pfSense - Bug #10178

crypt.inc: crypt_data() legacy mode using wrong message digest

01/10/2020 12:23 PM - Jim Pingle

Status:	Resolved	**Start date:**	01/10/2020
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Backup / Restore	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.5.0	**Affected Architecture:**	All

Description

On 2.4.x with OpenSSL 1.0.x, the default message digest (md) value was "md5" (eew). On 2.5.0 with OpenSSL 1.1.1 we manually set sha256.

Between the hardcoded md value and the difference in OpenSSL defaults between the versions, it needs a nudge before it could possibly decrypt an old config on a new system ("legacy" mode in the function). Old syntax examples like on the forum would not work as-is on 2.5.0.

So when $legacy is true, the OpenSSL command should pass -md md5 which should let it work fully.

Associated revisions

Revision ff383f32 - 01/10/2020 12:29 PM - Jim Pingle

Use correct md value in crypt_data(). Fixes #10178

History

#1 - 01/10/2020 12:35 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset ff383f323c0f8104e227d8af7401fdad6d383bbe.

#2 - 01/11/2020 02:46 AM - Viktor Gurov

- Status changed from Feedback to Resolved

tested on 2.5.0.a.20200110.1822 with 2.4.4-p3 and 2.5 encrypted backups