

## strongSwan - Bug #207

### ikev1, auto=route narrows subnet based TS to protocol port used

26.07.2012 14:29 - Kimmo Koivisto

<b>Status:</b>	Closed	<b>Start date:</b>	26.07.2012
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Martin Willi	<b>Estimated time:</b>	0.00 hour
<b>Category:</b>	charon	<b>Resolution:</b>	
<b>Target version:</b>	5.0.1		
<b>Affected version:</b>	5.0.0		
<b>Description</b>			
<p>When IKEv1, auto=route and /24 subnets in both sites, auto=route incorrectly narrows Traffic Selectors.</p> <p>When traffic is initiated, IPsec SA is narrowed/negotiated only for the protocol/port used but not for subnets. Example: using ssh from site1 to site2, TS is 172.16.60.10/32[tcp/ssh] === 172.16.50.10/32[tcp/49298]</p> <p>Expected behaviour is that TS would be 172.16.60.0/24[any] === 172.16.50.0/24[any]</p> <p>If auto=start is used, TS is as expected.</p> <p>ecdsa-comment: I think that bug was introduced in an attempt to fix IKEv1 reauthentication (where we do want to reuse the smaller TS in case of narrowing).</p>			

#### Associated revisions

##### Revision 777bcd0 - 26.07.2012 15:45 - Martin Willi

Don't include acquiring packet traffic selectors in IKEv1

As we only can negotiate a single TS in IKEv1, don't prepend the triggering packet TS, as we do in IKEv2. Otherwise we don't establish the TS of the configuration, but only that of the triggering packet.

Fixes #207.

#### History

##### #1 - 26.07.2012 15:50 - Martin Willi

- Status changed from New to Closed
- Assignee set to Martin Willi
- Target version set to 5.0.1

Ah yes, almost forgotten, thanks Kimmo.

The referenced patch should fix this issue.