pfSense - Bug #6668

IPSec tunnel + L2TP/IPSec VPN - wrong PSK chosen by pfSense

07/31/2016 04:22 PM - Janusz Baranek

Status:	Feedback	**Start date:**	07/31/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	2.3.1	**Affected Architecture:**	

Description

Setup:
1. IPSec, IKEv1 site to site tunnel, PSK, Main mode. FQDN identifier - talking to a Mac OS server (racoon)
2. L2TP/IPSec for mobile clients, PSK, Main mode.

Procedure:
1. The IPSec tunnel was set-up, all went well, tunnel established (no other VPN services yet)
2. The L2TP was set-up according to this guide [url]https://doc.pfsense.org/index.php/L2TP/IPsec[/url], however I needed to add "Any TCP flags" to my LAN and L2TP allow-all firewall rule to get connections to work (the floating rule for L2TP was not sufficient). L2TP Clients could connect.

All worked.... until the IPSec tunnel rekeyed a few hours later. Then impossible to reestablish the connection.
Debug logs showing that it was failing at the end of phase 1, hash not matching when I switched to aggressive mode, payload length incorrect in main mode. All DH shared secrets and auth data to hash were identical. This pointed to a PSK problem, yet the connection was established, so I knew my PSKs were correct.

After much head scratching, rebooting of servers, it turns out that the problem is that pfSense/strongSwan was selecting the wrong PSK.

Doing a cat /var/etc/ipsec/ipsec.secrets in the shell gives

```
%any : PSK 0s<base 64 encoded L2TP PSK>
vpn.mycompany.com : PSK 0s<base 64 encoded tunnel PSK>
```

It would seem that the %any has priority over the identified entry, so the L2TP PSK is always selected - according to the L2TP doc, any user is needed to configure L2TP... which would explain why the tunnel came up to start with (no other PSK candidates).
As a workaround, I changed the tunnel PSK to be the same as the L2TP PSK and, bingo, the tunnel came up.

It would seem that the PSK values are checked in the order they are listed, no hierarchization of matching identifiers, so the %any entry enumerated first, matches and returns the PSK, which is wrong for the IPSec tunnel.

Checking the strongSwan sources (5.5.0)
strongswan-5.5.0/src/libstrongswan/credentials/sets/mem_cred.c:504 -
create_shared_enumerator uses enumerator_create_filter which stops on the first match, only owners within each line in ipsec.secrets have a best match applied via shared_filter (line 454)

To correct:
Either:
1. Within pfSense would be to order secrets in ipsec.secrets so that wildcard ids are at the end,
or
2. Correct strongSwan to choose the best match rather that enumerating the secrets in a linear manner.

History

#1 - 07/31/2016 04:53 PM - Janusz Baranek

ERRATUM:

ipsec.secrets (mistyped) should be:

```
%any @vpn.mycompany.com : PSK 0s<base 64 encoded tunnel PSK>
 %any : PSK 0s<base 64 encoded L2TP PSK>
```

(this was the contents of the file when the problem occurred)

As the shared keys are in reverse order in the list (mem_cred.c:534 - add_shared_list calls insert_first) the %any rule would be enumerated first. So my suggested correction in pfSense should be:
1. Within pfSense would be to order secrets in ipsec.secrets so that wildcard ids are at the **start**,

#2 - 11/03/2016 09:53 PM - Jim Thompson

- Assignee set to Jim Pingle

- Target version set to 2.4.0

#3 - 11/04/2016 10:39 AM - Jim Pingle

- File psk-ordering.diff added

- Status changed from New to Feedback

- Assignee changed from Jim Pingle to Janusz Baranek

I'm hesitant to commit changes to the ordering without lots of testing first, so can you try the attached patch to see if it resolves the problem for you? (use the System Patches package, path strip = 2)

The patch changes the ordering so any PSK with a wildcard local ID is places last in the secrets file. It would appear to help, but I'm not sure it goes far enough. If it's not sufficient it may need review by Renato or Luiz.

#4 - 12/23/2016 09:02 AM - Jim Pingle

- Assignee deleted (Janusz Baranek)

- Target version deleted (2.4.0)

No response from the OP, can't seem to reproduce it.

If someone can reproduce it and test a potential fix, please provide feedback. Potential impact of changing the affected code is fairly large so any fix needs testing before it can be committed.

#5 - 04/02/2018 03:15 AM - Lasse not relevant

I tried the patch, without success.

ipsec.secrets (without patch):
<WANIP> @<DN> : PSK 0s<PSK-01>
: PSK 0s<PSK-01>
%any <IP-OTHER-SIDE> : PSK 0s<PSK-02>

ipsec.secrets (patch applied):
: PSK 0s<PSK-01>

#6 - 08/13/2019 10:16 AM - Jim Pingle

Is this still a problem, even on 2.5.0 snapshots?

Files

psk-ordering.diff	1.96 KB	11/04/2016	Jim Pingle