pfSense - Feature #2410

Support name based aliasing via CNAMEs or some other mechanism.

05/03/2012 12:55 PM - allen landsidel

Status:	New	**Start date:**	05/03/2012
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	DNS Forwarder	**Estimated time:**	0.00 hour
Target version:			

Description

Resubmission of feature request 129 from 1.2.2

I would like to request that this feature reconsidered. Regardless of what DJB may think, there are good reasons to use CNAMEs (or some other form of hostname aliasing).

In our network we have a single intranet server, intranet01. It gets its address from DHCP; in fact, everything on the LAN side of the network gets its address from DHCP, be it static or dynamic. Services hosted by intranet01 have their own hostnames that are accessed via apache named virtual hosting, such as cacti, nagios, svn, and so on. Presently the only way to create these named aliases in pfsense is by IP address, which means the address must (realistically) be static, and moving the host to a new address or subnet is tedious and error-prone.

Ideally the IP address for a server should only be entered once or never, and aliases used everywhere else, so the address can be changed quickly, easily, and safely.

This problem was demonstrated (somewhat catastrophically) today when we moved DHCP into a different network range, and were left with many invalid and non-working aliases throughout the system that had been created referencing the IP address of a DHCP client; in the aftermath we found that we could not fix these by changing the address to the server name.

Associated revisions

Revision 5a2a8349 - 05/05/2012 07:07 AM - Lorenz Schori

Add support for aliases in DNS Forwarder, fixes #2410

History

#1 - 05/04/2012 05:42 AM - Lorenz Schori

- File DNS-forwarder-Edit-host-with-alias.png added

Hi. I probably could put together something for pfSense 2.0. Instead of implementing "real" CNAME support I'd like to propose an interface improvement in the DNS forwarder edit screen. I've thrown together a mock by copying over some code from the firewall alias edit screen.

Behind the scenes all the entries from the alias table would be written to /etc/hosts - but only after the main ip. This will ensure that dnsmasq will resolve PTR to the main name which is critical in Kerberos-Deployments etc.

DNS-forwarder-Edit-host-with-alias.png

Would that solve your problem?

#2 - 05/04/2012 08:02 AM - allen landsidel

Hosts file would work great I suspect, interface mock looks good too. Thanks!

#3 - 05/05/2012 07:35 AM - Lorenz Schori

- File 0001-Add-support-for-aliases-in-DNS-Forwarder-fixes-2410.patch added

- File dnsmasq-overview.png added

Patch attached. It applies on an installed pfsense 2.0.1 as well as onto git master.

In order to patch a running system you have to copy the patch onto the machine (using scp), then login via ssh and issue the following command:

```
cd / && patch -p1 < /tmp/0001-Add-support-for-aliases-in-DNS-Forwarder-fixes-2410.patch
```

The output should then look like this:

```
Hmm...  Looks like a unified diff to me...
The text leading up to this was:
--------------------------
|From 5a2a83493cdb3f647b4913f3b84ef864103148f5 Mon Sep 17 00:00:00 2001
|From: Lorenz Schori <lo@znerol.ch>
|Date: Sat, 5 May 2012 13:07:04 +0200
|Subject: [PATCH] Add support for aliases in DNS Forwarder, fixes #2410
|
|---
| etc/inc/system.inc                      |    6 ++
| usr/local/www/services_dnsmasq.php      |   19 +++++
| usr/local/www/services_dnsmasq_edit.php |  114 ++++++++++++++++++++++++++++++-
| 3 files changed, 138 insertions(+), 1 deletions(-)
|
|diff --git a/etc/inc/system.inc b/etc/inc/system.inc
|index a1517ed..b902761 100644
|--- a/etc/inc/system.inc
|+++ b/etc/inc/system.inc
--------------------------
Patching file etc/inc/system.inc using Plan A...
Hunk #1 succeeded at 247 (offset -11 lines).
Hmm...  The next patch looks like a unified diff to me...
The text leading up to this was:
--------------------------
|diff --git a/usr/local/www/services_dnsmasq.php b/usr/local/www/services_dnsmasq.php
|index d010d0a..9dbfc3a 100755
|--- a/usr/local/www/services_dnsmasq.php
|+++ b/usr/local/www/services_dnsmasq.php
--------------------------
Patching file usr/local/www/services_dnsmasq.php using Plan A...
Hunk #1 succeeded at 277.
Hmm...  The next patch looks like a unified diff to me...
The text leading up to this was:
--------------------------
|diff --git a/usr/local/www/services_dnsmasq_edit.php b/usr/local/www/services_dnsmasq_edit.php
|index 9aea153..e69d2ee 100755
|--- a/usr/local/www/services_dnsmasq_edit.php
|+++ b/usr/local/www/services_dnsmasq_edit.php
--------------------------
Patching file usr/local/www/services_dnsmasq_edit.php using Plan A...
Hunk #1 succeeded at 68.
Hunk #2 succeeded at 91.
Hunk #3 succeeded at 145 (offset -1 lines).
Hunk #4 succeeded at 167 (offset -1 lines).
Hunk #5 succeeded at 220 (offset -1 lines).
Hmm...  Ignoring the trailing garbage.
done
```

