pfSense - Bug #6167

IPsec IPComp not working

04/15/2016 05:59 AM - Chris Buechler

Status:	Confirmed	**Start date:**	04/15/2016
Priority:	Normal	**Due date:**	
Assignee:	George Neville-Neil	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	Future		
Affected Version:	2.3.x	**Affected Architecture:**	

Description

IPsec connections that enable IPComp end up unable to pass traffic. Egress traffic goes out, ingress comes in, byte counters increment accordingly. Traffic is seen in tcpdump on enc0. But the traffic never makes it past enc0 on ingress. No apparent errors or anything. Multiple users have confirmed, and it's easily replicable by setting up a site to site VPN, verifying it works, then enabling IPComp on both sides.

Associated revisions

Revision c7759e4e - 05/13/2016 08:21 AM - Chris Buechler

Disable ipcomp regardless of config setting to avoid problem. Ticket #6167

Revision a23600ef - 05/13/2016 08:22 AM - Chris Buechler

Disable ipcomp regardless of config setting to avoid problem. Ticket #6167

History

#2 - 04/16/2016 08:47 PM - Jim Thompson

- Assignee set to George Neville-Neil

Assigned to gnn, in case it's related to tryforward.

#3 - 04/17/2016 05:19 AM - Chris Buechler

I'm testing stock FreeBSD 10.3 and will report back.

#4 - 04/17/2016 09:02 PM - George Neville-Neil

Test and config pushed here: https://github.com/gvnn3/netperf/tree/master/IPSEC/Tests/iperf-null-ipcomp-nopmc

What I'm seeing is that ipcomp doesn't work at all even in the absence of ESP etc. I'm digging into this now.

#5 - 04/18/2016 02:35 PM - Chris Buechler

It works fine on stock FreeBSD 10.3.

#6 - 04/22/2016 11:03 PM - Chris Buechler

- Status changed from Confirmed to Feedback

Pulled in the patch on https://reviews.freebsd.org/D6062 which gnn has confirmed fixes the issue.

#7 - 04/24/2016 06:32 PM - Ronald Antony

Is this already in the snapshots? Last I checked dataflow is still blocked when I enable IPComp...

#8 - 05/06/2016 12:44 AM - Chris Buechler

- Status changed from Feedback to Confirmed

patch broke the build of cryptostats so was reverted.

#9 - 05/12/2016 04:55 PM - Chris Buechler

Luiz merged the upstream fix for this in 384ae63efc9d676414c45591c9b6095197919513. With the note: "I changed the IPv6 part to use struct ip6protosw and wrote a wrapper for v4 version of ipcomp_nonexp_input()"

latest snapshot with that change exhibits the same behavior. Large packets are fine, small ones are dropped.

#10 - 05/13/2016 08:58 AM - Chris Buechler

- Target version changed from 2.3.1 to 2.3.2

We'll leave this as-is for 2.3.1 to avoid introducing any regressions for something that's little-used and off by default. I just pushed a change to not enable ipcomp regardless of config to prevent hitting the issue for 2.3.1.

#11 - 06/07/2016 04:50 AM - Ronald Antony

Chris Buechler wrote:

> We'll leave this as-is for 2.3.1 to avoid introducing any regressions for something that's little-used and off by default. I just pushed a change to not enable ipcomp regardless of config to prevent hitting the issue for 2.3.1.

I understand everything you wrote, except for the “little-used” part. Been using this on just abøut every platform that supports it for years, and most of the time it results in a performance increase well worth checking an option…
…frankly, I wonder why that’s even an option.

Anyway, main point I’m trying to make: it’s being used, so please don’t forget about it….

Also: the current band-aid fix only works when there’s pfSense on both sides of the connection, because generally a connection is only established when the options agree, and if pfSense ignores the setting, but the other side does not, the connection still won’t work and people will pull their hair…

BTW: the release notes for the 3.2 releases don’t list open issues, you could probably save a lot of people hassle and take traffic off the forums, if the release notes would list known issues, not just issues fixed, that way there’s a first document to check if things don’t behave as expected. Took me a while to find the IPComp issue after upgrading to 2.3, since the issue was listed in the blog, but not the release notes.

#12 - 07/08/2016 10:22 PM - Chris Buechler

- Target version changed from 2.3.2 to 2.4.0

- Affected Version changed from 2.3 to 2.3.x

#13 - 07/07/2017 03:30 PM - Jim Pingle

- Target version changed from 2.4.0 to 2.4.1

#14 - 10/12/2017 10:05 AM - Jim Pingle

- Target version changed from 2.4.1 to 2.4.2

#15 - 10/23/2017 12:19 PM - Jim Pingle

- Target version changed from 2.4.2 to 2.4.3

#16 - 01/16/2018 02:05 PM - Jim Pingle

- Target version changed from 2.4.3 to 2.4.4

#17 - 04/03/2018 11:16 AM - Ronald Antony

Is there any progress on this, other than that the target version moves to the next version each time a new version is released? :D
It would improve my network throughput quite a bit, since I'm on a bandwidth limited link...

#18 - 09/11/2018 01:50 PM - Jim Pingle

- Target version changed from 2.4.4 to 2.4.4-GS

#19 - 11/29/2018 09:41 AM - Jim Pingle

- Target version changed from 2.4.4-GS to 48

#20 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0

#21 - 05/09/2019 05:26 PM - Ronald Antony

Is this actually ever going to happen? For three years now, this is just moving from one release to the next, without visible progress, meanwhile, it would improve things were it done...

#22 - 09/05/2019 04:57 PM - Adam Gibson

I have this enabled with other firewall solutions and observed noticeable savings in bandwidth usage. I was hoping to enable this for a site seeing unexpected increase in traffic but it looks like it doesn't work yet with pfsense. Is there a workaround to get IPcomp working?

#23 - 01/06/2020 10:08 AM - Ronald Antony

Ping, Ping, Ping...

Is this thing working? It's been well over three years, different IPSec, kernel, BSD version,...
...and nothing?

Is this ever going to get any attention? I could use the bandwidth savings...

#24 - 06/16/2020 04:29 PM - Ronald Antony

Seeing that 2.5 is progressing, any chance this will finally make it?

Not sure what sort of wide, bandwidth-is-no-issue nets you all are working with, but I have a limited bandwidth and a monthly data limit, so any bit of extra performance and data cap I can squeeze out of the VPN is more than just "nice to have".

#25 - 09/22/2020 06:07 PM - Renato Botelho

- Target version changed from 2.5.0 to Future

When it's fixed on FreeBSD we can import the fix and target it to a version