Application Note 11

Main mode IPSec between a Windows® 2000 / XP (responder) and a Digi Transport Router (initiator)

November 2015

Contents

Figures

1 INTRODUCTION

1.1 Outline

This application note demonstrates how to create an IPSEC VPN tunnel between a Windows PC and a Digi Transport router.

In the figure below, “Net A” represents the private network address of the Window’s LAN. “Net B” represents the private network of the Digi Transport’s LAN.

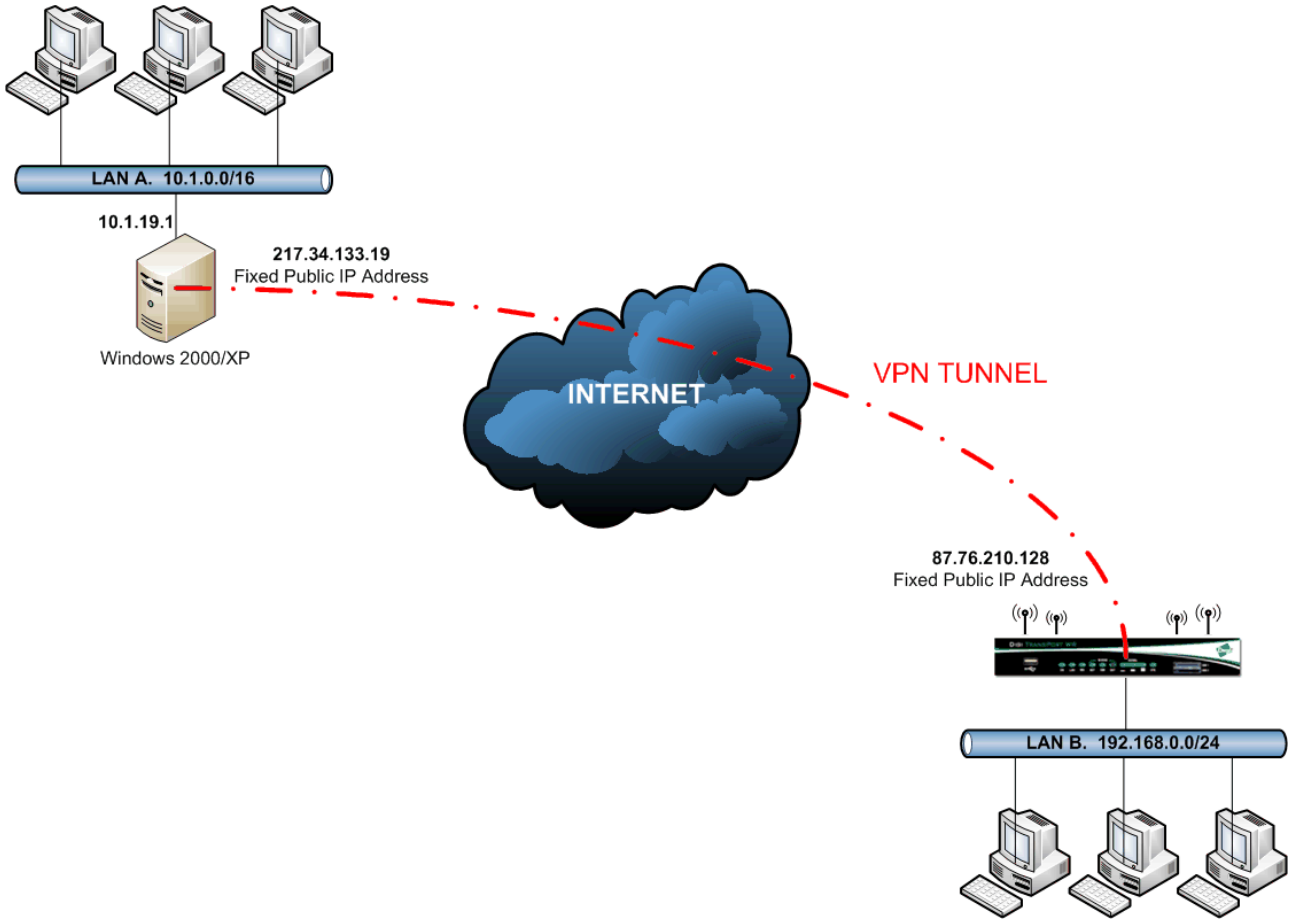


Figure 1-1: Overview Diagram

2 ASSUMPTIONS

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

The following is assumed:

- The user has prior knowledge of configuring both the Windows PC and the Digi Transport Router for connection to the Internet or other wide area network
- Both the Digi Transport and the Windows PC are assigned a public (not a "natted") fixed IP address on their public interfaces
- IPSEC is to be used in "main mode"
- IPSEC tunneling is used
- The Windows PC is NOT a member of a domain
- Pre-shared keys rather than certificates are to be used
- IPSEC with Windows only works correctly in Digi Transport firmware version 4.586 or later

Firmware versions: 4.586 or later

2.1 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: applicationnotes@Digi Transport.co.uk

Requests for new application notes can be sent to the same address.

2.2 Version

Version Number	Status
0.1	Draft

3 CONFIGURING THE WINDOWS PC

3.1 Creating a local IPSEC Policy

Use the **MMC** to work on the IP Security Policy Management snap-in (a quick way to load this is to click **Start**, click **Run**, and then type **secpol.msc**).

Right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**.

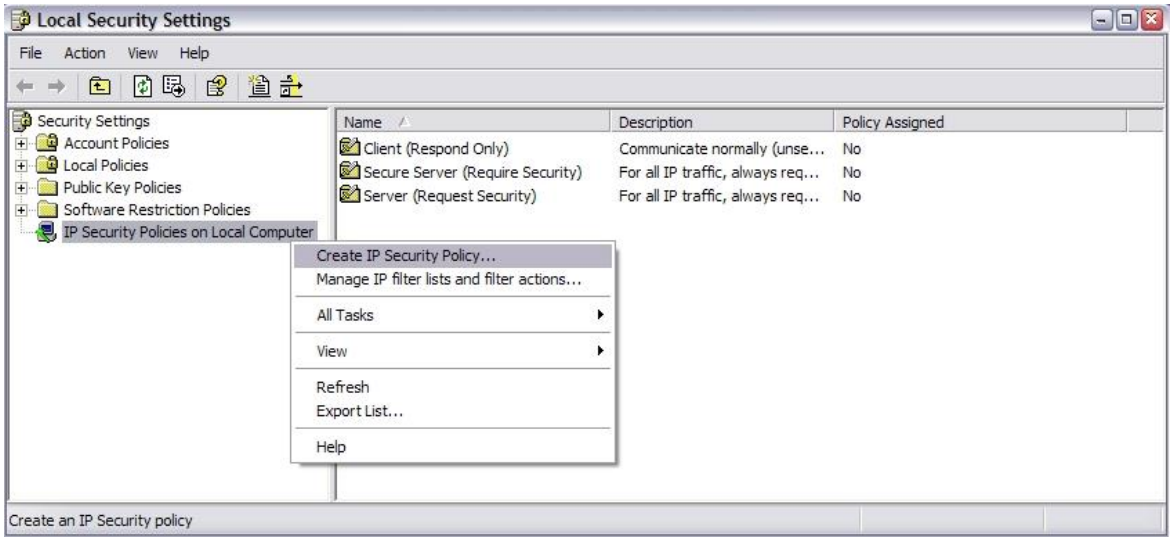


Figure 3-1: Local Security Settings

Click **Next**.

Figure 3-2: IP Security Policy Wizard

Type a name for your policy (for example, IPSEC Tunnel with Digi Transport). NOTE: You can also type more information in the Description box.

Figure 3-3: IP Security Policy Name

Click **Next**.

Figure 3-4: Requests for Secure Communication

Click to clear **the Activate the default response rule** check box if it is selected, and then click **Next**.

Figure 3-5: IP Security Policy Wizard Finish

Click **Finish** (keep the **Edit properties** check box selected).

3.2 How to Create a Filter List from NetA to NetB

In the new policy properties, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.

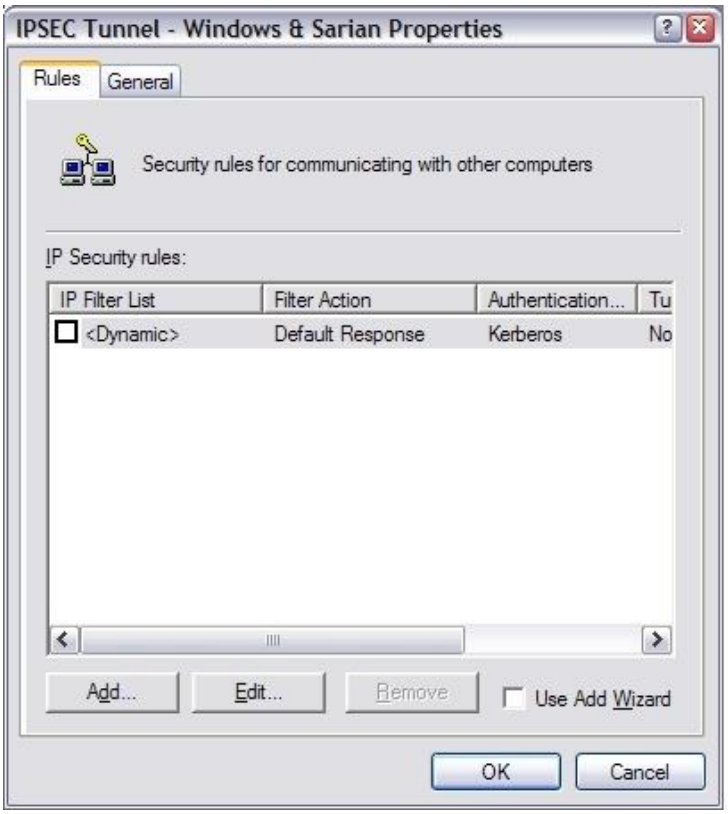


Figure 3-6: New Policy Properties

On the **IP Filter List** tab, click **Add**

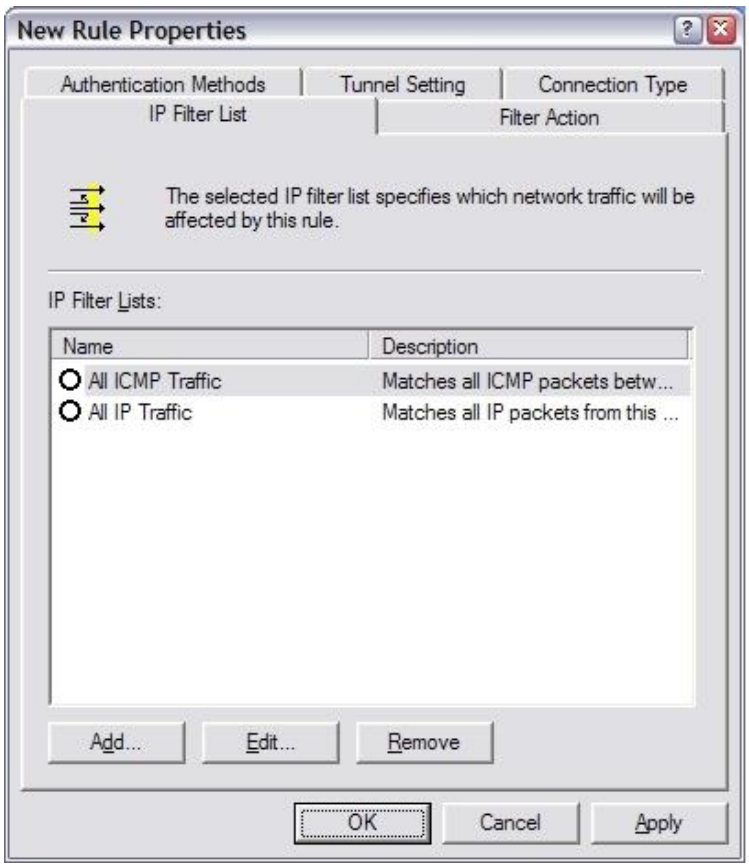


Figure 3-7: New Policy Properties – Net A to Net B

On the **IP Filter List** tab type an appropriate name for the filter list (i.e. Windows to Digi Transport), click to clear the **Use Add Wizard** check box, and then click **Add**.

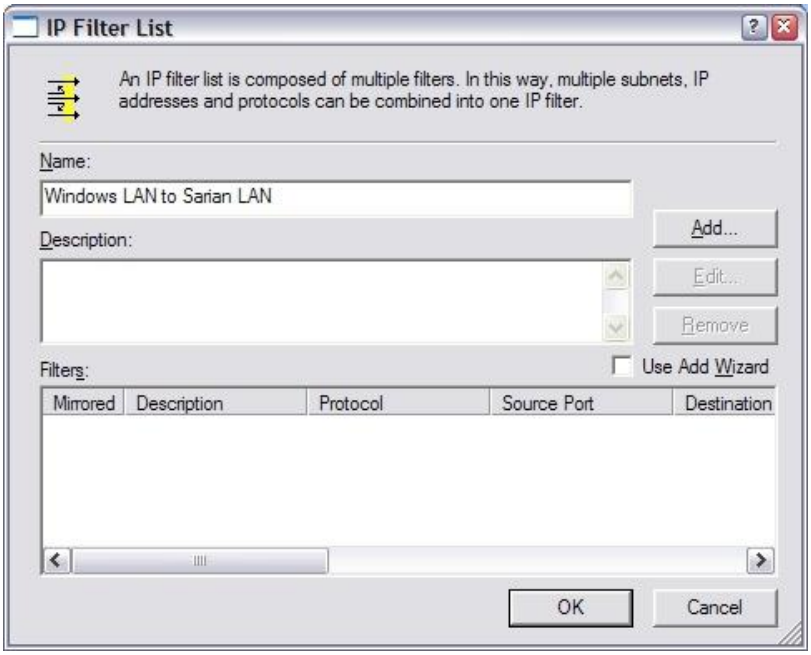


Figure 3-8: IP Filter List Name

In the Source address area, click **A specific IP Subnet**, and then fill in the IP Address and Subnet mask boxes to reflect NetA.

