pfSense - Bug #2042

NAT reflection doesn't apply to self-initiated traffic

12/09/2011 06:38 AM - Anonymous

Status:	Confirmed	**Start date:**	12/09/2011
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:	NAT Reflection	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	All	**Affected Architecture:**	All

Description

Squid can't access hosts inside a DMZ with DMZ hosts accessible only via 1:1 NAT.

My config:
- 4 interfaces: WAN (bge1), LAN (bge0), DMZ (em0), GUEST (em1)
- DMZ subnet is private ips, using 1:1 NAT and IP Alias with reflection redirects to map incoming traffic from the other interfaces and from the internet onto my public webservers

rules from the rules.debug:

1. Reflection redirects and NAT for 1:1 mappings
   rdr on { bge0 em0 em1 } from any to aaa.bbb.ccc.ddd -> 192.168.ccc.ddd bitmask
   no nat on em0 from em0 to 192.168.ccc.ddd
   nat on em0 from 192.168.ccc.ddd/27 to 192.168.ccc.ddd -> em0 port 1024:65535

I suppose adding the loopback interface (lo0?) to the "rdr on" rule would fix this issue.

A slightly longer version of this text can be found on the forum here: http://forum.pfsense.org/index.php/topic,43613.0.html

Best regards,
-Jan

History

#1 - 12/09/2011 04:44 PM - Chris Buechler

- Priority changed from Urgent to Normal

#2 - 09/16/2015 02:10 AM - Chris Buechler

- Subject changed from 1:1 NAT rdr rules don't apply to loopback interface (squid) to NAT reflection doesn't apply to self-initiated traffic

- Category changed from Rules/NAT to NAT Reflection

- Status changed from New to Confirmed

- Priority changed from Normal to Low

- Affected Version changed from 2.0 to All

Anything initiated from the firewall itself (squid, other possibilities) doesn't hit reflection. It's more complicated than adding lo0, that won't do anything in this case. Not a common need.