Smart Proxy - Bug #5651

The 'trusted_hosts' config key has an unintuitive (and potentially dangerous) behavior

05/09/2014 06:20 PM - Jon McKenzie

Status:	Duplicate		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.4.2
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

According to the Foreman documentation:

> [trusted_hosts] is the list of hosts from which the smart proxy will accept connections. If this list is empty then every verified SSL connection is allowed to access the API.

There are two issues:

- This behavior is unintuitive. An empty list of trusted hosts should imply that no hosts are trusted, not that all hosts are trusted. An implication of the current behavior is that I would need to enter in a bogus trusted host in order to disable all remote access.
- The proxy (at least in Foreman 1.4.2) accepts ALL connections when trusted_hosts is empty, not just verified connections. In a test deployment, we were able to access the API via curl without providing any credentials or certificates/keys when trusted_hosts was empty.

Related issues:

Is duplicate of Smart Proxy - Bug #7822: CVE-2014-3691 - Smart proxy doesn't ...	**Closed**	**10/06/2014**
Is duplicate of Smart Proxy - Bug #6589: Trusted host list seems to be ignored	**Closed**	**07/11/2014**

History

#1 - 05/13/2014 08:32 PM - Jon McKenzie

So this seems to be a larger problem than I originally thought. It seems to be that regardless of whether SSL information is specified, only DNS checking is done to validate clients.

Inserting a logger statement into lib/smart_proxy.rb (https://github.com/theforeman/smart-proxy/blob/04148e799c23d7b2024dfb812d04f803f80449da/lib/smart_proxy.rb#L62), I can see that it's picking up my SSL certificates. Yet if I add a host into the trusted_hosts, I can use plain curl (with -k) from that host to query the API (no certs specified at all).

#2 - 10/06/2014 06:40 AM - Dominic Cleal

- Is duplicate of Bug #7822: CVE-2014-3691 - Smart proxy doesn't perform verification of client SSL certificate on API requests added

#3 - 10/06/2014 06:41 AM - Dominic Cleal

- Is duplicate of Bug #6589: Trusted host list seems to be ignored added

#4 - 10/06/2014 06:41 AM - Dominic Cleal

- Status changed from New to Duplicate

Thanks very much for your report Jon, apologies for us taking so long to see and address it.

The trusted hosts behaviour I think I fixed in the course of #6589. The SSL verification behaviour we're addressing now via #7822.