Using Remote Desktop Software with the LAN-Cell

Technote LCTN0010

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

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 Firewall and NAT 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 LAN-Cell's user interface under the Firewall and NAT sections. See also the LAN-Cell's *User Guide* for more information.

Document Revision History:

Date	Comments
July 11, 2008	First release

Introduction

One common use for the LAN-Cell 2 3G Cellular Router is to provide access to a PC at a remote site. Users at a headquarters location (or on the road) want to be able to take control of a remote PC's screen and keyboard to operate the PC as if they were physically in front of the remote PC.

There are numerous “remote desktop” software packages available. Each one has unique and specific requirements for how it communicates between the Host (HQ) PC and the Remote (target) PC.

This TechNote includes examples configurations for:

1. Microsoft Windows Remote Desktop
2. VNC / RealVNC
3. pcAnywhere

For other packages, please consult with the software manufacturer to determine the necessary ports.

Example Network Topology

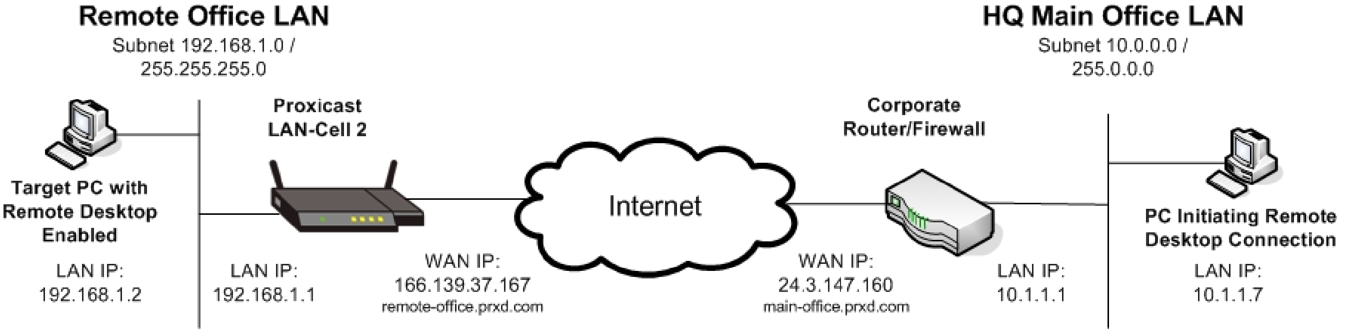


Figure 1: Example Network Topology

Usage Notes

- When configuring and testing remote desktop connections for the first time, it is helpful to have the LAN-Cell and the target PC physically near each other so that you can view the configuration and logs of each device while testing.

- In this example, the remote office LAN-Cell has a static WAN IP address (166.139.37.167). Some remote desktop software packages support fully qualified domain names (FQDN) in addition to IP addresses as the name of the target PC. If your LAN-Cell has a dynamic WAN IP address, you may be able to use a DNS name (e.g. *remote-office.prxd.com*) by setting up a DynDNS account, hostname, and configuring the remote LAN-Cell to update DynDNS with its current WAN IP address. See the *LAN-Cell User's Guide* for additional information on DDNS.

- Some cellular network operators restrict “inbound” traffic from the Internet to remote devices based on IP ports, addresses or your account. Please check with your cellular carrier to ensure that the ports necessary for your remote desktop software are not being blocked by their network. If the carrier is unwilling to open the necessary ports, you must implement a VPN solution to access your remote PC.

- If your HQ PC is behind a firewall, you must ensure that it is configured to pass the necessary IP traffic on the remote desktop software ports in both directions.

Overview

All remote desktop software works by employing a piece of “terminal server” software on the remote target PC and a “terminal emulator” piece of software on the initiating (HQ) PC. The terminal server software “listens” on a specific IP port for commands sent from the terminal emulator and then translates those commands into the equivalent keyboard and mouse inputs on the target PC. The terminal sever software also captures the screen (and sometimes audio) output of the target PC and sends that data back to the terminal emulator over an IP port (sometimes the same port as the commands, sometimes using different ports). The terminal emulator then paints the HQ PC’s screen with the updated image from the remote PC.

