

Windows XP VPN Client Example

Technote LCTN0007

Proxicast, LLC 312 Sunnyfield Drive Suite 200 Glenshaw, PA 15116

1-877-77PROXI 1-877-777-7694 1-412-213-2477

Fax: 1-412-492-9386

E-Mail: support@proxicast.com

Internet: www.proxicast.com © Copyright 2005-2008, Proxicast LLC. All rights reserved.

Proxicast is a registered trademark and LAN-Cell, and LAN-Cell Mobile Gateway are trademarks of Proxicast LLC. All other trademarks mentioned herein are the property of their respective owners.

This TechNote applies to LAN-Cell models:

LAN-Cell 2:

LC2-411 (firmware 4.02)

CDMA:

1xMG-401 1xMG-401S

GSM:

GPRS-401

Minimum LAN-Cell Firmware Revision: 3.62(XF2).

Note for Original LAN-Cell Model (1xMG & GPRS) Users:

The VPN configuration screens in the original LAN-Cell's Web GUI differ slightly from the examples in this Technote. Please locate the corresponding parameter fields in the VPN Configuration section of the LAN-Cell's user interface under VPN Rules (IKE). See also the LAN-Cell's *User Guide* for more information on VPN configuration. Contact Proxicast Technical Support for previous versions of this TechNote for firmware releases prior to 4.02.

Document Revision History:

Date	Comments
September 22, 2006	First release
July 16, 2007	Updated for LAN-Cell 2
March 3, 2008	Updated LAN-Cell 2 screens for firmware release 4.02 including VPN Wizard example.



Introduction

This Technote documents one example configuration for using the Windows XP built-in IPSec VPN Client software to create a VPN tunnel to a LAN-Cell 2 Cellular Router. Other configurations may also be possible, depending upon your requirements and network configuration. This Technote is for illustration purposes only.

Example Network Topology



Figure 1: Example Network Topology

Usage Notes

- This example was created using Windows XP Professional (5.1 Build 2600.xpsp_sp2_gdr.070227-2254: Service Pack 2) and LAN-Cell 2 firmware version 4.02(AQP.1). Use the "winver.exe" program to determine your version of Windows XP.
- The IPSec functionality in early versions of Windows XP contained anomalies that prevented it from establishing connections to "pure" IPSec devices such as the LAN-Cell. Proxicast recommends updating your Windows XP installation with all of the latest critical Microsoft patches.
- Disable or properly configure any local Windows Firewall or other Third-Party IP applications that may interfere with establishing an IPSec VPN.
- When configuring a VPN connection, it is helpful to have the LAN-Cell and your target PC/equipment physically near each other so that you can view the configuration and logs of each device while testing.
- In this example the LAN-Cell has a static WAN IP address. Windows XP's VPN Client does not support IPSec tunnels to host or domain names. If your LAN-Cell has a dynamic IP address, you must know the current IP address in advance to configure the XP client.
- Your HQ Router must be configured to allow IKE (UDP:500) packets to flow between your Windows XP PC and the LAN-Cell in order for the IPSec tunnel to be negotiated.
- This example demonstrates a Single Address (XP) VPN connection to a remote Subnet via a VPN Tunnel (LAN-Cell's LAN subnet). The LAN-Cell supports site-to-site VPN tunnels with all of the leading IPSeccompliant VPN routers/concentrators such as Cisco, Juniper, ZyXEL, SonicWall, etc.
- This example configuration will also work if your Windows XP PC is directly connected to the Internet and your ISP allows VPN requests to pass through their firewall. In the example, replace 192.168.0.51 with the IP address assigned by your ISP. <u>The HQ and Remote LANs must be on different subnets</u>.
- There is additional information on LAN-Cell VPN configuration parameters in the LAN-Cell User's Guide.



Example LAN-Cell Configuration

The LAN-Cell 2 includes a **VPN Wizard** feature to step you through the process of creating basic VPN connection rules and network definitions. We will use the VPN Wizard to create the Windows XP client connection parameters on the LAN-Cell 2. To reach this screen, select **SECURITY** then **VPN Wizard** from the left side menu. (See Figure 2).

proxicas	WIZARD - VPN	
HOME		
NETWORK 🛛 🖾		
WIRELESS 🛛 🗹	Gateway Policy Property	
SECURITY 🛛 🖂 FIREWALL	Name	
VPN WIZARD	Gateway Policy Setting	
VPN CONFIG CERTIFICATES	My LAN-Cell	0.0.0
AUTH SERVER	Remote Gateway Address	0.0.0.0
ADVANCED 🔤		
LOGS		
MAINTENANCE		
LOGOUT		Next

Figure 2: LAN-Cell 2 VPN Wizard

To begin the VPN Wizard, you must give the Gateway Policy a descriptive Name. (See Figure 3).

If your LAN-Cell has a static WAN IP address assigned by your ISP or cellular operator, enter that value as the <u>My LAN-Cell</u> address. Optionally you can enter a Dynamic DNS FQDN that is associated with your LAN-Cell's WAN (see the Advanced->DNS->DDNS screen) or you can enter 0.0.0.0 and the LAN-Cell will use its current WAN IP address. This value must match the <u>Tunnel Endpoint Address</u> parameter in the Windows XP client.

For the <u>Remote Gateway Address</u>, enter 0.0.0.0. This will create a default rule that will accept VPN connections from any remote IP address that presents the correct Phase 1 and Phase 2 parameters and keys. This configuration provides the most flexibility when connecting remote Windows XP clients from multiple PCs. Also, when the Windows XP VPN Client is used on a PC behind a NAT router, it does not present a consistent source IP address during IKE negotiations, preventing the tunnel from being established if either the router's public IP or the Windows XP client's private IP address is used as the Remote Gateway Address.

