strongSwan - Feature #223

Patch to allow multiple connections

08.09.2012 11:47 - Dmitry Korzhevin

Status:	Closed	**Start date:**	08.09.2012
Priority:	High	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.1		
Resolution:	Fixed		

Description

Hello,

I use strongSwan 5.0.0 compiled from source on Debian 6. In my configuration i need to allow multiple connections with same ip and same login/password. But, in default strongSwan configuration it doesn't accept multiple connections with same credentials (login/password), thru it normally support connections with same ip and different login/password.

I find a simple way to allow connections with same ip and same login/password:

In file **strongswan-5.0.0/src/libcharon/sa/ikev1/tasks/main_mode.c** i commented out this block of code:

```
@else if (type  INITIAL_CONTACT_IKEV1)  {
if (!this->initiator && this->state  MM_AUTH)    {
/* If authenticated and received INITIAL_CONTACT,     * delete any existing IKE_SAs with that peer.     * The delete takes place when the SA is checked in due     * to other id not known until the 3rd message.*/
//static int same_login_counter = 0;
//if (same_login_counter > 2)
//      this->ike_sa->set_condition(this->ike_sa, COND_INIT_CONTACT_SEEN, TRUE);
//else
//      same_login_counter++;
}
}@
```

This is fast and not elegant way to fix this. I understand that you can find another way, but it will be great, if you include come options for strongSwan to:

1. Allow connections from same ip and same login/password.
2. Options to limit number of incoming connections with same login/password (for exmample allow only 5 connections with same login/pass).

History

#1 - 10.09.2012 11:42 - Tobias Brunner

- File 0001-Add-an-option-to-ignore-INITIAL_CONTACT-notifies.patch added

- Category set to charon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

You can try the attached patch which adds the charon.ignore_initial_contact option in strongswan.conf. Enabling it makes charon ignore any received INITIAL_CONTACT notify. To allow multiple SAs by the same peer you also have to set uniqueids=no in ipsec.conf.

As an alternative we could add this as an option in ipsec.conf (later stored on peer_cfg_t) so it could be enabled per config (or even per peer). But that would be a bit more work.

Adding a limit on the number of concurrent connections by a given peer is not that easy. You might want to add a separate feature request for it. But just so you know, it will probably not have that high a priority for us.

#2 - 10.09.2012 12:35 - Dmitry Korzhevin

Hello, Tobias

Will this patch included in the next version of strongSwan?

P.S. I will help with testing and debugging (if needed)

#3 - 10.09.2012 18:04 - Tobias Brunner

- Status changed from Feedback to Resolved

- Resolution set to Fixed

I pushed a different patch to master (f4cc7ea1), which adds the value *never* to the uniqueids option in ipsec.conf. Configuring *never* instead of *no* forces the daemon to never check for duplicate IKE_SAs, even if it receives INITIAL_CONTACT notifies.

#4 - 25.09.2012 09:39 - Tobias Brunner

- Status changed from Resolved to Closed

Files

0001-Add-an-option-to-ignore-INITIAL_CONTACT-notifies.patch	4.61 KB	10.09.2012	Tobias Brunner