

Application Note 11

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

November 2015

Contents

1	Intr	oduction	5
	1.1	Outline	5
2	Assi	umptions	6
	2.1	Corrections	6
	2.2	Version	6
3	Con	nfiguring the windows pc	7
	3.1	Creating a local IPSEC Policy	7
	3.2	How to Create a Filter List from NetA to NetB	9
	3.3	How to Build a Filter List from NetB to NetA	12
	3.4	How to Configure a Rule for a NetA-to-NetB Tunnel	15
	3.5	How to Configure a Rule for a NetB-to-NetA Tunnel	20
	3.6	How to Assign Your New IPSec Policy to Your Windows Gateway	25
4	Con	nfiguring the Digi Transport Router	26
	4.1	Configuring the Digi Transport's Default Route	26
	4.2	Enabling IPSec	27
	4.3	Configuring IKE (Internet Key Exchange)	28
	4.4	Configuring the Digi Transport's Eroute	29
	4.5	Configuring the Pre-Shared Key	
5	Tes	ting	
	5.1	How to View the IKE SA's (Internet Key Exchange Security Associations)	
	5.2	How to View the IPSec SA's	
	5.3	How to View the IPSec Peers	
	5.4	How to check that data is being encrypted and sent down the tunnel	34

Figures
Figure 1-1: Overview Diagram5
Figure 3-1: Local Security Settings7
Figure 3-2: IP Security Policy Wizard7
Figure 3-3: IP Security Policy Name
Figure 3-4: Requests for Secure Communication8
Figure 3-5: IP Security Policy Wizard Finish9
Figure 3-6: New Policy Properties9
Figure 3-7: New Policy Properties – Net A to Net B10
Figure 3-8: IP Filter List Name
Figure 3-9: IP Filter Properties – Subnet IP Addresses11
Figure 3-10: IP Filter List
Figure 3-11: New Rule Properties – Net B to Net A12
Figure 3-12: IP Filter List Name
Figure 3-13: IP Filter Properties – Subnet IP Addresses
Figure 3-14: IP Filter List
Figure 3-15: IP Filter Properties – finish14
Figure 3-16: New Policy Properties – Net A to Net B Tunnel15
Figure 3-17: Edit Rule Properties – Net A to Net B Tunnel Endpoint15
Figure 3-18: New Policy Properties – Net A to Net B Tunnel – Connection Type16
Figure 3-19: New Policy Properties – Net A to Net B Tunnel – Filter Action
Figure 3-20: New Filter Action Properties – Net A to Net B Tunnel – Security Methods
Figure 3-21: New Security Method– Net A to Net B Tunnel – Encryption Integrity
Figure 3-22: New Filter Action Properties – Net A to Net B Tunnel – Security Method Finish
Figure 3-23: New Rule Properties – Net A to Net B Tunnel – Filter Action
Figure 3-24: New Rule Properties – Net A to Net B Tunnel – Edit Authentication
Figure 3-25: Authentication – Net A to Net B Tunnel – Preshared Key 19
Figure 3-26: New Rule Properties – Net A to Net B Tunnel – Authentication Finish
Figure 3-27: IPSEC Tunnel Properties – Net B to Net A

Figure 3-28: New Rule Properties – Net B to Net A Tunnel – IP Filter List	
Figure 3-29: New Rule Properties – Net B to Net A Tunnel – Tunnel Endpoint	21
Figure 3-30: New Rule Properties – Net B to Net A Tunnel – Tunnel Endpoint	22
Figure 3-31: New Rule Properties – Net B to Net A Tunnel – Filter Action	22
Figure 3-32: New Rule Properties – Net B to Net A Tunnel – Authentication Methods	23
Figure 3-33: Authentication – Net B to Net A Tunnel – Preshared Key	23
Figure 3-34: New Rules Properties – Net B to Net A Tunnel – Authentication Methods	24
Figure 3-35: IPSec Tunnel Properties – Net B to Net A	24
Figure 3-36: Local Security Settings – Assign IPSEC Policy	25
Figure 3-37: Local Security Settings – IPSEC Policy Assigned	25
Figure 4-1: Digi Transport – Default Route	26
Figure 4-2: Digi Transport – WAN Enable IPSEC	27
Figure 4-3: Digi Transport – IKE	
Figure 4-4: Digi Transport – IPSEC	29
Figure 4-5: Digi Transport – Preshared Key	31
Figure 5-1: Digi Transport – WAN Status	
Figure 5-2: Digi Transport – IKE Status	
Figure 5-3: Digi Transport – IPSEC SAs	
Figure 5-4: Digi Transport – IPSEC Peers	

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@DigiTransport.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.

