Smart Proxy - Feature #969

Direct Client->Foreman communication shouldn't be needed (and moved to the Proxy)

06/09/2011 05:23 AM - Marcello de Sousa

Status:	Closed		
Priority:	Normal		
Assignee:	dustin tsang		
Category:	TFTP		
Target version:	1.7.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1197806	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/smart-proxy/pull/224		

Description

When provisioning a machine, the client needs to access foreman unattended urls, such as:
http://foreman/unattended/kickstart
and
http://foreman/unattended/built

That means firewall open to foreman (and the API).
I think the architecture and security would improve if Foreman could be as isolated as possible, not depending on being open to the machines it manages... Those tasks should be left to the proxy.

The suggested solution:
Client communications directed to Foreman should me moved to proxy (in this case, the one running on the master) so you only need port 8140(puppetmaster) + 8443 (foreman-proxy) open.

Note:
The proxy doesn't really need to simply forward the request (although this is also a valid initial solution). It could have some intelligence to validate them or serve the unattended itself (pre fetching template information or something like it)…

http://i.imgur.com/aJlN5.png

Related issues:

Related to Foreman - Feature #1069: Unattended install behind firewall and bu...	**Closed**	**07/26/2011**
Related to Foreman - Bug #1208: Unauthenticated IP spoofing should not be all...	**Closed**	**10/04/2011**
Related to Foreman - Feature #1970: Override the foreman_url hostname	**New**	**11/22/2012**
Related to Smart Proxy - Feature #11582: Implement proxy API for "built" command	**Rejected**	**08/27/2015**
Related to Foreman - Feature #17316: Proxy templating needs TFTP feature to b...	**Closed**	**11/11/2016**
Blocks Katello - Tracker #8172: Isolate Client Communication through a Capsule	**New**	
Blocks Discovery - Feature #8147: Support for HTTP proxy	**New**	**10/29/2014**

Associated revisions

Revision 81159d4b - 10/04/2012 11:14 AM - Greg Sutcliffe

Use tokens for discovery of host identity during installation

- fixes #1069
- fixes #1720
- refs #969

Revision 2094e4e8 - 11/04/2014 12:28 PM - Greg Sutcliffe

Refs #969 - Foreman-side changes for serving templates from the proxy

Revision a53d835a - 11/04/2014 12:33 PM - dustin tsang

Refs #969 - Proxy-side changes for serving templates from the proxy

An update to @GregSutcliffe's original PR. Ports his original feature to the new plugin api.

Revision 8e01bb10 - 11/10/2014 09:53 AM - Greg Sutcliffe

Refs #969 - Foreman-side changes for serving templates from the proxy

(cherry picked from commit 2094e4e8b049e6cae32326c33a7ba73cc4047b9f)

History

#1 - 09/05/2011 04:19 PM - Ohad Levy

- Target version deleted (0.3)

#2 - 12/01/2011 05:03 PM - Marcello de Sousa

I can't use foreman in production with this issue so a workaround I'm using at the moment is to add to the vhost something like this:

```
  <Location />
    Order Deny,Allow
    Deny from all
        Allow from <my allowed nets ex: 192.168.0.0/24>
        Allow from 127.0.0.1
  </Location>
  <Location ~ "^/unattended/(kickstart|built)$" >
    Order Deny,Allow
    Deny from all
        Allow from <my client nets where only unattended should be available>
      </Location>
```

#3 - 08/08/2012 06:15 AM - Karl Vollmer

This is a barrier to my use of Foreman for provisioning due to my clients being on an internal non-routed network. As a short-term fix we've used iptables on the smart-proxy (only system with external access to the foreman) to forward requests from the internal clients, my configuration also requires https://github.com/theforeman/foreman/pull/102 as well to completely resolve the issue.

#4 - 08/22/2012 12:25 PM - Mike Doherty

I've tried my hand at allowing the Smart Proxy to manage the ACL for a Squid proxy, so hosts that can't reach Foreman directly can use the Squid proxy.

- https://github.com/doherty/smart-proxy/tree/969
- https://github.com/doherty/foreman/tree/969

#5 - 07/23/2013 11:02 AM - Greg Sutcliffe

- Category set to TFTP

- Status changed from New to Assigned

- Assignee set to Greg Sutcliffe

Here's an approach allowing the client to request it's template from the smart-proxy by adding new routes to the smart-proxy:

https://github.com/theforeman/foreman/pull/751
https://github.com/theforeman/smart-proxy/pull/100

Caveat: Proxy needs to be running in 'http' mode, not 'https' as it cannot currently listen on two ports.

#6 - 10/01/2014 08:01 AM - Ohad Levy

- translation missing: en.field_release set to 21

#7 - 10/16/2014 01:18 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Target version set to 1.7.2

- Pull request https://github.com/theforeman/smart-proxy/pull/224 added

#8 - 10/28/2014 05:22 AM - Dominic Cleal

- translation missing: en.field_release deleted (21)

#9 - 10/29/2014 01:08 PM - Eric Helms

- Blocks Tracker #8172: Isolate Client Communication through a Capsule added

#10 - 11/05/2014 11:54 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- Assignee changed from Greg Sutcliffe to dustin tsang

- % Done changed from 0 to 100

- translation missing: en.field_release set to 21

#11 - 11/06/2014 09:44 AM - dustin tsang

- Blocks Feature #8147: Support for HTTP proxy added

#12 - 03/02/2015 11:24 AM - Stephen Benjamin

- Bugzilla link set to 1197806

#13 - 08/27/2015 04:51 AM - Lukas Zapletal

For the record, it looks like clients still try to reach the Foreman server to do the "built" request. The ticket #1096 unfortunately did not solve what was in the subject text. Creating new ticket #11582 for this.

#14 - 08/27/2015 04:51 AM - Lukas Zapletal

- Related to Feature #11582: Implement proxy API for "built" command added

#15 - 11/11/2016 10:40 AM - Dominic Cleal

- Related to Feature #17316: Proxy templating needs TFTP feature to be turned on added

Files

Foreman_Arch.png	67.8 KB	06/09/2011	Marcello de Sousa