

strongSwan - Feature #1081

Active/standby VPN Gateway Failover

21.08.2015 22:01 - David Adams

Status:	New	Start date:	21.08.2015
Priority:	Normal	Due date:	
Assignee:		Estimated time:	0.00 hour
Category:			
Target version:			
Resolution:			
Description			
<p>I was just discussing on IRC with Thermi if it was possible to configure a primary and backup gateway. I would like to have 2 VPN gateways, one at each of my 2 data centres. I would configure the remote office or mobile users to connect to the primary DC VPN server automatically using auto=start (or route).</p> <p>If the connection to the Primary VPN server is unavailable or the connection drops and is unable to re-establish, the initiator then puts the primary conn definition into a "Failed" state and brings up the second conn to the secondary VPN server (could be more than one backup).</p> <p>the primary connection could still be tried periodically and if the SA is successfully established, the secondary is shutdown and the primary comes back online. This could be handles in a similar way to HSRP/VRRP where there is a priority and a preempt setting. if preempt is not enabled the secondary would stay active until it had a problem and the primary would not be tried unless the secondary went down.</p> <p>To impliment this feature I think it would require the following options</p> <ol style="list-style-type: none">1. Each conn assigned to a group2. Group members given a priority, this would determine the order the connections were tried.3. The Preempt option would determine whether to fail back to a higher priority connection if it came back online.4. Configurable timeout and/or failed retry attempts to trigger the failover. could be linked to DPD in some way5. A configurable delay and hold timer would be sensible to prevent flip flopping6. A command line "ipsec failover <group>" command to manually fail back a connection and for testing. Bring up the new conn before failing over7. The option to pre initialise the next highest priority but not route traffic to it could also be useful added to speed up the failover.			
Related issues:			
Related to Issue #541: List of servers in client config (Failover)		New	06.03.2014

History

#1 - 01.09.2015 12:00 - Tobias Brunner

- Related to Issue #541: List of servers in client config (Failover) added