Local Security Settings			- 0	×
File Action View Help				
← → 🗈 🖗 🗳 🍰				
Security Settings	Name /	Description	Policy Assigned	_
Account Policies Local Policies Dublic Key Policies Software Restriction Policies Policies Pescurity Policies on Local Computer	Client (Respond Only) Secure Server (Require Security) Server (Request Security)	Communicate normally (unse For all IP traffic, always req For all IP traffic, always req	No No No	
0	eate IP Security Policy			
M	anage IP filter lists and filter actions			
Al	l Tasks	•		
Vi	ew J			
Ri	efresh kport List			
H	elp			
reate an IP Security policy	1			

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.

Security Policy Wizard	2
IP Security Policy Name Name this IP Security policy and provide a brie	f description
Na <u>m</u> e:	
IPSEC Tunnel - Windows & Sarian	
Description:	
	<u>A</u>
	<u> </u>
	< <u>B</u> ack <u>N</u> ext > Cancel

Figure 3-3: IP Security Policy Name

Click Next.

IP Security Policy Wizard	28
Requests for Secure Commu Specify how this policy respo	inication Inds to requests for secure communication.
The default response rule res other rule applies. To commu secure communication.	ponds to remote computers that request security, when no nicate securely, the computer must respond to requests for
Activate the default respo	inse rule.
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

Security n	ules for communicating with	other computers	
P Security rules:	Filter Action	Authentication	T
		14.1	
Cynamic>	Default Response	Kerberos	No
Clynamic>	Default Response	Kerberos	N

Figure 3-6: New Policy Properties

Authentication Methods I · · · · · · · · · · · · · · · · · ·	Tunnel Setting Connection Type
The selected IP filter affected by this rule.	list specifies which network traffic will be
P Filter Lists: Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
	î

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**.

Windows	LAN to Sarian LAN			
Description	n:			<u>A</u> dd
			~	<u>E</u> dit
			-	<u>R</u> emove
Filter <u>s</u> :				Use Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Mirrored	Description	Protocol	Source Port	Destinat

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.

<u>I</u> P Address:	10	8	1		0		0
Subnet <u>m</u> ask:	255	25	255		0	•2	0
Destination address:							
A specific IP Subnet		_			1	-	
IP add <u>r</u> ess:	192		168		0	•	0
Subnet mas <u>k</u> :	255	55	255		255	•	0
Mimored. Also match pack destination addresses.	ets with t	the	exact o	pp	osite so	ource	e and

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**.

Name:	LANAS Codes LAN			
Description	LAN IO Sanah LAN			<u>A</u> dd
			<u>N</u>	Edit
			~	<u>R</u> emove
Filter <u>s</u> :			L Us	e Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	De
Minorea				

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**.

Authentication Methods 1	Funnel Setting Connection Type	
IP Hiter List	Filter Action	
The selected IP filter affected by this rule.	list specifies which network traffic will b	
P Filter <u>L</u> ists:	4	
Name	Description	
O All ICMP Traffic	Matches all ICMP packets betw	
All IP Traffic	Matches all IP packets from this	
Add	Remove	

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**.

<u>N</u> ame:				
Sarian LA Descriptior	N to Windows LAN	L;		<u>A</u> dd
			<u>^</u>	<u>E</u> dit
			~	<u>R</u> emove
Filter <u>s</u> :				Jse Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination

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.

<u>I</u> P Address:	192	×.	168	•	0		0
Subnet <u>m</u> ask:	255	25	255		255	•2	0
A specific IP Subnet	10				0	-	ol
A specific IP Subnet					2	1	
n ddd <u>i</u> caa.	955		- 955		0	•	0
Jubrier mask.	233	•	233		.0	•	0

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**.

