strongSwan - Feature #3651

Support for FC-SP-2

03.12.2020 19:11 - Christopher Winkler

Status:	New	**Start date:**	03.12.2020
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:			
Resolution:			

Description

Introduction ============
FC-SP-2 is a protocol that was developed to implement security in Fibre Channel fabric.
FC-SP-2 requires both - end point authentication and data in flight encryption/decryption.
Marvell has taken this specification and is progressing towards providing full implementation
of this protocol through hardware, firmware, drivers and application layers. Marvell has
selected strongSwan as the best choice for negotiating encryption keys using IKEv2 but
must extend the capabilities of IPSec into the particular requirements of FC-SP-2 Fibre Channel.

Key Differences between IPSec and FC-SP-2 ==
1. The most obvious difference is that IPSec uses IP as its transport layer where FC-SP-2 uses Fibre Channel.
Fibre Channel does not have an IP address but uses the WWPN and a PID (port ID) to create a tuple for a connection.
This creates two specific needs within strongSwan for the FC-SP-2 plugin that Marvell has developed called auth-els:
a. The PID is carried in 3 bytes of the IPv4 address.
b. The connections are managed by the auth-els plugin because IP sockets are not used.

2. The second difference is that the encryption keys do not go to the kernel but are managed
by the HW, FW and driver on the PCI-e card for Fibre Channel. This requires all kernel interface calls,
such as add_sa, delete_sa, etc, to be routed to the auth-els plugin and not the kernel.
The routing of these kernel calls is based on the address family (AF_xxx) stored in the host object.

Proposed core changes required to support FC-SP-2 ==
1. host object: Since there is no AF_FC, identifying Fibre Channel hosts is done with AF_NETLINK which is
not used except in isolated applications. The overloading of AF_NETLINK may be fixed in the future if
an appropriate address family (AF_xxx) is created.

2. libcharon/network/socket_manager:
a. Create separate IP socket and FC socket.
b. Route socket calls to the appropriate socket based on AF type.

3. libcharon/kernel/kernel interface:
a. Create a separate fc_sp interface in addition to the ipsec interface.
b. Route kernel calls to the appropriate "kernel" based on the AF type.

4. Other minor changes required to handle the Fibre Channel addressing differences such as changes to the traffic selector.

Status of development ====================
A full implementation of a local version of strongSwan has been developed that supports IPSec and FC-SP-2 where secure traffic
of both types is running after IKE negotiation completes for each connection type. A suite of tests to insure that IPSec is not
affected by core changes in anyway has been completed. Set of patches can be provided when requested.

History

#1 - 07.01.2021 20:04 - Christopher Winkler

- File ss_fork_010721.tgz added

A github fork has been created for this request:

https://github.com/cwinkler-marvell/strongswan.git

A patchset is also attached if that is preferred.

Files

ss_fork_010721.tgz	40.3 KB	07.01.2021	Christopher Winkler