Smart-Proxy - Feature #11039
Support more specific authorization of wildcard certificates
07/07/2015 12:20 PM - Justin T.

Status: New
Priority: Normal
Assigned To: 
Category: Core
Target version: 
Difficulty: 
Found in release: 1.8.2

Start date: 07/07/2015
Due date: 
% Done: 0%
Estimated time: 0.00 hour
Bugzilla link: 
Pull request: 

Description
After updating from 1.7.3 to 1.8.2, we can no longer change the Operating System of a managed host. The web UI fails with an error related to TFTP. We're using a wildcard SSL certificate installed to the Foreman master as well as each remote Smart Proxy; all servers are in the same domain name as the wildcard certificate.

Web UI error:
TFTP Settings for server.domain.com task failed with the following error: ERF12-5472 [ProxyAPI::ProxyException]: Unable to set TFTP boot entry for 00:50:56:a3:57:94 ([RestClient::Forbidden]: 403 Forbidden) for proxy
https://dev-foreman01.domain.com:8443/tftp

Foreman Proxy error (DEBUG):
D, [2015-07-07T10:07:41.794749 #26957] DEBUG -- : verifying remote client 100.124.30.61 against trusted_hosts
foreman.domain.comforeman01.domain.com100.124.30.61
100.124.30.61 - - [07/Jul/2015 10:07:41] "POST /syslinux/00:50:56:a3:57:94 HTTP/1.1" 403 121 0.0009

Related issues:
Related to Smart-Proxy - Feature # 7849: trusted_hosts should determine hostn... Closed 10/08/2014

History
#1 - 07/07/2015 12:21 PM - Justin T.
- Related to Feature #7849: trusted_hosts should determine hostname from certificate CN on SSL requests added

#2 - 07/08/2015 03:43 AM - Dominic Cleal
- Category set to Core
- Status changed from New to Feedback

Can you just add the *.domain.com to your trusted hosts list?

#3 - 07/08/2015 03:59 AM - Markus Frosch
I think his problem is caused by the introduced reverse lookup verification.

Justin seems to have a wildcard cert "*.domain.com", which could work against the trusted_hosts list, but not with forward_verify and not since we test based in the certificate CN, and not the PTR only.

Before my refactoring, we tested the PTR record against trusted_hosts, and the certificate was only authenticated as a client against the smart_proxies's CA, and not if the certificate presented is on the list.

I think a safe solution would be to allow reverse testing to be disabled, while whitelisting the wildcard CN.

01/21/2016
I don't think forward verification is used at all with HTTPS requests, it only looks to be in the HTTP code path.

https://github.com/theforeman/smart-proxy/blob/1.9.0-RC1/lib/sinatra/authorization.rb#L14-L21

So for an HTTPS request, it'll pull the CN from the presented certificate, which is the wildcard hostname and then check the trusted hosts list for it.

Dominic, while adding "*.domain.com" to my trusted hosts does work, now any host with access to our wildcard certificate is trusted to make calls to Foreman. From a security view, that's less than ideal (I'll admit using a wildcard is, in itself, its own set of issues).

From my testing, the value of 'fqdn', stored as the CN from the certificate, is what's tripping foreman-proxy up.

So I guess you'd want the option to use authorisation based on the remote host, like HTTP uses, instead of the CN from the cert? If so, that makes some sense.

Correct. I'm thinking along the lines of an enable-able option, defaulting to false as I believe wildcard usage is rare, or as an additional code check.

For the code check, it could be along the lines of if code detects that the CN from the certificate is a wildcard, then it requires both:

1. First matching the certificate's are valid and domain matches.
2. Also requires the remote host name to match against the trusted_hosts list.