<u>N</u> ame:				
Sarian LA	N to Windows LAN	1		
Description	1:			<u>A</u> dd
			~	<u>E</u> dit
				<u>R</u> emove
Filter <u>s</u> :			Г	Use Add Wizard
	Description	Protocol	Source Port	Destinatio
Mirrored	Description			
Mirrored No	Description	ANY	ANY	ANY
Mirrored No	Description	ANY	ANY	ANY

Figure 3-14: IP Filter List

Authentication Methods Tunnel Setting Connection Ty IP Filter List Filter Action Image: The selected IP filter list specifies which network traffic will affected by this rule. P Filter Lists: Name Description O All ICMP Traffic Matches all ICMP packets betw. O All IP Traffic Matches all IP packets from this O Sarian LAN to Windows LAN O Windows LAN to Sarian LAN	r Kule Properties	
The selected IP filter list specifies which network traffic will affected by this rule. P Filter Lists: Name Description All ICMP Traffic Matches all ICMP packets betw. All IP Traffic Matches all IP packets from this O Sarian LAN to Windows LAN O Windows LAN Windows LAN to Sarian LAN Edit	Authentication Methods Tu IP Filter List	unnel Setting Connection Type Filter Action
P Filter Lists: Name Description O All ICMP Traffic Matches all ICMP packets betw. O All IP Traffic Matches all IP packets from this O Sarian LAN to Windows LAN Sarian LAN to Sarian LAN O Windows LAN to Sarian LAN Bemove	The selected IP filter lit affected by this rule.	st specifies which network traffic will b
All ICMP Traffic Matches all ICMP packets betw. All IP Traffic Matches all IP packets from this Sarian LAN to Windows LAN Windows LAN to Sarian LAN Windows LAN to Sarian LAN Bernove	⁹ Filter <u>L</u> ists: Name	Description
O All IP Traffic Matches all IP packets from this O Sarian LAN to Windows LAN O Windows LAN to Sarian LAN O Windows LAN to Sarian LAN Edit Add Edit	O All ICMP Traffic	Matches all ICMP packets betw
Sarian LAN to Windows LAN Windows LAN to Sarian LAN Add Edit	O All IP Traffic	Matches all IP packets from this
Windows LAN to Sarian LAN Add Edit	Sarian LAN to Windows LAN	
	A11	-

Figure 3-15: IP Filter Properties - finish

Click **OK** again.

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.

	?
Authentication Methods T IP Filter List	unnel Setting Connection Type Filter Action
P Filter Lists:	Description
O All IP Traffic O Sarian LAN to Windows LAN ⊙ Windows LAN to Sarian LAN	Matches all IP packets from this

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).

IP Filter List Filter Action Authentication Methods Tunnel Setting Connection Ty This rule only applies to network traffic over connections o the selected type. All <u>petwork connections</u> Local area network (LAN) <u>Bemote access</u>			
Authentication Methods Tunnel Setting Connection Ty This rule only applies to network traffic over connections o the selected type. All <u>n</u> etwork connections Local area network (LAN) <u>Remote access</u>	IP Filter List		Filter Action
This rule only applies to network traffic over connections of the selected type.	Authentication Methods	Tunnel Setting	Connection Type
All <u>n</u> etwork connections Local area network (LAN) <u>Remote access</u>	This rule only app the selected type	olies to network tra a.	affic over connections of
<u>L</u> ocal area network (LAN) <u>R</u> emote access	All network connections		
™ <u>R</u> emote access	<u>L</u> ocal area network (LAN)		
	<u>R</u> emote access		

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.

v Rule Properties	(
Authentication Methods Tu	unnel Setting Connection Type Filter Action
The selected filter acti for secure network traf	on specifies whether this rule negotiat fic, and how it will secure the traffic.
ilter Actions:	
Name O D1	Description
O Request Security (Optional) O Require Security	Accepts unsecured communicat Accepts unsecured communicat
A <u>d</u> d	Remove Use Add Wizar

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.

C Block C <u>N</u> ego Security	c otiate security: method preference	order:	
Туре	AH Integrity	ESP Confidential E	S Add
			<u>E</u> dit
			Bemove
			Move <u>up</u>
<	III	2	Move dowr
Acce	pt unsecured communication key perfect forv	munication, but always resp unication <u>wi</u> th non-IPSec-a ward secrecy (PFS)	oond using <u>I</u> PSec ware computer

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.

lew Security Method	?
Security Method	
Encryption and Integrity Data will be encrypted and verified as authentic and unmodified	
C Integrity only	
Data will be verified as authentic and unmodified, but will not be encrypted	
C Custom	
ОК	Cancel

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

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

lew Filter Ac	tion Pro	perties		2
Security Metho Permit Block Negotiate Security meth	ds Genera	e order:		
Туре	AH Int	ESP Confidential	ESP Int	A <u>d</u> d
Encryption	<none></none>	3DES	SHA1	<u>E</u> dit
				<u>H</u> emove
				Move <u>up</u>
<	Ш		>	Move down
C Accept ur	nsecured co ecured com ey <u>p</u> erfect fi	mmunication, but alw munication <u>wi</u> th non- orward secrecy (PFS)	vays respond IPSec-aware)	using <u>I</u> PSec computer
		ОК	Cancel	Apply

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

Select the filter action you just created.

