pfSense - Feature #4230

Prefer SSL Perfect Forward Secrecy ciphers in UI

01/17/2015 07:19 AM - Phil Koller

Status:	Resolved	**Start date:**	01/17/2015
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	100%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:	2.2.1		
Plus Target Version:		**Release Notes:**	Default

Description

Perfect Forward Secrecy (PFS) ciphers should be preferred in the admin interface to further harden the admin web server.

Suggested changed/added settings to the webConfigurator configuration:

```
ssl.use-compression = "disable"
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "AES128+EECDH:AES128+EDH:AES128-SHA:!aNULL:!eNULL:!DSS"
```

This configuration explicitly disables TLS compression and defines the correct cipher order. AES128-SHA is added as a fallback, DSS ciphers should not be used.

The result of

```
openssl ciphers -v 'AES128+EECDH:AES128+EDH:AES128-SHA:!aNULL:!eNULL:!DSS'
```

will be:

```
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2 Kx=ECDH Au=RSA   Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256       TLSv1.2 Kx=ECDH Au=RSA   Enc=AES(128)  Mac=SHA256
ECDHE-ECDSA-AES128-SHA256     TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128)  Mac=SHA256
ECDHE-RSA-AES128-SHA          SSLv3 Kx=ECDH   Au=RSA   Enc=AES(128)  Mac=SHA1
ECDHE-ECDSA-AES128-SHA        SSLv3 Kx=ECDH   Au=ECDSA Enc=AES(128)  Mac=SHA1
DHE-RSA-AES128-GCM-SHA256     TLSv1.2 Kx=DH   Au=RSA   Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256         TLSv1.2 Kx=DH   Au=RSA   Enc=AES(128)  Mac=SHA256
DHE-RSA-AES128-SHA            SSLv3 Kx=DH     Au=RSA   Enc=AES(128)  Mac=SHA1
AES128-SHA                    SSLv3 Kx=RSA    Au=RSA   Enc=AES(128)  Mac=SHA1
```

Background:
https://raymii.org/s/tutorials/Strong_SSL_Security_On_lighttpd.html

Associated revisions

Revision bd583dc2 - 03/11/2015 12:24 AM - Chris Buechler

Update cipher-list in web interface to prefer PFS. Ticket #4230

Revision 0f575511 - 03/11/2015 12:25 AM - Chris Buechler

Update cipher-list in web interface to prefer PFS. Ticket #4230

Revision 0d443728 - 03/11/2015 12:09 PM - Renato Botelho

Explicit disable ssl.use-compression on lighty config. It should fix #4230

Revision cd8ce13c - 03/11/2015 12:09 PM - Renato Botelho

Explicit disable ssl.use-compression on lighty config. It should fix #4230

History

#1 - 01/17/2015 06:50 PM - Chris Buechler

- Project changed from pfSense Packages to pfSense

- Category set to Web Interface

- Target version set to 2.2.1

- Affected Version deleted (2.2)

this is something I'd noted for 2.2.1 but don't think we have a ticket on it.

#2 - 03/10/2015 09:39 AM - Renato Botelho

Any specific reason to disable AES256 ones?

#3 - 03/10/2015 05:25 PM - Phil Koller

As stated in the background paper:

"AES128 is preferred to AES256. There have been discussions on whether AES256 extra security was worth the cost, and the result is far from obvious. At the moment, AES128 is preferred, because it provides good security, is really fast, and seems to be more resistant to timing attacks."

Another discussion on the topic:
http://security.stackexchange.com/questions/14068/why-most-people-use-256-bit-encryption-instead-of-128-bit

In case this isn't convincing, AES256 can be added again. Just make sure EECDH is always used first, e.g.

```
ssl.use-compression = "disable"
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "AES256+EECDH:AES128+EECDH:AES256+EDH:AES128+EDH:AES256-SHA:AES128-SHA:!aNULL:!eNULL:!DSS"
```

#4 - 03/11/2015 12:35 AM - Chris Buechler

- Assignee set to Chris Buechler

- % Done changed from 0 to 80

It looks like the best compromise is enabling both 128 and 256, and preferring 128, which is the change I just committed. With that, it scores an A on ssllabs.com. Its only complaint is considering TLS_DHE_RSA_WITH_AES_* options "weak." But, disabling those breaks several clients/browsers. The config as committed only breaks with IE on Windows XP (which is fine, and already known broken by 2.2's list).

AES 256 doesn't break with glxsb, including where only AES256 is in the cipher-list. So that's not a concern. Also no issue with AES-NI, but didn't expect any problems there.

Only thing remaining to test with hifn card, which I'll do in the morning. If someone else has a hifn and can help test, it'd be appreciated. Depending on the result of that, we may be able to get rid of the BEAST option.

#5 - 03/11/2015 12:00 PM - Chris Buechler

- % Done changed from 80 to 90

Fine with hifn cards too. Renato's removing the BEAST option since it's no longer necessary then this will be complete.

#6 - 03/11/2015 12:10 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 90 to 100

Applied in changeset 0d443728d5ba55565f23ee71db117dbc1e1bb496.

#7 - 03/11/2015 12:10 PM - Renato Botelho

Applied in changeset cd8ce13c29fb03714d90c4e9599b77aa1faa1a80.

#8 - 03/11/2015 03:00 PM - Chris Buechler

- Status changed from Feedback to Resolved

all good.