pfSense - Feature #4683

Support for elliptic curve for IPsec on webconfigurator

05/07/2015 06:48 AM - Lars Pedersen

Status:	Resolved	**Start date:**	05/07/2015
Priority:	High	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.3		

Description

In pfSense 2.2.2 strongswan runs with version 5.3.0 and it looks like it supports elliptic curves in the dh-group:

[2.2.2-RELEASE][admin@pfSense.localdomain]/root: ipsec listalgs

List of registered IKE algorithms:

```
encryption: AES_CBC[aes] 3DES_CBC[des] DES_CBC[des] DES_ECB[des] BLOWFISH_CBC[blowfish] RC2_CBC[rc
2]
              CAMELLIA_CBC[openssl] RC5_CBC[openssl] CAST_CBC[openssl] IDEA_CBC[openssl] NULL[open
ssl]
  integrity:  HMAC_MD5_96[openssl] HMAC_MD5_128[openssl] HMAC_SHA1_96[openssl] HMAC_SHA1_128[opens
sl]
              HMAC_SHA1_160[openssl] HMAC_SHA2_256_128[openssl] HMAC_SHA2_256_256[openssl] HMAC_SH
A2_384_192[openssl]
              HMAC_SHA2_384_384[openssl] HMAC_SHA2_512_256[openssl] HMAC_SHA2_512_512[openssl] CAM
ELLIA_XCBC_96[xcbc]
              AES_XCBC_96[xcbc] AES_CMAC_96[cmac]
  aead:       AES_GCM_8[openssl] AES_GCM_12[openssl] AES_GCM_16[openssl]
  hasher:     HASH_SHA1[sha1] HASH_SHA224[sha2] HASH_SHA256[sha2] HASH_SHA384[sha2] HASH_SHA512[sh
a2] HASH_MD4[md4]
              HASH_MD5[md5]
  prf:        PRF_KEYED_SHA1[sha1] PRF_HMAC_MD5[openssl] PRF_HMAC_SHA1[openssl] PRF_HMAC_SHA2_256[
openssl]
              PRF_HMAC_SHA2_384[openssl] PRF_HMAC_SHA2_512[openssl] PRF_FIPS_SHA1_160[fips-prf] PR
F_AES128_XCBC[xcbc]
              PRF_CAMELLIA128_XCBC[xcbc] PRF_AES128_CMAC[cmac]
  dh-group:   MODP_2048[openssl] MODP_2048_224[openssl] MODP_2048_256[openssl] MODP_1536[openssl]
MODP_3072[openssl]
              MODP_4096[openssl] MODP_6144[openssl] MODP_8192[openssl] MODP_1024[openssl] MODP_102
4_160[openssl]
              MODP_768[openssl] MODP_CUSTOM[openssl] ECP_256[openssl] ECP_384[openssl] ECP_521[ope
nssl] ECP_224[openssl]
              ECP_192[openssl] ECP_224_BP[openssl] ECP_256_BP[openssl] ECP_384_BP[openssl] ECP_512
_BP[openssl]
  random-gen: RNG_WEAK[openssl] RNG_STRONG[random] RNG_TRUE[random]
  nonce-gen:  [nonce]
[2.2.2-RELEASE][admin@pfSense.localdomain]/root:
```

By looking at strongswans cipher suites it is the **NIST Elliptic Curve Groups** and **Brainpool Elliptic Curve Groups** that is missing in the webconfigurator.

https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites

Associated revisions

Revision 7dc35024 - 06/19/2015 05:47 AM - Ermal Luçi

Ticket #4683 merge in brainpool for DH parameters

History

#1 - 05/26/2015 12:41 AM - Lars Pedersen

Can be closed: Solved with https://github.com/pfsense/pfsense/pull/1649

#2 - 05/26/2015 11:39 AM - Chris Buechler

- Status changed from New to Feedback

- Assignee set to Chris Buechler

- Target version set to 2.2.3

#3 - 06/11/2015 05:06 PM - Chris Buechler

- Status changed from Feedback to Resolved

confirmed. Thanks!

#4 - 06/15/2015 04:04 AM - Lars Pedersen

Chris Buechler wrote:

> confirmed. Thanks!

Can see that you have set the target version to 2.2.3. Will you cherry pick this patch to RELENG_2_2?

#5 - 06/15/2015 09:52 AM - Ermal Luçi

It is already in 2.2.3 since the merge.
I merged it manually.

#6 - 06/16/2015 01:39 AM - Lars Pedersen

Ermal Luçi wrote:

> It is already in 2.2.3 since the merge.
> I merged it manually.

I'm still not convinced that it has been merged since ”brainpool” is nowhere to be found in:
https://github.com/pfsense/pfsense/blob/RELENG_2_2/etc/inc/ipsec.inc

Besides the ipsec.inc file last update was 2 months ago.

#7 - 06/19/2015 05:44 AM - Ermal Luçi

Merged.

#8 - 06/22/2015 08:21 AM - Lars Pedersen

Can see that you have only merged parts of the 1649 pull request. Things like IPsec phase 1 is missing AES GCM support and the function vpn_ipsec_convert_to_modp has not been updated too. So the current snapshot is broken with the new functionalities.

So will you be kind to do a fully merge of the given pull request :)

#9 - 06/22/2015 01:32 PM - Chris Buechler

- Target version changed from 2.2.3 to 2.3

Thanks for the heads up, Lars. We're short on time for 2.2.3, plus don't generally put features into maintenance releases, so I reverted the partial incorrect merge. 2.3 isn't too far into the future.