New Rule Properties	? 🛛
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected filter action for secure network traffi	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Filter Actions:	•
Name	Description
Permit Request Security (Optional) Require Security	Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat
A <u>d</u> d	Remove Use Add Wizard
Clos	se Cancel <u>Apply</u>

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

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

IP Filter	List	1	Filter Action
Authentication Me	thods Tun	nel Setting	Connection Type
Auther betwe offered compu	ntication methods en computers. The d and accepted w iter.	specify how tru ese authenticat hen negotiating	st is established ion methods are i security with anothe
uthentication <u>m</u> eth Method	od preference ord	er:	Add
Kerberos	- Ortano		
			<u>Edit</u>
			Bemove
			Move <u>up</u>
			Move d <u>o</u> wr
			121

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'

ntication Method Properties	?
ion Method	
The authentication method specifies how trust is ex between the computers.	stablished
Directory <u>d</u> efault (Kerberos V5 protocol)	
certificate from this certification authority (CA):	
<u>_</u>	rowse
is <u>s</u> tring (preshared key):	
	^
	<u>×</u>
ОК	Cancel
	Ition Method Interaction Method Properties Ition Method Interaction method specifies how trust is experiment to computers. Interaction default (Kerberos V5 protocol) Interaction authority (CA): Interaction Int

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

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

IP Filter List		Filter Action
Authentication Method	Is Tunnel Setting	g Connection Type
Authentica between o offered an computer.	ation methods specify ho computers. These authe d accepted when negot	ow trust is established ntication methods are tiating security with anothe
uthentication <u>m</u> ethod p Method	preference order:	Add
Preshared Key	test	
		Bemove
		Move <u>up</u>
		Move d <u>o</u> wr

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.

SEC Tunnel - Windows &	Sarian Properties	3
P Security rules:	Filter Action	Authentication
Windows LAN to Sarian	IPSEC Tunnel with E Default Response	Preshared Key Kerberos
<]		>
Add <u>E</u> dit	<u>R</u> emove	Use Add <u>W</u> izard
	Close	Cancel

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).

IP Filter List	Tunnel Setting	Connection Type ilter Action	
The selected IP filte	er list specifies which 	network traffic will b	
P Filter <u>Li</u> sts:	Description		
O All ICMP Traffic	Matches all IC	Matches all ICMP packets betw	
O All IP Traffic	Matches all IP	Matches all IP packets from this	
⊙ Sarian LAN to Windows LAN	4		
v e waren 2008 ta 1000 ta 10000 ta 1000	140 		

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.)

w Rule Properties			3
IP Filter List		Filter Actio	on
Authentication Methods	Tunnel Set	ting Conn	ection Type
This rule only app the selected type	olies to network	traffic over conr	nections of
• All network connections			
C Local area network (LAN)			
C <u>R</u> emote access			
		1 1	
	OK	Cancel	Apply



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

Authentication Methods T	unnel Setting Connection Typ	
IP Filter List	Filter Action	
The selected filter actions the former of the selected filter actions the selected fil	on specifies whether this rule negotia fic, and how it will secure the traffic.	
Name	Description	
IPSEC Tunnel with ESP Permit	Permit unsecured IP packets to	
O Request Security (Optional)	Accepts unsecured communicat	
O Require Security	Accepts unsecured communicat	
Add	Remove Use Add Wiza	

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**.

	¥2	
IP Filter List		Filter Action
Authentication Methods	Tunnel Setting	Connection Type
Authenticati between co offered and computer.	on methods specify how tr mputers. These authentica accepted when negotiatin	ust is established ation methods are Ig security with anothe
uthentication <u>m</u> ethod pre	eference order:	
Method	Details	A <u>d</u> d
Kerberos		Edit
		<u>L</u>
		Bemove
		Move <u>up</u>
		Move dowr

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**.

