pfSense - Feature #9883

Allow CAs to use randomized serials when signing

11/04/2019 01:02 PM - Jim Pingle

Status:	Resolved	**Start date:**	11/04/2019
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.5.0		

Description

Various guidelines suggest using randomized serial numbers when signing certificates, rather than using sequential numbers.

Add an option to CA entries (off by default) which will allow them to generate random serial numbers when signing for extra security.

The generated numbers must be tested against all known serials for a given CA to avoid accidentally duplicating a serial.

Associated revisions

Revision 2c9601c9 - 11/04/2019 01:02 PM - Jim Pingle

Add support for randomized cert serial numbers. Implements #9883

Revision a6bd9e78 - 11/05/2019 10:31 AM - Jim Pingle

Validate CA/CRL serial input. Issue #9883 Issue #9869

Revision 94ce250e - 11/20/2019 10:29 AM - Jim Pingle

Move CA random serial option to upper section. Issue #9883

This allows it to be set when creating a new CA, so it doesn't have to
be edited in later.

Also show the next serial/random status in the CA info block
Hide trust store line from non-CA entries since it's not relevant to
certificates, only CAs.

History

#1 - 11/04/2019 01:10 PM - Jim Pingle

- Status changed from In Progress to Feedback

- % Done changed from 0 to 100

Applied in changeset 2c9601c978589f34089f25cc7569ed67dbbc37e8.

#2 - 11/27/2019 11:12 AM - Viktor Gurov

tested on pfSense 2.5.0.a.20191126.1832

it successfully creates random serials when creating certificates or signing CSR

Resolved

#3 - 11/27/2019 11:26 AM - Jim Pingle

- Status changed from Feedback to Resolved