Smart Proxy - Bug #12576

Logjam - doesn't allow custom DHE groups

11/24/2015 03:41 AM - Brandon Weeks

Status:	Closed		
Priority:	Normal		
Assignee:	Brandon Weeks		
Category:	SSL		
Target version:	1.11.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	Nightly
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/smart-proxy/pull/347		

Description

The Smart-Proxy suffers from two limitations regarding Diffie-Hellman key exchange:

- The Ruby OpenSSL implementation doesn't include DHE groups above 1024-bits, so it does not scale with larger key sizes.
- The Smart-Proxy lacks a way to specify a custom DH groups.

Further reading:

- https://wiki.mozilla.org/Security/Server_Side_TLS#DHE_handshake_and_dhparam
- https://wiki.mozilla.org/Security/Server_Side_TLS#Pre-defined_DHE_groups
- https://weakdh.org/

Related issues:

Related to Smart Proxy - Bug #12572: Smart-Proxy includes RC4 in ciphersuites	**Closed**	**11/23/2015**

History

#1 - 11/24/2015 03:48 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Brandon Weeks

- Pull request https://github.com/theforeman/smart-proxy/pull/347 added

#2 - 01/14/2016 08:18 AM - Anonymous

Was closed in favour of http://projects.theforeman.org/issues/12572

#3 - 01/14/2016 08:18 AM - Anonymous

- Related to Bug #12572: Smart-Proxy includes RC4 in ciphersuites added

#4 - 01/14/2016 08:18 AM - Anonymous

- Status changed from Ready For Testing to Closed

#5 - 01/14/2016 08:25 AM - Dominic Cleal

- translation missing: en.field_release set to 71