Authentication Met	thod		
Na The bet	e authentication method s ween the computers.	pecifies how trust is	established
C Active Directo	ory <u>d</u> efault (Kerberos V5 p ate from this certification	protocol) authority (CA):	Breuman
		L	<u>Diowse</u>
Use this string test	g (preshared key):		~
100t			
			1

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

Click **OK** again.

Rule Properties		
IP Filter List		Filter Action
Authentication Method	s Tunnel Setting	Connection Type
Authentica between c offered and computer.	tion methods specify how omputers. These authent d accepted when negotia	r trust is established ication methods are ting security with anothe
uthentication <u>m</u> ethod p Method	reference order: Details	Add
Preshared Key	test	
		Remove
		17011040
		Move <u>up</u>
		Move d <u>o</u> wr
	ок	Cancel

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**.

SEC Tunnel - Windows &	Sarian Properties	?
Rules General Security rules for co	ommunicating with other co	omputers
IP Security rules:	Either Action	Authentientien
Mindawa I AN ta Sarian	IDSEC Turanal with E	Pershared Kay
Sarian LAN to Windows	IPSEC Tunnel with E	Preshared Key
CDynamic>	Default Response	Kerberos
A <u>d</u> d <u>E</u> dit		Vse Add Wizard
	Close	Cancel

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**.

Local Security Settings				×
File Action View Help				
← → 🗈 🗙 🕾 🗟 🖄 着	1 2			
Becurity Settings	Name /	Description	Policy Assigned	
🗄 🤷 Account Policies	Client (Respond Only)	Communicate normally (unse	No	
E Gal Policies	MIPSEC Tunnel - Windows & Sarian	Accien	No	
Public Key Policies	Secure Server (Require Security)	Assign always req	No	
IP Security Policies on Local Computer	Server (Request Security)	All Tasks 🔹 🕨 Ilways req		
÷		Delete		
		Rename Properties Help		
]			_
Assign this policy, attempt to make it active				

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**.

😼 Local Security Settings				2
<u>File Action View H</u> elp				
←→ € ×88. 8 12 ±	• 🖹 <u>a</u>			
Security Settings	Name 🔺	Description	Policy Assigned	
Account Policies	Client (Respond Only)	Communicate normally (unse	No	
🕂 🤐 Local Policies	IPSEC Tunnel - Windows & Sarian		Yes	
	Secure Server (Require Security)	For all IP traffic, always req	No	
IP Security Policies on Local Computer	Server (Request Security)	For all IP traffic, always req	No	

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.

<u>Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0</u>
Description:
Default route via
Gateway:
Interface: PPP 🕴 1
Metric: 1

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.

Configuration - Network > Interfaces > DSL		
▼ Interfaces		
Ethernet		
▶ Wi-Fi		
▶ Mobile		
▼ DSL		
Enable DSL		
Configure PVC 0 🗸		
PVC Configuration		
Enable this PVC		
Encapsulation: PPPoA VC-Mux		
VPI: 0 VCI: 38		
DSL Network Settings		
This DSL PVC is using PPP 1		
Description ADSL		
Username: Enter ADSL Username		
Password:		
Confirm password:		
 Enable NAT on this interface IP address IP address and Port 		
NAT Source IP address: 0		
Enable IPsec on this interface		
Keep Security Associations (SAs) when this DSL interface is disconnected		
Use interface Default 👻 0 for the source IP address of IPsec packets		

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

<u>Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0</u>		
▼ Virtual Private Networking (VPN)		
▼ IPsec		
IPsec Tunnels		
IPsec Default Action		
▶ IPsec Groups		
Dead Peer Detection (DPD)		
▼ IKE		
> IKE Debug		
▼ IKE 0		
Use the following settings for negotiation Encryption: None DES 3DES AES (128 bit) AES (192 bit) AES (256 bit) Authentication: None MD5 SHA1 Mode: Main Aggressive MODP Group for Phase 1: 2 (1024) MODP Group for Phase 2: No PFS Renegotiate after 8 hrs 0 mins 0 secs		
▼ Advanced		
Retransmit a frame if no response after 10 seconds Stop IKE negotiation after 2 retransmissions Stop IKE negotiation if no packet received for 30 seconds I Enable Dead Peer Detection Enable NAT-Traversal		

Figure 4-3: Digi Transport - IKE

Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE
Енстурион		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	2 (1024)	The key length used in the IKE Diffie-Hellman
Phase 1		exchange
Enable NAT-	No	Disables NAT traversal
Traversal	NO	DISADLES NAT LIAVEISAL

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.