In the **Destination address** area, click **A specific IP Subnet**, and fill in the IP Address and Subnet mask boxes to reflect NetB.

Ensure that there is a **not** a tick in the **Mirrored** check box.

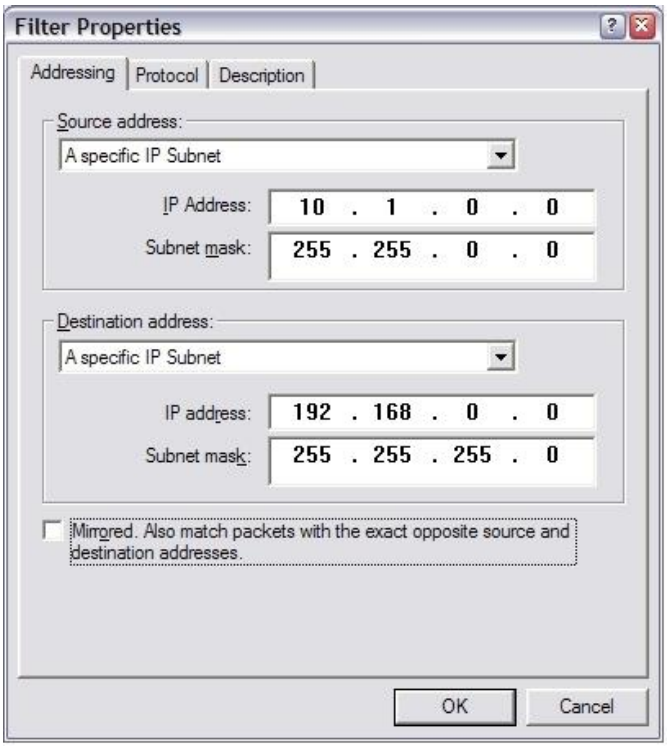


Figure 3-9: IP Filter Properties – Subnet IP Addresses

On the **Protocol tab**, make sure the protocol type is set to **Any**, because IPSec tunnels do not support protocol-specific or port-specific filters.

If you want to type a description for your filter, click the **Description tab**. It is generally a good idea to give the filter the same name you used for the filter list. The filter name is displayed in the IPSec monitor when the tunnel is active.

Click **OK**.

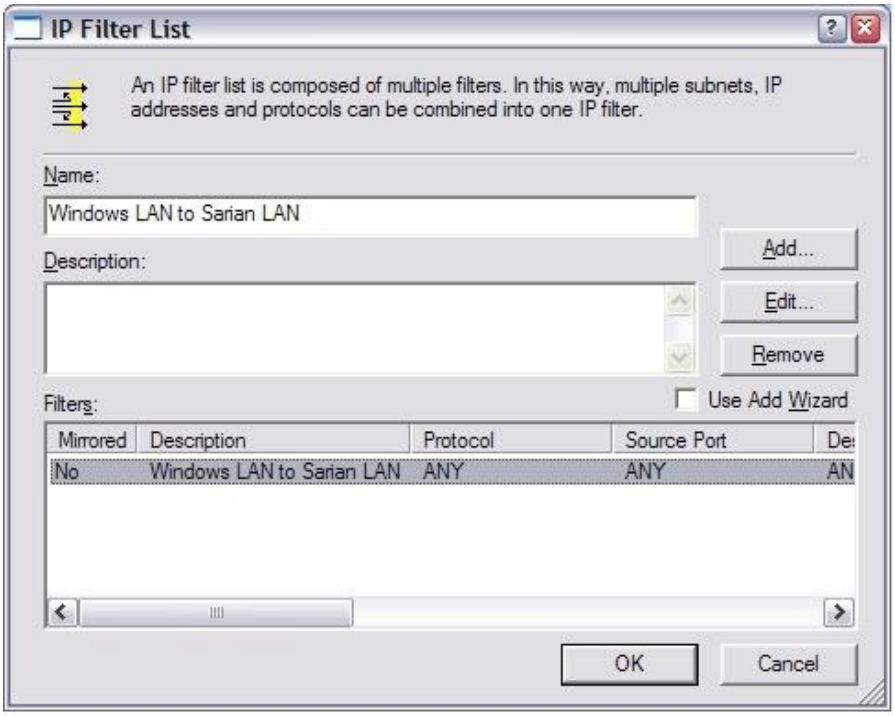


Figure 3-10: IP Filter List

Click **OK** again.

3.3 How to Build a Filter List from NetB to NetA

On the IP Filter List tab, click **Add**.

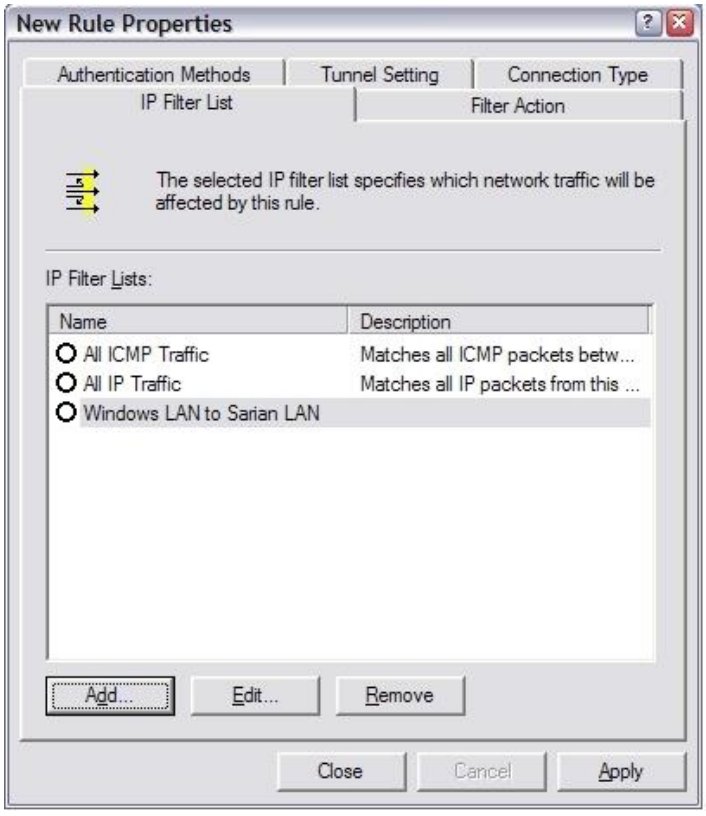


Figure 3-11: New Rule Properties – Net B to Net A

Type an appropriate name for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.

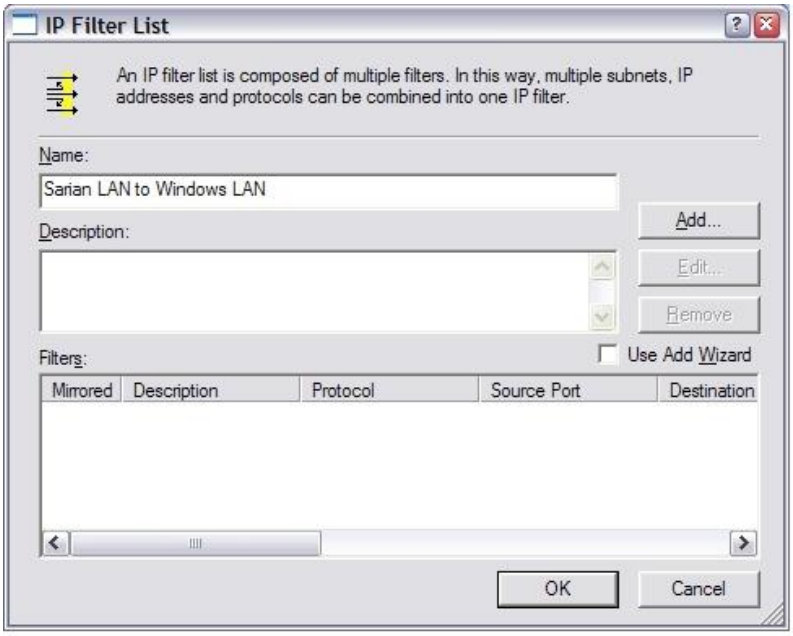


Figure 3-12: IP Filter List Name

In the **Source** address area, click **A specific IP Subnet**, and then fill in the **IP Address** and **Subnet mask** boxes to reflect NetB.

In the **Destination address** area, click **A specific IP Subnet**, and fill in the **IP Address** and **Subnet mask** boxes to reflect NetA.

Click to clear the **Mirrored** check box.

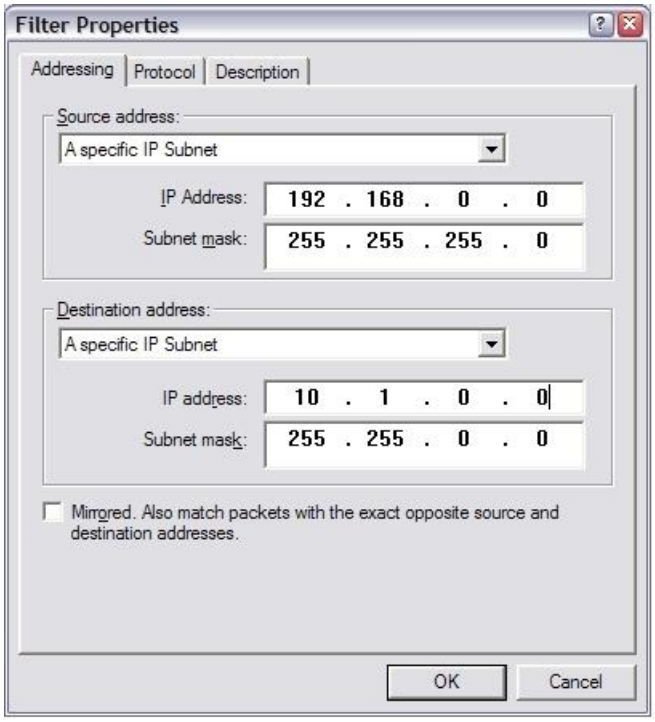


Figure 3-13: IP Filter Properties – Subnet IP Addresses

On the **Protocol tab**, make sure the protocol type is set to Any, because IPSec tunnels do not support protocol-specific or port-specific filters.

If you want to type a description for your filter, click the **Description tab**.

Click **OK**.

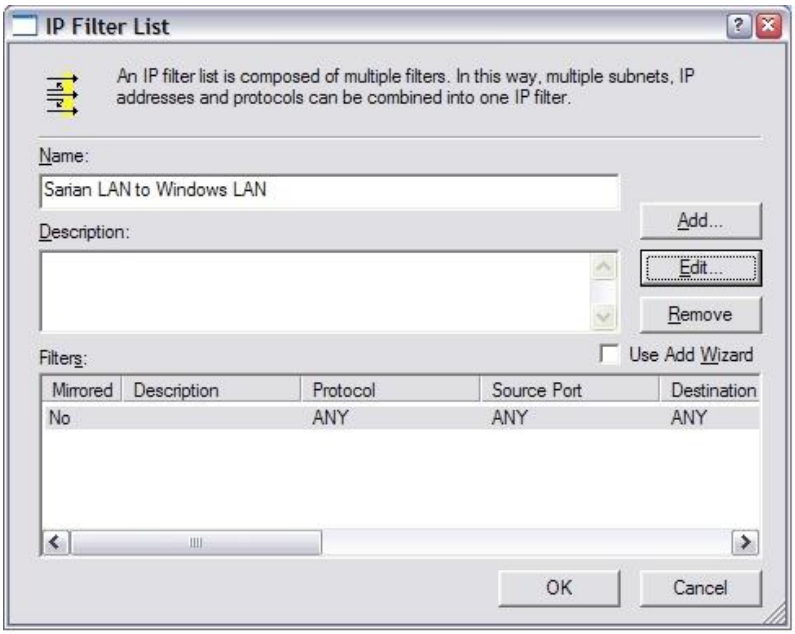


Figure 3-14: IP Filter List

Click **OK** again.

