Purpose: To initiate an IPSec tunnel from the NSE to allow secure management from the NOC.

Under Configuration -> IPSEC

Enable IPSec and NAT Traversal.

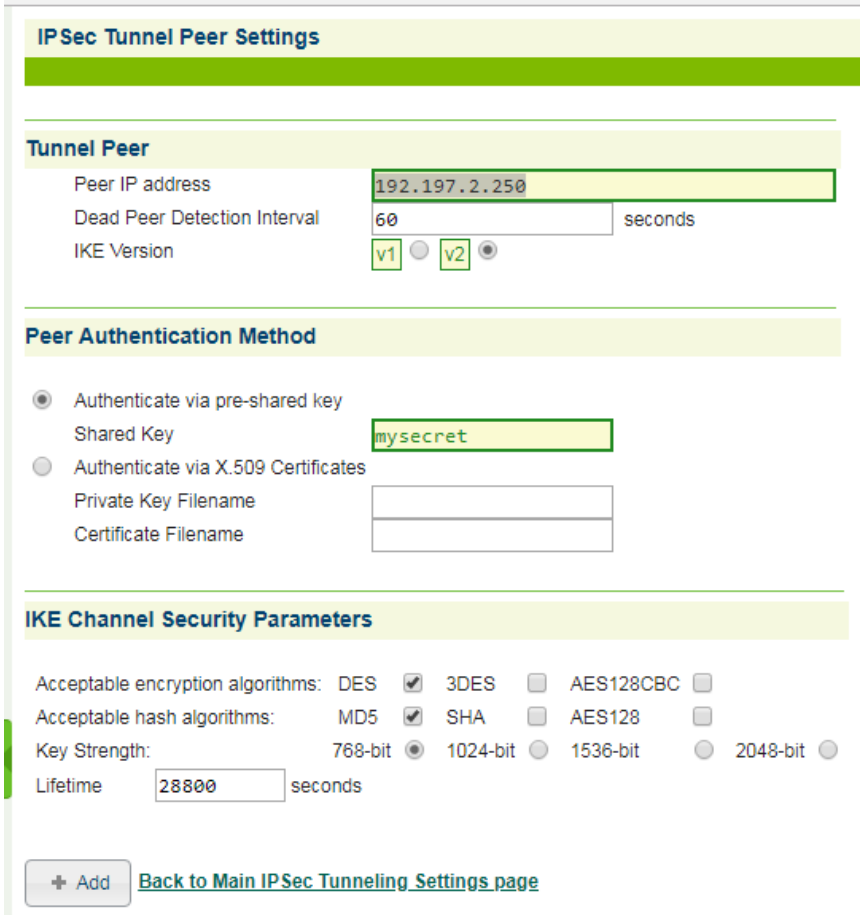
Under Configuration -> IPSEC -> IPSec Tunnel Peers -> Add

Establish the Tunnel Peer Settings:

IP Address	IP address of the remote IPSEC server
Dead Peer Detection Interval	Send IKE message to determine tunnel is still up
IKE Version	version 1or version 2 select which will be used

Peer Authentication Method and Security Parameters:

All parameters to match remote IPSEC server settings.



To manage only the NSE through the IPSec tunnel.

Remote End

Peer IP	this is the IP address of the VPN server
Remote/IP Subnet	this is the subnet behind the VPN server
Subnet Mask	this is the mask for the subnet behind the VPN Server

Local End select “Use most current Network IP Address”

IPSec Tunnel Security Policy Settings

Tunnel peer IP address (required for ESP and AH tunnels) 192.197.2.250

Traffic Selectors

Protocol: ANY

Remote End

Remote IP/Subnet: 172.30.5.2

Subnet Mask: 255.255.255.0

Remote UDP/TCP Port: 0 (or 0 for all ports)

Local End

Use current Network Interface IP Address

Use this static IP address/subnet:

Local IP/Subnet: ::

Subnet Mask: ::

IP address of network interface for this policy: :: (*Optional*)

Local UDP/TCP Port: 0 (or 0 for all ports)

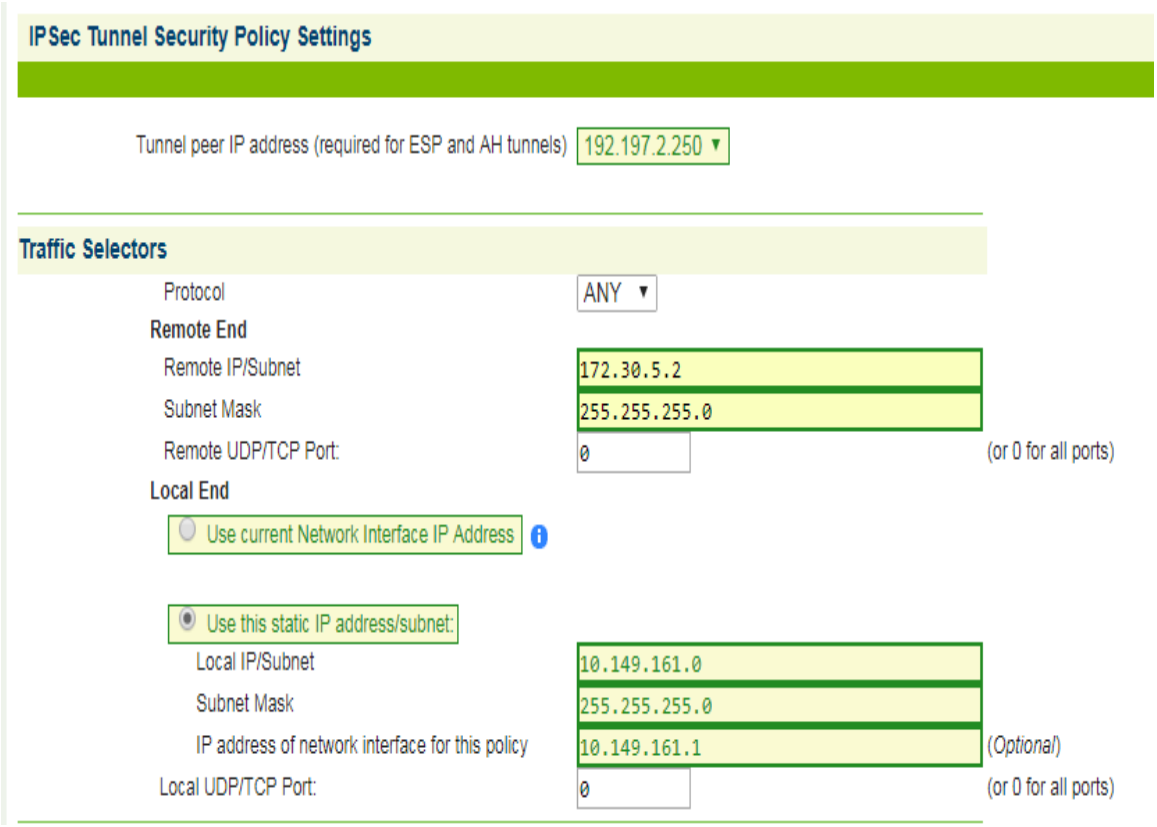
To manage a private network behind the NSE through the IPSec tunnel.

Remote End

Peer IP	this is the IP address of the VPN server
Remote/IPSubnet	this is the subnet behind the VPN server
Subnet Mask	this is the mask for the subnet behind the VPN Server

Local End Select “Custom Settings”

Local IP/Subnet	this is the subnet behind the NSE
Subnet Mask	this is the mask for this subnet



Enable IPSec and NAT Traversal.