<u>Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tur</u>	<u>nnels</u> > <u>IPsec 0 - 9</u> > <u>IPsec 0</u>
▼ Virtual Private Networking (VPN)	
▼ IPsec	
▼ IPsec Tunnels	
▼ IPsec 0 - 9	
▼ IPsec 0	
Description:	
The IP address or hostname of the remote unit 217.34.133.19	
Use as a b	ackup unit
Local LAN Remote LAN	
Use these settings for the local LAN	se settings for the remote LAN
IP Address: 192.168.0.0 IP Addres	ess: 10.1.0.0
Mask: 255.255.255.0 Ma	ask: 255,255,0,0
♥ Use interface PPP → 0	Subnet ID:
Use the following security on this tunnel Off Preshared Keys XAUTH Init Preshared Keys F Our ID: Our ID type IKE ID FQDN User FQE Remote ID: 217.34.133.19 Use 3DES - encryption on this tunnel Use SHA1 - authentication on this tunnel Use Diffie Hellman group No PFS - Use IKE v1 - to negotiate this tunnel Use IKE v1 - to negotiate this tunnel	RSA Signatures © XAUTH Init RSA DN © IPv4 Address
Bring this tunnel up All the time Whenever a route to the destination is available On demand If the tunnel is down and a packet is ready to be sent bring the tunnel Bring this tunnel down if it is idle for 0 hrs 0 mins Renew the tunnel after 8 hrs 20 mins 0 secs 0 KBytes of traffic	nel up 🗸 🗸

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 <mark>y</mark> 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

<u>Conf</u>	iquration - Security	<u>v > Users > User 10 - 19 > User 10</u>
•	System	
-	Users	
) User 0 - 9	
	▼ User 10 - 19	
	▼ User 10	
		Username: 217.34.133.19
		Password: ••••
		Confirm Password: ••••
		Access Level: Low 🗸

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	0×ffffffff
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** \rightarrow **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,(70) New Phase 1 IKE Session 217.34.133.19,Initiator

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** \rightarrow **STATUS** \rightarrow **IPSEC** \rightarrow **IKE SAs**.

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

Diagnostics - Status > IPsec > IKE SAs

IKE Status

V1 SAs

Our ID	Peer ID	Peer IP	Our IP	Session ID	Time Left	Internal ID	
	217.34.133.19	217.34.133.19	81.76.210.128	0x0	1034	70	Remove
Remov	e All V1 SAs						

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** \rightarrow **STATUS** \rightarrow **IPSEC** \rightarrow **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.

Diagnos	Diagnostics - Status > <u>IPsec</u> > <u>IPSec SAs</u> > <u>Eroute 0 - 9</u> > <u>Eroute 0</u>												
IPSec St	Sec Status: Eroutes 0 -> 0												
Outboun	utbound V1 SAs												
SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
90a227c9	o	217.34.133.19	10.1.0.0/16	192.168.0.0/24	N/A	SHA1	3DES	N/A	0	o	1131	PPP 1	Remove
Remove	All												
Inbound	V1 SAs												
SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
96ee0a35	0	217.34.133.19	10.1.0.0/16	192.168.0.0/24	N/A	SHA1	3DES	N/A	0	0	1131	PPP 1	Remove
Remove	All												

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** \rightarrow **STATUS** \rightarrow **IPSEC** \rightarrow **IPSEC PEERS**

Diagnostics - S	Status :	> <u>IPsec</u> > <u>IPsec</u>	c Pee	<u>rs</u>	
IPSec Peers					
Peer IP	Our ID	Peer ID	DPD	NATT local port	NATT remot
217.34.133.19	L	217.34.133.19	N/A	N/A	N/A

Remove all unused



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

Firstly browse to **DIAGNOSTICS** \rightarrow **STATUS** \rightarrow **IPSEC** \rightarrow **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:

