pfSense - Bug #8426

Mobile IPSec login not working after upgrade from 2.4.2p1

04/03/2018 02:46 PM - Michael Newton

Status:	Resolved		**Start date:**	04/03/2018
Priority:	Normal		**Due date:**	
Assignee:	Jim Pingle		**% Done:**	100%
Category:	IPsec		**Estimated time:**	0.00 hour
Target version:	2.4.3_1			
Affected Version:	2.4.3		**Affected Architecture:**	All

Description

Since performing the upgrade from 2.4.2p1 to 2.4.3, users have been unable to connect; OS X clients get an error suggesting the problem is with the shared secret.

Associated revisions

Revision af7c0311 - 04/12/2018 11:19 AM - Jim Pingle

For IPsec mobile clients, write out a more specific ipsec.secrets line to help clients find the right key with strongSwan's new lookup code. Fixes #8426

Revision fad13c41 - 04/12/2018 11:21 AM - Jim Pingle

For IPsec mobile clients, write out a more specific ipsec.secrets line to help clients find the right key with strongSwan's new lookup code. Fixes #8426

(cherry picked from commit af7c0311b89656198e00ded91c1a2a87f34c331b)

History

#1 - 04/09/2018 07:33 AM - Jay2k1 *

Yes, I can confirm this issue. Mobile Client ("Roadwarrior") IPSec access no longer works after upgrading to 2.4.3 (we're using IKEv1).

Apparently others are affected too: https://forum.pfsense.org/index.php?topic=145891.0

A quick fix for this would be very highly appreciated, because this is quite critical for us. Thanks a lot!

#2 - 04/10/2018 12:16 AM - Daniel Becker

Seeing the same error ("The VPN Shared Secret is incorrect.") on iOS. Exact same config worked before the update to 2.4.3.

#3 - 04/12/2018 10:34 AM - Jim Pingle

- Status changed from New to Confirmed

- Assignee set to Jim Pingle

Looks like the PSK for another tunnel is being used instead of the more exact match. It works when it is the only entry. I'll have a look.

#4 - 04/12/2018 10:55 AM - Jim Pingle

Well, ipsec.secrets is written out identically on both a working (2.4.2) and non-working (2.4.3, 2.4.4, 2.3.6) setup and the only difference I see is the strongSwan version. 5.6.0 is working, 5.6.2_1 is not.

strongSwan 5.6.2 release notes say "The lookup for PSK secrets for IKEv1 has been improved for certain scenarios.", which seems to be associated with https://wiki.strongswan.org/issues/2497 but apparently that has broken secrets that were working previously.

There is probably a way to reformat ipsec.secrets to work around it. Lots of info on that strongSwan ticket to sort through.

#5 - 04/12/2018 11:30 AM - Jim Pingle

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset [af7c0311b89656198e00ded91c1a2a87f34c331b](af7c0311b89656198e00ded91c1a2a87f34c331b).

#6 - 04/12/2018 11:36 AM - Jay2k1 *

I tested the diff and can confirm it works again. Thank you so much for fixing this so quickly Jim!

#7 - 04/20/2018 03:01 PM - Chris Macmahon

Was able to confirm fix worked.

#8 - 04/20/2018 03:04 PM - Jim Pingle

- Status changed from Feedback to Resolved

#9 - 05/03/2018 01:21 PM - Jim Pingle

- Target version changed from 2.4.4 to 2.4.3_1

Files

Screenshot 2018-04-02 10.43.09.png	98.5 KB	04/03/2018	Michael Newton