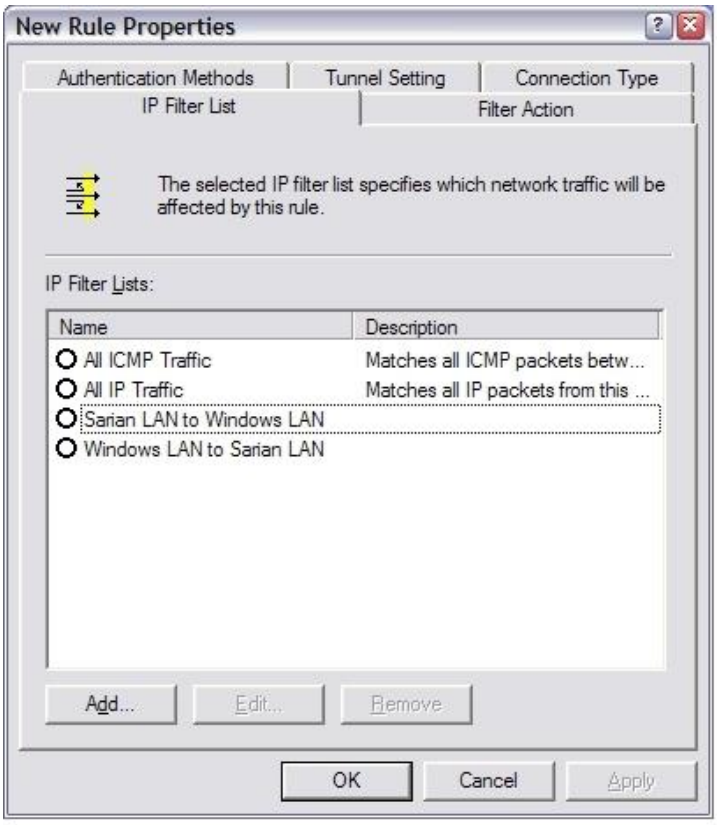


Figure 3-15: IP Filter Properties – finish

3.4 How to Configure a Rule for a NetA-to-NetB Tunnel

On the **IP Filter List** tab, click the filter list you created for Windows to Digi Transport.

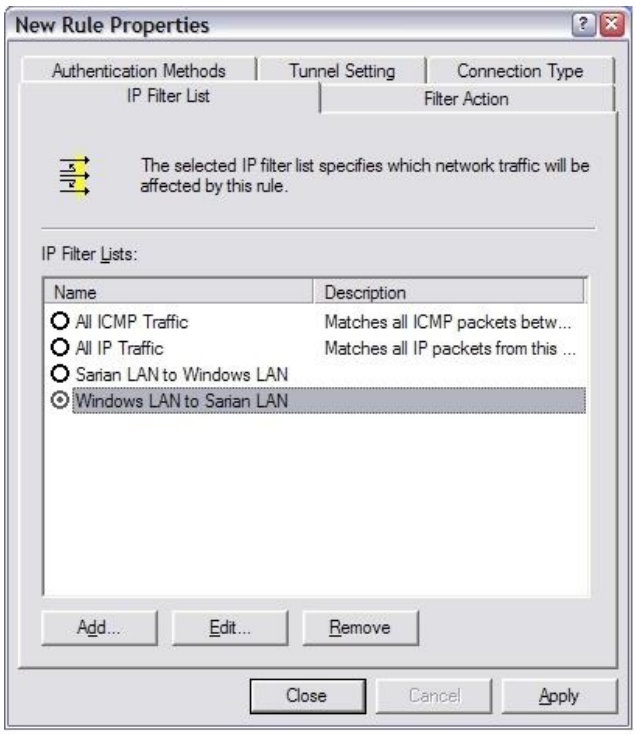


Figure 3-16: New Policy Properties – Net A to Net B Tunnel

On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the Digi Transport Router's fixed public IP address.

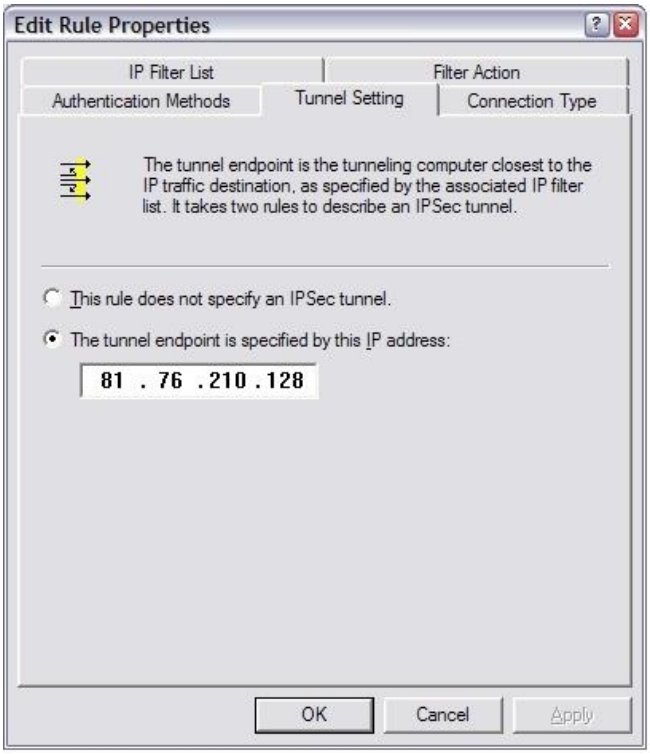


Figure 3-17: Edit Rule Properties – Net A to Net B Tunnel Endpoint

On the **Connection Type** tab, click **All network connections** (or click **LAN connections** if the Windows public interface is not an ISDN, PPP, or direct connect serial connection).

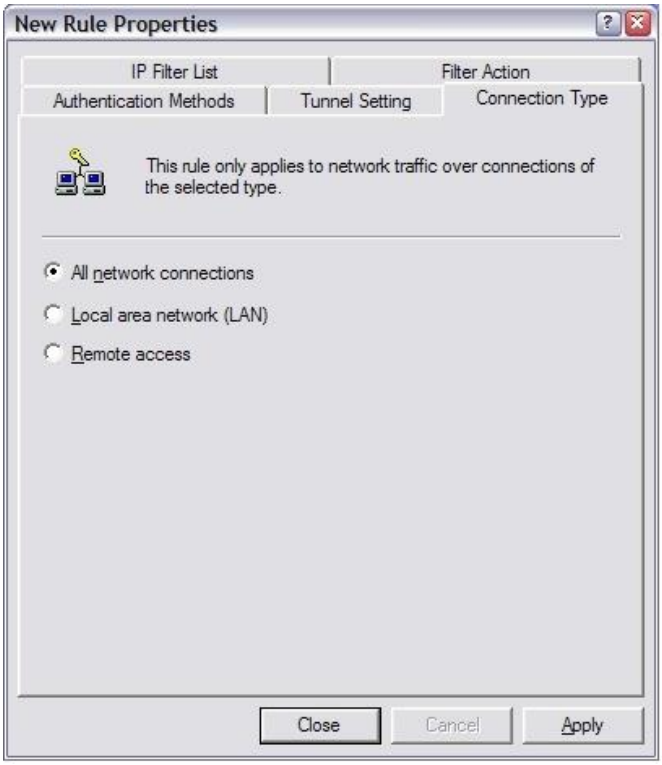


Figure 3-18: New Policy Properties – Net A to Net B Tunnel – Connection Type

On the **Filter Action** tab, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new filter action because the default actions allow incoming traffic in the clear.

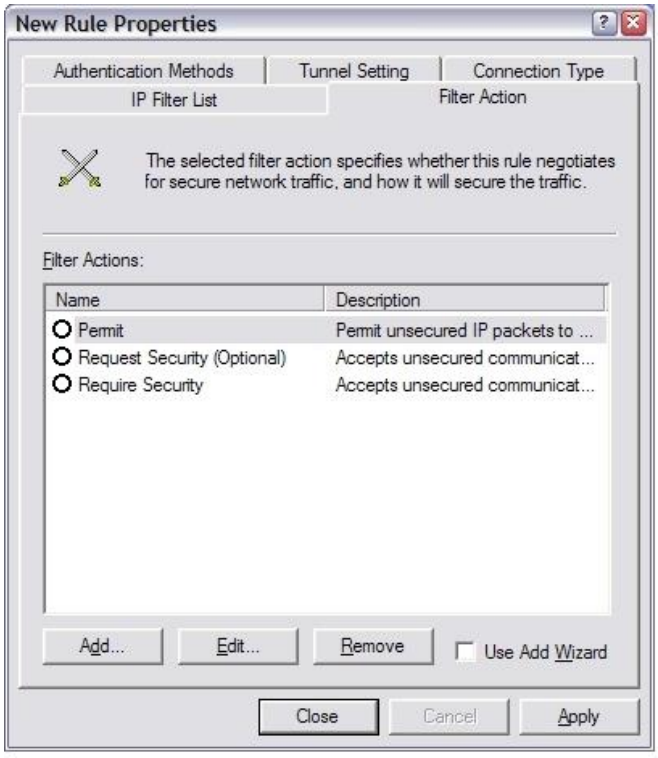


Figure 3-19: New Policy Properties – Net A to Net B Tunnel – Filter Action

Keep the **Negotiate security** option enabled, and click to clear the **Accept unsecured communication, but always respond using IPSec** check box. You must do this to ensure secure operation.

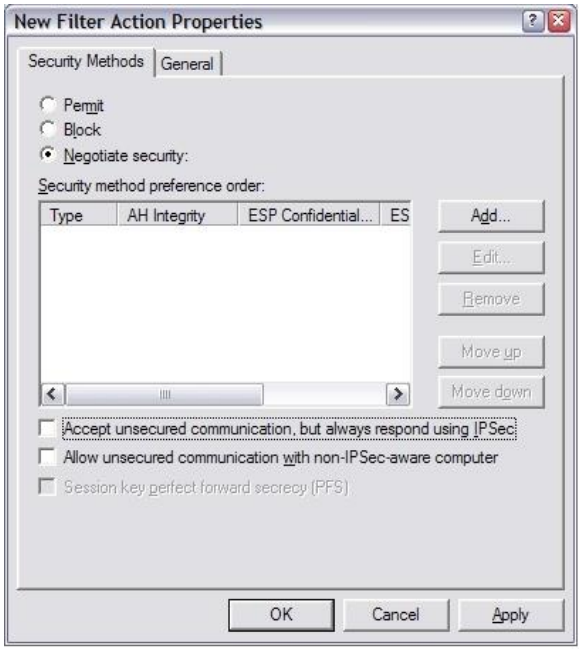


Figure 3-20: New Filter Action Properties – Net A to Net B Tunnel – Security Methods

NOTE: None of the check boxes at the bottom of the Filter Action dialog box should be checked as an initial configuration for a filter action that applies to tunnel rules. Only the Perfect Forward Secrecy (PFS) check box is a valid setting for tunnels if the other end of the tunnel is also configured to use PFS. The other two check boxes are not valid for tunnel filter actions.

Click **Add,** and select **Encryption and Integrity (Represents ESP). Although the following can not be seen from this window, SHA1 for the integrity algorithm and 3DES for the encryption** are selected by default. To view these select **custom** instead. Click **OK**.

Figure 3-21: New Security Method– Net A to Net B Tunnel – Encryption Integrity

On the **General** tab, type a name for the new filter action (for example, IPSec tunnel: ESP), and then click **OK**.

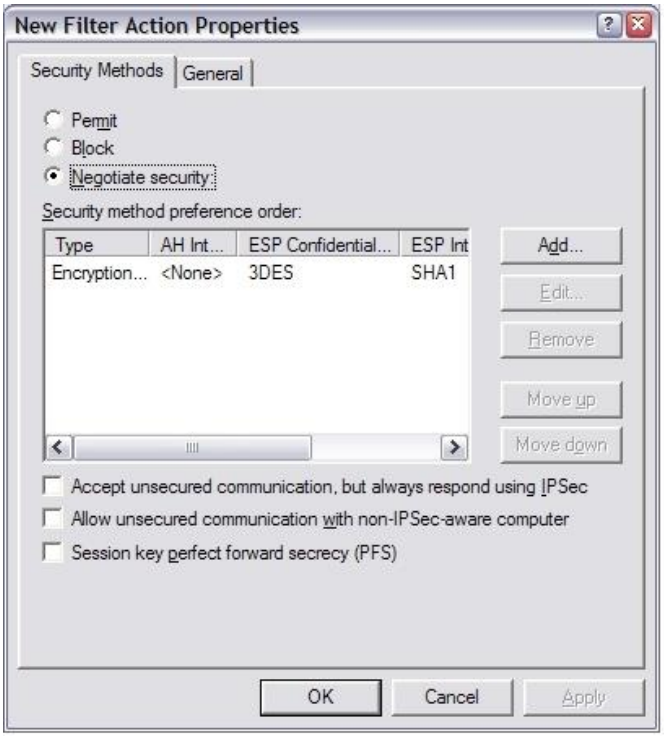


Figure 3-22: New Filter Action Properties – Net A to Net B Tunnel – Security Method Finish

Select the filter action you just created.