I've also updated the dns forwarder interface such that aliases are shown in the list:

dnsmasq-overview.png

HTH

#4 - 05/05/2012 11:30 AM - Jim Pingle

Was that patched against 2.0.1 or 2.1? It doesn't appear to apply to 2.1.

#5 - 05/05/2012 12:22 PM - Lorenz Schori

Actually the patch is against the master branch on github. The last commit i see in my git log is https://github.com/bsdperimeter/pfsense/commit/a52706d5d8bbaff13e22c78990648f2e4e17b1c7 which is also the current head over here (a52706d5).

There is neither a tag nor a branch relating to version 2.1. Where exactly can I find that one?

#6 - 05/05/2012 12:40 PM - Jim Pingle

mater is 2.1 (for now)

Interesting, I just did another gitsync to bring my VM up to the most current code and it still doesn't want to apply, but I re-fetched the patch and told it to ignore whitespace and now it likes it.

If you have that patch in a fork of the pfsense repo on github, you could submit a pull request once people have tested it out.

#7 - 05/05/2012 03:16 PM - Lorenz Schori

Done. https://github.com/znerol/pfsense Branch: feature/master/dns-host-alias

#8 - 05/05/2012 03:45 PM - Lorenz Schori

Whitespace is handled somewhat inconsistently throughout the pfsense codebase. I tried hard to mimic the style of existing code but apparently failed in services_dnsmasq_edit.php. I've pushed another one that should blend in better with the existing code.

#9 - 05/05/2012 05:46 PM - Jim Pingle

Whitespace could use some cleanup, but usually patches will work so long as they are clean. It may have been that the newlines on your patch were DOS (I didn't check) but a patch on the box expects UNIX newlines.

The "System Patches" package I just added yesterday pulls them in as-is, so I just had to check the box to ignore whitespace and off it went. It makes testing things like this really easy from supplied patches. You can just paste in the download URL for the patch from redmine or a git commit url, tell it to fetch, then apply, no muss, no fuss.

#10 - 05/05/2012 05:51 PM - Jim Pingle

The code seems to work fine for me. I added a host, gave it an alias, and it was populated in /etc/hosts as expected. Looks good to me. Submit a pull request and I'll approve it.

#11 - 05/06/2012 04:35 AM - Lorenz Schori

https://github.com/bsdperimeter/pfsense/pull/99

#12 - 05/06/2012 08:10 AM - Anonymous

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 5a2a83493cdb3f647b4913f3b84ef864103148f5.

#13 - 07/05/2012 06:35 PM - Jim Pingle

- Status changed from Feedback to Resolved

#14 - 07/17/2012 05:45 PM - Univa IT

This doesn't address the original user's request. I have the same request that he does. I want a CNAME to work for DHCP entries.

The first hint that this wasn't going to work was when the UI said the IP was a required field. For a CNAME (or plain old /etc/hosts alias) there is no IP. It's an alias to another hostname, not an IP.

I went to hack the /etc/hosts PHP in pfSense to fix this, but what I found was that the lines aren't being generated by the PHP. The lines that are incorrect are being apparently written by a binary file called /usr/local/sbin/dhcpleases.

