

strongSwan - Feature #215

strongswan NetworkManager plugin: make the "normal" ipsec configuration usable

12.08.2012 04:45 - Christoph Anton Mitterer

Status:	New	Start date:	12.08.2012
Priority:	Normal	Due date:	
Assignee:		Estimated time:	0.00 hour
Category:			
Target version:			
Resolution:			
Description			
<p>Hi.</p> <p>I configure Strongswan on my systems (including desktops/notbooks) via the "normal" configuration; i.e. /etc/ipsec.conf , /etc/ipsec.d , /etc/ipsec.secrets .</p> <p>It would be great if this was exported automatically to NM and selectable in the applet GUI, thus not having to configure it there again (and maintaining both locations).</p> <p>Of course there must be some thoughts spent on security. It would be fatal, to simply export all connections defined system wide. IMHO, the strongswan NM plugin should allow a user to use system wide defined connections only, if the user can read all the necessary files. ipsec.conf is typically globally readable (it contains just the parameters anyway)... if that's the case... show the user the connection names/settings.</p> <p>If a want's to connect though, then only if he has read access to the necessary credentials (either ipsec.secrets, or certificates files in /etc/ipsec.d/certs/ . Allowed users may be selected in the system, either via a special group that has read access, or via ACLs on the credential files. Of course the CRLs, CACerts, etc. need also to be handled, as far as they touch NM.</p> <p>Would be good as a follow up, if there was something like. /etc/ipsec.secrets.d ... where one can place files with passwords, readable by different users.</p> <p>Cheers, Chris.</p>			

History

#1 - 12.08.2012 04:47 - Christoph Anton Mitterer

Oh... and IMHO, NM should never allow the user to edit any of the system wide config files...
These should be handled outside of NM and only be used for reading/exporting connections.