Note: If you want to restrict the IP address(es) that can establish a VPN connection using this default global rule, you can add a CELL-CELL/LAN-Cell Firewall Rule to restrict IKE (UDP:500) traffic to a specific IP address or range. See the *User's Guide* for more information on creating firewall rules.



Name	Windows-XP-Clients	
ateway Policy Setting		
My LAN-Cell	166.139.37.167	
Remote Gateway Address	0.0.0.0	

Figure 3: Gateway Policy Parameters

Next, we must create a Network Policy that defines which IP addresses (or subnets) will be used on each end of the VPN tunnel. Figure 4 illustrates the correct settings for our example VPN tunnel.

etwork Bolicy Setting	
Local Network	O Single O Range IP O Subject
Starting IP Address	192 . 168 . 1 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Remote Network	💿 Single 🔍 Range IP 🔍 Subnet 🛛 🚽 🔤
Starting IP Address	0.0.0.0
Ending IP Address / Subnet Mask	0,0,0,0

Figure 4: Network Policy Parameters

Be certain to check the Active option. You must also give the Network Policy a descriptive Name.

For the <u>Local Network</u> section, select the <u>Subnet</u> option and enter the LAN-Cell's current LAN subnet and mask. Note that when specifying the subnet, the last octet is 0 for a full Class-C network (255 devices). For our example, the subnet is 192.168.1.0 / 255.255.255.0

For the <u>Remote Network</u>, select <u>Single Address</u> as the type and enter an IP address of 0.0.0.0. This creates a default rule that allows the remote VPN client to have any IP address that is not part of the LAN-Cell's subnet. You can optionally specify the exact remote client IP address that you will assign to the Windows XP Client VPN.



Next, we define the IKE Phase 1 parameters that will be used to negotiate the initial VPN tunnel connection between an XP Client and the LAN-Cell.

Negotiation Mode	💿 Main Mode 🔘 Aggressive Mode
Encryption Algorithm	💿 des 🔍 aes 🔍 bdes
Authentication Algorithm	🔘 SHA1 🖲 MD5
Key Group	🖸 DH1 🔍 DH2
SA Life Time	28800 (Seconds)
Pre-Shared Key	12345678

Figure 5: IKE Phase 1 Parameters

Figure 5 shows the default values for the IKE Phase 1 parameters. For our example, we will accept the default values and adjust the Windows XP client to match these settings.

The LAN-Cell supports several different types of authentication, including X.509 digital certificates. However, it is easiest to configure the VPN tunnel with Pre-Shared Keys that are the same on both the Windows XP client and the LAN-Cell. Enter a <u>Pre-Shared Key</u> that is at least an 8 character string. Avoid non-alphanumeric characters such as dashes, underscores, asterisks, etc. In our example, the Pre-Shared Key is 12345678.

Encapsulation Mode	💿 Tunnel 🔍 Transport
IPSec Protocol	🖲 ESP 🔍 AH
Encryption Algorithm	
Authentication Algorithm	📀 SHA1 🔘 MD5
SA Life Time	28800 (Seconds)
Perfect Forward Secrecy (PFS)	🖲 None 🔍 DH1 💭 DH2

Figure 6: IKE Phase 2 Parameters

The settings on this screen are the LAN-Cell defaults and do not need to be changed for our example. You will configure the Windows XP VPN Client to match these settings.



The VPN Wizard will now display a summary screen of all of the parameters you've entered for the VPN tunnel (Figure 7). Review these values and go back through the Wizard if any changes are required. You may wish to print this screen to document the LAN-Cell's VPN configuration parameters.

Gateway Policy Property	
Name	Windows-XP-Clients
Gateway Policy Setting	
My LAN-Cell	166.139.37.167
Remote Gateway Address	0.0.0.0
Network Policy Property	
Active	Yes
Name	Remote-XP-Clients
Network Policy Setting	
Local Network	
Starting IP Address	192.168.1.0
Subnet Mask	255,255,255,0
Starting ID Address	0000
Ending IP Address	N/A
IKE Tuppel Setting (IKE Phase 1)	
Authentication For Activating VPN	
Authenticated By	
User Name	
Password	
Negotiation Mode	Main Mode
Encryption Algorithm	DES
Authentication Algorithm	MD5
Key Group	DH1
SA Life Time	28800 (Seconds)
Pre-Shared Key	12345678
IPSec Setting (IKE Phase 2)	
Encapsulation Mode	Tunnel Mode
IPSec Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA LITE TIME Destant Ferminard Secretary (DES)	28800 (Seconds)
Periect Forward Secrecy (PFS)	None

Figure 7: VPN Wizard Summary Screen

Click Finish on the summary screen to save the VPN configuration. The confirmation screen shown in Figure 8 will be displayed.



Configuration of the LAN-Cell is now complete. You can review and modify the VPN configuration parameters using the **VPN Config** option on the left side menu (Figure 9).

Click on the LOGS Menu, clear any existing entries, and then configure the Windows XP VPN Client software.

proxicast	N	HE
номе	VPN Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting	
NETWORK 🗹	VPN Rules	
WIRELESS 🗹		
SECURITY S FIREWALL VPN WIZARD VPN CONFIG CERTIFICATES	Local Network	
AUTH SERVER	🛙 # VPN Rules 😽	
ADVANCED 🗵	🖬 1 Windows-XP-Clients 🔊 166.139.37.167 🕥 Dynamic 📝 🗊 💞	
LOGS		
MAINTENANCE		
LOGOUT		

Figure 9: VPN Configuration Screen

To view the network policies associated with each rule, click the [+] symbol to the left of the Gateway Policy. To edit either the Network or Gateway Policy parameters, click the edit icon \mathbb{F} on right of the corresponding line (Figure 10).