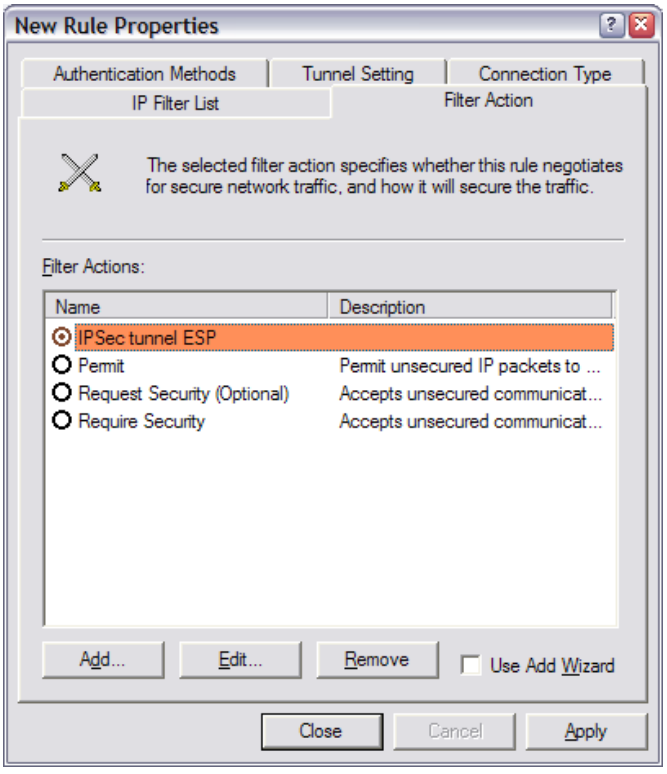


Figure 3-23: New Rule Properties – Net A to Net B Tunnel – Filter Action

On the **Authentication Methods** tab, highlight **Kerberos** and click **Edit**.

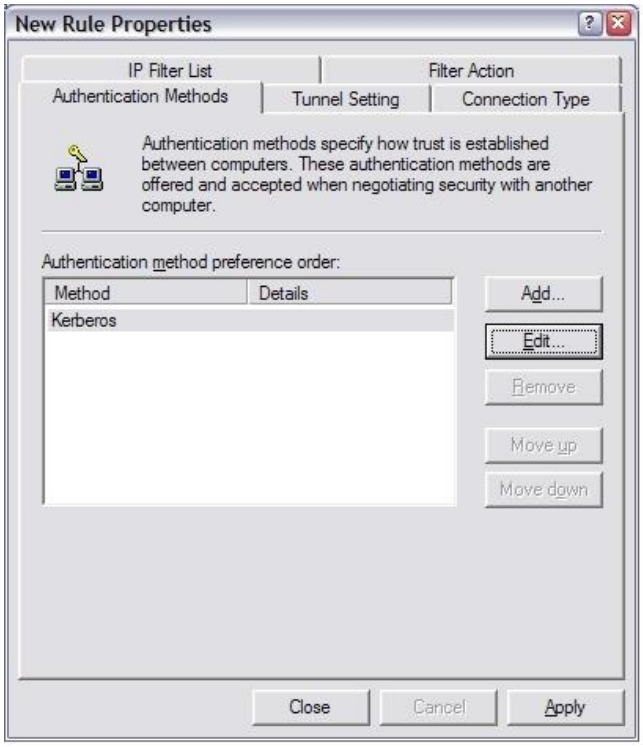


Figure 3-24: New Rule Properties – Net A to Net B Tunnel – Edit Authentication

Click **Use this string (preshared key)**. (This will remove the Kerberos and replace it with pre-shared key. Kerboros is for PC's who are a member of a domain only). Configure the pre-shared key. In this example the pre-shared key is 'test'

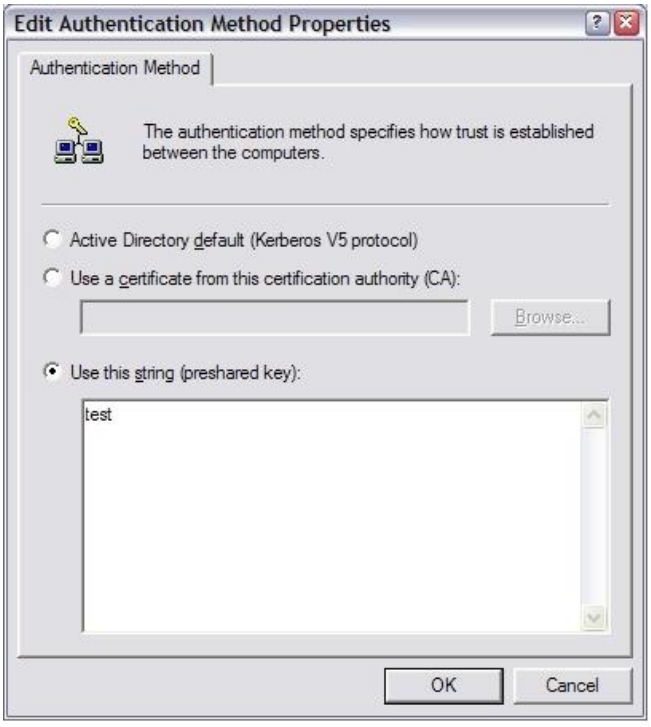


Figure 3-25: Authentication – Net A to Net B Tunnel – Preshared Key

Click **OK** and then **Close**.

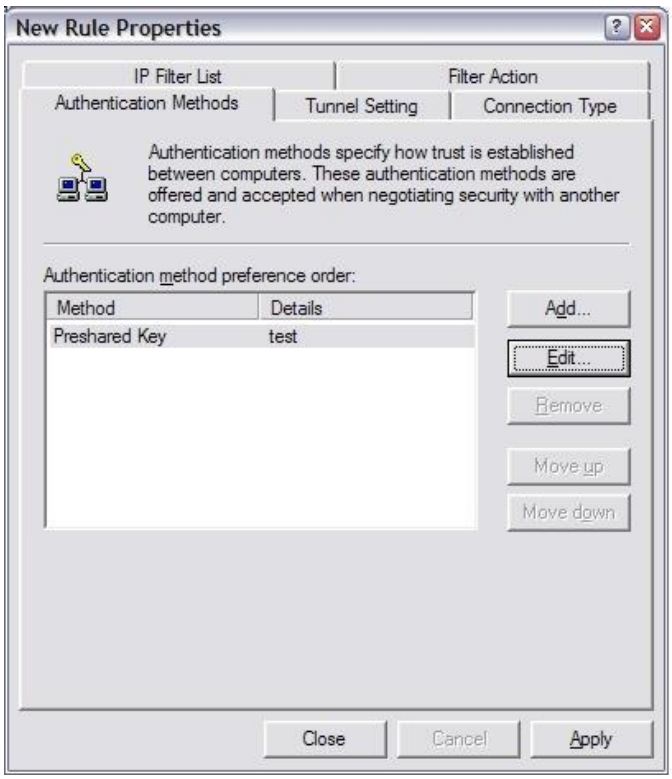


Figure 3-26: New Rule Properties – Net A to Net B Tunnel – Authentication Finish

3.5 How to Configure a Rule for a NetB-to-NetA Tunnel

In IPSec policy properties, click **Add** to create a new rule.

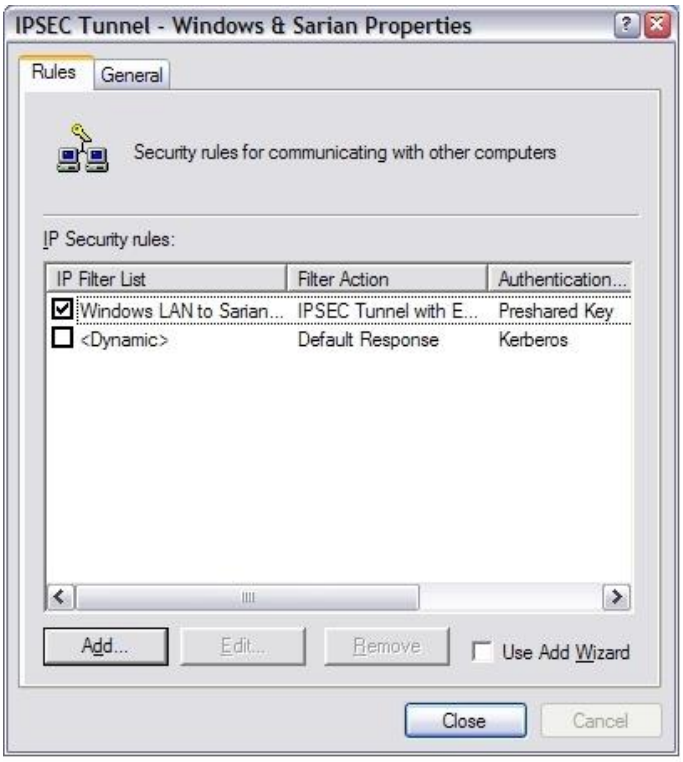


Figure 3-27: IPSEC Tunnel Properties – Net B to Net A

On the **IP Filter List tab**, click the filter list you created (from NetB to NetA).

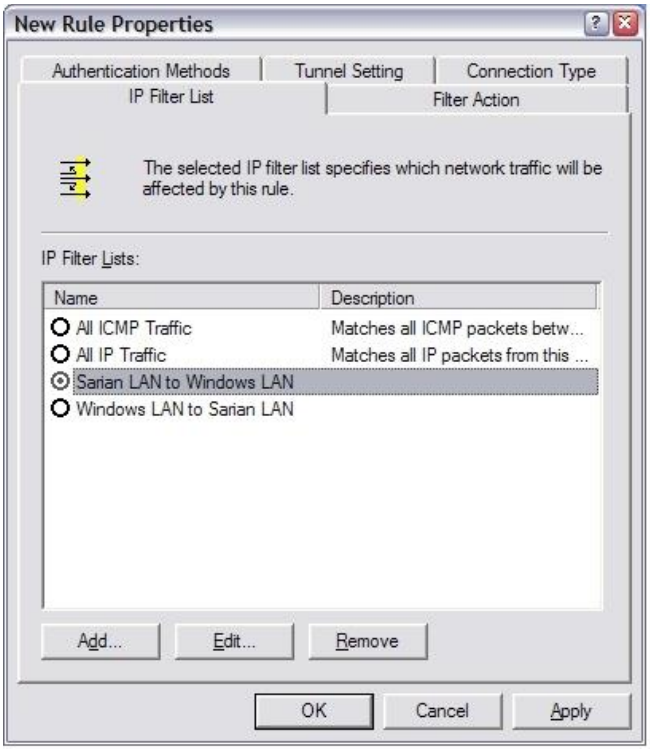


Figure 3-28: New Rule Properties – Net B to Net A Tunnel – IP Filter List

On the Tunnel Setting tab, select **The tunnel endpoint is specified by this IP Address**, and then type the fixed IP address assigned to the Windows gateway external network adapter, i.e. the public IP address of the Windows PC.

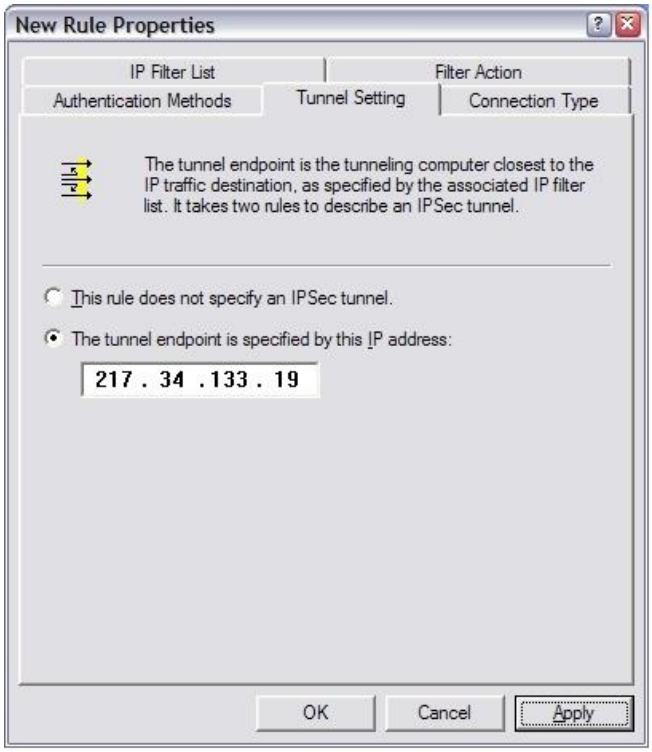


Figure 3-29: New Rule Properties – Net B to Net A Tunnel – Tunnel Endpoint

On the Connection Type tab, click **All network connections** (or click LAN connections if Windows external network adapter is not on an ISDN, PPP, or direct connect serial connection.)

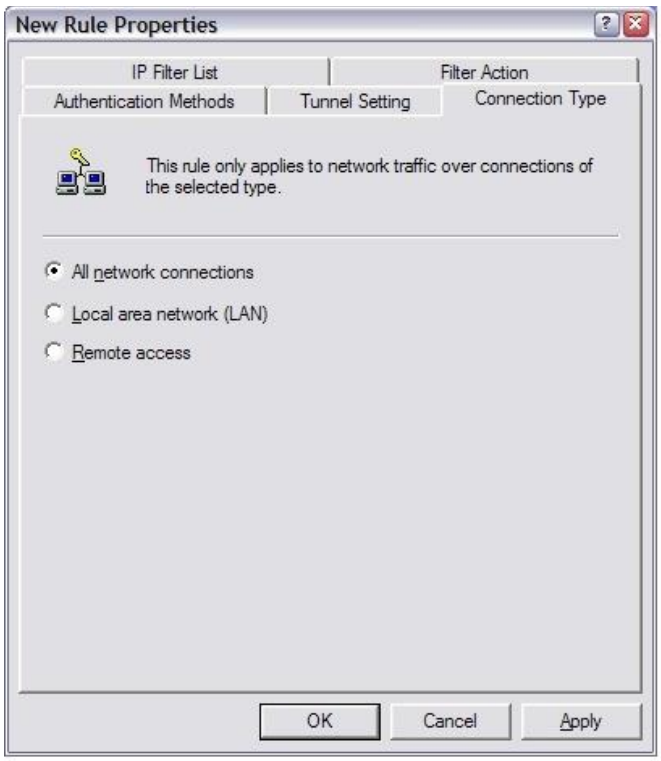


Figure 3-30: New Rule Properties – Net B to Net A Tunnel – Tunnel Endpoint

On the **Filter Action tab**, click the filter action you created earlier.

