pfSense - Bug #7856

IPsec status does not show all connected mobile clients

09/12/2017 02:55 PM - Jim Pingle

Status:	Resolved	**Start date:**	09/12/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.4.2		
Affected Version:	All	**Affected Architecture:**	All

Description

The IPsec status page only shows one connected mobile client, no matter how many are connected. All clients are shown in ipsec statusall and swanctl --list-sas but they are shown as being under 'con1' with different identifiers underneath.

The IPsec status page prints everything it gets back from ipsec_list_sa() (/etc/inc/ipsec.inc) which in turn calls the pfSense PHP module function pfSense_ipsec_list_sa()

In freebsd-ports:devel/php56-pfSense-module/files/pfSense.c that function gets data from strongSwan via VICI and runs it through build_ipsec_sa_array() in the same file.

Looking at the returned array, there is only one 'con1' entry which makes sense since it's an array key and should be unique, but the entry also contains a 'uniqueid' that should probably be combined in some way with the connection ID. Otherwise, it would appear, that whichever entry was parsed last is output.

For example:

```
: swanctl --list-sas
con1: #7, ESTABLISHED, IKEv1, d0a16a030b678f99_i 33fd68d09613def2_r*
  local  '198.51.100.11' @ 198.51.100.11[4500]
  remote 'vpn@dw.example.com' @ 198.51.100.6[45008] XAuth: 'river' [10.11.200.2]
  AES_CBC-128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 406s ago, reauth in 85302s
  con1: #11, reqid 2, INSTALLED, TUNNEL-in-UDP, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 404s ago, rekeying in 2145s, expires in 3196s
    in  cb41f9da,      0 bytes,     0 packets,   404s ago
    out 009ccd0b,      0 bytes,     0 packets
    local  10.11.0.0/24|/0
    remote 10.11.200.2/32|/0
  con1: #12, reqid 3, INSTALLED, TUNNEL-in-UDP, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 403s ago, rekeying in 2329s, expires in 3197s
    in  c7552f69,   1100 bytes,    25 packets,   398s ago
    out 0d8e9be7,   1352 bytes,    13 packets,   398s ago
    local  0.0.0.0/0|/0
    remote 10.11.200.2/32|/0
con1: #3, ESTABLISHED, IKEv1, f46b7f72c0dc671c_i 2cc011e96df6b524_r*
  local  '198.51.100.11' @ 198.51.100.11[4500]
  remote 'vpn@dw.example.com' @ 198.51.100.3[16058] XAuth: 'jimp' [10.11.200.1]
  AES_CBC-128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 652s ago, reauth in 84892s
con2: #2, ESTABLISHED, IKEv2, b6ab01a3839d5454_i 34602494f7b54879_r*
  local  '198.51.100.11' @ 198.51.100.11[500]
  remote '198.51.100.2' @ 198.51.100.2[500]
  AES_CBC-256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 20110s ago
  con2: #10, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-256/HMAC_SHA1_96
    installed 1025s ago
    in  c8b033f1,   1344 bytes,    16 packets,   174s ago
    out cf9278de,   2432 bytes,    16 packets,   174s ago
    local  10.11.0.0/24|/0
```

```
    remote 10.2.0.0/24|/0
```

Note that it's "con1, #7" and "con1, #3".

Now look at the output from ipsec_list_sa():

```
array (
  'con1' =>
  array (
    'uniqueid' => '3',
    'version' => '1',
    'state' => 'ESTABLISHED',
    'local-host' => '198.51.100.11',
    'local-port' => '4500',
    'local-id' => '198.51.100.11',
    'remote-host' => '198.51.100.3',
    'remote-port' => '16058',
    'remote-id' => 'vpn@dw.example.com',
    'remote-xauth-id' => 'jimp',
    'initiator-spi' => 'f46b7f72c0dc671c',
    'responder-spi' => '2cc011e96df6b524',
    'nat-local' => 'yes',
    'nat-remote' => 'yes',
    'nat-any' => 'yes',
    'encr-alg' => 'AES_CBC',
    'encr-keysize' => '128',
    'integ-alg' => 'HMAC_SHA1_96',
    'prf-alg' => 'PRF_HMAC_SHA1',
    'dh-group' => 'MODP_1024',
    'established' => '404',
    'reauth-time' => '85140',
    'remote-vips' =>
    array (
      0 => '10.11.200.1',
    ),
    'child-sas' =>
    array (
    ),
  ),
)
```

The entry has a 'uniqueid' property which corresponds to its # under con1, but there is only a single array entry and not one for each mobile client.

If that is changed then some code in the status page will likely need changed as well since that key is used for connect/disconnect and other actions.

Assuming it's not actually a bug with strongSwan's VICI code, it will need someone a familiar with the C and/or VICI code in the pfSense PHP module to address it.

Associated revisions

Revision 1144e24c - 09/21/2017 11:27 AM - Steve Beaver

Fixed #7856

Revision 130f3c92 - 10/24/2017 09:13 AM - Stephen Jones

Fixed #7856 fixed an issue with a slightly different array format. Also updated the child key and id to be more robust.

History

#1 - 09/15/2017 10:38 AM - Steve Beaver

- Assignee set to Anonymous

#2 - 09/21/2017 11:40 AM - Steve Beaver

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset 1144e24cabeda458b266b9874b827746f4c0f8a0.

#3 - 10/11/2017 07:17 AM - Jim Pingle

- Status changed from Feedback to Assigned

It looks like this change caused a regression, see #7923

Also one person on the forum reported that the status breaks when there are no tunnels defined or active.

#4 - 10/12/2017 09:46 AM - Jim Pingle

- Target version changed from 2.4.1 to 2.4.2

Moving target to 2.4.2 as we need 2.4.1 sooner than anticipated.

#5 - 10/17/2017 08:47 AM - Azamat Khakimyanov

- File crash-report.txt added

I did some tests with SG-2220 (2.4.1-DEVELOPMENT (amd64)) and IPsec widget was on Dashboard, but there wasn't any IPsec tunnel. But I caught 2 crashes. I attached this crashreport

#6 - 10/23/2017 12:24 PM - Jim Pingle

Looks like there are a couple systems here I have which don't want to print child SAs with this code in place again. Some work though, and some do not. Need to gather more info about what may be happening.

#7 - 10/24/2017 09:30 AM - Anonymous

- Status changed from Assigned to Feedback

Applied in changeset 130f3c9266e0b8c626aa6e8991467bb417ff8fd2.

#8 - 10/25/2017 11:37 AM - Jim Pingle

- Status changed from Feedback to Assigned

On 2.4.2 snapshots, at least with an IKEv1 PSK+Xauth connection it's still only showing one connected client at a time.

#9 - 11/02/2017 09:31 AM - Anonymous

- Status changed from Assigned to Feedback

#10 - 11/02/2017 09:33 AM - Anonymous

Applied in changeset a65b41a9e455786dd969a1ffcd110fdf195f9031.

#11 - 11/04/2017 04:13 PM - Anonymous

tested on 2.4.2.a.20171103.1355, not seeing duplicate entries

#12 - 11/09/2017 03:49 PM - Jim Pingle

- Status changed from Feedback to Resolved

Files

crash-report.txt	146 KB	10/17/2017	Azamat Khakimyanov