strongSwan - Bug #356

Strongswan ignores rightsubnet, when "handling UNITY_LOCAL_LAN attribute failed"

10.07.2013 00:40 - Noel Kuntze

Status:	Closed	**Start date:**	10.07.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.0		
Affected version:	5.0.4	**Resolution:**	Fixed

Description

Hello,

When Strongswan encounters "handling UNITY_LOCAL_LAN attribute failed" when initiating a IKEv1 SA, then it doesn't set the route defined in rightsubnet, but sets the default route to go through the Tunnel.
I don't think this is intended.

Regards,
Noel

ipsec.conf:

```
conn fh
        xauth_identity=nkuntze
        leftauth=psk
        leftauth2=xauth
        leftid=$INITIATOR_ID
        leftsourceip=%config
        rightauth=psk
        rightid=$RESPONDER_ID
        right=$RESPONDER
        rightsubnet=141.79.0.0/16
        keyexchange=ikev1
        ike=aes256-sha1-modp1024
        esp=aes256-sha1
        aggressive=yes
        compress=no
        auto=add
        inactivity=0
        ikelifetime=30m
        #marginbytes=3000000000
        #marginpackets=150000
        leftupdown=/usr/lib/strongswan/fh.sh # this is my own hook to set up SNAT for that route
        dpdaction=restart
```

command:

```
# ipsec up fh
initiating Aggressive Mode IKE_SA fh[2] to 193.197.x.x
generating AGGRESSIVE request 0 [ SA KE No ID V V V V V ]
sending packet: from 192.168.178.48[500] to 193.197.x.x[500] (403 bytes)
received packet: from 193.197.x.x[500] to 192.168.178.48[500] (478 bytes)
parsed AGGRESSIVE response 0 [ SA KE No ID HASH V V V V NAT-D NAT-D V V V ]
received Cisco Unity vendor ID
received XAuth vendor ID
received DPD vendor ID
received NAT-T (RFC 3947) vendor ID
received FRAGMENTATION vendor ID
received unknown vendor ID: 69:dd:00:4f:ef:7a:c1:1f:72:39:5c:80:c1:36:7d:81
received unknown vendor ID: 1f:07:f7:0e:aa:65:14:d3:b0:fa:96:54:2a:50:01:00
```

```
local host is behind NAT, sending keep alives
generating AGGRESSIVE request 0 [ NAT-D NAT-D HASH ]
sending packet: from 192.168.178.48[4500] to 193.197.x.x[4500] (108 bytes)
received packet: from 193.197.x.x[4500] to 192.168.178.48[4500] (76 bytes)
parsed TRANSACTION request 2312482182 [ HASH CP ]
generating TRANSACTION response 2312482182 [ HASH CP ]
sending packet: from 192.168.178.48[4500] to 193.197.x.x[4500] (92 bytes)
received packet: from 193.197.x.x[4500] to 192.168.178.48[4500] (76 bytes)
parsed TRANSACTION request 2655167844 [ HASH CP ]
XAuth authentication of 'nkuntze' (myself) successful
IKE_SA fh[2] established between 192.168.178.48[$INITIATOR_ID]...193.197.x.x[$RESPONDER_ID]
scheduling reauthentication in 1591s
maximum IKE_SA lifetime 1771s
generating TRANSACTION response 2655167844 [ HASH CP ]
sending packet: from 192.168.178.48[4500] to 193.197.x.x[4500] (76 bytes)
generating TRANSACTION request 122847407 [ HASH CP ]
sending packet: from 192.168.178.48[4500] to 193.197.x.x[4500] (92 bytes)
received packet: from 193.197.x.x[4500] to 192.168.178.48[4500] (108 bytes)
parsed TRANSACTION response 122847407 [ HASH CP ]
installing DNS server 141.79.128.10 via resolvconf
installing DNS server 141.79.128.4 via resolvconf
handling UNITY_LOCAL_LAN attribute failed
installing new virtual IP 141.79.x.x
generating QUICK_MODE request 2883248040 [ HASH SA No ID ID ]
sending packet: from 192.168.178.48[4500] to 193.197.x.x[4500] (204 bytes)
received packet: from 193.197.x.x[4500] to 192.168.178.48[4500] (188 bytes)
parsed QUICK_MODE response 2883248040 [ HASH SA No ID ID N((24576)) ]
CHILD_SA fh{2} established with SPIs c53bfdf0_i 74550fcb_o and TS 141.79.x.x/32 === 0.0.0.0/0
connection 'fh' established successfully
```

