

## strongSwan - Bug #302

### No matching outbound IPsec policy

01.03.2013 11:03 - Stefan Tomas

<b>Status:</b>	Feedback	<b>Start date:</b>	01.03.2013
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Tobias Brunner	<b>Estimated time:</b>	0.00 hour
<b>Category:</b>	android		
<b>Target version:</b>			
<b>Affected version:</b>	5.0.2	<b>Resolution:</b>	

#### Description

I'm seeing this log occurring too often:

```
03-01 10:57:28.079: I/charon(4647): 09[IKE] installing new virtual IP 172.1.1.11
03-01 10:57:28.079: I/charon(4647): 09[IKE] CHILD_SA android{2} established with SPIs d13927de_i c
dc26a8a_o and TS 172.1.1.11/32 === 0.0.0.0/0
03-01 10:57:28.079: I/charon(4647): 09[DMN] setting up TUN device for CHILD_SA android{2}
03-01 10:57:28.144: I/charon(4647): 09[DMN] successfully created TUN device: 71
03-01 10:57:28.144: I/charon(4647): 09[IKE] received AUTH_LIFETIME of 1446s, scheduling reauthenti
cation in 846s
03-01 10:57:28.144: I/charon(4647): 09[IKE] peer supports MOBIKE
03-01 10:58:08.829: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:09.099: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:09.639: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:10.719: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:12.884: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:17.219: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:24.999: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:25.384: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:25.879: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:26.144: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:27.669: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:30.719: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:36.819: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
03-01 10:58:39.299: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:43.199: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:44.869: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
46.137.117.201
03-01 10:58:48.999: I/charon(4647): 06[ESP] no matching outbound IPsec policy for 192.168.10.14 ==
173.194.70.188
```

Note that 192.168.10.14 is an IP address of the physical adapter (wlan0).

Is this indicating a problem or can it be safely ignored? If it can be ignored, perhaps log level should be different.

#### History

**#1 - 01.03.2013 12:19 - Tobias Brunner**

- *Status changed from New to Feedback*

- *Assignee set to Tobias Brunner*

I saw these messages too. I'm not sure what the exact reason is but it seems some apps (or parts of the OS) use an address of the currently active physical interface as source address. Since the IPsec policy is for the virtual IP installed on the TUN device the packets don't match and are dropped. I suppose we could increase the log level of this message to 2 in order to avoid flooding the log.

Another option would be to modify the source address of all packets read from the TUN device to the virtual IP. But I guess that doesn't work if these apps/sockets are bound to the physical address (we'd have to do some NATing to deliver the response, which I'd rather avoid).