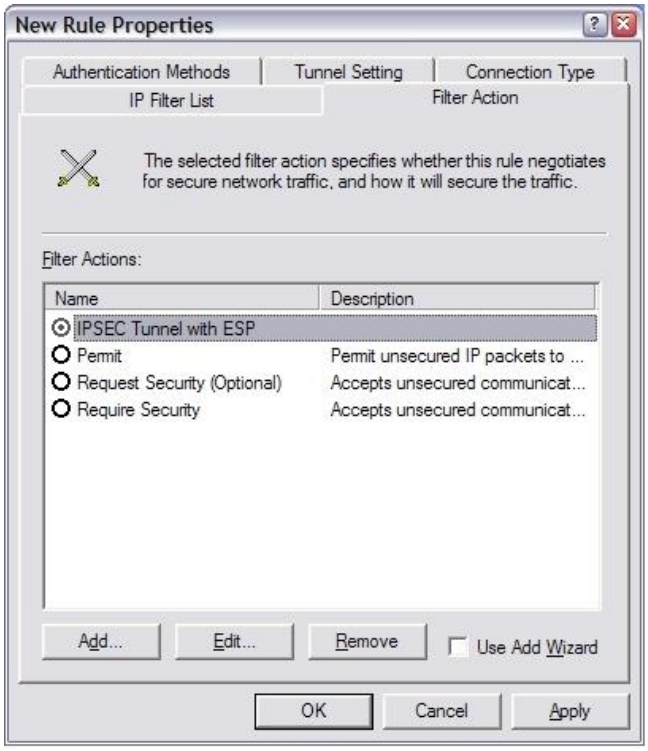


Figure 3-31: New Rule Properties – Net B to Net A Tunnel – Filter Action

On the **Authentication Methods tab**, configure the same method used in the first rule (same method must be used in both rules). Highlight **Kerberos** and click **Edit**.

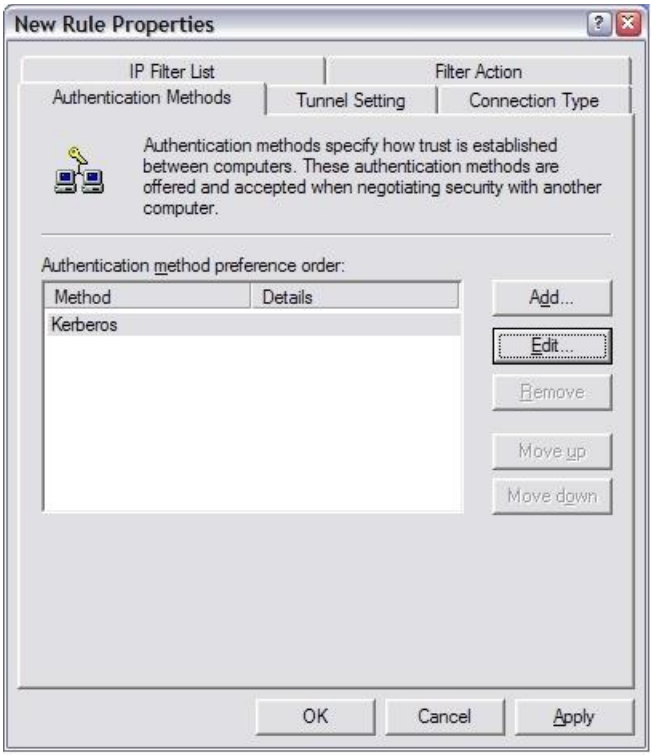


Figure 3-32: New Rule Properties – Net B to Net A Tunnel – Authentication Methods

Click **Use this string (preshared key)**, configure the pre-shared key. As previous the pre-shared key is 'test'. You must use the same pre-shared key as last time. Click **OK**.

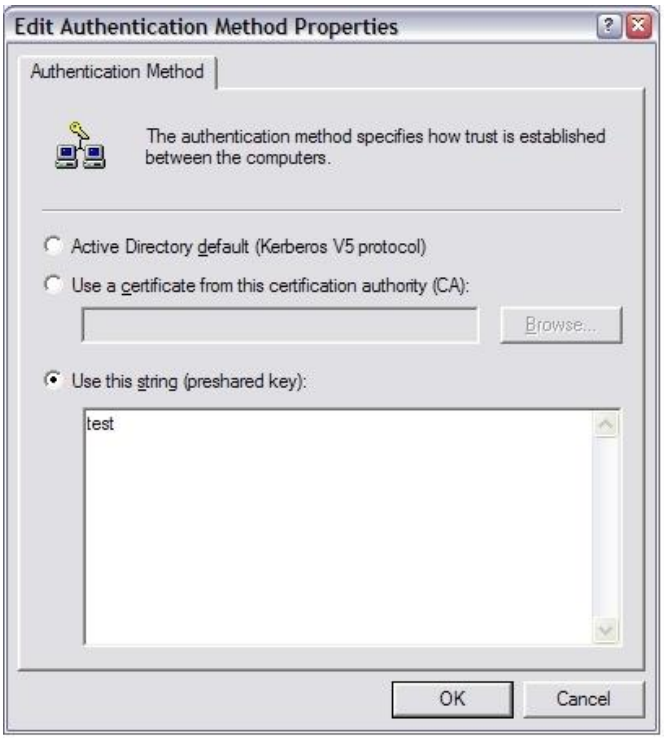


Figure 3-33: Authentication – Net B to Net A Tunnel – Preshared Key

Click **OK** again.

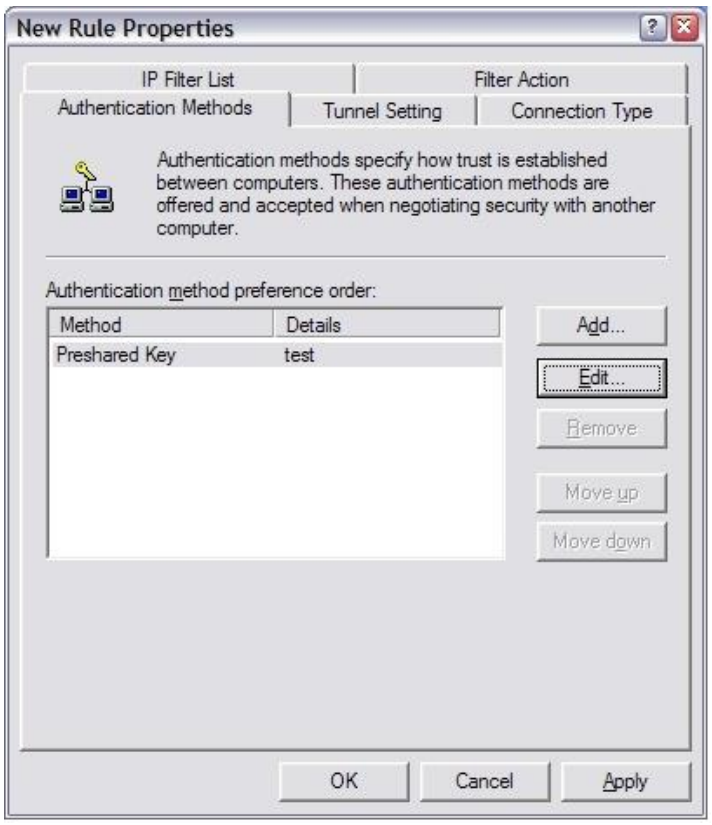


Figure 3-34: New Rules Properties – Net B to Net A Tunnel – Authentication Methods

Make sure both rules you created are enabled in your policy, and then click **Close**.

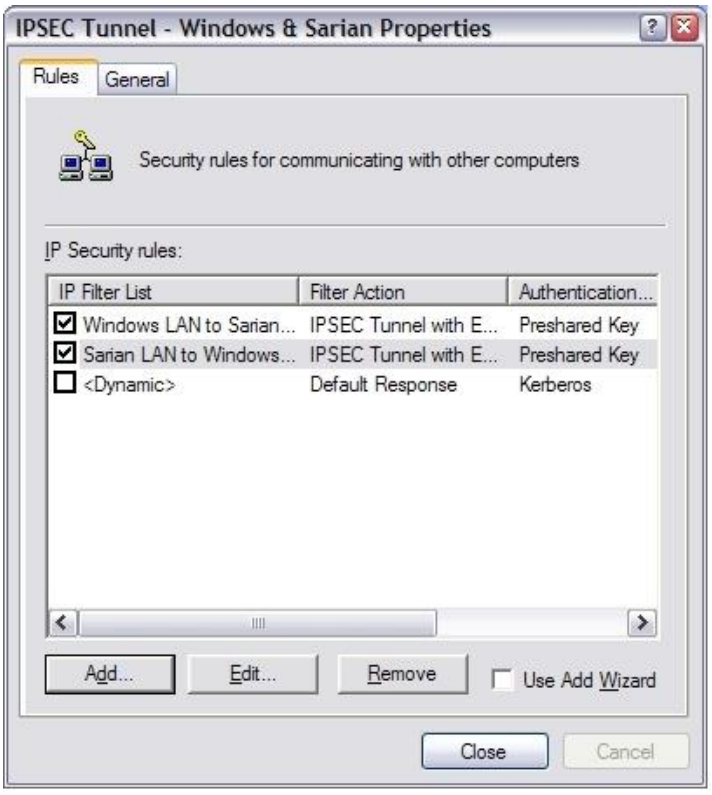


Figure 3-35: IPSec Tunnel Properties – Net B to Net A

3.6 How to Assign Your New IPSec Policy to Your Windows Gateway

In the IP Security Policies on Local Machine MMC snap-in, right-click your new policy, and then click **Assign**.

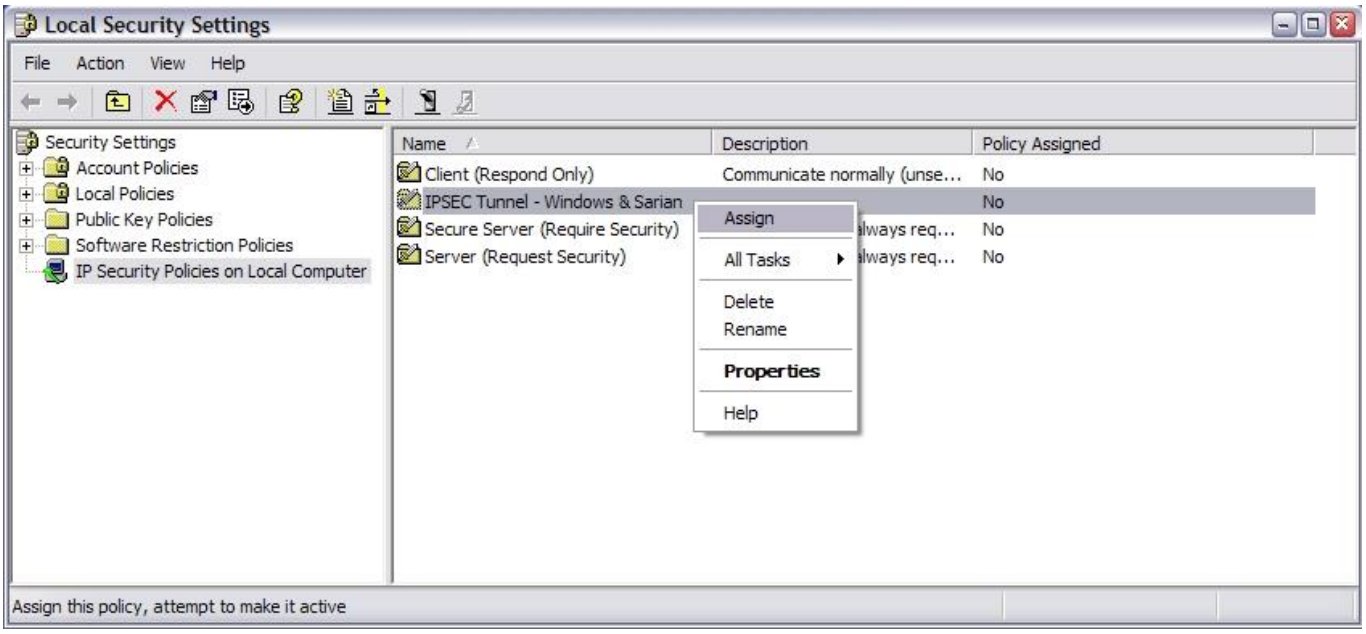


Figure 3-36: Local Security Settings – Assign IPSEC Policy

A green arrow appears in the folder icon next to your policy and **Yes** will appear under **policy assigned**.