In order to configure the LAN-Cell 2 for remote desktop software, you will need the following information:

- Public WAN IP address of the LAN-Cell (or a DDNS hostname)
- Private static LAN IP address of the target PC
- The IP port number(s) and type (TCP/UDP) that your remote desktop software package uses for communications

In the examples below, it is assumed that you have already installed and configured both the terminal server and terminal emulator pieces of software on the respective PCs. Please consult your software application documentation for further information. The examples also assume that the LAN-Cell configuration is at “factory defaults” before starting the remote desktop configuration.

Configuring the LAN-Cell for remote desktop access is straight-forward and involves 3 basic steps:

1. Static LAN IP

You must assign the target PC a fixed IP address so that the LAN-Cell will know where to send remote desktop traffic on its private LAN subnet. You can either manually assign a static IP address to your PC using its operating system tools, or let the LAN-Cell’s DHCP server assign the same address to the PC every time (see Appendix A).

2. Firewall

To protect your remote LAN-attached devices, the LAN-Cell blocks all traffic from the Internet (WAN) to its LAN and WLAN subnets. To enable your remote desktop software to pass through the firewall, you will create a “rule” which defines the specific conditions under which the firewall should allow traffic to your remote PC. If your remote PC is on a DMZ subnet, you can skip the firewall configuration step, as all traffic is permitted to the DMZ.

3. NAT & Port-Forwarding

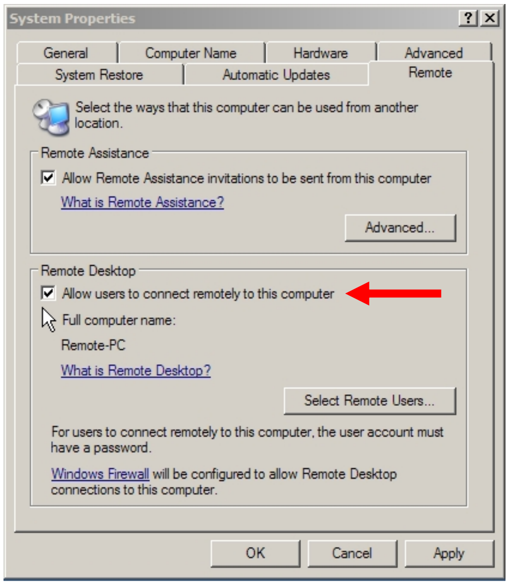
By default, all WAN traffic is terminated in the LAN-Cell and must be forwarded to specific addresses on the LAN. This is because the LAN-Cell performs Network Address Translation, converting the single public WAN IP address into the private subnet addresses of your LAN. You will define specifically where WAN traffic received on a given port will be sent on the LAN subnet.

Microsoft Windows Remote Desktop Example

The Remote Desktop software built into Windows XP, Vista, etc. uses TCP port 3389 (RDP) for both command and response data traffic. This is the only port which must be opened in the firewall and forwarded to the PC.

Step 1:

Ensure that your remote PC has Remote Desktop Connections enabled (Figure 2). This is configured in Control Panel->System->Remote



Select the ways that this computer can be used from another location.

Remote Assistance

☑ Allow Remote Assistance invitations to be sent from this computer

What is Remote Assistance?

Remote Desktop

☑ Allow users to connect remotely to this computer

Full computer name:

Remote-PC

What is Remote Desktop?

