pfSense - Bug #1813

Static routes on WAN interfaces overridden by route-to for firewall-initiated traffic

08/22/2011 05:50 PM - Chris Buechler

Status:	Confirmed	**Start date:**	08/22/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	All	**Affected Architecture:**	

Description

the 'pass out' rules such as:

pass out route-to (em1 9.2.2.1) from 9.2.3.17 to !9.2.2.0/21 keep state allow-opts label "let out anything from firewall host itself"

Break connectivity from the firewall itself to any networks reachable via a static route on a WAN for traffic initiated from the firewall itself.

For example if you add a static route in the above scenario pointing 1.0.0.0/24 to 9.2.3.20, traffic initiated from the firewall to that destination will go to 9.2.2.1, not 9.2.3.20.

Associated revisions

Revision 75eb2012 - 09/27/2008 11:31 PM - Chris Buechler

run hostap later in script, fixes ral(4) card difference in FreeBSD 7.0. Works with ath(4) also.

Ticket #1813

History

#1 - 08/22/2011 06:01 PM - Chris Buechler

- Priority changed from Normal to High

#2 - 08/22/2011 06:11 PM - Chris Buechler

floating rules can work around this

#3 - 11/06/2016 01:03 AM - Jim Thompson

- Assignee set to Jim Pingle

- Priority changed from High to Normal

Can't be "high", it's five years old.

JimP, please reeval to see if this is still and issue.

#4 - 11/09/2016 02:06 PM - Jim Pingle

- Status changed from New to Confirmed

- Assignee deleted (Jim Pingle)

- Affected Version changed from 2.0 to All

It is still an issue but it can be easily worked around by adding a floating rule to pass outbound to the destination network.

We could automatically add rules behind the scenes for static route destinations on WAN-type interfaces that do not use the interface gateway if we wanted, but given that the situation is so rare, we may just want to document the quirk and let the user choose to add the workaround if they need it.