pfSense - Bug #4479

Firewall rules won't match GRE interface after applying IPSEC transport encryption on GRE tunnel

02/27/2015 03:25 PM - Jonathan Black

Status:	New	**Start date:**	02/27/2015
Priority:	Normal	**Due date:**	
Assignee:	Luiz Souza	**% Done:**	0%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	Future		
Affected Version:	All	**Affected Architecture:**	All

Description

I have an issue with IPSEC where my GRE tunnels work fine until I turn on transport encryption with IPSEC. After IPSEC is enabled, I can ping across the tunnel (I can also ping between the hosts on both ends), but any connections across the tunnel will be blocked by the PFSense router on the far end (It appears that none of my rules match anymore and only the default block rule will match). I have been able to reproduce this bug in a physical and virtual environment (I have it running in Hyper-V and can produce that if you wish). Everything will start working correctly again if I disable IPSEC on both ends of the tunnel.

I've attached the backup files for both R1 and R2 PFsense routers. They are configured just as show in the Network Map attached. The GRE tunnel is not shown on the map. R1's GRE interface is 192.168.112.1/24. R2's GRE interface is 192.168.112.2/24. The 192.168.25.X network is the WAN interfaces on the routers with the 172.X.X.X interfaces are the LAN interfaces. The default password is "pfsense" on these.

I've also attached pictures of my firewall rules (Allow Everything) and then pictures of the log where an RDP connection is being blocked.

Please let me know if there is anything else I can do to help provide you additional information.

History

#1 - 09/15/2015 11:23 PM - Chris Buechler

- Category changed from IPsec to Operating System

- Status changed from New to Confirmed

- Assignee set to Chris Buechler

- Affected Version changed from 2.2 to 2.2.x

this is an issue, end up with state mismatches. Can work around with floating rules w/sloppy state and any TCP flags.

Needs review on stock FreeBSD 11 to see if it's been fixed yet.

#2 - 09/18/2015 09:51 PM - Chris Buechler

this doesn't appear to happen on stock FreeBSD 11 unless there's something more to it than a single pass rule with keep state. Need to evaluate further to determine if it's still an issue in 2.3/10-STABLE.

#3 - 06/20/2016 05:37 PM - Jorge Albarenque

I can confirm this still happens with both GRE and GIF tunnels over IPsec on pfSense 2.3.1

#4 - 07/08/2016 10:37 PM - Chris Buechler

- Assignee deleted (Chris Buechler)

- Affected Version changed from 2.2.x to All

#5 - 11/28/2016 09:12 PM - Jim Thompson

- Assignee set to Jonathan Black

yet another case where we lost track of the bug because Chris just removed himself when he left.

assigned back to original reporter to see if it still occurs. assign to me if still valid on 2.3.2 or later.

#6 - 11/29/2016 04:47 AM - Jorge Albarenque

I can confirm this still occurs on 2.3.2. Probably worth checking on 2.4 since Chris had mentioned it seemed to be resolved on FreeBSD 11

#7 - 11/29/2016 11:07 AM - Jonathan Black

Jorge Albarenque wrote:

> I can confirm this still occurs on 2.3.2. Probably worth checking on 2.4 since Chris had mentioned it seemed to be resolved on FreeBSD 11

It is broken in 2.4 as well.

#8 - 11/29/2016 11:15 AM - Jonathan Black

It appears to be worse than before now too.... ICMP doesn't work across the tunnel now either.

#9 - 11/29/2016 11:16 AM - Jim Pingle

Testing on 2.4 won't be reliable until #6937 is fixed.

#10 - 12/01/2016 11:54 AM - Jonathan Black

Jim Pingle wrote:

> Testing on 2.4 won't be reliable until #6937 is fixed.

Apparently this only affects mobile IPSEC. Is this still applicable?

After some further testing, ICMP does work across the tunnel (Windows Firewall tricked me), but TCP connections are still being blocked (I can see it in the log)

#11 - 03/14/2017 02:25 PM - Phil Lavin

Has anyone managed to test on 2.4 yet? Experiencing this issue in 2.3 latest.

#12 - 03/16/2017 09:18 AM - Phil Lavin

Confirmed still not working on 2.4

#13 - 03/21/2017 10:44 AM - Brett Howard

This affects both GRE over IPSEC transport and IPSEC tunnel mode carrying a GRE

All traffic exiting the GRE tunnel is seen as coming from the host itself and matched by the following rule inserted by filter.inc, which comes way before any user rules:

1. let out anything from the firewall host itself and decrypted IPsec traffic
   pass out {$log['pass']} inet all keep state allow-opts tracker {$increment_tracker($tracker)} label "let out anything IPv4 from firewall host itself"

It is therefore impossible to filter traffic coming in across the GRE at all and state is not created for the return traffic on the GRE interface.

The 'workaround' of creating a floating rule on GRE with sloppy state, combined with the matching above effectively means no firewall at all on the GRE tunnel and is not an accepable solution!

Tested on the latest 2.4 snapshot:
2.4.0-BETA (amd64)
built on Tue Mar 21 07:14:38 CDT 2017
FreeBSD 11.0-RELEASE-p8

#14 - 03/22/2017 10:19 AM - Jim Thompson

- Assignee changed from Jonathan Black to Luiz Souza

#15 - 07/14/2017 03:25 PM - Jorge Albarenque

I don't see any target version on this bug. Is this being worked on? Any chances this could be fixed for 2.4?