-			2	26-1	11-2	2003	3 1	L4:1	12:3	39.0	570						
4	5 (00	00	3C	00	6E	00	00	20	01	BC	A8	C0	A8	00	01	En%"À"
0	A	01	13	01	08	00	48	5C	03	00	02	00	61	62	63	64	Habcd
6	5	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	efghijklmnopqrst
7	5	76	77	61	62	63	64	65	66	67	68	69					uvwabcdefghi
I	Р	(Ir	1) I	- ron	n RE	ЕМ Т	TO L	.0C			IFA	ACE :	: E ⁻	TH (9		
4	5					IΡ	Ver	י:			4						
						Hdr	۲Le	en:			20						
0	0					TOS	5:				Rou	utir	ne				
						De]	Lay:	:			Nor	rma	L				
						Thr	roug	ghpι	it:		Nor	rma]	L				
						Re]	liał	oili	ty	:	Nor	rma]	L				
0	0	3C				Ler	ngtł	ו:			60						
0	0	6E				ID:	:				110	3					
0	0	00				Fra	ag (Offs	set	:	0						
						Cor	nges	stic	on:		Nor	rma]	L				
											May	/ Fi	ragi	nen	t		
											Las	st I	- ra	gmei	nt		
2	0					TTL	.:				32						
0	1					Pro	oto:	:			ICN	1P					
В	C	A8				Che	ecks	sum:			482	296					

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.

		2	26-1	L1-2	2003	5 1	4:1	12:3	39.0	570							
45	00	00	3C	00	6E	00	00	1F	01	BD	A8	C0	A8	00	01	En½¨À¨	
0A	01	13	01	80	00	48	5C	03	00	02	00	61	62	63	64	Habcd	
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	
IPS	Sec	(cc	ont)) Fr	rom	LOC	C T () RI	EM	IF	ACE :	: PI	PP :	1			
45					IΡ	Ver	י :			4							
					Hdr	• Le	en:			20							
00					TOS	:				Roi	utir	ne					
					Del	ay:				Noi	rmal	1					
					Thr	oug	ghpι	ut:		Noi	rmal	1					
					Rel	iab	ili	ity	:	Noi	rmal	1					
00	3C				Len	igth	n:	-		60							
00	6E				ID:	-				11(9						
00	00				Fra	ig C)ffs	set	:	0							
					Con	iges	stic	on:		Noi	rmal	1					
						U				May	y Fi	ragr	nent	t			
										Las	, st I	Frag	gmei	nt			
1F					TTL	:				31			,				
01					Pro	to:				IC	٩P						
BD	A8				Che	cks	sum	:		48	552						
C0	A8	00	01		Src	IP:	:			192	2.16	58.6	9.1				
0A	01	13	01		Dst	: IP	·:			10	.1.3	19.3	1				
ICM	1P:																
08					Tvp	e:				ECI	HO F	REO					
00					Cod	le:				0		č					
48	5C				Che	cks	um			18	524						

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 14:12:39.67								39.6	570	-							
	45	00	00	70	00	4A	00	00	FA	32	3E	0F	51	4C	D2	80	Ep.J2QLÒ€
l	D9	22	85	13	EE	FΒ	78	D9	00	00	00	02	63	C1	4C	BC	xcÁL¼
l	B7	F7	01	95	DB	D9	4B	03	78	3B	31	Β3	F8	25	E4	B8	••K.x.1³ø.ä,
l	3F	D6	31	4B	BB	1E	85	37	98	2D	EF	88	4A	5A	E9	AE	1K»7~^JZ.®
l	35	61	DE	F8	8A	9C	3B	44	ΒE	6B	6C	5E	AB	52	5B	E9	5a.øŠD¾kl.«R
l	37	45	82	04	A4	04	E0	19	7A	57	13	73	53	2D	24	93	7E,.¤.à.zW.sS"
l	1B	BB	00	39	EF	22	6B	56	C9	7D	27	B0	CD	28	D1	50	.».9kVɰÍ.ÑP
I																	
I	IPS	Sec	(co	ont) Fr	rom	LOO	с то) RE	EM	IFA	ACE :	: PF	PP 1	L		
	45					IΡ	Ver	`:			4						
l						Hdr	۲ Le	en:			20						
	00					TOS	5:				Rou	utir	ne				
l						Del	lay	:			Nor	rma	L				
l						Thr	rou	ghpu	ut:		Nor	rma	1				
Reliability:									Nor	rma	L						

00 70	Length:	112
00 4A	ID:	74
00 00	Frag Offset:	0
	Congestion:	Normal
	Ū	May Fragment
		Last Fragment
FA	TTL:	250
32	Proto:	ESP
3E ØF	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.

.

