pfSense - Bug #4785

IKEv2 w/PSK not matching where remote is FQDN

06/22/2015 05:21 PM - Chris Buechler

Status:	Resolved	**Start date:**	06/22/2015
Priority:	Very High	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.2.3		
Affected Version:	2.2.3	**Affected Architecture:**	

Description

Where using IKEv2 with PSK on a site to site VPN, where the identifiers are IPs, and the remote is a FQDN, you end up with something like the following:

```
Jun 22 16:29:44    charon: 01[NET] <con3|1> sending packet: from 172.27.44.52[500] to 172.27.44.51[500] (300 bytes)
Jun 22 16:29:44    charon: 01[NET] <con3|1> received packet: from 172.27.44.51[500] to 172.27.44.52[500] (76 bytes)
Jun 22 16:29:44    charon: 01[ENC] <con3|1> parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Jun 22 16:29:44    charon: 01[IKE] <con3|1> received AUTHENTICATION_FAILED notify error
Jun 22 16:29:44    charon: 01[IKE] <con3|1> received AUTHENTICATION_FAILED notify error
```

or:

```
Jun 22 16:27:14    charon: 05[IKE] <con3|3> no shared key found for '172.27.44.52' - '172.27.44.51'
Jun 22 16:27:14    charon: 05[IKE] <con3|3> no shared key found for '172.27.44.52' - '172.27.44.51'
```

where ipsec.secrets is configured like:

```
%any 172.27.44.51 : PSK 0sFjeRIUgndkfjEiufeskFD
```

Change %any to the specific local identifier and it works fine.

```
172.27.44.52 172.27.44.51 : PSK 0sFjeRIUgndkfjEiufeskFD
```

Associated revisions

Revision fe96d725 - 06/22/2015 07:42 PM - Chris Buechler

Use $myid in ipsec.secrets. Ticket #4785

Revision d812e83e - 06/22/2015 07:43 PM - Chris Buechler

Use $myid in ipsec.secrets. Ticket #4785

Conflicts:

etc/inc/vpn.inc

Revision 29c9e140 - 06/23/2015 07:59 AM - Renato Botelho

Add a workaround for ticket #4785:

There was a regression on strongswan between 5.3.0 and 5.3.2 as reported
at [1]. To workaround this issue, add an extra line on ipsec.secrets
with right fqdn.

Revision 019ee2bc - 06/23/2015 08:22 AM - Renato Botelho

Add a workaround for ticket #4785:

There was a regression on strongswan between 5.3.0 and 5.3.2 as reported
at [1]. To workaround this issue, add an extra line on ipsec.secrets
with right fqdn.

Revision dbd43cc2 - 06/23/2015 12:12 PM - Renato Botelho

Instead of sending USR1, just call ipsec reload. And before it, call ipsec rereadsecrets to make sure new secretes are updated. It should fix #4785

Revision a241d6b5 - 06/23/2015 12:12 PM - Renato Botelho

Instead of sending USR1, just call ipsec reload. And before it, call ipsec rereadsecrets to make sure new secretes are updated. It should fix #4785

Revision 9edeadc5 - 06/23/2015 12:15 PM - Renato Botelho

Replace ipsec rereadsecrets + reload by single rereadall, that will re-read also cert changes. Ticket #4785

Revision 8961801d - 06/23/2015 12:15 PM - Renato Botelho

Replace ipsec rereadsecrets + reload by single rereadall, that will re-read also cert changes. Ticket #4785

Revision 2f898d6a - 06/23/2015 12:31 PM - Renato Botelho

rereadall is not enough here, restore reload call to make sure everything works. Ticket #4785

Revision 96072f52 - 06/23/2015 12:31 PM - Renato Botelho

rereadall is not enough here, restore reload call to make sure everything works. Ticket #4785

History

#1 - 06/22/2015 07:41 PM - Chris Buechler

- Status changed from Confirmed to Feedback

- Assignee set to Chris Buechler

should be fixed, need to double check every type of config to verify all still work.

#2 - 06/23/2015 12:20 PM - Renato Botelho

- % Done changed from 0 to 100

Applied in changeset dbd43cc24d6c18f6bf279c4e52a7a01d2bdfb8c5.

#3 - 06/23/2015 12:20 PM - Renato Botelho

Applied in changeset a241d6b53ac8d1aefe854d673ed5f41693ce9388.

#4 - 06/23/2015 03:54 PM - Chris Buechler

- Status changed from Feedback to Resolved

confirmed good.