(((н
proxicast		
VPN		
HOME	Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting	
NETWORK 🗵	VPN Rules	
WIRELESS		
SECURITY 🔤	Local Internet Remote Network	
VPN WIZARD		
VPN CONFIG	My LAN-Cell Remote Gateway	
CERTIFICATES		
AUTH SERVER	■ # VPN Rules 😒	
ADVANCED 💌	🗖 1 Windows-XP-Clients 🔊 166.139.37.167 🖓 Dynamic 📝 🗊 🚓	
LOGS	Remote-XP-Clients 💭 192.168.1.0 / 💮 Any 🕅 📝 🗊 🖓	
MAINTENANCE		
LOGOUT		



Figure 11 shows the VPN Gateway Policy Edit screen.

VPN - GATEWAY POLICY - EDIT

Name	Windows-XP-Clients	
🗖 NAT Traversal		
ateway Policy Information		
My LAN-Cell		
My Address	166.139.37.167	(Domain Name or IP Address)
🔍 My Domain Name	None 🔽 (See DDNS)	
Same Primary Remote Gateway	0.0.0.0	(Domain Name or IP Address)
Enable IPSec High Availability		
😡 Redundant Remote Gateway		(Domain Name or IP Address)
Fall back to Primary Remote Gatev	vay when possible	
Fall Back Check Interval*	28800 (180~8640	10 seconds)
*Fall Back Chook Internal, The time intern	al for absolving availability of Dui	many Romoto Catoway, IRCas CA life time w
be superseded by this value when it is larg	ai for checking availibility of Pri er than this value.	mary Remote Gateway, IPSec SA life time w
uthentication Key	9.	
Construction	10345678	
Cartificate	auto deperated self signed	cett 🔽 (Cas My Castification)
Local ID Type		(See <u>My Certificates</u>)
Content	0.0.0	
Peer ID Type	IP V	
Content	0.0.0.0	
xtended Authentication		
Enable Extended Authentication		
C Server Mode	(Search <u>Local User</u> first th	en <u>RADIUS</u>)
Client Mode		
User Name		
Password		
(E Proposal		
Negotiation Mode	Main	
Encryption Algorithm	DES 🔹	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Key Group	DH1 💌	
🗖 Enable Multiple Proposals		
ssociated Network Policies		
# Name	Local Network	Remote Network
	102 168 1 0 / 255 255 255	.0 (R) Any
Remote-XP-Clients C		

Figure 12 shows the VPN Network Policy Edit screen.

VPN - NETWORK POLICY - EDIT

🔽 Active	
Name	Remote-XP-Clients
Protocol	
🗖 Nailed-Up	
📃 🔲 Allow NetBIOS broadcast Traffic T	Fhrough IPSec Tunnel
🗌 🗖 Check IPSec Tunnel Connectivity	Log
Ping this Address	0.0.0
Gateway Policy Information	
Sateway Policy	Windows-XP-Clients
.ocal Network	
🟠 Address Type	Subnet Address
Starting IP Address	192 . 168 . 1 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Local Port	Start 0 End 0
Remote Network	
🕅 Address Type	Single Address 💌
Starting IP Address	0,0,0,0
Ending IP Address / Subnet Mask	0.0.0.0
Remote Port	Start 0 End 0
PSec Proposal	
Encapsulation Mode	Tunnet
Active Protocol	ESP V
Encryption Algorithm	DES 💌
Authentication Algorithm	SHA1 V
SA Life Time (Seconds)	28800
Perfect Forward Secrecy (PFS)	NONE V
Enable Replay Detection	
Enable Multiple Proposals	

Figure 12: Editing the VPN Network Policy Parameters

Example Windows XP VPN Client Configuration

To configure Windows XP's built-in IPSec VPN Client software, you must define a series of local security policies. The easiest way to do this is using the **Local Security Policy Editor** (secpol.msc) found under Control Panel / Administrative Tools (Figure 13).

Figure 13: Starting Windows Security Policy Editor

After launching the Security Policy Editor, select **IP Security Policies on Local Computer** in the left-side pane, right click the mouse and select **Create IP Security Policy** from the pop-up menu (Figure 14).

Local Security Settings				
File Action View Help				
← → 🗈 🗗 💀 😤 🗎	<u>≜</u>			
Security Settings		Name A	Description	Policy Assigned
Account Policies		Client (Respond Only)	Communicate normally (unsecur	No
Hocal Policies		Secure Server (Require Security)	For all IP traffic, always require	No
Comparing the second seco	outor	Server (Request Security)	For all IP traffic, always reques	No
IP Security Policies on Local Comp	Creat	e IP Security Policy	—	
	Manag	ge IP filter lists and filter actions		
	All Tas	sks 🔸		
Create an IP Security policy	View	•		
	Refre	sh		
	Expor	t List		
	Help			

This will launch the IP Security Policy Wizard. Follow the wizard to create a new policy (Figure 15).

Figure 15: New IP Security Policy Wizard

You must uncheck the Activate the default response rule option box (Figure 16).

Figure 16: Deactivate the Default Response Rule

Complete the wizard and edit the resulting IP Security Policy (Figure 17).

Figure 17: Completing the Wizard

The Properties page will display. Uncheck the **Use Add Wizard** option and click **Add...** (Figure 18). Then click **Add...** again on the next screen to add a new IP Filter List (Figure 19).