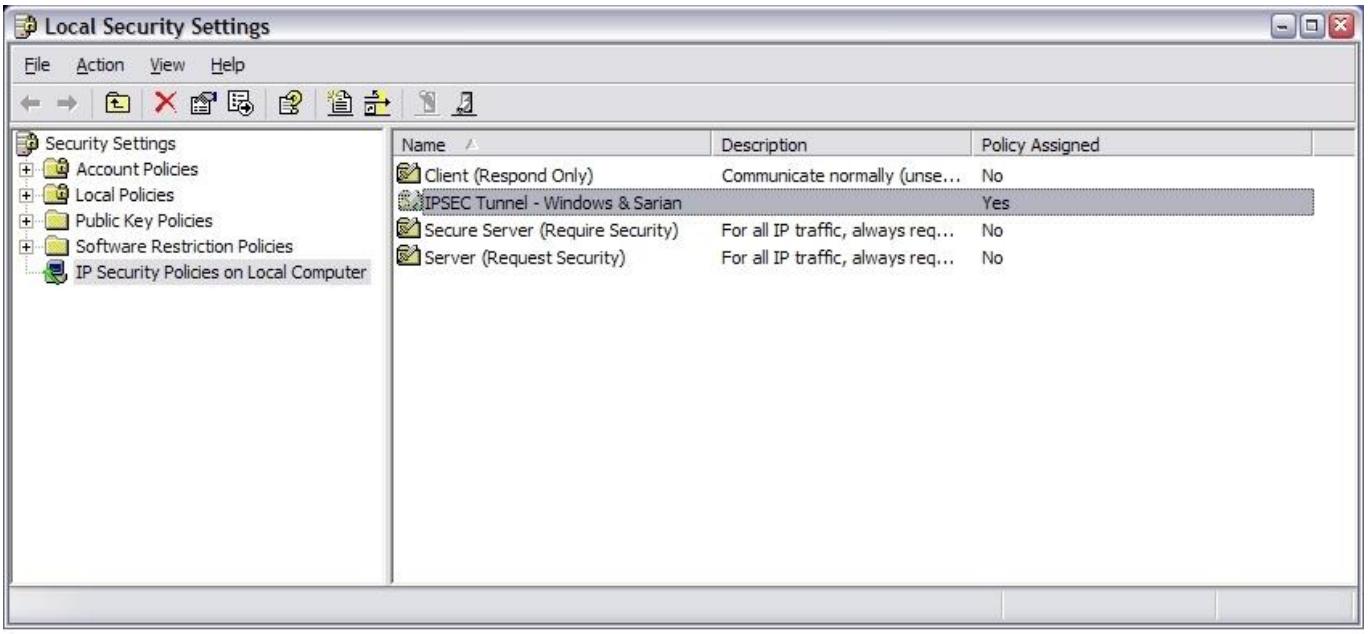


Figure 3-37: Local Security Settings – IPSEC Policy Assigned

4 CONFIGURING THE DIGI TRANSPORT ROUTER

The following instructions assume that the Digi Transport is connected to the Internet (or other WAN) via PPP 1. If the Digi Transport is connected to the internet via Ethernet 0 and not PPP 1 as shown, take this into account when configuring the Digi Transport.

4.1 Configuring the Digi Transport's Default Route

The default route defines which of the Digi Transport's network interfaces is used to send out packets NOT bound for the local LAN. Browse to **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0** and ensure that the Digi Transport's public interface (in this case PPP Interface #1) is selected.

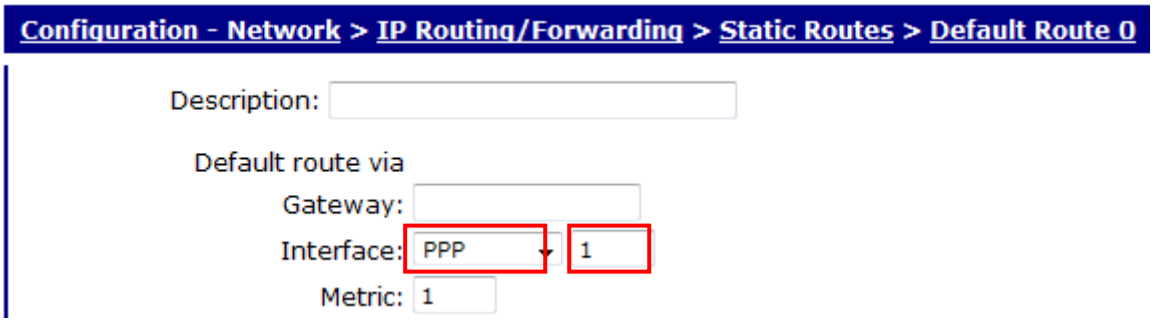


Figure 4-1: Digi Transport – Default Route

Parameter	Setting	Description
Interface	PPP 1	Interface type

Click "**Apply**".

4.2 Enabling IPSec

Browse to **Configuration - Network > Interfaces > DSL**

Enable IPSEC.

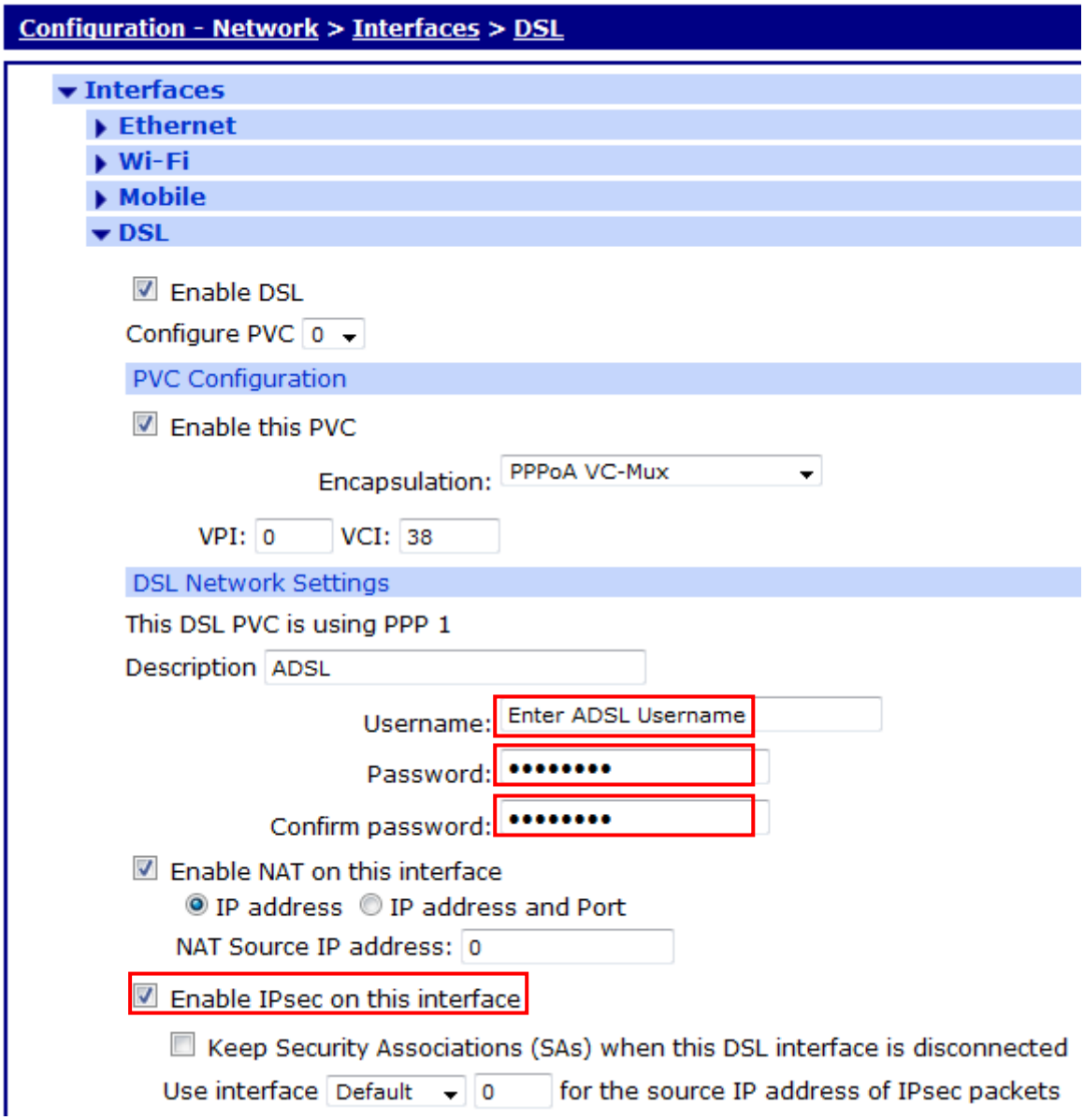


Figure 4-2: Digi Transport – WAN Enable IPSEC

Parameter	Setting	Description
IPsec	Enable IPSec on this interface	Enables IPSec on the DSL interface

Click "**Apply**".

4.3 Configuring IKE (Internet Key Exchange)

IKE is the first stage in establishing a secure link between two endpoints and has to be configured to match the settings in the windows configuration. It is important to ensure that "**main mode**" is selected. Also note that the **IKE MODP group** is set to "2 (1024)" and the **Authentication algorithm** is set to "SHA1" as these were the Windows default configuration. NB these settings weren't visible in the screen shots from Windows.

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

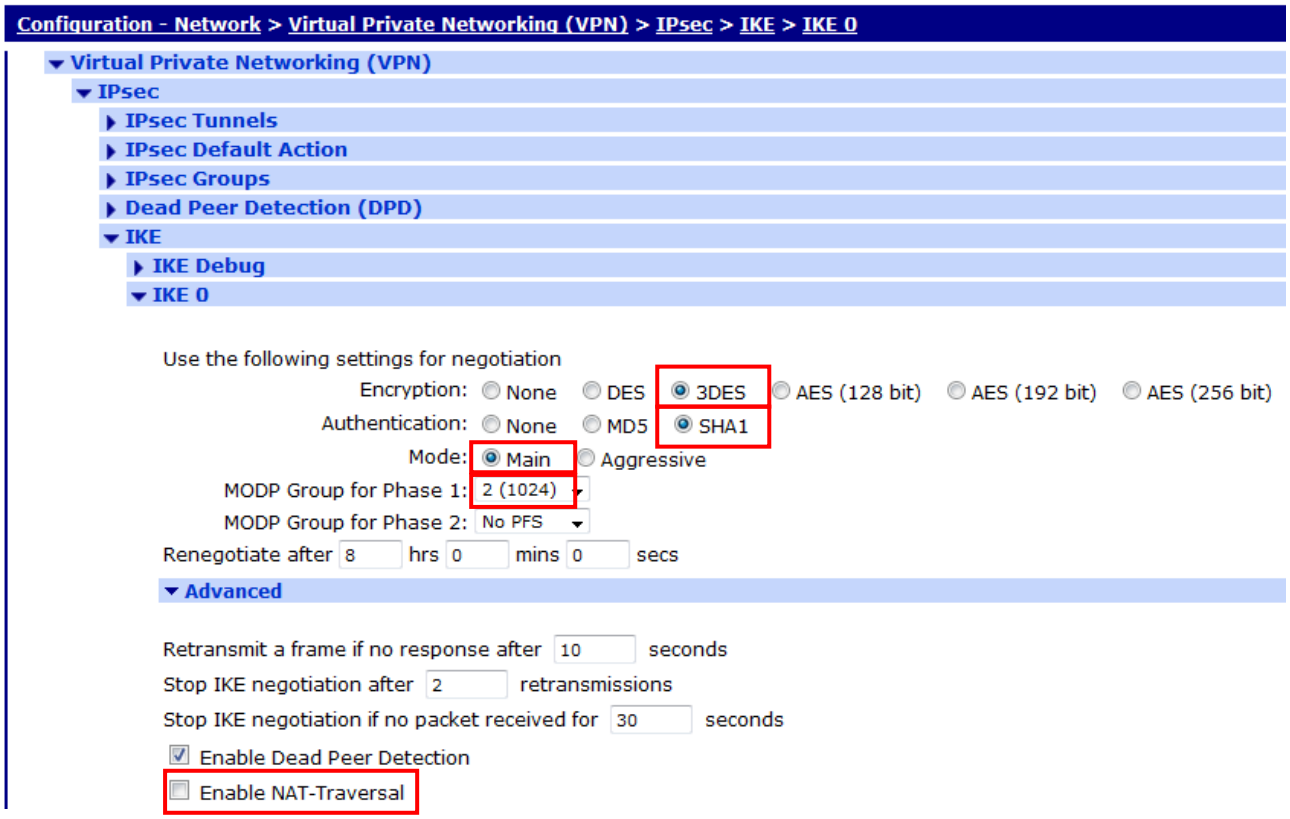


Figure 4-3: Digi Transport – IKE

Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	SHA1	The algorithm used to verify that packet contents have not been changed
Mode	Main	Enables Main Mode
MODP group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange
Enable NAT-Traversal	No	Disables NAT traversal

Click "Apply".

4.4 Configuring the Digi Transport's Eroute

The Eroutes define the characteristics of the encrypted routes. I.e. configure local and remote subnets, authentication and encryption methods, etc. Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0.** Fill out all the parameters with the appropriate settings.

