strongSwan - Feature #2727

single pair of selectors per CHILD_SA

22.08.2018 13:52 - Marco Berizzi

Status:	New	**Start date:**	22.08.2018
Priority:	Low	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:	configuration		
Target version:			
Resolution:			

Description

Hello everyone,

Alas, many commercial IKEv2 implementation (Fortinet, Cisco and CheckPoint), only allows a single pair of selectors per CHILD_SA. They behave as IKEv1.

It would be nice to enable the swanctl.conf to automagically process multiple comma separated list of local traffic selectors to include in CHILD_SA, instead of duplicating local_ts and remote_ts in the swanctl.conf file.

Obviously, when connections.<conn>.version is set to 0 or 2 another parameter should be added to swanctl.conf to keep the current behaviour. For example something like:

single_pair_selectors_per_child_sa=0 (default)

to enable strongswan falling back to single pair of selectors:

single_pair_selectors_per_child_sa=1

Thanks in advance

History

#1 - 23.08.2018 12:08 - Marco Berizzi

Hello everyone,

Alas, many commercial IKEv2 implementations (Fortinet, Cisco and CheckPoint), only allows a single pair of selectors per CHILD_SA. They behave as IKEv1.

It would be nice to enable the swanctl.conf to process multiple comma separated list of local_ts and remote_ts and automagically generate every pair of selector combinations, instead of duplicating local_ts and remote_ts in the swanctl.conf file.

For example this swanctl.conf:

```
children {
net-net {
local_ts  = 10.1.0.0/16,99.99.99.90/24
remote_ts = 10.2.0.0/16,88.88.88.80/24
start_action = trap
}
}
```

would trap the following traffic selector combinations:

from 10.1.0.0/16 to 10.2.0.0/16
from 10.1.0.0/16 to 88.88.88.80/24
from 99.99.99.90/24 to 10.2.0.0/16

from 99.99.99.90/24 to 88.88.88.80/24

from 10.2.0.0/16 to 10.1.0.0/16
from 88.88.88.80/24 to 10.1.0.0/16
from 10.2.0.0/16 to 99.99.99.90/24
from 88.88.88.80/24 to 99.99.99.90/24

Obviously, when connections.<conn>.version is set to 0 or 2
another parameter should be added to swanctl.conf to keep
the current behaviour. For example something like:

single_pair_selectors_per_child_sa=0 (default)

to enable strongswan falling back to single pair of selectors:

single_pair_selectors_per_child_sa=1

Thanks in advance