ID Eilter Liet	Filter Action	Authentication	Tu
Oynamic>	Default Response	Kerberos	No

Figure 18: Adding a New Rule

XP to LAP	V-Cell			
Description	n:			Add.
Filter pack	kets flowing from my	XP PC to the remote	LAN-Cell	Edit
			*	Remove
Filters:				Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination

Figure 19: Adding IP Filter List for XP to LAN-Cell

Name this rule that defines the packet filtering scheme for packets flowing from your XP computer to the remote private LAN subnet of the LAN-Cell. Uncheck the **Use Add Wizard** option box, then click **Add...** to define the filter parameters (Figure 20).

- Source address:	20					7		
My IP Address					1	-		
Destination address								
A specific IP Subnet						-		-
ID addmas:	102		168		1		0	
Coheat wash	955		200	•	1 9EE	13	0	
Subnet mask.	200		299	•	200	•	U	
Mirrored. Also match pack	ets with t	the	exact of	pp	osite so	urce	e and	
destination addresses.								
Ň								

Figure 20: XP to LAN-Cell Filter Properties

Figure 20 shows the correct values for the example VPN network. Set the <u>Source Address</u> to "My IP Address" and the <u>Destination Address</u> to "A specific IP Subnet". For the <u>Subnet IP Address</u>, enter the LAN IP subnet address & mask of the LAN-Cell (192.168.1.0/255.255.255.0 in our example). Uncheck the <u>Mirrored</u> option box.

When complete, close the Filter Properties dialog box and the IP Filter List dialog box to return to the Rule Properties dialog box shown in Figure 21.

IP Filter List	Tunnel Setting Connection Typ
The selected IP (ilter list snecifies which network traffic wi
affected by this n	ile ist specifies which hetwork traffic wi ile.
IP Filter Lists:	1.
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
All IP Traffic All IP Traffic	Filter packets flowing from my Y

Figure 21: XP to LAN-Cell IP Filter List

Highlight the newly added Filter to apply it to the current Rule and go to the Filter Action tab (Figure 22).

Figure 22: Filter Action – Require Security

Click Edit... to define the security properties as shown in Figure 23.

None>	DES		
	DES	SH	-
None>	DES	ME	Edit
None>	3DES	ME	
None>	DES	SH	Remove
None>	3DES	SH	
None>	DES	SH	Move up
None>	DES	ME	move up
		I	Move down
	None> None> None> None> secured comm	None> JUES None> DES None> JDES None> DES None> DES secured communication, but always	None> JUES ML None> DES SH None> JDES SH None> DES SH None> DES ME DES ME

Figure 23: Filter Action – Security Methods (Phase 2)

Select Negotiate Security and ensure that the one of the methods is:

AH Integrity = <None> ESP Confidentiality = DES ESP Integrity = SHA1 Key Lifetimes = 0 / 28800

Check the <u>Accept Unsecured Communication</u>, <u>But Always Respond Using IPSec</u> option box. Uncheck the <u>Session Key Perfect Forward Secrecy (PFS)</u> option box.

These are the security method settings for our VPN example. You may select other settings as long as they match the corresponding Phase 2 settings in your LAN-Cell's VPN rule. We recommend that you move the desired security method to the top of the list.

If the desired security method is not present, then click **Add...** or **Edit...** to modify the settings as shown in Figures 24 and 25.

Figure 24: New Custom Security Method

stom 9	Security	Method Settings	;	?
pecify t	he setting	s for this custom se	curity method.	
Data Integ	and addr	<mark>ess integrity witho</mark> ut hm:	encryption (AH) :	
MD	5	v		
7 Data Integ	integrity a rity algorit	and encryption (ESF hm:):	
SH/	\1	•		
Encr	yption alg	orithm:		
DES	5	•		
Sessio	n key sett enerate a 100	ings: new key every: Kbytes	Generate a new	key every
				Canaal
				Cancer

Figure 25: Security Method Properties

Click **OK** on the **Require Security Properties** dialog box to return to the **Edit Rule Properties** page. Select the **Authentication Method** tab (Figure 26).

Security Methods Author betwo offere comp	Authentication Methods entication methods specify hov sen computers. These authen d and accepted when negotia uter.	v trust is established ication methods are tting security with another
Authentication met	nod preference order:	
Method	Details	Add
Kerberos		Edit
		Remove
I		Move up
		Move down

Figure 26: Authentication Method

Click Edit... to change the Authentication Method to Preshared Key (Figure 27).

48	Authentication Method	
	The authentication method specifies how trust i between the computers.	s established
	C Active Directory default (Kerberos V5 protocol)	
	C Use a certificate from this certification authority (CA):	Province
	C Usadhia daina (madamad kua).	DIDWSC
	12345678	2

Figure 27: Edit Authentication Method to Preshared Key

In our example, we are using a preshared key of 12345678. Click **OK** to return to the **Edit Rule Properties** page and select the **Tunnel Setting** tab (Figure 28).

	IP Filter List	1	Filter Action
Authentic	cation Methods	Tunnel Setting	Connection Typ
	The tunnel end; IP traffic destina list. It takes two	point is the tunneling c tion, as specified by th rules to describe an IF	omputer closest to the ne associated IP filter PSec tunnel.
C This ru	le does not specify	an IPSec tunnel.	
The tu	nnel endpoint is sp	ecified by this <u>I</u> P addre	ess:
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37.	167	
16	6.139.37 .	167	

Figure 28: VPN Tunnel Endpoint

The IP address to enter as the <u>Tunnel Endpoint</u> is the public IP address of the WAN interface on the LAN-Cell (166.139.37.167 in our example). Click **Apply** to save the IP address.

Note: the Windows XP VPN Client does not allow a domain name as the Tunnel Endpoint, so your LAN-Cell must either have a static IP assigned by your cellular service provider, or you must edit these IPSec settings for the current WAN IP address of the LAN-Cell each time you wish to connect.

