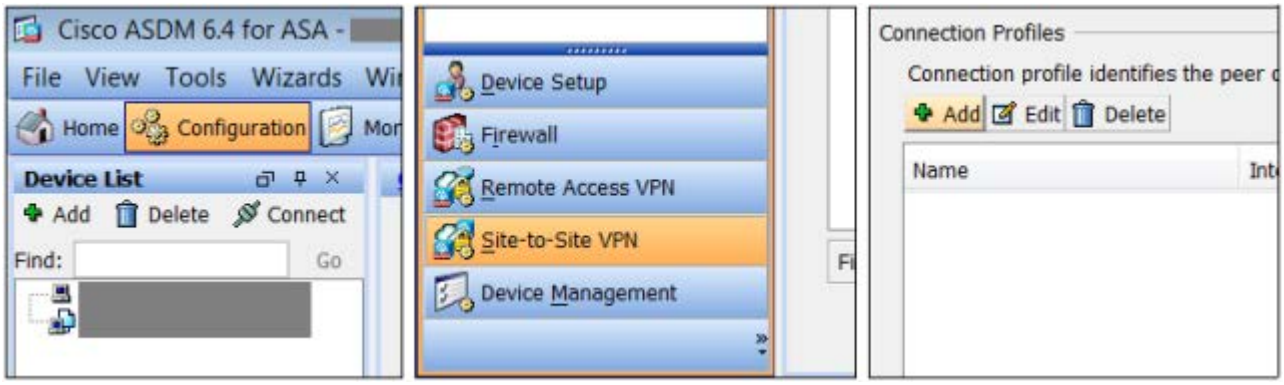
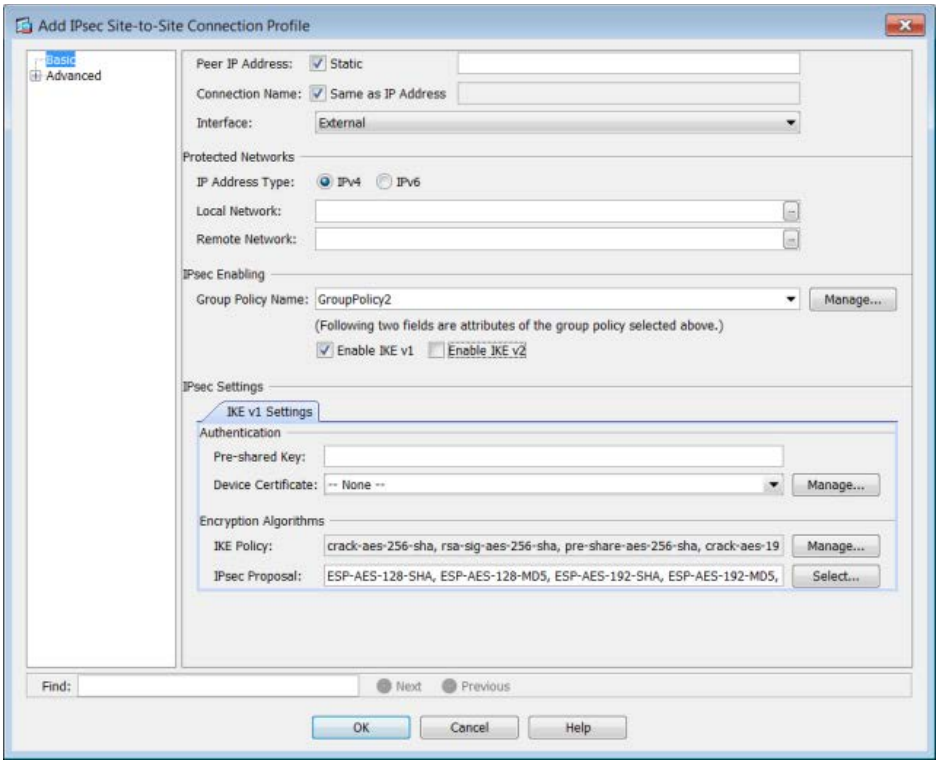
# SITE-TO-SITE VPNS PART III: CISCO ASA

Third part of the S2S VPN series. Again with Cisco, but this time on an ASA. Since the ASA can be managed in GUI with ASDM, configuration is quite straightforward.

