pfSense - Bug #8964

IPsec async cryptography advanced setting - TCP traffic not passing through

09/27/2018 02:25 AM - Vladimir Lind

Status:	New	**Start date:**	09/27/2018
Priority:	High	**Due date:**	
Assignee:	Luiz Souza	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	CE-Next		
Affected Version:	2.4.4	**Affected Architecture:**	

Description

Test setup:

Windows <-> SG2220 2.4.4-rel <---IPSEC---> SG3100 2.4.4-rel <-> Windows

IPsec (tunnel mode) with following settings:
P1 - mode Auto, AES128, SHA256, DH14
P2 - AES128GCM, no hash, PFS 14

ICMP between Win hosts is OK.
But SMB traffic is not going through with Async Crypto enabled on any side. I do see established TSP session. When I disable async crypto - SMB download immediately begin to flow.
Attached a packet dump sniffed on LAN of the 3100 - it is a snippet of the moment when async was disabled (lines 12-15) and SMB began to work.

Please refer also to trouble tickets 12812 and 12864 for additional details.

History

#1 - 09/28/2018 02:10 AM - Vladimir Lind

Repeated the same tests with different combination of HW:

SG4860 <--> SG2440 with enabled Async crypto on both sides - no problem with SMB traffic flow. Test OK.

SG4860 <--> SG3100 with enabled Async crypto on both sides - SMB is not being passed through. Disabled it only on 3100 - began to work. Test FAIL.

SG4860 <--> SG2220 with enabled Async crypto on both sides - no problem with SMB traffic flow. Test OK.

Note: all boxes had AES-NI crypto hw enabled - except 3100! (under Advanced>Misc)

I disabled AES-NI crypto hw on SG2220 and re-tested SG4860 <--> SG2220 enabled Async crypto on both sides - SMB is not being passed through. Disabled async mode - began to work. Test FAIL.

Re-tested SG4860 <--> SG3100 with enabled AES-NI crypto hw on both nodes. Hm, with enabled IPsec Async mode SMB traffic goes through but very slow 355Kb/s and less - it takes a very long time to finalize a humble SMB download. Disabling Async mode on 3100 makes things working.

Also tested SG4860 <--> SG3100 with disabled AES-NI crypto hw on both nodes and enabled IPsec Async mode. Works, but worse then with enabled AES-NI on SG4860 - saw a lot of pauses in SMB traffic transmission.

Trying to summarize what I see:

SG2220 with enabled AES-NI crypto hw AND enabled IPsec Async mode - OK.
SG2220 with enabled AES-NI crypto hw AND disabled IPsec Async mode - OK.
SG2220 with disabled AES-NI crypto hw AND and enabled IPsec Async mode - FAIL.
SG2220 with disabled AES-NI crypto hw AND and disabled IPsec Async mode - OK.

SG3100 with enabled AES-NI crypto hw AND enabled IPsec Async mode - FAIL - very slow bw throughput.
SG3100 with enabled AES-NI crypto hw AND disabled IPsec Async mode - OK.
SG3100 with disabled AES-NI crypto hw AND and enabled IPsec Async mode - FAIL - just not working.
SG3100 with disabled AES-NI crypto hw AND and disabled IPsec Async mode - OK.

*By AES-NI I mean AES-NI and cryptodev

#2 - 10/03/2018 08:44 AM - Steve Beaver

- Target version changed from 2.4.4-GS to 2.4.4-p1

#3 - 10/15/2018 04:17 PM - Clinton Cory

I see the same issues on a SG-1100.

#4 - 10/15/2018 04:20 PM - → luckman212

Whoa, SG-1100 is out? Where do I get one?

#5 - 10/15/2018 10:00 PM - Jim Thompson

@luke they’re not for sale yet
@clinton please be more specific
@vladimir please explain how you enabled aes-ni on an arm system. (Do you mean he crypto?)

#6 - 10/16/2018 03:18 AM - Vladimir Lind

@Jim I mean "AES-NI and BSD Crypro Device"

#7 - 10/16/2018 02:47 PM - Clinton Cory

System -> Cryptographic:
AES-NI and BSD Crypto Device (aesni, cryptodev)

IPSec -> Advanced Settings -> Asynchronous Cryptography: Enabled

IPSec -> Tunnels:
AES128-GCM (128 bits)
P1 DH-Group: 2 (1024 bit)
No P2 Auth Methods

Running iperf3 across the IPsec tunnel with this topology:
CLIENT -> DUT-A -> DUT-B -> SERVER

Reports a couple Kbps once or twice, then traffic drops completely.

When I disable Async Crypto, I see 75Mbps consistently with PF disabled and 69Mbps with PF enabled (for some reason IPsec GCM is much slower than IPSec CBC).

This is running the latest 2.4.5 snapshot. FYI - The SG-5100 had no issues with this on 2.4.4.

#8 - 10/19/2018 12:02 PM - Steve Beaver

- Assignee set to Luiz Souza

- Priority changed from Normal to High

#9 - 10/22/2018 10:36 AM - Paul Bucher

I'm seeing this bug occur on my SG-3100s when using one of the AES-GCM based algorithms for my IPSEC Phase2 with async crypto turned on.

If I switch to plain AES the issue goes away, which happens to use hardware based crypto on the SG-3100s(Which would be a better choice for my SG3100 <--> SG3100 connections probably). I also have SG-3100 <--> intel based pfsense boxes with AES-NI enabled on them. If I just turn off async on the SG-3100 side the problem also goes away. What I haven't tested is trying a non-hardware accelerated algorithm on the intel side with async crypto enabled.

In summary it appears to me that async crypto breaks non-hardware accelerated crypto algorithms or at least the AESXXX-GCM ones.

#10 - 11/27/2018 10:44 AM - Renato Botelho

- Target version changed from 2.4.4-p1 to 48

Do not enable it by default for now and move to 2.4.5

#11 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0

#12 - 12/08/2020 12:09 PM - Steve Beaver

- Target version changed from 2.5.0 to CE-Next

Files

dump_capt_on_lan.pcap	11.9 KB	09/27/2018	Vladimir Lind