Select the **Connection Type** tab and check the <u>Local Area Network</u> option (Figure 29). Press **Apply** to save this setting and then click OK to return to the Rules List page.

Rule Properties		
IP Filter List	T	Filter Action
Authentication Methods	Tunnel Setting	Connection Type
This rule only appl	ies to network tr	affic over connections of
C All network connections		
Local area network (LAN)	-	_
C Remote access		
_		
		2 2 31 2 2

Figure 29: Connection Type

At this point, we have defined the "outbound" side of the VPN tunnel – XP to LAN-Cell. Close any open properties pages to return to the main **VPN Rule Property** page as shown in Figure 30.

P Security rules:	Filter Action	Authentication	Т
XP to LAN-Cell	Require Security	Preshared Key	16

Figure 30 "Outbound" VPN Tunnel Definition

Now we must repeat the steps above to define the "inbound" side of the Tunnel from the LAN-Cell back to XP.

Click **Add...** to bring up the Rule Properties page and then click **Add...** again to create a new IP Filter List to define how packets flow from the LAN-Cell to your XP PC. (Figures 31 & 32).

IP Filter List	Filter Action
The selected IP fill affected by this rul	ter list specifies which network traffic will l le.
Name	Description
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets betw Matches all IP packets from this
♀ XP to LAN-Cell	Hiter packets flowing from my X

Figure 31: Adding a New IP Filter List for LAN-Cell to XP

LAN-Cell t	o XP			
Description	1:			Add
Filter pack	ets flowing from the	e remote LAN-Cell to m	ny XP PC	Edit
			Ŧ	Remove
Filters:				Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destinatio

Figure 32: Defining the IP Filter List for LAN-Cell to XP

Click **Add...** on the IP Filter List page to define the inbound filter. For this filter, set the <u>Source Address</u> to the LAN-Cell's LAN subnet, (192.168.1.0/255.255.255.0 in the example) and the <u>Destination Address</u> to "My IP Address" (Figure 33).

IP Address:	192 .	168		1	•	0	1 🔶
Subnet mask:	255 .	255	•	255	-	0	
Minored Also match back	ate with the	event	200	neita er		boo	

Figure 33: LAN-Cell to XP Filter Properties

Click **OK** twice to return to the New Rule Properties dialog box (Figure 34).

Rule Properties	
Authentication Methods IP Filter List	Tunnel Setting Connection Typ Filter Action
The selected IP filte	r list specifies which network traffic will l
P Filter Lists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
LAN-Cell to XP	Packets flowing from the remote
Add Edit	Remove

Figure 34: LAN-Cell to XP Filter Properties

Highlight the LAN-Cell to XP filter and select the **Filter Action** tab. Select <u>Require Security</u> and click **Edit...** (Figure 35).

Authentication Methods	Tunnel Setting	Connection Type	
IP Filter List		Filter Action	
The selected filt for secure netwo	er action specifies who ork traffic, and how it v	ether this rule negotiate vill secure the traffic.	
Iter Actions: Name	Description		
O Permit	Permit unsec	Permit unsecured IP packets to	
C Request Security (Option	al) Accepts unse	Accepts unsecured communicat	
Require Security	Accepts unse	ecured communicat	
Q Require Security	Accepts unse	ecured communicat	

Figure 35: Filter Action for LAN-Cell to XP

For our example VPN, ensure that the Security Methods shown in Figure 36 include:

AH Integrity = <None> ESP Confidentiality = DES ESP Integrity = SHA1 Key Lifetimes = 0 / 28800

Check the <u>Accept Unsecured Communication</u>, <u>But Always Respond Using IPSec</u> option box. Uncheck the <u>Session Key Perfect Forward Secrecy (PFS)</u> option box. Click **OK** when complete.

	ESP Confidential	ES	Add
<none></none>	DES	SH	
<none></none>	DES	ME	Edit
<none></none>	3DES	ME	Demo
<none></none>	DES	SH	Hemove
<none></none>	JUES DEC	SH CL	
<none></none>	DES	ME	Move up
CINOLIES	DES	ML	
		•	Move dow
	<none> <none> <none> <none> <none> <none> <none> unsecured comm</none></none></none></none></none></none></none>	<pre><none> DES <none> DES <none> 3DES <none> DES </none></none></none></none></none></none></none></none></none></none></none></pre>	OES SF <none> DES ME <none> 3DES ME <none> DES SH <none> 3DES SH <none> DES SH <none> DES SH <none> DES SH <none> DES ME unsecured communication, but always respond SH</none></none></none></none></none></none></none></none>

Figure 36: Filter Action – Security Methods (Phase 2)

Now select the **Authentication Method** tab and change the default Kerberos authentication to a <u>preshared key</u> of 12345678 (Figure 37).

22	The authentication methors between the computers.	od specifies how trust is es	tablisl
C Active	Directory default (Kerberos	V5 protocol)	
C Use a	certificate from this certificat	tion authority (CA):	
			TOWSE
• Use thi	s string (preshared key):		
120			

Figure 37: Preshared Key

Click OK and then select the Tunnel Setting tab (Figure 38).

For this <u>Tunnel Endpoint</u>, enter an IP address that is **NOT** part of the remote LAN-Cell's LAN subnet. Typically you will enter the private IP address of your XP PC. In our example, enter 192.168.0.51.

Note: If your Windows XP PC has a public IP address (from your ISP), use that address as the Tunnel Endpoint on this page.

If you defined the VPN rule on the LAN-Cell to allow only a specific remote IP address (instead of using 0.0.0.0), then enter the same IP address on this page that you entered for the <u>Remote Single Address</u> in the LAN-Cell's VPN rule.

