strongSwan - Feature #196

Add support for right=%any (for auto=route)

18.06.2012 11:23 - Tobias Brunner

Status:	Closed	**Start date:**	18.06.2012
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.3.3		
Resolution:	Fixed		

Description

We could use the addresses from the kernel's acquire to try to establish a tunnel. We could also add some something like right=<addr>, <ip-range>, <subnet>.

Related issues:

Related to Feature #92: IPv6 and %defaultroute	**Closed**	**24.09.2009**
Related to Feature #878: Support for remote ranges in transport mode	**Closed**	**06.03.2015**
Blocks Issue #513: Fully meshed VPN Sessions using right=%any is not working	**Closed**	**11.02.2014**

Associated revisions

Revision 301a0bad - 19.08.2015 11:31 - Tobias Brunner

trap-manager: Enable auto=route with right=%any for transport mode connections

Fixes #196.

History

#1 - 19.06.2012 17:33 - Tobias Brunner

- Assignee deleted (Martin Willi)

#2 - 12.02.2014 10:26 - Tobias Brunner

- Blocks Issue #513: Fully meshed VPN Sessions using right=%any is not working added

#3 - 01.03.2015 14:46 - Simon Deziel

Adding this functionality would be very welcome. It would also bridge the gap with what Windows provides.

#4 - 06.03.2015 10:35 - Tobias Brunner

- Related to Feature #878: Support for remote ranges in transport mode added

#5 - 23.03.2015 16:03 - J. Bill Chilton

Found my way to this issue when I couldn't get my right-any, auto-route config to work also.

Tobias, is there perhaps a patch to implement this behavior in existence that I could undertake to make work on v. 5.1.1?

/jwc

#6 - 19.08.2015 11:59 - Tobias Brunner

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

- Resolution set to Fixed

I've pushed this to master. With the referenced commit it is now possible to configure

```
conn trap-any
    right=%any
    ...
    type=transport
```

```
    auto=route
```

The hosts can be limited by specifying *rightsubnet* (e.g. *rightsubnet=192.168.1.0/24,192.168.2.0/30,10.0.2.2/32*). It is even possible to limit this to a specific protocol/port (for any remote host use *%dynamic[<proto>/<port>]*, not *0.0.0.0/0[...]*). A new test scenario (ikev2/trap-any, bb1d9e45) provides some examples.

Authentication can easily be done via certificates, but using PSKs is also possible. However, because there is no pattern/subnet matching for IP-based identities you need to either use a single secret for all hosts or use identities appropriately if you want to use different PSKs for different groups of hosts (e.g. use *leftid=<host>@<group>.example.com* and *rightid=*@<group>.example.com* in ipsec.conf and *@<group>.example.com : PSK "..." in ipsec.secrets).