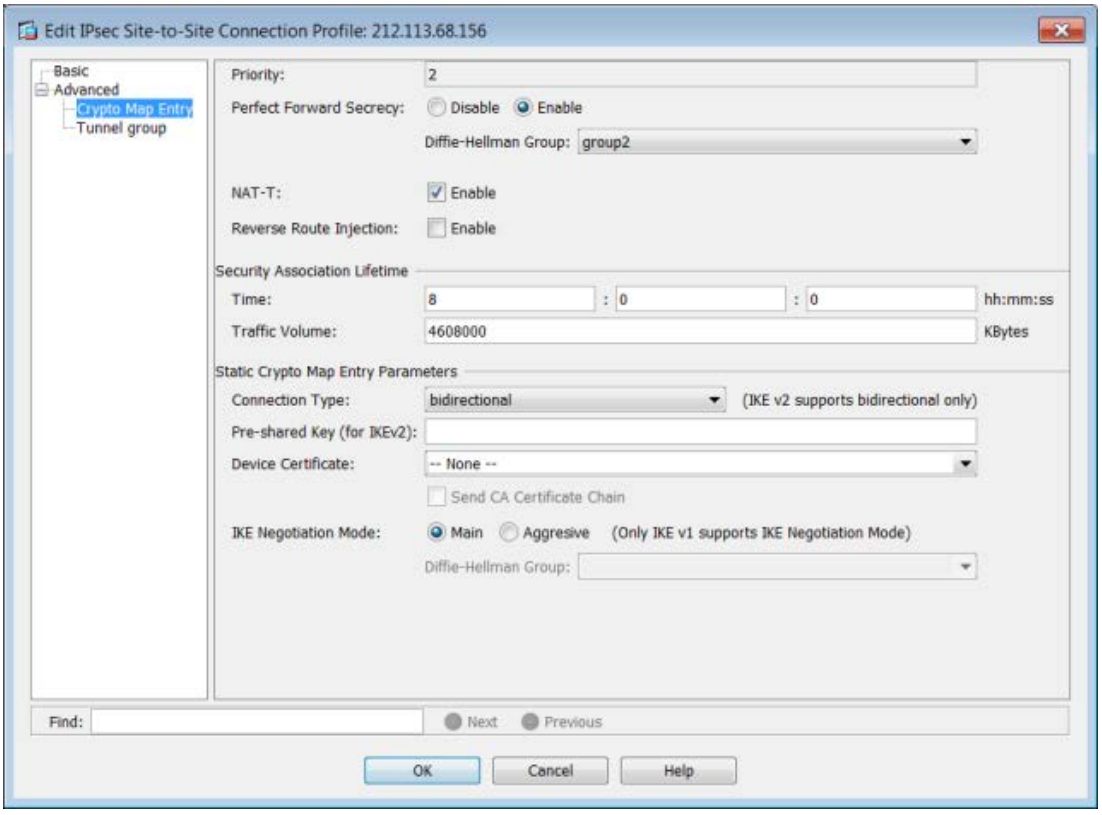



The S2S VPN configuration menu can be found under ‘Configuration’, ‘Site-to-Site VPN’. There you can add a new VPN connection, or edit an existing one.



The configuration menu needs little explanation, as it nicely covers everything a S2S VPN needs (see part I). Only worth noting is IKEv2, which isn't used a lot these days and can safely be disabled. The IKE and IPsec proposals are already filled in with all supported combinations. The VPN will work this way but it can be easier to troubleshoot and understand to just allow the proposals that are needed for a VPN.

If you want to use PFS, it can be found under 'Advanced', 'Crypto Map Entry', together with some more options.




Unfortunately, seeing whether a VPN is up or not in the GUI isn't possible. But the GUI does have logging, which can show the buildup and even reasons for failure in real-time. The CLI, just like with a Cisco IOS, uses the commands 'show crypto isakmp sa' for Phase 1 and 'show crypto ipsec sa' for Phase 2. Straightforward, isn't it?

Source : http://reggle.wordpress.com/2012/10/31/site-to-site-vpns-part-iii-cisco-asa/