	IP Filter List	. [Filter Action
Authentic	ation Methods	Tunnel Setting	Connection Ty
	The tunnel end IP traffic destina list. It takes two	point is the tunneling stion, as specified by t rules to describe an l	computer closest to th the associated IP filte IPSec tunnel.
C This rul	le does not specify	an IPSec tunnel.	
 The tur 	nnel endpoint is sp	ecified by this IP addr	meet.
			000.
19	2.168.0.	51	
19	2.168.0.	51	
19	2.168.0.	51	
19	2.168.0.	51	
19	2.168.0.	51	
19	2.168.0.	51 }	
19	2.168.0.	51 ₃	
19	2.168.0.	51 L _S	

Figure 38: XP PC Tunnel Endpoint

Next, select the **Connection Type** tab and choose <u>Local Area Network</u> (Figure 39).

ID Dis Los	30	E-11 A .:-
IP Filter List		Filter Action
Authentication Methods	Tunnel Settin	ig connection type
This rule only app the selected type	olies to network t	raffic over connections of
All network connections		
Local area network (LAN)	-	_
Remote access		

Figure 39: Connection Type

Click **OK** to close the Rule Properties page. You should now have 2 custom rules as shown in Figure 40.

P Security rules:	Charles		Γ.T.
	Pequine Security	Preshared Key	10
	Require Security	Preshared Key	10
CDynamic>	Default Response	Kerberos	No

Figure 40: Inbound & Outbound VPN Rules

Select the General tab (Figure 41).

n to Dan Centroperdes	?
Rules General	
IP Security policy general properties	
 <u>N</u> ame:	
VPN to LAN-Cell	
Description:	
Mobile Gateway at 166.139.37.167	
	-
Check for policy changes every: 180 minute(s)	¥
Qheck for policy changes every: 180 minute(s) Perform key exchange using these settings: Advanced	

Figure 41: General Rule Settings

Click Advanced, then Methods (Figure 42).

480		sy ditor overy.	
Authenticate a	and generate a new ke	after every:	
0	session(s)	, and every.	
Protect identit	es with these security	methods:	
Methods			
		1 10	

Figure 42: Advanced Key Exchange Settings (Phase 1)

Ensure that at least one of the Key Exchange Methods shown in Figure 43 is:

Type = IKE Encryption = DES Integrity = MD5 Diffie-Hellman Group = Low (1)

Use the **Add/Edit** buttons to create this combination if it does not already exist. Move this combination to the top of the list as shown.

Note: These settings are appropriate for our example and LAN-Cell's default configuration. You may select other combinations as long as they match the Phase 1 settings in the LAN-Cell's VPN Gateway Policy rule page.

Security me	thod preference or	ler:		
Туре	Encryption	Integrity	[Ad
IKE	DES	MD5	L	-
IKE	3DES	MD5	P.	EC
IKE	DES	SHA1	Ľ	Ren
				Mos
4			•	Move

Figure 43: Key Exchange Methods

Close all property dialog boxes and return to the Local Security Policy Editor. Highlight the **VPN to LAN-Cell** Policy set that you just built, right click and select **Assign** from the pop-up menu (Figure 44).

Local Security Settings			
File Action View Help			
← → 🖻 🗙 📽 🗟 😫 撞 🖄	<u>8</u> 3		
Security Settings	Name /	Description	Policy Assigned
E Account Policies	Client (Respond Only)	Communicate normally (unsecur	No
	Secure Server (Require Security)	For all IP traffic, always require	No
Public Key Policies	Server (Request Security)	For all IP traffic, always reques	No
Software Restriction Policies IP Security Policies on Local Computer	VPN to LAN-Cell	Assign	No
			•
		All Tasks	
		Delete	
ssign this policy, attempt to make it active		Rename	
		Properties	
		Help	

Figure 44: Assigning the IPSec Policy

Your XP VPN Client configuration is now complete and you can establish the tunnel by opening a Command Prompt (DOS) window and pinging the remote LAN-Cell's LAN IP address (or any other device in that subnet). XP will negotiate IPSec security and eventually bring up the tunnel. It may take several seconds for the tunnel to be established, so additional ping's may be required (see Figure 45).

🔤 DOS Prompt	- 0 ×
C:\WINDOWS\system32>ping 192.168.1.1	-
Pinging 192.168.1.1 with 32 bytes of data:	
Negotiating IP Security. Negotiating IP Security. Negotiating IP Security. Negotiating IP Security.	
Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),	
C:\WINDOWS\system32>ping 192.168.1.1	
Pinging 192.168.1.1 with 32 bytes of data:	
Reply from 192.168.1.1: bytes=32 time=525ms TIL=254 Reply from 192.168.1.1: bytes=32 time=486ms TIL=254 Reply from 192.168.1.1: bytes=32 time=529ms TIL=254 Reply from 192.168.1.1: bytes=32 time=546ms TIL=254	
Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 486ms, Maximum = 546ms, Average = 521ms	•

Figure 45: Establishing the VPN Tunnel from XP

If the VPN Tunnel is not established, review your settings on the XP client compared to the LAN-Cell. If you change your XP settings, you should **Unassign** the policy, restart the **IPSec Service** (using the Services Manager in Control Panel/Administrative Tool (Figure 46), and then **re-assign** the VPN Policy before attempting to build the tunnel again. A troubleshooting guide follows this section with more information on the meaning of various LAN-Cell log entries.

