pfSense - Bug #1841

TCP state issue when traffic passing through a GRE tunnel within IPSEC

09/06/2011 03:03 AM - Nigel Wright

Status:	Duplicate	**Start date:**	09/06/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Interfaces	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Version:**	
Release Notes:		**Affected Architecture:**	

Description

When running a GRE tunnel between two Pfsense 2.0 RC3 TCP traffic is shown as having its SYN/ACK packets dropped on the returning firewall.
This has been established in two scenarios.

Scenario 1 GRE tunnel between WAN interfaces, IPSEC in transport mode between the two WAN interfaces. Ping works fine TCP sessions have SYN/ACK packets dropped on the returning firewall. When IPSEC is disabled everything works fine.

Scenario 2 IPSEC tunnel between LAN interface addresses, GRE tunnel bound to LAN interface. Ping works fine TCP SYN/ACK packets dropped on return.

History

#1 - 09/06/2011 03:52 AM - Chris Buechler

- Category set to Interfaces

- Target version deleted (2.0)

#2 - 02/27/2012 03:51 PM - Jim Pingle

- Status changed from New to Feedback

Is this happening on 2.0.1? Does it happen only with GRE or also with GIF?

We have a few people running with that sort of config and I don't recall seeing any issues like this in the process, but I think most of the ones I saw were using GIF, not GRE.

#3 - 02/27/2012 05:10 PM - Nigel Wright

- File Pfsense_GRE.zip added

It's still happening in 2.0.1. I've just set up a test bed, two sites Site A and Site B each with a pfsense firewall with a link between them. With only GRE tunnel established it's possible to ping from site A to site B and telnet from a server in site A to the server in Site B as seen in a packet capture (GRE_ONLY_WAN.cap).

With IPSEC enabled in transport mode between the two firewall WAN IPs pinging from the site A server to the Site B server works fine but telnet no longer does. The screenshot SITE_B_SVR-2012-02-27-22-06-58.png shows the site B firewall rejecting the TCP:SA syn ack packets and the TELNET_Reject.cap shows the return packets coming from the site B server and the firewall responding with a destination unreachable.

The two firewall configs are also included.

I've not tried it with GIF interfaces only with GRE.

#4 - 03/19/2012 08:31 AM - stephane stephane

I've got exactly the same issue. The main reason for me to use this configuration, is to be able to have VPN and dynamic routing protocol between multiple sites.

#5 - 06/20/2012 05:44 AM - Colin Petrie

I have the same problem as well, over gif tunnels as well as gre.

I use IPSEC transport mode between the CARP WAN IPs of pfsense pairs at each end. Then have a PtP Gif or Gre on top of that, and then use either static routes or OSPF down the tunnel.

Pings work fine, but again TCP SYN/ACK packets dropped on return.

#6 - 06/20/2012 05:45 AM - Colin Petrie

Sorry, should have mentioned, both pairs of firewalls are running 2.0.1

#7 - 06/26/2012 01:44 PM - Martin Saini

Hi! Have setuped the same config - same issue here :(soo is there any "manual" workaround to that?

#8 - 07/03/2012 03:48 AM - Colin Petrie

Martin Saini wrote:

> Hi! Have setuped the same config - same issue here :(soo is there any "manual" workaround to that?

I managed to get ours working by adding a 'floating' rule in the web interface. We have an allow all rule already on the GRE interface, but the state tracking seemed broken on this, I found a hint somewhere saying to add an allow all 'floating' rule, with interface set to the GRE interface, and direction set to any. Also, note that both the rule on the GRE interface, and the floating rule have advanced option 'State Type' set to 'none'.

looking at the generated pf rules, the following two rules result from this:
pass quick on gre0 all no state label "USER_RULE: Allow all traffic over xxxx"
pass in quick on gre0 all no state allow-opts label "USER_RULE: Allow all internal xxxx traffic"

The first rule us the floating rule, it seems to be the one that makes it work. So I guess there's something funny about it that make the direction (in) bit on the second rule be insufficient.

Hope this helps

#9 - 08/23/2012 06:41 AM - Martin Saini

Hi! Thanks for the info - i will configure that as in one of my next projects, as i have to configure some tunneling stuff with fortinet and cicso. in the meantime i was using openvpn between pfSense Firewalls!

thx alot
m.

#10 - 09/16/2015 06:15 PM - Chris Buechler

- Status changed from Feedback to Duplicate

- Affected Version deleted (2.0)

duplicate of #4479

Files

Pfsense_GRE.zip	121 KB	02/27/2012	Nigel Wright