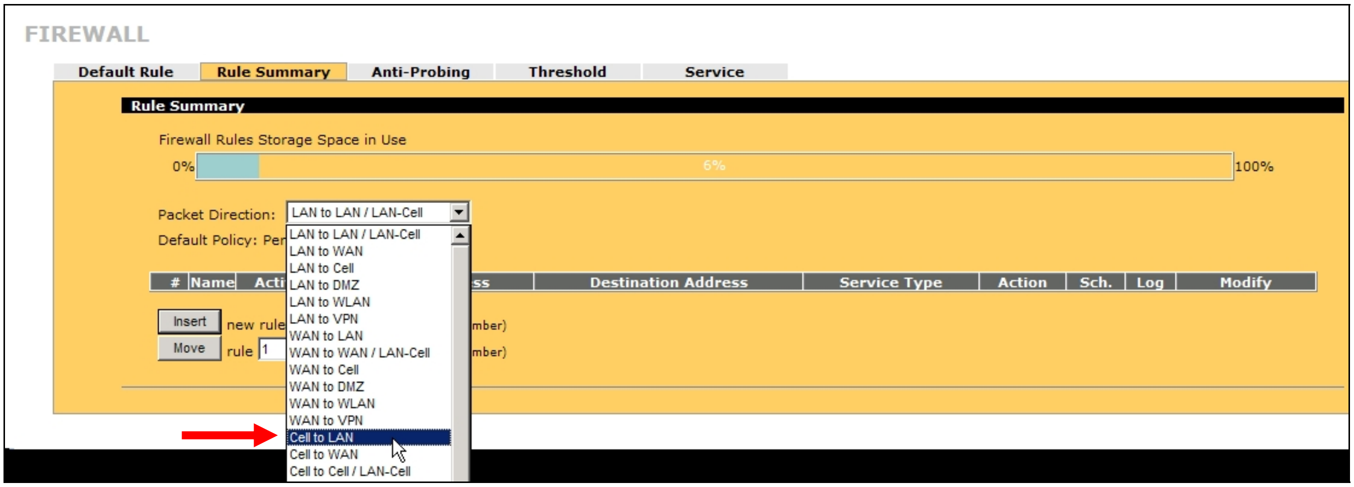
For users to connect remotely to this computer, the user account must have a password.

Windows Firewall will be configured to allow Remote Desktop connections to this computer.

Figure 2: Enabling Remote Desktop Connections in Windows XP

Step 2:

In the LAN-Cell, go to the Firewall Rules Summary screen (SECURITY->FIREWALL) and select the packet direction: **Cell-to-LAN** (Figure 3).



Firewall Rules Storage Space in Use

0% 6% 100%

Packet Direction: LAN to LAN / LAN-Cell

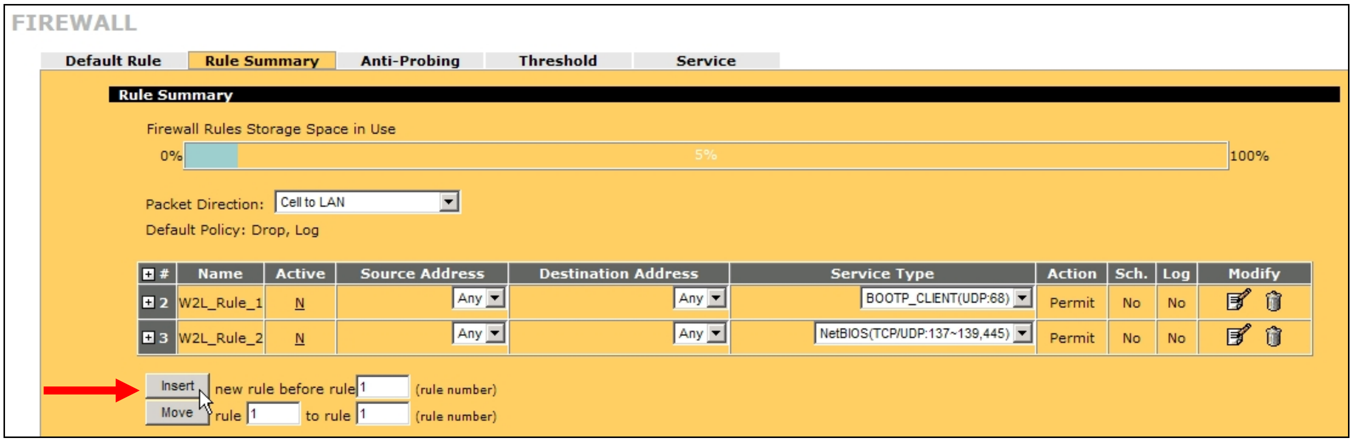
Default Policy: Per

new rule mber)

rule 1 mber)

Figure 3: Firewall Rules Summary Screen

As shown in Figure 4, there are already some example rules for this packet direction, but they are disabled. We will insert a new rule for the RDP traffic. Click on the Insert button to display the Firewall Edit Rule screen.



