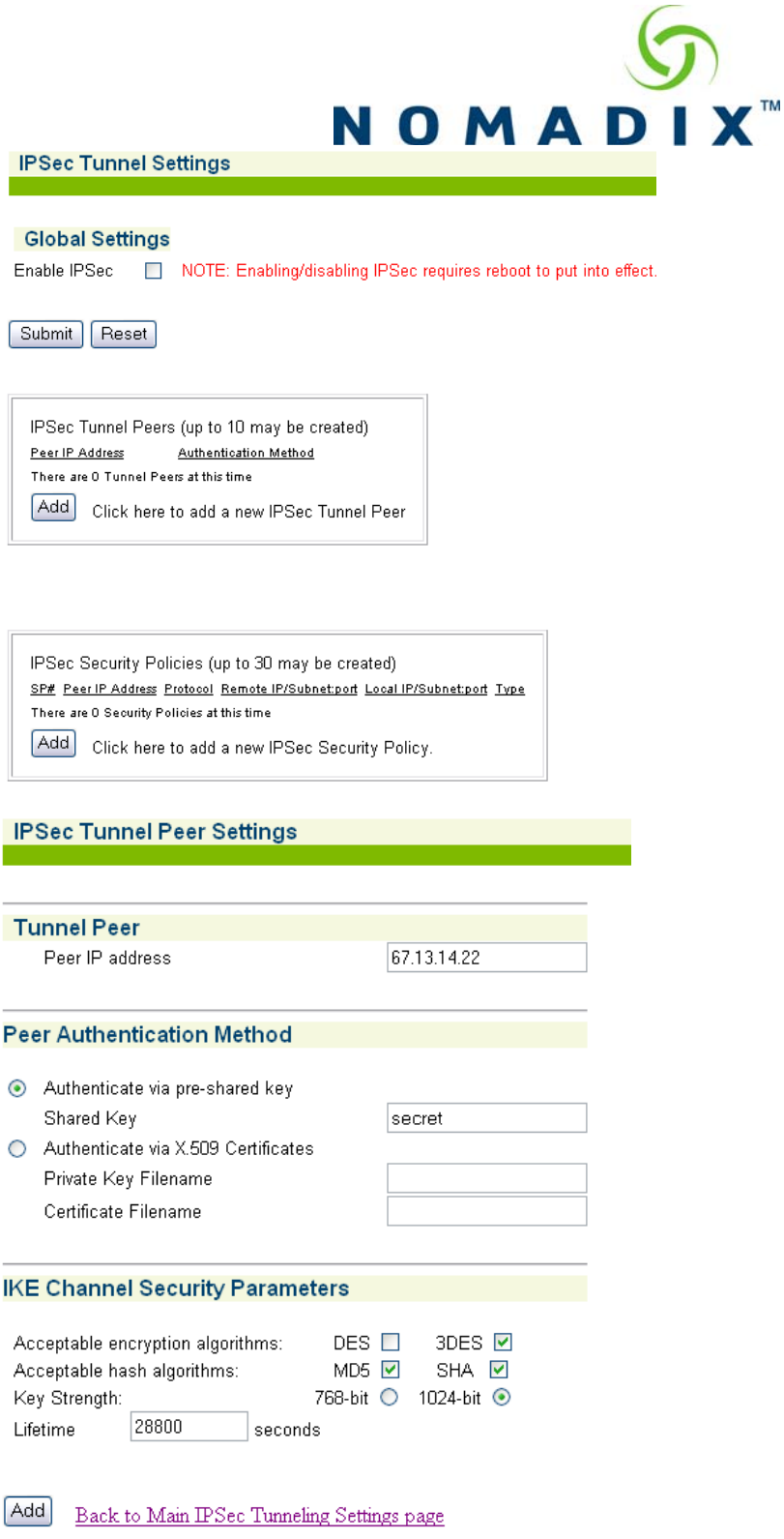
Purpose: To initiate an IPSec tunnel from the NSE to allow secure management from the NOC.

Step 1 Define the end point of the tunnel.

Peer IP Address	This is the IP address of the end point of the tunnel
Peer Authentication Method	Select which method you will be using When using X.509 Certificates, they must first be t ransferred to the /flash/ipseccrt/ directory on the NSE.
IKE Channel Security Parameters	Sets the security parameters that have to match on the PEER-setup for the tunnel to be created.


NOMADIX™
IPSec Tunnel Settings
Global Settings
Enable IPSec
NOTE: Enabling/disabling IPSec requires reboot to put into effect.
Submit
Reset
IPSec Tunnel Peers (up to 10 may be created)
Peer IP Address
Authentication Method
There are 0 Tunnel Peers at this time
Add
Click here to add a new IPSec Tunnel Peer
IPSec Security Policies (up to 30 may be created)
SP# Peer IP Address Protocol Remote IP/Subnet:port Local IP/Subnet:port Type
There are 0 Security Policies at this time
Add
Click here to add a new IPSec Security Policy.
IPSec Tunnel Peer Settings
Tunnel Peer
Peer IP address
67.13.14.22
Peer Authentication Method
Authenticate via pre-shared key
Shared Key
secret
Authenticate via X.509 Certificates
Private Key Filename
Certificate Filename
IKE Channel Security Parameters
Acceptable encryption algorithms:
DES
3DES
Acceptable hash algorithms:
MD5
SHA
Key Strength:
768-bit
1024-bit
Lifetime
28800
seconds
Add
Back to Main IPSec Tunneling Settings page

