strongSwan - Bug #247

UNITY_SPLIT_INCLUDE attribute exists in configuration payload even if 'leftsubnet' is absent in ipsec.conf

29.10.2012 19:32 - Maxim Izergin

Status:	Closed	**Start date:**	29.10.2012
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.2		
Affected version:	5.0.1	**Resolution:**	Fixed

Description

I'm going further in configuration of StrongSwan with Apple iOS devices.
During configuration of cisco_unity plugin I faced with the problem that StrongSwan sends UNITY_SPLIT_INCLUDE = 'dynamic' inside CONFIGURATION_V1 payload even if 'leftsubnet' is not defined in ipsec.conf.
Device log is:

```
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration started.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-ADD
RESS = 172.17.18.223.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-MAS
K = 255.255.255.0.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-DNS
 = 172.17.18.1.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: LOCAL-LAN[0] = d
estination 172.17.18.223/8 -> gateway 172.17.18.223/32.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: LOCAL-LAN[0] = d
estination 172.17.18.223/13 -> gateway 172.17.18.223/32.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: SPLIT-INCLUDE.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Error>: cannot write on routing socket: File exists (a
ddress 0.0.0.0, gateway 172.17.18.223)
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Phase2 starting.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration established.
Oct 29 17:16:57 iPhone-Maximus configd[50] <Notice>: IPSec Phase1 established.
```

Error is **cannot write on routing socket: File exists (address 0.0.0.0, gateway 172.17.18.223)**

StrongSwan log is:

```
Oct 29 18:38:02 12[CFG] <fignya|1> proposing traffic selectors for us:
Oct 29 18:38:02 12[CFG] <fignya|1>  dynamic
Oct 29 18:38:02 12[CFG] <fignya|1> sending UNITY_SPLIT_INCLUDE: dynamic
Oct 29 18:38:02 12[IKE] <fignya|1> building UNITY_SPLIT_INCLUDE attribute
Oct 29 18:38:02 12[ENC] <fignya|1> added payload of type CONFIGURATION_V1 to message
```

I have tested racoon with same configuration (split_network is not defined in config) and everything works fine. Here is log from device:

```
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration started.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-ADD
RESS = 172.17.18.100.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-MAS
K = 255.255.0.0.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: SAVE-PASSWORD =
0.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-DNS
 = 172.17.18.1.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: BANNER = Hi!
.
```

```
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: DEF-DOMAIN = .
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: LOCAL-LAN[0] = d
estination 172.17.18.100/24 -> gateway 172.17.18.100/32.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: DEFAULT-ROUTE =
local-address 172.17.18.100/32.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Phase2 starting.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration established.
Oct 29 17:22:15 iPhone-Maximus configd[50] <Notice>: IPSec Phase1 established.
```

As you can see there is no need to send SPLIT-INCLUDE. Is it possible to issue patch which removes SPLIT-INCLUDE from CONFIGURATION_V1 payload if 'leftsubnet' is not defined in ipsec.conf?
I'll perform tests and report the status.

Thank you in advance!

History

#1 - 29.10.2012 20:11 - Maxim Izergin

I have managed to reproduce same error with racoon. If I set *split_network include 0.0.0.0/0;* then same problem occurs. It means that for routing all traffic (0.0.0.0/0) to VPN there should **not** be SPLIT-INCLUDE in the payload. With other subnets in SPLIT-INCLUDE both StrongSwan and racoon work fine.

#2 - 30.10.2012 09:21 - Martin Willi

- File 0001-Exclude-dynamic-TS-from-Unity-Split-Include-attribut.patch added

> proposing traffic selectors for us:
> dynamic
> sending UNITY_SPLIT_INCLUDE: dynamic

I didn't have time to test this in detail with iOS, but you may try the attached patch. I'm a little skeptic though that a to-host connection works at all with iOS devices.

#3 - 30.10.2012 16:33 - Maxim Izergin

Hi Martin,
I confirm that patch solves the problem. Here is device log:

```
Oct 30 16:24:38 iPhone-Maximus racoon[2024] <Notice>: >>>>> phase change status = phase 1 established
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration started.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-ADDRESS = 172.1
7.18.223.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-MASK = 255.255.
255.0.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: INTERNAL-IP4-DNS = 172.17.18
.1.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: LOCAL-LAN[0] = destination 1
72.17.18.223/8 -> gateway 172.17.18.223/32.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: LOCAL-LAN[0] = destination 1
72.17.18.223/32 -> gateway 172.17.18.223/32.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration: DEFAULT-ROUTE = local-addres
s 172.17.18.223/32.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Phase2 starting.
Oct 30 16:24:38 iPhone-Maximus configd[50] <Notice>: IPSec Network Configuration established.
```

All traffic on device goes through VPN if SPLIT-INCLUDE is absent in configuration payload. LOCAL-LAN also works in this case.
Thank you very much for help!

#4 - 31.10.2012 09:26 - Martin Willi

- Status changed from New to Closed

- Assignee set to Martin Willi

- Target version set to 5.0.2

- Resolution set to Fixed

Files

0001-Exclude-dynamic-TS-from-Unity-Split-Include-attribut.patch	808 Bytes	30.10.2012	Martin Willi