Bip - Enhancement #301

Allow cipher spec setting

2012-08-11 04:39 - Christopher Head

Status:	Resolved	**Start date:**	2012-08-11
Priority:	Normal	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Target version:	0.9.0		
Patch Available:	Yes	**Branch:**	
Found in Versions:		**Security:**	Yes
Confirmed:	Yes	**Help Needed:**	No

Description

I want to use an RSA certificate because RSA is more widely supported. However, I want to refuse to use straight-RSA key exchange cipherspecs; I want to only ever use RSA+DHE key exchanges because they add perfect forward secrecy. I can't do that because bip doesn't allow me to enter a cipherspec string restricting what types of cipherspecs to use. Basically I want Apache/mod_ssl's <http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite> in bip. This would also allow the administrator to disable other miscellaneous cipherspecs if they prove to be insecure without having to wait for new versions of software to come out.

Associated revisions

Revision 6691f89c - 2016-04-13 01:04 - Pierre-Louis Bonicoli

Add cipher specifications setting

Allow to configure cipher specifications for the listening bip
connection and for each outgoing IRC connection.

Closes #301

Revision ab8e5eec - 2016-11-07 11:25 - Pierre-Louis Bonicoli

Add cipher specifications setting

Allow to configure cipher specifications for the listening bip
connection and for each outgoing IRC connection.

Closes #301

History

#1 - 2014-10-15 18:30 - Marian S

I'd like to push this and I'd think this is not an enhancement but a bug.
Even though bip maybe isn't vulnerable to the SSL 3.0 vulnerability exposed today (poodle), something else can come out any day. And, generally, it is a very good idea to be able to blacklist ciphers/protocols that are no longer in use.
Thus I'd say this deserves a high priority and I'd be very happy to see this implemented!

#2 - 2016-04-13 01:18 - Pierre-Louis Bonicoli

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset bip|6691f89c382fd32d2511166fd95af4f7f964d36a.

#3 - 2016-04-13 01:21 - Pierre-Louis Bonicoli

- Status changed from Resolved to In Progress

- Assignee set to Pierre-Louis Bonicoli

- Target version set to 0.9.0

- % Done changed from 100 to 50

- Patch Available changed from No to Yes

- Confirmed changed from No to Yes

Test in progress: see 6691f89c382fd32d2511166fd95af4f7f964d36a.

#4 - 2016-11-07 12:15 - Pierre-Louis Bonicoli

- Status changed from In Progress to Resolved

- % Done changed from 50 to 100

Applied in changeset bip|ab8e5eece1a80c9096de1c8abd9dc2a447548287.