pfSense - Feature #6373

RFC2136 DDNS could be more configurable to improve security

05/19/2016 07:30 PM - Marc Dye

Status:	Resolved		**Start date:**	05/19/2016
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	100%
Category:	Dynamic DNS		**Estimated time:**	0.00 hour
Target version:	2.4.0			

Description

Our RFC2136-style DDNS depends on external determination of the real IP address (usu. DHCP-assigned by the ISP). Such dynamically-assigned addressing is pervasive, but the design is half-baked: there is no specification of any means by which devices inside the boundary created by the client device (e.g. cable router) may officially, authentically, and privately discover their effective external IP from the entity which has assigned it.

So presently this determination is made by querying a hardcoded URL. (To reiterate: this isn't about where the DDNS name-to-address mapping is registered, this is about how pfSense discovers a dynamically-assigned external IP address.)

While this might be tolerable for personal or casual use, we can easily do much better.

There are two improvements needed:

(1) Allow the URL used for external IP discovery to be user-configurable, on a per-mapping basis,

(2) Support "https://" URLs in this configurable item.

The second should essentially 'just work' once the first is done. However, help text and other documentation needs to reference appropriate configuration of, e.g., external CA certificates in a fashion similar to that of certificate-based authentication of IPsec endpoints, etc.

(An ancilliary topic is: to what should the default configurable be set?)

Subtasks:

Feature # 6374: Provide sample server-side logic to report peer's IP address for use wi...	**Resolved**

History

#1 - 05/19/2016 08:46 PM - Jim Thompson

- Assignee set to Marc Dye

#2 - 07/10/2016 03:52 AM - Chris Buechler

- Target version changed from 2.3.2 to 2.4.0

#3 - 08/24/2016 04:05 PM - Jeremy Porter

This is a quick and dirty way for us to add checkip services to nginx on our production web boxes:
location = /ip {
default_type text/html;
content_by_lua '
ngx.say("<html><head><title>Current IP Check</title></head><body>Current IP Address: ")
ngx.say(ngx.var.remote_addr)
ngx.say("</body></html>")
';
}
We could support https through the *.pfsense.org certificate.
My recommendation is use checkip.pfsenes.org for the host name

#4 - 01/24/2017 06:08 AM - Renato Botelho

- Assignee deleted (Marc Dye)

#5 - 01/26/2017 12:28 PM - Jim Pingle

- Status changed from New to Resolved

Items 1 and 2 were completed under [#6591](#) which was resolved by PR <u>https://github.com/pfsense/pfsense/pull/3037</u>