		4	26-1	LI-4	200:	3]	[4:]	12:3	59. 6	5/0	-					
45	00	00	70	00	4A	00	00	FA	32	3E	0F	51	4C	D2	80	Ep.J2QLÒ€
D9	22	85	13	EE	FΒ	78	D9	00	00	00	02	63	C1	4C	BC	xcÁL¼
Β7	F7	01	95	DB	D9	4B	03	78	3B	31	Β3	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~^JZ.®
35	61	DE	F8	8A	9C	3B	44	ΒE	6B	6C	5E	AB	52	5B	E9	5a.øŠD¾kl.«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	Β0	CD	28	D1	50	.».9kVɰÍ.ÑP
IΡ	(Fi	inal	l) I	ror	n LC	DC 1	TO F	REM		IFA	ACE :	: PF	PP 1	1		
45					IΡ	Ver	י:			4						
					Hdr	r Le	en:			20						
00					T05	5:				Rou	utir	ne				
					De]	Lay:	:			Nor	rma]	L				
					Thr	roug	ghpι	ut:		Nor	rma]	L				
					Rel	liat	oili	ity:		Nor	rma]	L				
00	70				Ler	ngtł	ו:			112	2					
00	4A				ID:	:				74						
00	00				Fra	ag (Offs	set:		0						
					Cor	nges	stic	on:		Nor	rma]	L				
										Мау	/Fr	ragn	nent	t		
										Las	st F	ra	gmer	nt		
FA					TTL	_:				256)					
32					Pro	oto:	:			ESF	>					
3E	0F				Che	ecks	sum	:		158	387					
51	4C	D2	80		Sro	: IF	:			81.	76.	216	0.12	28		
D9	22	85	13		Dst	t IF):			217	7.34	1.13	33.2	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.... QLÒ€.y.»...pL'~ 51 4C D2 80 0E 79 10 BB 00 00 00 02 70 4C 91 98 1C FB 2F 54 B3 D3 BE 8E 8B 3F CB A8 AC F7 35 D2T³Ó¾Ž<..˨¬.5Ò 47 1D 96 C1 D6 F9 BA 6E BE 21 23 24 3C 7A A8 92 G.-Á..ºn¾....z¨' .u⊇z.¥."."..Z¢.G F7 75 81 7A 1A A5 1D 93 19 93 3F DA 5A A2 04 47 3A B7 AD 34 A9 BF B2 03 82 F0 06 76 F9 08 0F 28 ...4©¿².,..v.... >r....fhD.".sô.° 9B 72 23 EA 04 DC 66 68 44 E5 93 FA 73 F4 84 B0 IP (In) From REM TO LOC IFACE: PPP 1 45 IP Ver: 4 Hdr Len: 20

0	0	TOS: Delay: Throughput: Reliability:	Routine Normal Normal
0	0 70	length:	112
7	Δ 28		31272
0	0 00	Frag Offset:	0
		Congestion:	Normal May Fragment Last Fragment
7	5	TTL:	117
3	2	Proto:	ESP
4	9 31	Checksum:	18737
D	9 22 85 13	Src IP:	217.34.133.19
5	1 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.

26-11-2	2003 14:12:39.7	750	
45 00 00 3C 28	79 00 00 80 01	34 9D 0A 01 13 01	Ey€.4
C0 A8 00 01 00	00 50 5C 03 00	02 00 61 62 63 64	À Pabcd
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	TTI:	128	
01	Proto:	TCMP	
34 9D	Checksum:	13469	
0A 01 13 01	Src IP:	10.1.19.1	
C0 A8 00 01	Dst TP:	192.168.0.1	
TCMP:	550 111	19211001011	
99	Type.	ECHO REPLY	
99	Code:	0	
50 50	Checksum.	20572	
	checkball.	20372	

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
 03C
 28
 79
 00
 07
 01
 35
 9D
 0A
 01
 13
 01

 45
 00
 01
 28
 79
 00
 00
 7F
 01
 35
 9D
 0A
 01
 13
 01

 C0
 A8
 00
 01
 00
 05
 5C
 03
 00
 02
 00
 61
 62
 63
 64

 65
 66
 67
 68
 69
 6A
 6B
 6C
 6D
 6E
 6F
 70
 71
 72
 73
 74

 75
 76
 77
 61
 62
 63
 64
 65
 66
 67
 68
 69

E....y....b. À^{..}...P....abcd efghijklmnopqrst 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