version:		**Affected Version:**	2.0.1
Release Notes:	Default	**Affected Architecture:**	

Description

If you enable NAT reflection for 1:1 NAT and also the outbound NAT rules to assist 1:1 NAT, the resulting rules only cover the LAN subnet.

If you try to reach the public IP of a 1:1 NAT entry from a static route subnet, it doesn't work properly.

For example on a LAN of 192.168.66.x with a static route on LAN to 192.168.77.x the resulting rule for a 1:1 NAT targeting 192.168.66.5 is:

```
nat on em1 from 192.168.66.0/24 to 192.168.66.5 -> em1 port 1024:65535
```

But it should have one entry per subnet reachable on that interface, such as:

```
nat on em1 from 192.168.66.0/24 to 192.168.66.5 -> em1 port 1024:65535
nat on em1 from 192.168.77.0/24 to 192.168.66.5 -> em1 port 1024:65535
```

Associated revisions

Revision 1716682b - 02/04/2012 04:30 AM - Erik Fonnesbeck

Add static route subnets if their gateway is within the source subnet for the nat rule. Ticket #2163

Revision b9f637a7 - 02/04/2012 06:14 AM - Erik Fonnesbeck

Add nat rule if the target is in a subnet handled by a static route whose gateway is in the interface's subnet. Ticket #2163

Revision aa8d9918 - 02/04/2012 06:41 AM - Erik Fonnesbeck

Add static route subnets if their gateway is within the source subnet for the nat rule. Ticket #2163

Revision 530b980c - 02/04/2012 06:41 AM - Erik Fonnesbeck

Add nat rule if the target is in a subnet handled by a static route whose gateway is in the interface's subnet. Ticket #2163

History

#1 - 02/04/2012 02:42 AM - Erik Fonnesbeck

It appears that this only happens when the gateway referenced by the static route is directly reachable (on the same subnet) by the NAT target. The target gets an ICMP redirect and caches the return route, bypassing the router on the reply. If the gateway to route to 192.168.77.x is not on 192.168.66.x, it routes fine without the extra NAT, since no route gets pushed for a gateway that is not directly reachable on its subnet.

Based on this, only the subnets for static routes whose gateway lies in the same subnet will need to be added to the nat line.

#2 - 02/04/2012 06:49 AM - Erik Fonnesbeck

- Status changed from New to Feedback

It should be good now with these two fixes and the one just before them for a separate related issue.

#3 - 07/05/2012 06:27 PM - Jim Pingle

- Status changed from Feedback to Resolved