#16 - 08/23/2017 03:54 AM - Wagner Sartori Junior

I'm on 2.4-RC... if I reset the states, it starts working.

#17 - 08/23/2017 06:03 AM - Jim Pingle

Wagner Sartori Junior wrote:

> I'm on 2.4-RC... if I reset the states, it starts working.

Check your states for traffic matching what should be the GRE outer and inner traffic when it does and does not work. What is the difference?

#18 - 08/23/2017 06:18 AM - Wagner Sartori Junior

1. Working
   enc0 gre 1.1.1.1 -> 2.2.2.2 MULTIPLE:MULTIPLE

1. Not Working

> pppoe0 gre 1.1.1.1 -> 2.2.2.2 MULTIPLE:MULTIPLE

I tried to kill only this state, but it also doesn't work. only flushing the whole state table made it work again.

#19 - 08/23/2017 06:50 AM - Jim Pingle

Add a floating rule to block, quick, in the out direction on that WAN (pppoe0) any GRE traffic, then reboot and see if it makes a difference.

#20 - 08/23/2017 07:02 AM - Wagner Sartori Junior

- File floating_rule_to_block_gre_output.png added

good idea, it did the trick.

#21 - 08/23/2017 07:23 AM - Jim Pingle

OK, if that fixed it, then it isn't related to the problem originally stated on this ticket, which is for a state issue inside the tunnel.

#22 - 08/23/2017 07:26 AM - Wagner Sartori Junior

sorry for that than.

#23 - 10/09/2017 12:49 PM - Michael OBrien

Any chance 2.4.0, with the FreeBSD 11.1 ipsec changes, may resolve this?

#24 - 10/12/2017 02:19 PM - Michael OBrien

Michael OBrien wrote:

> Any chance 2.4.0, with the FreeBSD 11.1 ipsec changes, may resolve this?

Just loaded up 2.4.0 on a few firewalls and tested. Unfortunately, the bug still exists.

#25 - 12/20/2017 07:52 AM - Daniel B

I can confirm that 2.4.2_1 is still affected. So for now, its not possible to do site to site IPSec tunnel (except in tunnel mode, which doesn't scale as soon as you have more than two or three networks per site). Any workaround ? For now I'm using OpenVPN, which is far easier to deal with, but is a bottleneck performance wise on high speed links.

#26 - 02/28/2018 10:10 PM - Eric Dombroski

Can someone confirm whether or not this bug explains the following situation?

I have a GRE tunnel set up between OpenBSD and pfSense, secured via IPSec in transport mode. From the remote OpenBSD system, I can ping a host in my pfSense "LAN" subnet even though there is no rule allowing that traffic (I've disabled the default any/any). I can also send TCP SYN packets; the replies never get back through, blocked by the default IPv4 block rule.

Running 2.4.2_p1. Is this also an issue with upstream FreeBSD?

#27 - 03/06/2018 03:26 PM - Eric Dombroski

For what it is worth, I have reproduced this on stock 12-CURRENT.
-Eric

#28 - 03/13/2018 05:46 AM - Daniel B

For reference, the upstream bug opened by Eric: https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=226411

#29 - 03/17/2018 09:06 PM - Jim Thompson

Ermal says there is code in Darwin that addresses this.

#30 - 03/17/2018 09:06 PM - Jim Thompson

- Target version set to 2.4.4

- Affected Architecture All added

- Affected Architecture deleted ()

#31 - 05/07/2018 12:59 PM - Wagner Sartori Junior

Does pfSense patch freebsd kernel for some custom/not working on plain kernel? It will take some time until somebody on freebsd actually implement that.

Darwin freebsd kernel probably have this fixed as explained earlier.

He recently said to check the current code and compare:
https://github.com/apple/darwin-xnu/blob/master/bsd/net/pf.c

#32 - 07/27/2018 12:05 PM - Steve Beaver

- Status changed from Confirmed to New

#33 - 07/27/2018 12:06 PM - Steve Beaver

- Status changed from New to 13

#34 - 07/27/2018 12:19 PM - Steve Beaver

- Status changed from 13 to New

#35 - 08/15/2018 01:26 PM - Steve Beaver

- Target version changed from 2.4.4 to 48

#36 - 08/15/2018 01:27 PM - Steve Beaver

- Priority changed from High to Normal

#37 - 08/15/2018 01:33 PM - Wagner Sartori Junior

Interested to know why do you (or pfSense) think this is not a high priority.

On my point of view (that I know doesn't matter to you or pfSense), this is a huge problem as there's no way to restrict the traffic on the GRE interfaces when running through ipsec.

#38 - 11/28/2018 09:35 AM - Vladyslav Halapsin

I confirm the problem in the version 2.4.4

#39 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0

#40 - 10/19/2020 11:14 AM - Steve Beaver

- Target version changed from 2.5.0 to Future

Files

config-R1.localdomain-20150227194833.xml	16.5 KB	02/27/2015	Jonathan Black
config-R2.localdomain-20150227194831.xml	16.5 KB	02/27/2015	Jonathan Black
Firewall_Log.JPG	64.4 KB	02/27/2015	Jonathan Black
Firewall_Rules_GRE.JPG	26.5 KB	02/27/2015	Jonathan Black
Firewall_Rules_IPSEC.JPG	26.7 KB	02/27/2015	Jonathan Black
Network_Map.JPG	99.1 KB	02/27/2015	Jonathan Black
floating_rule_to_block_gre_output.png	71.8 KB	08/23/2017	Wagner Sartori Junior