pfSense - Bug #9443

Captive Portal Vouchers feature is broken in 2.5.0

03/31/2019 11:25 AM - A FL

Status:	Resolved	**Start date:**	03/31/2019
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	100%
Category:	Captive Portal	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.5.0	**Affected Architecture:**	

Description

Hello,

When enabling vouchers on 2.5.0, fields "Voucher Public Key" and "Voucher Private Key" are empty, and clicking on "Generate new keys" has no effect.

The error seems to come from OpenSSL v1.1.1 that now prevent an RSA key under 512 bits to be generated :

ybCIzIlp

The C++ constant preventing RSA keys to be generated is defined here :
https://github.com/pfsense/FreeBSD-src/blob/RELENG_2_5/crypto/openssl/crypto/rsa/rsa_locl.h#L14

Associated revisions

Revision ad1d975a - 05/27/2019 02:54 PM - Renato Botelho

Fix #9443: Use phpseclib to create RSA key

OpenSSL doesn't allow to create a 64 RSA key anymore. Use phpseclib to
do it using PHP.

History

#1 - 03/31/2019 11:38 AM - A FL

The change has been made in OpenSSL here : https://github.com/openssl/openssl/commit/cac19d19e7d6f252ff9aea60d85e0c0fd71a117f

#2 - 04/01/2019 01:53 PM - Jim Pingle

- Assignee set to Renato Botelho

Rather than patching OpenSSL, we could use a pure PHP implementation of RSA to generate the voucher keys:

http://phpseclib.sourceforge.net/

```
include_once('Crypt/RSA.php');
$rsa = new Crypt_RSA();
$key = $rsa->createKey(64);
$private_key = $key["privatekey"];
$public_key = $key["publickey"];
```

Similar to what we did for x509 CRLs for PHP 7.x.

The code above works with the files from that library copied to the host and with the directory it's in added to the PHP include path. The contents of the generated public and private keys are in the correct format.

We'd need to make a port for it, but that still seems like a better idea than patching OpenSSL.

Once the port is in place we can update the code to use it.

#3 - 05/27/2019 03:05 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset ad1d975acce7a0b7562baca0a6cadab2629de51e.

#4 - 06/01/2019 12:58 PM - A FL

I can confirm that the changeset is working correctly.
This issue can be marked as resolved

#5 - 06/01/2019 05:28 PM - Jim Pingle

- Status changed from Feedback to Resolved