Log:

```
charon[30143]: 03[CFG] received stroke: initiate 'fh'
charon[30143]: 05[IKE] initiating Aggressive Mode IKE_SA fh[1] to 193.197.x.x
charon[30143]: 02[IKE] IKE_SA fh[1] established between 192.168.178.48[$INITIATOR_ID]...193.197.x.
x[$RESPONDER_ID]
charon[30143]: 15[CFG] handling UNITY_LOCAL_LAN attribute failed
charon[30143]: 01[IKE] CHILD_SA fh{1} established with SPIs c6e6abc0_i d8536829_o and TS 141.79.x.
x/32 === 0.0.0.0/0
charon[30143]: 16[CFG] received stroke: terminate 'fh'
charon[30143]: 02[IKE] closing CHILD_SA fh{1} with SPIs c6e6abc0_i (524 bytes) d8536829_o (375 byt
es) and TS 141.79.x.x/32 === 0.0.0.0/0
charon[30143]: 02[IKE] deleting IKE_SA fh[1] between 192.168.178.48[$INITIATOR_ID]...193.197.x.x[$
RESPONDER_ID]
```

History

#1 - 12.07.2013 19:57 - Noel Kuntze

- File charon_debug.log added

I think this is not just an issue, but a bug.
The log attached is a log of charon with default=3.
If there is anything I can assist you with, please say so.

#2 - 15.07.2013 15:31 - Tobias Brunner

- File 0001-unity-Allow-UNITY_LOCAL_LAN-to-be-longer-than-8-byte.patch added

- File 0002-unity-Replicate-default-behavior-if-no-UNITY_SPLIT_I.patch added

- Tracker changed from Issue to Bug

- Description updated

- Category set to charon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

"handling UNITY_LOCAL_LAN attribute failed"

This seems to be because the responder sends an unusual value in this attribute, as can be seen in the log:

```
27[ENC] parsing CONFIGURATION_ATTRIBUTE_V1 payload, 24 bytes left
27[ENC] parsing payload from => 24 bytes @ 0x7fb104000bb8
27[ENC]    0: 70 06 00 0E 00 00 00 00 FF FF FF FF 00 00 00 00  p...............
27[ENC]   16: 00 00 00 00 00 00 00 00                          ........
27[ENC]   parsing rule 0 ATTRIBUTE_FORMAT
27[ENC]    => 0
27[ENC]   parsing rule 1 ATTRIBUTE_TYPE
27[ENC]    => 28678
27[ENC]   parsing rule 2 ATTRIBUTE_LENGTH_OR_VALUE
27[ENC]    => 14
27[ENC]   parsing rule 3 ATTRIBUTE_VALUE
27[ENC]    => 14 bytes @ 0x7fb104001160
27[ENC]    0: 00 00 00 00 FF FF FF FF 00 00 00 00 00 00          ..............
```

That is, it sends 0.0.0.0 as subnet and 255.255.255.255 as net mask. Not sure how this is useful (perhaps it's some magic value for Cisco clients to automatically exclude the LAN they are connected to) but it's not what trips up the parser, anyway. Instead it's its the length. The *unity* plugin expects the length to be exactly 8 bytes, but the data here is 14 bytes for some reason. I suppose checking for at least 8 bytes might work (see attached patch) or actually looping over all contained subnets (if the attribute can, in fact, contain more than one subnet - what the 6 extra bytes in the above payload actually mean, I don't know).

But this error has nothing to do with the issue that 0.0.0.0/0 is installed as remote traffic selector. The problem is that the responder does not send any UNITY_SPLIT_INCLUDE attributes. Which probably means that it is not configured to do or even allow split tunneling.
With the *unity* plugin loaded charon kind of ignores *rightsubnet* and proposes 0.0.0.0/0 instead. It's a bit confusing that "proposing traffic selectors for other: 141.79.0.0/16" is logged but that's because the plugin changes the traffic selector after the initial config selection already logged this. It would later use the subnets received in UNITY_SPLIT_INCLUDE attributes to narrow down the received traffic selector (which is most likely 0.0.0.0/0). Since there are no UNITY_SPLIT_INCLUDE attributes available here the remote traffic selector is not changed so 0.0.0.0/0 is used. On the other hand, without the unity plugin being loaded charon would simply narrow the received traffic selector down to whatever is configured for *rightsubnet*. The second patch tries to fix this by replicating the default behavior (i.e. what charon already does before the plugin is called) if no UNITY_SPLIT_INCLUDE attributes are received.

#3 - 15.07.2013 19:47 - Noel Kuntze

I patched strongswan with both patches and the VPN works as I intended now. I don't know how strongswan will behave, when it gets valid attributes.

#4 - 22.07.2013 14:05 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.1.0

- Resolution set to Fixed

Files

charon_debug.log	1.04 MB	12.07.2013	Noel Kuntze
0001-unity-Allow-UNITY_LOCAL_LAN-to-be-longer-than-8-byte.patch	757 Bytes	15.07.2013	Tobias Brunner
0002-unity-Replicate-default-behavior-if-no-UNITY_SPLIT_I.patch	2.93 KB	15.07.2013	Tobias Brunner