Instead of:
10.10.0.1 foo.internal foo # dynamic entry from dhcpd.leases

it needs to write a line like:
10.10.0.1 foo.internal foo thing-that-points-to-foo.internal thing-that-points-to-foo another.internal another # dynamic entry from dhcpd.leases

... assuming that you had two alias entries called "thing-that-points-to-foo" and "another", both with an alias of "foo"

#15 - 07/19/2012 09:54 AM - allen landsidel

Sorry for the delay, but the more I think about it yes, Univa IT is correct. This is a partial solution, but it does still require me to enter an IP address to begin with, which doesn't help if I'm creating an alias for a hostname outside the purview of pfsense; e.g. an internal CNAME to an external host.

I think the hosts file aliasing as presented is useful in its own right, but it's not the same as supporting CNAMEs, and not quite as flexible.

#16 - 07/30/2012 10:49 AM - Jim Pingle

- Status changed from Resolved to New

Only partially fixed.

#17 - 07/30/2012 02:07 PM - Lorenz Schori

CNAME-support in dnsmasq is somewhat limited. If I'm not mistaken there is no way to specify a CNAME record pointing to a host whose IP address is not managed by / not known to dnsmasq.

The following excerpts from the dnsmasq documentation are relevant:

> **--cname=<cname>,<target>**
> Return a CNAME record which indicates that <cname> is really <target>. There are significant limitations on the target; it must be a DNS name which is known to dnsmasq from /etc/hosts (or additional hosts files) or from DHCP. If the target does not satisfy this criteria, the whole cname is ignored. The cname must be unique, but it is permissable to have more than one cname pointing to the same target.

That means that we have to specify each alias entry as a separate command line flag. Additionally the target must be managed by dnsmasq. And then later on:

> Addresses in /etc/hosts will "shadow" different addresses for the same names in the upstream DNS, so "mycompany.com 1.2.3.4" in /etc/hosts will ensure that queries for "mycompany.com" always return 1.2.3.4 even if queries in the upstream DNS would otherwise return a different address. There is one exception to this: if the upstream DNS contains a CNAME which points to a shadowed name, then looking up the CNAME through dnsmasq will result in the unshadowed address associated with the target of the CNAME. To work around this, add the CNAME to /etc/hosts so that the CNAME is shadowed too.

IMHO people which need a really flexible DNS setup should probably use a more sophisticated software than dnsmasq.

#18 - 07/30/2012 02:08 PM - Lorenz Schori

Forgot the manpage link: http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html

#19 - 07/30/2012 02:14 PM - Univa IT

Are you saying that dnsmasq is the product that ships the /usr/local/sbin/dhcpleases file that generates the dhcpd.leases per my comment above?

(FYI, I'm not clear on what advantage at all their is to the current patch, since it fails to address the original issue. If this can't be fixed, it may make sense to revert the patch from the repository.)

#20 - 07/30/2012 02:55 PM - allen landsidel

There is no need to revert the change. Just because it doesn't address **this** issue does not mean it's useless. It's not exactly what I want, but it is "enough" to prevent the problem that caused me to open this ticket from occurring again.

If anything, I would suggest a patch to the dnsmasq people to allow CNAMEs to point to targets unknown to dnsmasq -- this seems like an arbitrary and pointless limitation -- and then proceed with adding true CNAME support. Once it's in place, then the proposed solution could potentially be backed out, as this would cover both cases.

#21 - 12/11/2012 09:56 PM - Brendan Miller

FWIW, the tomato project uses dnsmasq with DNS forwarder-like functionality and allows mapping multiple hostnames to single IP addresses, optionally as part of a fixed DHCP lease by MAC address. This is exactly what I would like (of course, as I'm coming from a Tomato-product), but I believe is what's being asked here. I don't know if it has anything to do with /etc/hosts created from dhcpleases or not, as I have not delved into the dnsmasq code. I, too, would like to see this feature, but did I read somewhere that the pfsense dnsmasq could not support aliases/CNAMEs because it would interfere with the DHCP failover? Is that correct and the source of the "missing" feature? What if a user has no intention of using DHCP failover--it seems like the dnsmasq CNAME support could be used if it didn't conflict with something else the user was attempting. Just a thought from another camp. (And, yes, I'm a relative n00b trying to migrate from tomato to pfsense.)

Files

DNS-forwarder-Edit-host-with-alias.png	112 KB	05/04/2012	Lorenz Schori
0001-Add-support-for-aliases-in-DNS-Forwarder-fixes-2410.patch	8.19 KB	05/05/2012	Lorenz Schori
dnsmasq-overview.png	79.8 KB	05/05/2012	Lorenz Schori