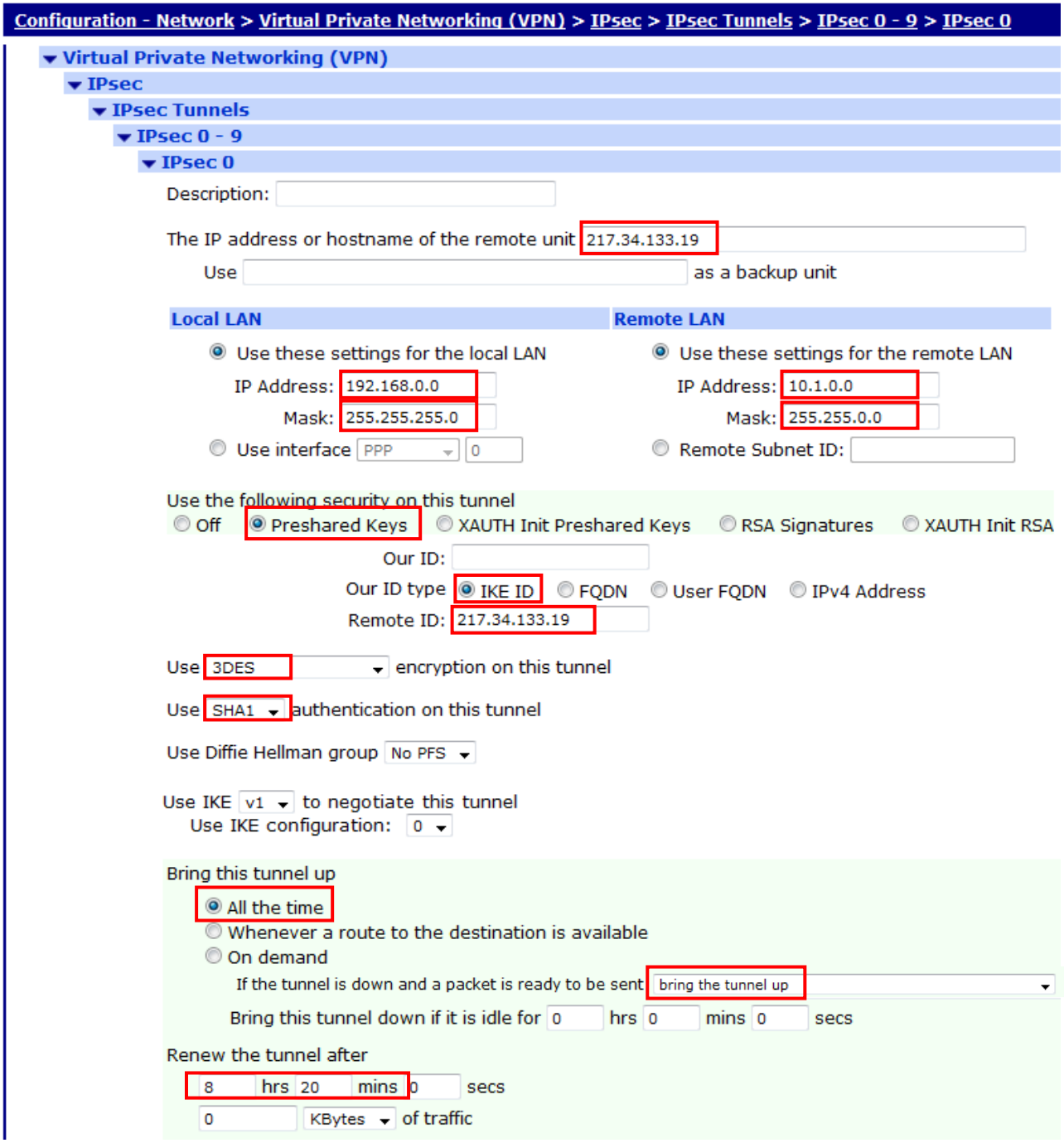


Figure 4-4: Digi Transport – IPSEC

NB: **both the "Peer IP/hostname" and the "Peer ID" need to be set to the public IP address of the Windows PC.**

Parameter	Setting	Description
Peer IP/hostname	217.34.133.19	The public IP address of the Windows PC
Peer ID	217.34.133.19	The public IP address of the Windows PC
Use these settings for the local LAN		
IP address	192.168.0.0	The Digi Transport's private IP address
Mask	255.255.255.0	The Digi Transport's private LAN subnet
Use these settings for the remote LAN		
IP address	10.1.0.0	The Windows PC's private IP address
Mask	255.255.0.0	The Windows PC's private LAN subnet
Use the following security on this tunnel	Preshared Keys	The "key" used between VPN endpoints to encrypt and de-crypt data.
Use x authentication on this tunnel	SHA1	The algorithm used to verify that packet contents have not been changed
Use y encryption on this tunnel	3DES	The cryptographic algorithm to be used when securing the packet payload
Renew the tunnel after	8 Hours 20 Mins	The Digi Transport is configured to expire the IPSec SA based upon the renewal timer.
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	If a packet matches this IPSec tunnel and no SA exists then try to create one
Bring this tunnel up	All the time	The IPSec tunnel will automatically attempt to create an SA (VPN Tunnel) regardless of whether the Digi Transport needs to route any packets to the remote subnet or not.

Click "Apply".

4.5 Configuring the Pre-Shared Key

The pre-shared key is defined in the user table next to an entry which matches the Peer ID parameter in the Eroute. Where the word 'secret' is shown in the screen shot is where the pre-shared key must be typed. This has to match exactly the pre-shared key entered in the Windows configuration and in this case should be ***test***.

Browse to **Configuration - Security > Users > User 10 - 19 > User 10**

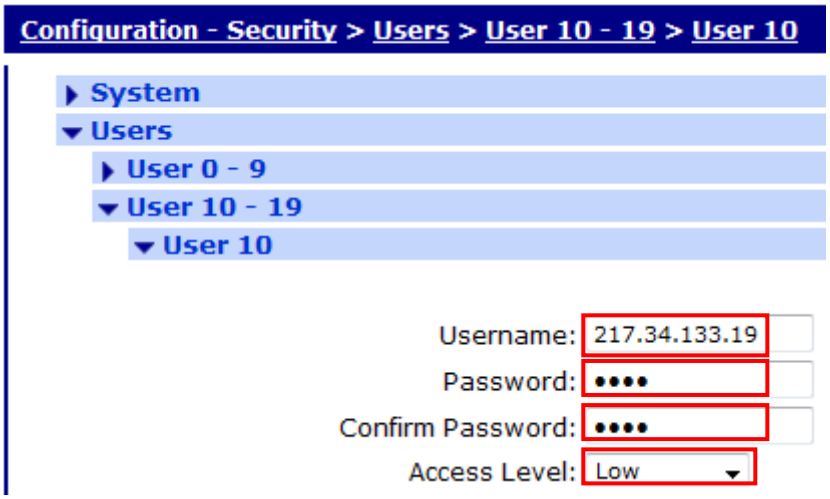


Figure 4-5: Digi Transport – Preshared Key

Parameter	Setting	Description
Username	217.34.133.19	The public IP address of the Windows PC
Password/Confirm Password	test	The pre-shared key

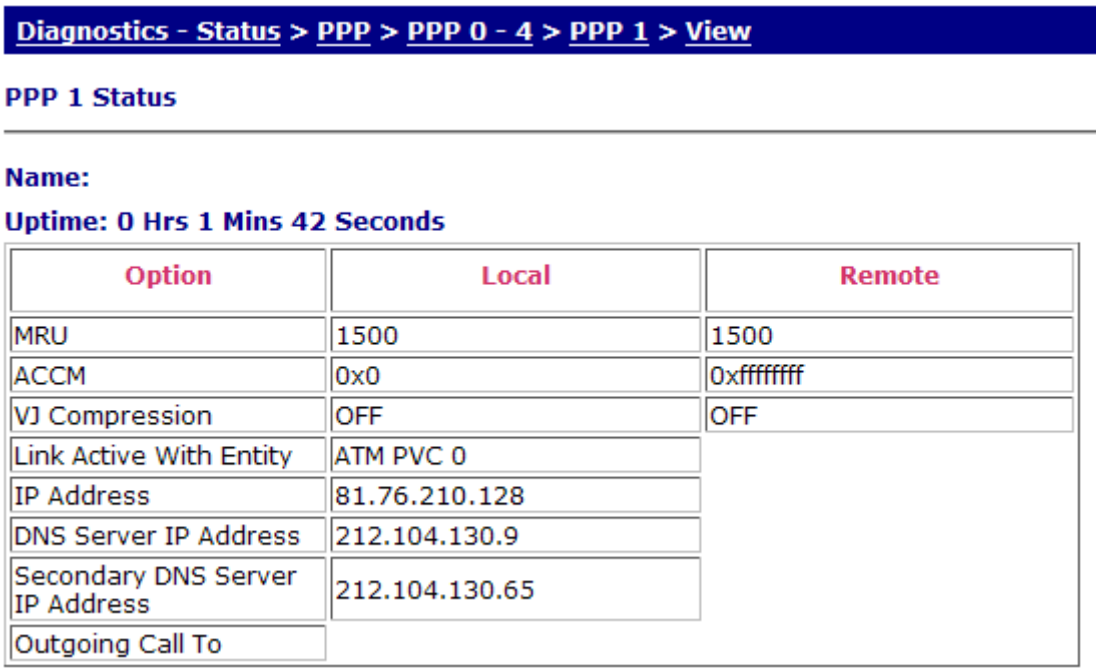
Click “Apply”.

5 TESTING

The configuration of both the Windows PC and the Digi Transport is now complete. If the Digi Transport's public Interface is a PPP instance then it may be necessary to drop and raise the link before the IPSEC negotiation will start.

Browse to **DIAGNOSTICS → STATUS → PPP → PPP 0 – 4 → PPP 1 → VIEW**

Click **Drop Link** and then **Raise Link**. Check that Digi Transport's public interface has an IP address and that it matches that configured in the Windows as the remote tunnel end point.



Diagnostics - Status > PPP > PPP 0 - 4 > PPP 1 > View

PPP 1 Status

Name:

Uptime: 0 Hrs 1 Mins 42 Seconds

Option	Local	Remote
MRU	1500	1500
ACCM	0x0	0xffffffff
VJ Compression	OFF	OFF
Link Active With Entity	ATM PVC 0	
IP Address	81.76.210.128	
DNS Server IP Address	212.104.130.9	
Secondary DNS Server IP Address	212.104.130.65	
Outgoing Call To		

Figure 5-1: Digi Transport – WAN Status

Once this is complete browse to **DIAGNOSTICS → EVENTLOG**.

Near the top of the event log you should see some entries similar to the following successful example:

```
15:44:49, 12 Nov 2009,(71) IKE SA Removed. Peer: 217.34.133.19,Successful Negotiation
15:44:49, 12 Nov 2009,Eroute 0 VPN up peer: 217.34.133.19
15:44:49, 12 Nov 2009,New IPSec SA created by 217.34.133.19
15:44:49, 12 Nov 2009,(71) New Phase 2 IKE Session 217.34.133.19,Initiator
15:44:49, 12 Nov 2009,(70) IKE Keys Negotiated. Peer:
15:44:47, 12 Nov 2009,(70) New Phase 1 IKE Session 217.34.133.19,Initiator
15:44:47, 12 Nov 2009,IKE Request Received From Eroute 0
```

5.1 How to View the IKE SA's (Internet Key Exchange Security Associations)

To view the current state of the IKE exchange between the Digi Transport and the remote Windows PC Browse to **DIAGNOSTICS → STATUS → IPSEC → IKE SAs**.

The remote IP should match that of the Windows tunnel endpoint. An entry here confirms that IKE is being attempted.

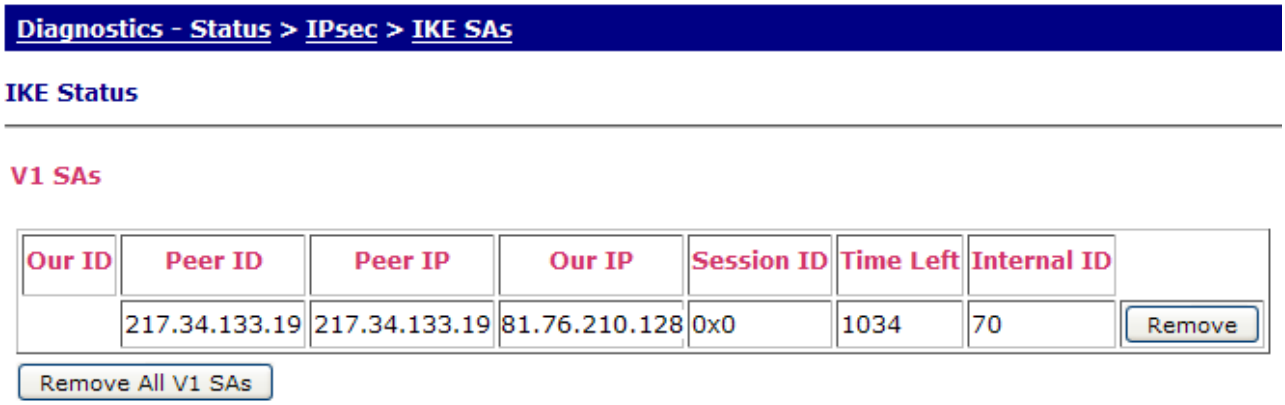


Figure 5-2: Digi Transport – IKE Status

5.2 How to View the IPSec SA's

To view the current state of the VPN Tunnels browse to **DIAGNOSTICS → STATUS → IPSEC → IPSEC SAs**.