Services (Local)				
g our rices (cours)	TPSEC Services	Name A	Description	Status
		IPSEC Services	Manages I	Started
	Stop the service	LiveUpdate	LiveUpdate	
	Restart the service	Logical Disk Manager	Detects an	Started
		Logical Disk Manage	Configures	
	Description:	Machine Debug Man	Supports lo	Started
	ISAKMP/Oakley (IKE) and the IP security	Messenger	Transmits	
	driver.	MS Software Shado	Manages s	
		Net Logon	Supports p	
		NetMeeting Remote	Enables an	
		Network Connections	Manages o	Started
		Network DDE	Provides n	
		Network DDE DSDM	Manages D	
		Network Location A	Collects an	Started
		Network Provisionin	Manages X	
		Norton AntiVirus Au	Handles No	Started
		68,		

Figure 46: Restarting IPSec Services on XP

On the LAN-Cell, you can observe the status of the tunnel using the **SA Monitor** tab under the **SECURITY->VPN CONFIG** menu (see Figure 47).

	#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
•	1	Remote-XP-Clients	192.168.1.0 / 255.255.255.0	192.168.0.160	Tunnel	ESP DESSHA1

Figure 47: LAN-Cell SA Monitor Screen

You can also observe the VPN tunnel status on the bottom of the Home screen (Figure 48) and use the VPN button to display the SA Monitor window shown in Figure 47.

Interfaces	Status	IP/Netmask	IP Assignment	Renew	Latest Alerts				
WAN	Down	0.0.0.0/ 0.0.0.0	DHCP dient	Renew	Date/Time	Mess	age		
Cellular	Up	166.139.37.167/ 255.255.255.255	IPCP dient	Drop	2008-03-02 17:1	0:04 Rule [succes	Remote-X sfully	(P-Clients] Tunnel	built
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial	2008-03-02 17:10	0:03 Receiv tunnel	e IPSec p exists	acket, but no corr	esponding
E LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A	2008-03-02 17:0	9:19 Cellula	ar connect	ion is up.	
H WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A	2008-03-02 17:0	6:32 Cellula 4:29 WAN c	ar connect onnection	ion is down. is down.	
⊕ DMZ	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A					
					System Status				
					Port Statistics	DHCP Table	VPN	Bandwidth	

Figure 48: LAN-Cell Home Screen

Troubleshooting

Here are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:

#	Time 🔺	Message	Source	Destination	Note
1	2008-03-02 16:48:47	Rule [Remote-XP-Clients] Tunnel built successfully	67.165.53.197	166.139.37.167	IKE
2	2008-03-02 16:48:47	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
3	2008-03-02 16:48:46	Adjust TCP MSS to 1390	166.139.37.167	67.165.53.197	IKE
4	2008-03-02 16:48:46	Recv:[HASH]	67.165.53.197	166.139.37.167	IKE
5	2008-03-02 16:48:46	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166,139.37.167	IKE
6	2008-03-02 16:48:46	Receive IPSec packet, but no corresponding tunnel exists	67.165.53.197	166.139.37.167	IPSEC
7	2008-03-02 16:48:46	Send:[HASH][SA][NONCE][ID][ID]	166.139.37.167	67.165.53.197	IKE
8	2008-03-02 16:48:46	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	166.139.37.167	67.165.53.197	IKE
9	2008-03-02 16:48:46	Swap rule to rule [Remote-XP-Clients]	67.165.53.197	166,139.37.167	IKE
10	2008-03-02 16:48:46	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
11	2008-03-02 16:48:46	Start Phase 2: Quick Mode	67.165.53.197	166.139.37.167	IKE
12	2008-03-02 16:48:46	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
13	2008-03-02 16:48:46	Recv:[HASH][SA][NONCE][ID][ID]	67.165.53.197	166.139.37.167	IKE
14	2008-03-02 16:48:46	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
15	2008-03-02 16:48:45	Phase 1 IKE SA process done	166.139.37.167	67.165.53.197	IKE
16	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	166.139.37.167	67.165.53.197	IKE
17	2008-03-02 16:48:45	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	67.165.53.197	IKE
18	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	166.139.37.167	67.165.53.197	IKE
19	2008-03-02 16:48:45	Recv:[ID][HASH]	67.165.53.197	166.139.37.167	IKE
20	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
21	2008-03-02 16:48:45	Send:[KE][NONCE]	166.139.37.167	67.165.53.197	IKE
22	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	166.139.37.167	67.165.53.197	IKE
23	2008-03-02 16:48:45	Recv:[KE][NONCE]	67.165.53.197	166.139.37.167	IKE
24	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
25	2008-03-02 16:48:45	Send:[SA][VID][VID]	166.139.37.167	67.165.53.197	IKE
26	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	166.139.37.167	67.165.53.197	IKE
27	2008-03-02 16:48:45	Recv:[SA][VID][VID][VID]	67.165.53.197	166.139.37.167	IKE
28	2008-03-02 16:48:45	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE
29	2008-03-02 16:48:45	Recv Main Mode request from [67.165.53.197]	67.165.53.197	166.139.37.167	IKE
30	2008-03-02 16:48:45	Rule [Windows-XP-Clients] Receiving IKE request	67.165.53.197	166.139.37.167	IKE
31	2008-03-02	The cookie pair is : 0x9F1E57418A47093B / 0x4555D3F42DF762D5	67.165.53.197	166.139.37.167	IKE