To define the remote network at the end point

Tunnel Peer IP	from the drop down select the Peer IP from the step above

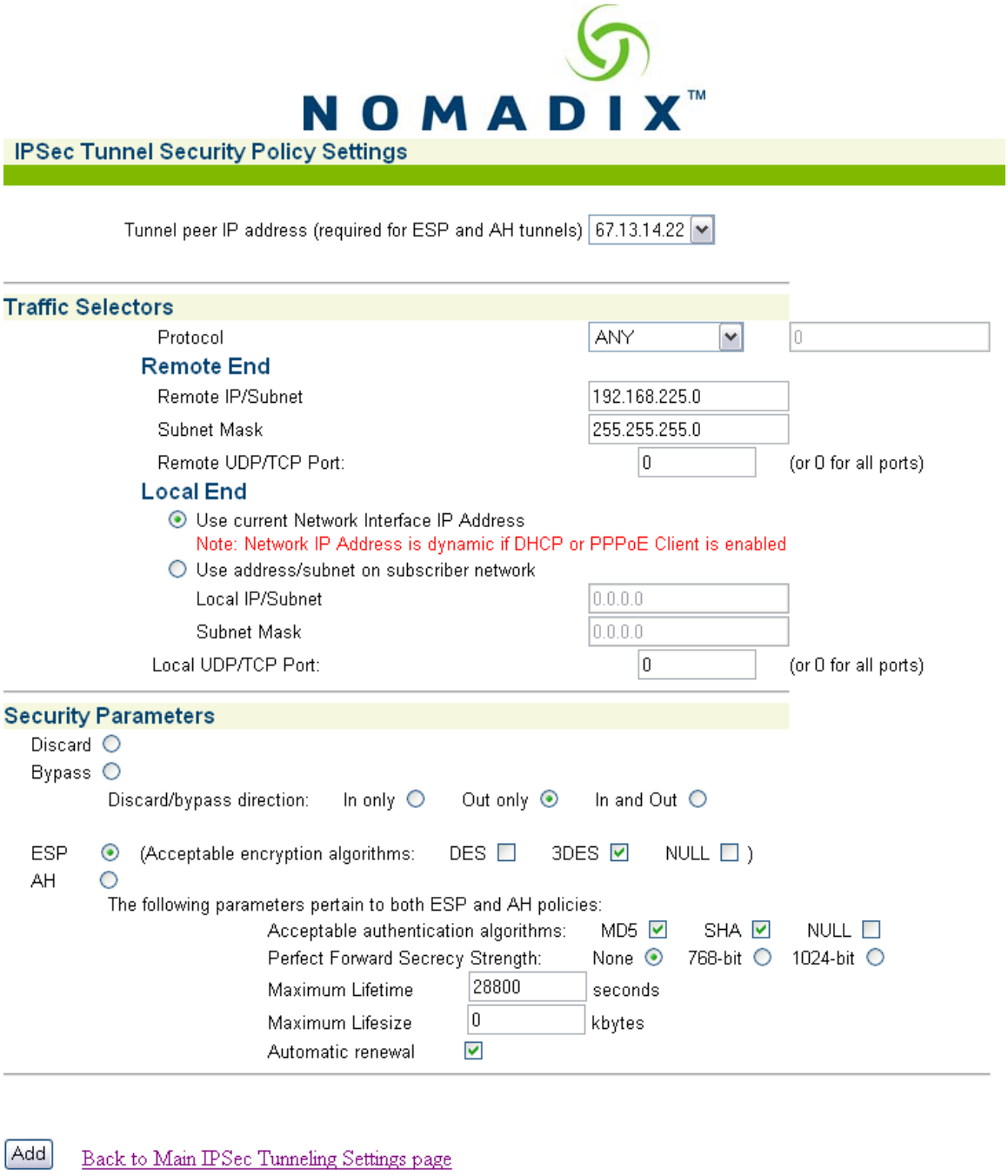
Traffic selectors

Protocol	defines which protocol is defined in this policy

Remote End

Remote IP/Subnet	defines the network on the other side of the end point
Subnet Mask	what is the mask for the remote network
Remote UDP/TCP ports.	defines if the policy allows only 1 port through the tunnel, or all

Security Parameters defines what to do with the packets for the tunnel


NOMADIX™
IPSec Tunnel Security Policy Settings
Tunnel peer IP address (required for ESP and AH tunnels) 67.13.14.22
Traffic Selectors
Protocol ANY 0
Remote End
Remote IP/Subnet 192.168.225.0
Subnet Mask 255.255.255.0
Remote UDP/TCP Port: 0 (or 0 for all ports)
Local End
Use current Network Interface IP Address
Note: Network IP Address is dynamic if DHCP or PPPoE Client is enabled
Use address/subnet on subscriber network
Local IP/Subnet 0.0.0.0
Subnet Mask 0.0.0.0
Local UDP/TCP Port: 0 (or 0 for all ports)
Security Parameters
Discard
Bypass
Discard/bypass direction: In only Out only In and Out
ESP (Acceptable encryption algorithms: DES 3DES NULL)
AH
The following parameters pertain to both ESP and AH policies:
Acceptable authentication algorithms: MD5 SHA NULL
Perfect Forward Secrecy Strength: None 768-bit 1024-bit
Maximum Lifetime 28800 seconds
Maximum Lifesize 0 kbytes
Automatic renewal
Add
Back to Main IPSec Tunneling Settings page