



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 1 or version 2 select which will be used

Peer Authentication Method and Security Parameters:

All parameters to match remote IPSEC server settings.



IPSec Tunnel Peer Settings

Tunnel Peer

Peer IP address:

Dead Peer Detection Interval: seconds

IKE Version: v1 v2

Peer Authentication Method

Authenticate via pre-shared key

Shared Key:

Authenticate via X.509 Certificates

Private Key Filename:

Certificate Filename:

IKE Channel Security Parameters

Acceptable encryption algorithms: DES 3DES AES128CBC

Acceptable hash algorithms: MD5 SHA AES128

Key Strength: 768-bit 1024-bit 1536-bit 2048-bit

Lifetime: seconds

[Back to Main IPSec Tunneling Settings page](#)

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)

Traffic Selectors

Protocol	<input type="text" value="ANY"/>	
Remote End		
Remote IP/Subnet	<input type="text" value="172.30.5.2"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Remote UDP/TCP Port:	<input type="text" value="0"/>	(or 0 for all ports)
Local End		
<input checked="" type="radio"/> Use current Network Interface IP Address	i	
<input type="radio"/> Use this static IP address/subnet:		
Local IP/Subnet	<input type="text" value="::"/>	
Subnet Mask	<input type="text" value="::"/>	
IP address of network interface for this policy	<input type="text" value="::"/>	(Optional)
Local UDP/TCP Port:	<input type="text" value="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

The screenshot shows the configuration interface for an IPsec tunnel. It is divided into two main sections: "IPSec Tunnel Security Policy Settings" and "Traffic Selectors".

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: 10.149.161.0
- Subnet Mask: 255.255.255.0
- IP address of network interface for this policy: 10.149.161.1 (Optional)
- Local UDP/TCP Port: 0 (or 0 for all ports)



Enable IPsec and NAT Traversal.