#	Time 🔺	Message	Source	Destination	Note
1	2008-03-02 16:51:31	Send:[NOTFY:NO_PROP_CHOSEN]	166.139.37.167	67.165.53.197	IKE
2	2008-03-02 16:51:31	The cookie pair is : 0x09FCD66829A3EE5A / 0x45E951667E37C7CC	166.139.37.167	67.165.53.197	IKE
3	2008-03-02 16:51:31	[SA] : No proposal chosen	67.165.53.197	166.139.37.167	IKE
4	2008-03-02 16:51:31	[SA] : Rule [Windows-XP-Clients] Phase 1 authentication algorithm mismatch	67.165.53.197	166.139.37.167	IKE
5	2008-03-02 16:51:31	The cookie pair is : 0x09FCD66829A3EE5A / 0x45E951667E37C7CC	67.165.53.197	166.139.37.167	IKE
6	2008-03-02 16:51:31	Recv:[SA][VID][VID][VID]	67.165.53.197	166.139.37.167	IKE
7	2008-03-02 16:51:31	The cookie pair is : 0x09FCD66829A3EE5A / 0x45E951667E37C7CC	67.165.53.197	166.139.37.167	IKE
8	2008-03-02 16:51:31	Recv Main Mode request from [67.165.53.197]	67.165.53.197	166.139.37.167	IKE
9	2008-03-02	Rule [Windows-XP-Clients] Receiving IKE request	67.165.53.197	166.139.37.167	IKE

Phase 1 Parameter Mismatch

Compare the Phase 1 parameters on both the LAN-Cell VPN Gateway Policy Edit page and Windows XP VPN client's General Key Exchange (Phase 1) page, in particular the Encryption, Authentication and the Key Group. Note: DH1 = DH768 and DH2 = DH1024.

Incorrect ID Type/Content

#	Time 🔺	Message	Source	Destination	Note
1	2008-03-02 16:53:00	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	67.165.53.197	IKE
2	2008-03-02 16:53:00	The cookie pair is : 0x5310560F212AD8E9 / 0x7C9FB78E1F04FE4C	166.139.37.167	67.165.53.197	IKE
3	2008-03-02 16:53:00	[ID] : ID type mismatch. Local / Peer: DNS / IP	67.165.53.197	166.139.37.167	IKE
4	2008-03-02 16:53:00	The cookie pair is : 0x5310560F212AD8E9 / 0x7C9FB78E1F04FE4C	67.165.53.197	166.139.37.167	IKE
5	2008-03-02	[ID] : Rule [Windows-XP-Clients] Phase 1 ID mismatch	67.165.53.197	166.139.37.167	IKE

This error is commonly caused when the Local and Remote ID types and/or Content values are not the same on each device. Remember that the Local and Remote values are relative to each device -- e.g. LAN-Cell Local = Windows XP Remote. Leaving the IP Content field blank on the LAN-Cell will use the current IP addresses of the devices. The Windows XP VPN Client uses the IP Address ID Type by default.

Phase 2 Parameter Mismatch

#	Time 人	Message	Source	Destination	Note
1	2008-03-02 16:56:21	Send:[HASH][DEL]	166.139.37.167	67.165.53.197	IKE
2	2008-03-02 16:56:21	The cookie pair is : 0xA0ABF46943242CDB / 0x3304E47F1627E2D6	166.139.37.167	67.165.53.197	IKE
3	2008-03-02 16:56:21	Send:[HASH][NOTFY:NO_PROP_CHOSEN]	166.139.37.167	67.165.53.197	IKE
4	2008-03-02 16:56:21	The cookie pair is : 0xA0ABF46943242CDB / 0x3304E47F1627E2D6	166.139.37.167	67.165.53.197	IKE
5	2008-03-02 16:56:21	[SA] : No proposal chosen	67.165.53.197	166.139.37.167	IKE
6	2008-03-02 16:56:21	[SA] : Rule [Remote-XP-Clients] phase 2 mismatch	67.165.53.197	166.139.37.167	IKE
7	2008-03-02 16:56:21	The cookie pair is : 0xA0ABF46943242CDB / 0x3304E47F1627E2D6	67.165.53.197	166.139.37.167	IKE
8	2008-03-02 16:56:21	Swap rule to rule [Remote-XP-Clients]	67.165.53.197	166.139.37.167	IKE
9	2008-03-02 16:56:21	The cookie pair is : 0xA0ABF46943242CDB / 0x3304E47F1627E2D6	67.165.53.197	166.139.37.167	IKE
10	2008-03-02 16:56:21	Start Phase 2: Quick Mode	67.165.53.197	166.139.37.167	IKE

Similar to a Phase 1 proposal error, this indicates that the Phase 2 parameters do not match. Check the LAN-Cell's VPN Network Policy page settings against the Windows XP VPN Client's settings for each Filter Action set (Phase 2).

Frequently Asked Questions

Q: Can I have more than 1 Windows XP PC make a VPN connection to the LAN-Cell at the same time?

A: Yes. The configuration shown will permit up to 5 simultaneous XP clients to establish VPN tunnels with the LAN-Cell 2 at the same time (using different IP addresses on the HQ LAN network). You can either create 1 default rule (as in this example) or 5 specific rules, one for each remote XP computer. The LAN-Cell 2 supports 5 simultaneous VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels.

Q: Can I create a VPN tunnel to my LAN-Cell that has a dynamic IP address?

A: The XP VPN Client does not support using a fully qualified domain name (FQDN) as a remote gateway at this time. You must know the current public WAN IP address of the LAN-Cell in order to configure the XP VPN client.

Q: Will the XP VPN tunnel stay up permanently?

A: No. Windows XP will automatically disconnect the VPN tunnel after several minutes of inactivity. Any new packets destined for the LAN-Cell's LAN subnet will automatically cause the tunnel to be rebuilt.

Q: Can the LAN-Cell initiate the VPN tunnel connection?

A: Not with the configuration shown in this example. The LAN-Cell can initiate a VPN tunnel if it knows the address (or FQDN) of the remote gateway you want to connect with (in either site-to-site or client-to-site mode). This example is strictly for remote client initiated VPN tunnels.

Q: Can I force the remote VPN user to enter a username & password?

A: No. The XP VPN client does not support "Extended Authentication (X-AUTH)" at this time.

###