Rule Summary

Firewall Rules Storage Space in Use

0% 5% 100%

Packet Direction: Cell to LAN

Default Policy: Drop, Log

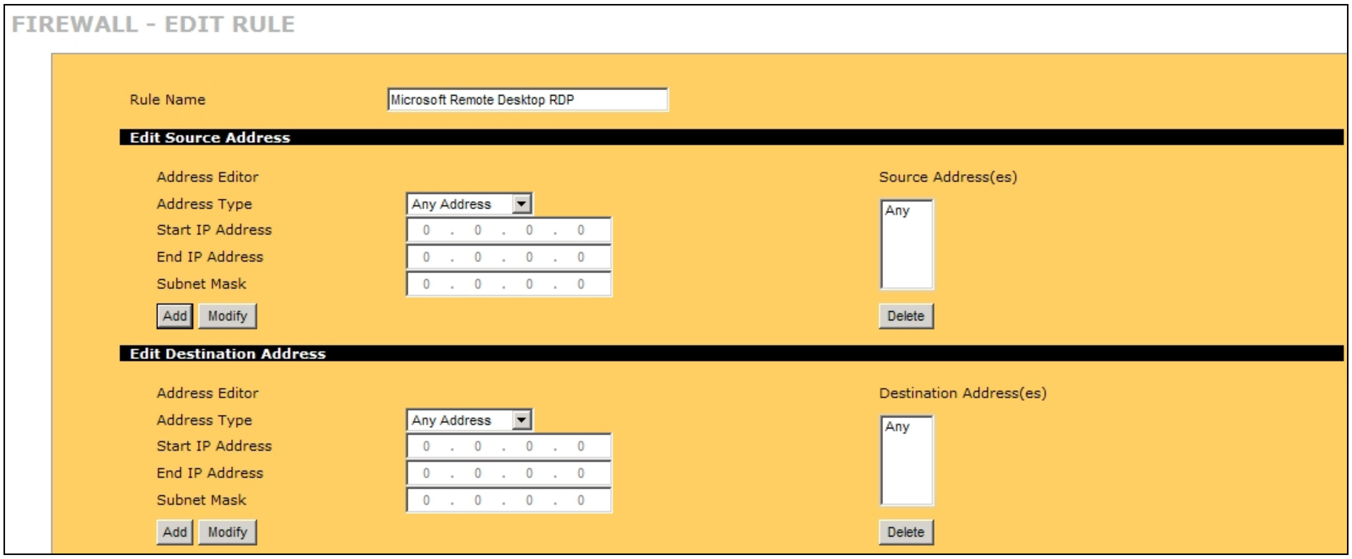
#	Name	Active	Source Address	Destination Address	Service Type	Action	Sch.	Log	Modify
2	W2L_Rule_1	N	Any	Any	BOOTP_CLIENT(UDP:68)	Permit	No	No	
3	W2L_Rule_2	N	Any	Any	NetBIOS(TCP/UDP:137~139,445)	Permit	No	No	

Insert new rule before rule 1 (rule number)

Move rule 1 to rule 1 (rule number)

Figure 4: Cell-to-LAN Firewall Rule Summary Screen

As shown in Figure 5, you must give the Firewall Rule a descriptive Rule Name (up to 31 characters long).



Rule Name: Microsoft Remote Desktop RDP

Edit Source Address

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

Edit Destination Address

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

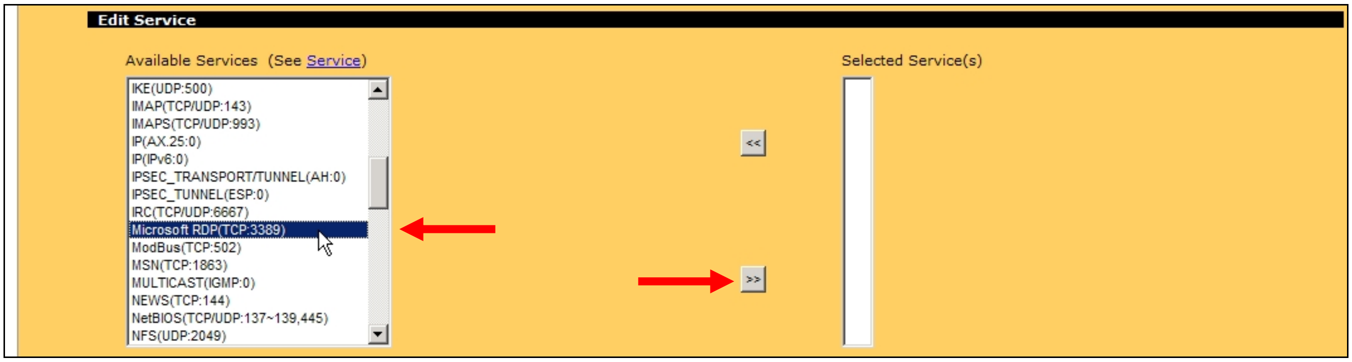
Destination Address(es): Any

Figure 5: Firewall Rule Edit Screen (top)

The Edit Source Address section allows you to specify the source address of a specific device (or subnet) that is permitted to send traffic through the firewall using this rule. This can be used to further secure your remote PC by limiting access to only known IP addresses (such as the WAN IP address of your corporate Internet router). For this example, we will permit any remote IP address send traffic to this rule.