The screen shot shows both the inbound and outbound IPSEC security associations. Note that the "Peer IP" is the IP address of the Windows public network interface and that both subnets are represented.

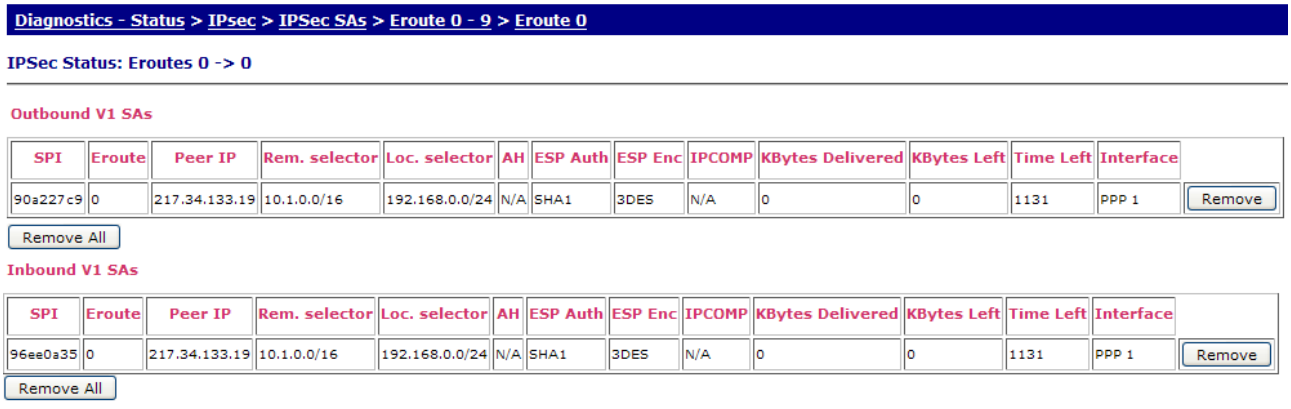


Figure 5-3: Digi Transport – IPSEC SAs

5.3 How to View the IPSec Peers.

A dynamic Eroute is an internal table that the Digi Transport needs to create in order to route data through the correct tunnel. To view this table browse to **DIAGNOSTICS → STATUS → IPSEC → IPSEC PEERS**

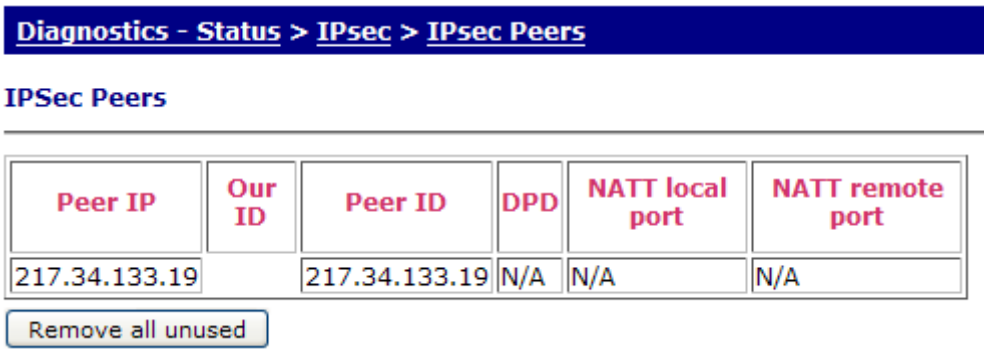


Figure 5-4: Digi Transport – IPSEC Peers

5.4 How to check that data is being encrypted and sent down the tunnel

Firstly browse to **DIAGNOSTICS → STATUS → IPSEC → IKE SAs**.

- Ensure that Analyser is set to "On"
- Ensure that the IP sources PPP 1 and ETH 0 are enabled.
- Enter 80,23 in the filter field. (To prevent your Internet Explorer traffic from being recorded).
- Ensure that "Ethernet Sources" and all other check boxes are cleared.

To test the tunnel send a ping from a device attached to the Digi Transport's private LAN to the IP address of the Window's private Interface. In this example this would be achieved by the following Windows command "ping 10.1.19.1".

Next, browse to **DIAGNOSTICS → ANALYSER → ANALYSER TRACE**.

You should see something like the following trace.

This is the ping packet coming into the Digi Transport's Ethernet Interface from a PC on its local LAN. Note the source and destination IP addresses:

```
-----   26-11-2003  14:12:39.670   -----
45 00 00 3C 00 6E 00 00 20 01 BC A8 C0 A8 00 01     E....n....¼¨À¨..
0A 01 13 01 08 00 48 5C 03 00 02 00 61 62 63 64     ......H.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

IP (In) From REM TO LOC       IFACE: ETH 0
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
00 6E          ID:            110
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
20             TTL:           32
01             Proto:         ICMP
BC A8          Checksum:      48296
```

```
   C0 A8 00 01    Src IP:        192.168.0.1
   0A 01 13 01    Dst IP:        10.1.19.1
   ICMP:
   08             Type:          ECHO REQ
   00             Code:          0
   48 5C          Checksum:      18524
   ----------
```

This is the ping packet being processed by the IPSec code in the Digi Transport. Note the source and destination IP addresses have not changed.

```
-----   26-11-2003  14:12:39.670   -----
45 00 00 3C 00 6E 00 00 1F 01 BD A8 C0 A8 00 01     E....n....½¨À¨..
0A 01 13 01 08 00 48 5C 03 00 02 00 61 62 63 64     ......H.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

IPSec (cont) From LOC TO REM  IFACE: PPP 1
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 3C          Length:        60
00 6E          ID:            110
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
1F             TTL:           31
01             Proto:         ICMP
BD A8          Checksum:      48552
C0 A8 00 01    Src IP:        192.168.0.1
0A 01 13 01    Dst IP:        10.1.19.1
ICMP:
08             Type:          ECHO REQ
00             Code:          0
48 5C          Checksum:      18524
----------
```

This is the ping packet being processed further by the IPSec code in the Digi Transport. The data has now been encrypted by ESP. Note that both the source and destination IP addresses have now changed. In fact the original ping packet has now been encapsulated into an ESP packet.

```
-----   26-11-2003  14:12:39.670   -----
45 00 00 70 00 4A 00 00 FA 32 3E 0F 51 4C D2 80     E..p.J...2..QLÒ€
D9 22 85 13 EE FB 78 D9 00 00 00 02 63 C1 4C BC     ......x.....cÁL¼
B7 F7 01 95 DB D9 4B 03 78 3B 31 B3 F8 25 E4 B8     ·..•..K.x.1³ø.ä¸
3F D6 31 4B BB 1E 85 37 98 2D EF 88 4A 5A E9 AE     ..1K»..7˜..ˆJZ.®
35 61 DE F8 8A 9C 3B 44 BE 6B 6C 5E AB 52 5B E9     5a.øŠ..D¾kl.«R..
37 45 82 04 A4 04 E0 19 7A 57 13 73 53 2D 24 93     7E,.¤.à.zW.sS..“
1B BB 00 39 EF 22 6B 56 C9 7D 27 B0 CD 28 D1 50     .».9..kVÉ..°Í.ÑP

IPSec (cont) From LOC TO REM  IFACE: PPP 1
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
```

```
00 70          Length:        112
00 4A          ID:            74
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
FA             TTL:           250
32             Proto:         ESP
3E 0F          Checksum:      15887
51 4C D2 80    Src IP:        81.76.210.128
D9 22 85 13    Dst IP:        217.34.133.19
----------
```

This packet shows the ESP packet actually being sent out of the Digi Transport's PPP 1 interface. Note that "Final" in "IP (Final) From LOC TO REM IFACE: PPP 1" denotes that the packet is actually going out of the Interface rather than being processed internally by the Digi Transport.

```
-----   26-11-2003  14:12:39.670   -----
45 00 00 70 00 4A 00 00 FA 32 3E 0F 51 4C D2 80     E..p.J...2..QLÒ€
D9 22 85 13 EE FB 78 D9 00 00 00 02 63 C1 4C BC     ......x.....cÁL¼
B7 F7 01 95 DB D9 4B 03 78 3B 31 B3 F8 25 E4 B8     ·..•..K.x.1³ø.ä¸
3F D6 31 4B BB 1E 85 37 98 2D EF 88 4A 5A E9 AE     ..1K»..7˜..ˆJZ.®
35 61 DE F8 8A 9C 3B 44 BE 6B 6C 5E AB 52 5B E9     5a.øŠ..D¾kl.«R..
37 45 82 04 A4 04 E0 19 7A 57 13 73 53 2D 24 93     7E‚.¤.à.zW.sS..“
1B BB 00 39 EF 22 6B 56 C9 7D 27 B0 CD 28 D1 50     .».9..kVÉ..°Í.ÑP

IP (Final) From LOC TO REM    IFACE: PPP 1
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 70          Length:        112
00 4A          ID:            74
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
FA             TTL:           250
32             Proto:         ESP
3E 0F          Checksum:      15887
51 4C D2 80    Src IP:        81.76.210.128
D9 22 85 13    Dst IP:        217.34.133.19
----------
```

The following packet is the ping reply encapsulated in an ESP packet. Note the source IP address is the Windows PC and the Interface is PPP 1.

```
   -----   26-11-2003  14:12:39.750   -----
   45 00 00 70 7A 28 00 00 75 32 49 31 D9 22 85 13     E..pz...u2I1....
   51 4C D2 80 0E 79 10 BB 00 00 00 02 70 4C 91 98     QLÒ€.y.»....pL‘˜
   1C FB 2F 54 B3 D3 BE 8E 8B 3F CB A8 AC F7 35 D2     ...T³Ó¾Ž‹.Ë¨¬.5Ò
   47 1D 96 C1 D6 F9 BA 6E BE 21 23 24 3C 7A A8 92     G.–Á..ºn¾....z¨’
   F7 75 81 7A 1A A5 1D 93 19 93 3F DA 5A A2 04 47     .u.z.¥.“.“..Z¢.G
   3A B7 AD 34 A9 BF B2 03 82 F0 06 76 F9 08 0F 28     .·-4©¿².‚ð.vù..(
   9B 72 23 EA 04 DC 66 68 44 E5 93 FA 73 F4 84 B0     ›r#ê.Üfh.å“ús.°

   IP (In) From REM TO LOC       IFACE: PPP 1
   45             IP Ver:        4
                  Hdr Len:       20
```

```
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 70          Length:        112
   7A 28          ID:            31272
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   75             TTL:           117
   32             Proto:         ESP
   49 31          Checksum:      18737
   D9 22 85 13    Src IP:        217.34.133.19
   51 4C D2 80    Dst IP:        81.76.210.128
   ----------
```

The following entry represents the Digi Transport decrypting the ESP packet and extracting the embedded ping packet in preparation for onward routing. Note that the source and destination IP addresses are now the private addresses.

```
   -----   26-11-2003  14:12:39.750   -----
   45 00 00 3C 28 79 00 00 80 01 34 9D 0A 01 13 01     E....y..€.4.....
   C0 A8 00 01 00 00 50 5C 03 00 02 00 61 62 63 64     À¨....P.....abcd
   65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
   75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

   IP (Cont) From REM TO LOC     IFACE: PPP 1
   45             IP Ver:        4
                  Hdr Len:       20
   00             TOS:           Routine
                  Delay:         Normal
                  Throughput:    Normal
                  Reliability:   Normal
   00 3C          Length:        60
   28 79          ID:            10361
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   80             TTL:           128
   01             Proto:         ICMP
   34 9D          Checksum:      13469
   0A 01 13 01    Src IP:        10.1.19.1
   C0 A8 00 01    Dst IP:        192.168.0.1
   ICMP:
   00             Type:          ECHO REPLY
   00             Code:          0
   50 5C          Checksum:      20572
   ----------
```

This is the final packet and shows the ping reply actually being sent out of the Digi Transport's Ethernet interface back to the PC that originally sent the ping request.

```
-----   26-11-2003  14:12:39.750   -----
45 00 00 3C 28 79 00 00 7F 01 35 9D 0A 01 13 01     E....y....5.....
C0 A8 00 01 00 00 50 5C 03 00 02 00 61 62 63 64     À¨....P.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69                 uvwabcdefghi

IP (Final) From LOC TO REM    IFACE: ETH 0
```

```
45              IP Ver:         4
                Hdr Len:        20
00              TOS:            Routine
                Delay:          Normal
                Throughput:     Normal
                Reliability:    Normal
00 3C           Length:         60
28 79           ID:             10361
00 00           Frag Offset:    0
                Congestion:     Normal
                                May Fragment
                                Last Fragment
7F              TTL:            127
01              Proto:          ICMP
35 9D           Checksum:       13725
0A 01 13 01     Src IP:         10.1.19.1
C0 A8 00 01     Dst IP:         192.168.0.1
ICMP:
00              Type:           ECHO REPLY
00              Code:           0
50 5C           Checksum:       20572
```