pfSense - Bug #7685

OpenVPN Auth Digest Algorithm list contains entries that are functionally identical and thus redundant

07/10/2017 07:37 AM - Jim Pingle

Status:	Resolved	**Start date:**	07/10/2017
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.4.0		
Plus Target Version:		**Affected Version:**	All
Release Notes:		**Affected Architecture:**	All

Description

The way "openvpn --show-digests" works it ends up listing several algorithms that are functionally equivalent but some of the duplicate options do not work on other clients, which can be confusing for users.

For example, both RSA-SHA256 and SHA256 are in the list, but in this context openvpn only uses the SHA256 portion. Some clients can't use "RSA-SHA256" but can instead use "SHA256" and it works for both ends.

See https://security.stackexchange.com/questions/91908/using-rsa-sha-as-instead-hmac-in-openvpn and #7681

History

#1 - 07/10/2017 08:52 AM - Jim Pingle

This also appears to be confirmed by openssl list-message-digest-algorithms, which lists which names/aliases map to underlying digests.

```
DSA
DSA-SHA
DSA-SHA1 => DSA
DSA-SHA1-old => DSA-SHA1
DSS1 => DSA-SHA1
MD4
MD5
MDC2
RIPEMD160
RSA-MD4 => MD4
RSA-MD5 => MD5
RSA-MDC2 => MDC2
RSA-RIPEMD160 => RIPEMD160
RSA-SHA => SHA
RSA-SHA1 => SHA1
RSA-SHA1-2 => RSA-SHA1
RSA-SHA224 => SHA224
RSA-SHA256 => SHA256
RSA-SHA384 => SHA384
RSA-SHA512 => SHA512
SHA
SHA1
SHA224
SHA256
SHA384
SHA512
DSA
DSA-SHA
dsaWithSHA1 => DSA
dss1 => DSA-SHA1
ecdsa-with-SHA1
MD4
md4WithRSAEncryption => MD4
MD5
md5WithRSAEncryption => MD5
MDC2
mdc2WithRSA => MDC2
ripemd => RIPEMD160
```

```
RIPEMD160
ripemd160WithRSA => RIPEMD160
rmd160 => RIPEMD160
SHA
SHA1
sha1WithRSAEncryption => SHA1
SHA224
sha224WithRSAEncryption => SHA224
SHA256
sha256WithRSAEncryption => SHA256
SHA384
sha384WithRSAEncryption => SHA384
SHA512
sha512WithRSAEncryption => SHA512
shaWithRSAEncryption => SHA
ssl2-md5 => MD5
ssl3-md5 => MD5
ssl3-sha1 => SHA1
whirlpool
```

#2 - 07/10/2017 09:40 AM - Jim Pingle

- Status changed from Assigned to Feedback

I pushed a fix for this in f49ef559060ec8cad5c7a3a548d509cf08b5549b but forgot to put this ticket number on the commit so it would automatically set to feedback.

It should be all OK now, and existing settings that used the aliased names will be corrected to the actual underlying names on upgrade.

If someone has issues with exporting or other functional problems because of the value on 2.3.x or other versions, simply edit the server or client and choose the correct digest algorithm (e.g. the one without RSA- or other prefixes in front, in most cases).

#3 - 07/10/2017 03:24 PM - Jim Pingle

- Status changed from Feedback to Resolved

Fixed.

Only actual digest algorithms show now, and not their aliases. Configurations that referenced an alias are migrated to the actual underlying digest algorithm on upgrade.