pfSense - Bug #11167

Insecure default values for user certificates created via User Manager

12/15/2020 02:26 PM - Jim Pingle

Status:	Resolved	**Start date:**	12/15/2020
Priority:	High	**Due date:**	
Assignee:		**% Done:**	100%
Category:	User Manager / Privileges	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	

Description

When creating a user certificate for a new user under System > User Manager (system_usermanager.php) the default values for **Key Length** and **Digest Algorithm** are insecure.

Key Length should default to 2048

Digest Algorithm should default to sha256

This will match the default values on system_certmanager.php.

Associated revisions

Revision 293c7335 - 12/18/2020 02:40 PM - Jim Pingle

Use stronger cert defaults when creating a user cert. Fixes #11167

History

#1 - 12/18/2020 02:50 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 293c7335c11ce111624dd551bb81775ba4499481.

#2 - 12/22/2020 11:49 AM - Danilo Zrenjanin

- Status changed from Feedback to Resolved

Tested on the latest snapshot.

It looks fine now. When creating a new user certificate under System > User Manager:

The **Key Length** default value is **2048**
The **Digest Algorithm** default value is **sha256**

Ticket resolved.