strongSwan - Bug #445

UNITY_SPLIT_INCLUDE attributes contains no data

15.11.2013 08:59 - Alexander Kalashnikov

Status:	Closed	**Start date:**	15.11.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

Hello,

tried to check if UNITY_SPLIT_INCLUDE works, so I've setup small VPN server with the following config:

```
conn Corp-VPN-RSA-XAuth
    leftauth=pubkey
    leftcert=10000000000000.pem
    left=%any
    leftsubnet=192.168.254.0/23
    right=%any
    rightauth=pubkey
    rightauth2=xauth-eap
    rightsourceip=192.168.254.16/28
    rightdns=192.168.254.1
    keyexchange=ikev1
    ike=aes256-sha1-modp1536!
    esp=aes256-sha1!
    compress=yes
    fragmentation=yes
    auto=add
```

I've tried to connect there by using both Cisco VPN client and ShrewSoft VPN client but both of them refused to use leftsubnet for split tunnelling and tried to use 0.0.0.0/0.

Logs from Cisco VPN client said that UNITY_SPLIT_INCLUDE attrs contained no data:

```
283    09:43:13.960  11/15/13  Sev=Info/4    IKE/0xA3000015
MODE_CFG_REPLY: Received MODECFG_UNITY_SPLIT_INCLUDE attribute with no data

284    09:43:13.960  11/15/13  Sev=Info/4    IKE/0xA3000015
MODE_CFG_REPLY: Received MODECFG_UNITY_SPLIT_INCLUDE attribute with no data
```

However Strongswan log claims that there was some data in that payload:

```
Nov 15 09:43:21 13[IKE] assigning virtual IP 192.168.254.17 to peer 'st41ker'
Nov 15 09:43:21 13[CFG] sending UNITY_SPLIT_INCLUDE: 192.168.254.0/23
Nov 15 09:43:21 13[ENC] generating TRANSACTION response 2009454997 [ HASH CPRP(ADDR DNS DNS U_SPLI
TINC) ]
```

I have no idea how to see what exactly was in the packet, so I've posted the issue here.

Associated revisions

Revision fa9b6e88 - 23.01.2014 11:19 - Tobias Brunner

Merge branch 'unity-fixes'

Improves compatibility with the Cisco and Shrew clients.

Fixes #445.

History

#1 - 15.11.2013 17:55 - Tobias Brunner

- Tracker changed from Issue to Bug

- Description updated

- Category set to charon

- Status changed from New to Assigned

- Assignee set to Tobias Brunner

- Priority changed from High to Normal

- Target version set to 5.1.2

> Logs from Cisco VPN client said that UNITY_SPLIT_INCLUDE attrs contained no data

I was able confirm this with both clients (Shrew simply ignores the payload).

What was thought to be 6 bytes of superfluous padding after the subnet and the netmask in *UNITY_SPLIT_INCLUDE* and *UNITY_LOCAL_LAN* configuration attributes is apparently used to transmit the IP protocol and the source and destination ports of the traffic selector:

```
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001

SPLIT_NET #1
    subnet = 192.168.254.0
    mask = 255.255.254.0
    protocol = 0
    src port = 0
    dest port=0
```

Both clients wont accept the configuration attributes if the additional bytes are missing. So far these attributes have mainly been used with *racoon* on iOS and Mac OS X, which apparently has no problems if the payloads are shorter.

With the additional bytes added the clients can properly parse the payloads but they are not able to complete Quick Mode successfully. The problem is that both expect the remote peer to return 0.0.0.0/0 as remote traffic selector, but strongSwan actually uses the subnets that were configured as *leftsubnet*. For Shrew there is a workaround by setting the "Policy Generation Level" option to *unique* instead of *auto*. For Cisco clients patching strongSwan is required.

Another problem is that the Cisco client does not handle multiple *UNITY_SPLIT_INCLUDE* attributes. It only uses the first one.

I pushed fixes for these issues to the *unity-fixes* branch of our repository.

The handling of *UNITY_SPLIT_INCLUDE* and *UNITY_LOCAL_LAN* attributes in the attr and attr-sql plugins would need similar fixes in order to work successfully with these clients.

#2 - 16.11.2013 19:38 - Alexander Kalashnikov

Tobias,

I've downloaded unity_narrow.c and unity_provider.c from unity-fixes branch and rebuilded Strongswan
Now Cisco client works as expected and routes all subnets from leftsubnet through VPN. Thank you for pathes.

I'm still working on checking the issue with Shrewsoft client. Seems like it is still not working, but I'm not sure.
Please, wait for my update.

Thank you.

#3 - 16.11.2013 20:20 - Alexander Kalashnikov

Tobias,

Cisco client (5.0.07.0290) never asked for 0.0.0.0/0 TS in my case.
It uses only networks from leftsubnet, so it handles multiple UNITY_SPLIT_INCLUDE attributes. Your patches resolved the issue for this client completely.
Seems like you (or someone competent) should proceed with fixes for attr and attr-sql plugins.

Shrewsoft tries to configure 0.0.0.0/0 TS because it failing to perform autoconfiguration (when "Obtain Topology Information or Tunnel all" checked).
So, when it fails Obtain Topology it tries to Tunnel all traffic through the remote gateway. This should be investigated further.

Thank you.

#4 - 21.11.2013 17:56 - Tobias Brunner

> Cisco client (5.0.07.0290) never asked for 0.0.0.0/0 TS in my case.

I used the same version in my tests. And it definitely sends 0.0.0.0/0 as remote TS (you can see that if you increase the log level of the CFG log group to 2):

```
selecting traffic selectors for us:
  config: 192.168.254.0/23, received: 0.0.0.0/0 => match: 192.168.254.0/23
```

Without the patch that changes the TS (i.e. if strongSwan sends back the TS configured in *leftsubnet*) the client would abort Quick Mode and log something like this:

```
700    17:24:15.388  11/21/13  Sev=Info/4    IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID) from 192.168.1.1

701    17:24:15.388  11/21/13  Sev=Warning/3    IKE/0xE3000060
Unable to validate the responder ID, ID=192.168.254.0/255.255.254.0 Protocol=0 port=0, the peer sent

702    17:24:15.388  11/21/13  Sev=Warning/2    IKE/0xE300009B
Failed to process ID payload (MsgHandler:681)
```

> Shrewsoft tries to configure 0.0.0.0/0 TS because it failing to perform autoconfiguration (when "Obtain Topology Information or Tunnel all" checked).
> So, when it fails Obtain Topology it tries to Tunnel all traffic through the remote gateway. This should be investigated further.

I can't reproduce this. With my patches applied and the following settings in Shrew's *Policy* tab this works as it should:

- Policy Generation Level: auto
- [ ] Maintain Persistent Security Associations
- [x] Obtain Topology Automatically or Tunnel All

While Shrew, like the Cisco client, requests 0.0.0.0/0 as remote TS, it correctly installs the narrowed traffic selectors. You can see the IPsec policies in Shrew's *Trace Utility* (*Security Policies* tab).

Could you please post Shrew's log file (*IKE Service* tab in the Trace Utility) if you think there is still a problem.

#5 - 10.01.2014 14:37 - Alexander Kalashnikov

Hello,

sorry for the late reply.

Seems like your patches fixed the issue, so you may close this bug as resolved and all that left is to patch corresponding attr plugin.

Thank you.

#6 - 23.01.2014 11:22 - Tobias Brunner

- Status changed from Assigned to Closed

- Resolution set to Fixed