Similar to the Source Address option, the Edit Destination Address section permits you to restrict this Firewall Rule to specific IP addresses on the LAN-Cell's LAN subnet. This can protect your LAN devices from be accessed remotely if another PC on the LAN inadvertently has remote desktop enabled. In our example, we have only 1 PC connected, so we will leave the destination as "Any" to allow traffic to any LAN IP address.

The Selected Services section (Figures 6 & 7) is where we define which IP ports are to be “opened” through the firewall by this rule. Microsoft RDP (TCP 3389) is a predefined service in the LAN-Cell 2, so scroll down to that entry, highlight it and click the right arrow to move RDP into the list of selected services.



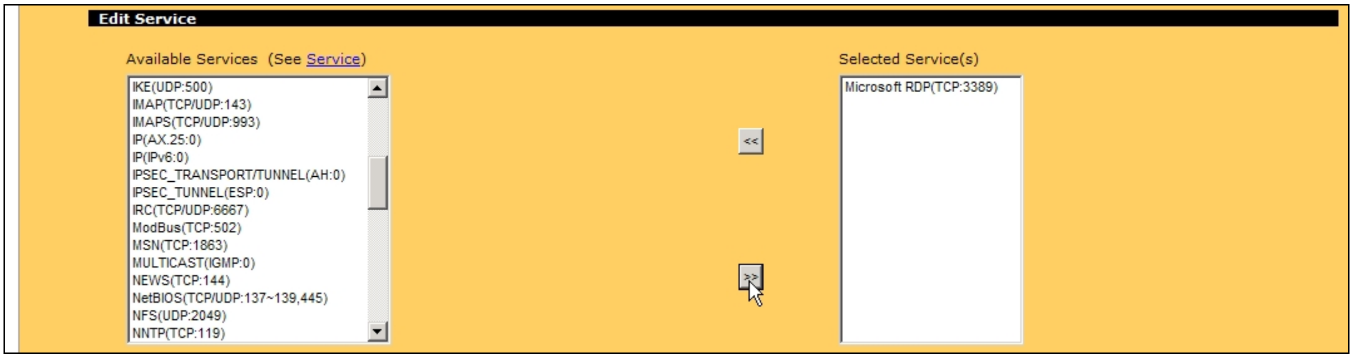
Edit Service

Available Services (See Service)

- IKE(UDP:500)
- IMAP(TCP/UDP:143)
- IMAPS(TCP/UDP:993)
- IP(AX.25:0)
- IP(IPv6:0)
- IPSEC_TRANSPORT/TUNNEL(AH:0)
- IPSEC_TUNNEL(ESP:0)
- IRC(TCP/UDP:6667)
- Microsoft RDP(TCP:3389)
- ModBus(TCP:502)
- MSN(TCP:1863)
- MULTICAST(IGMP:0)
- NEWS(TCP:144)
- NetBIOS(TCP/UDP:137~139,445)
- NFS(UDP:2049)

Selected Service(s)

Figure 6: Firewall Rule Edit Screen (Edit Service)



Edit Service

Available Services (See Service)

- IKE(UDP:500)
- IMAP(TCP/UDP:143)
- IMAPS(TCP/UDP:993)
- IP(AX.25:0)
- IP(IPv6:0)
- IPSEC_TRANSPORT/TUNNEL(AH:0)
- IPSEC_TUNNEL(ESP:0)
- IRC(TCP/UDP:6667)
- ModBus(TCP:502)
- MSN(TCP:1863)
- MULTICAST(IGMP:0)
- NEWS(TCP:144)
- NetBIOS(TCP/UDP:137~139,445)
- NFS(UDP:2049)
- NNTP(TCP:119)

Selected Service(s)

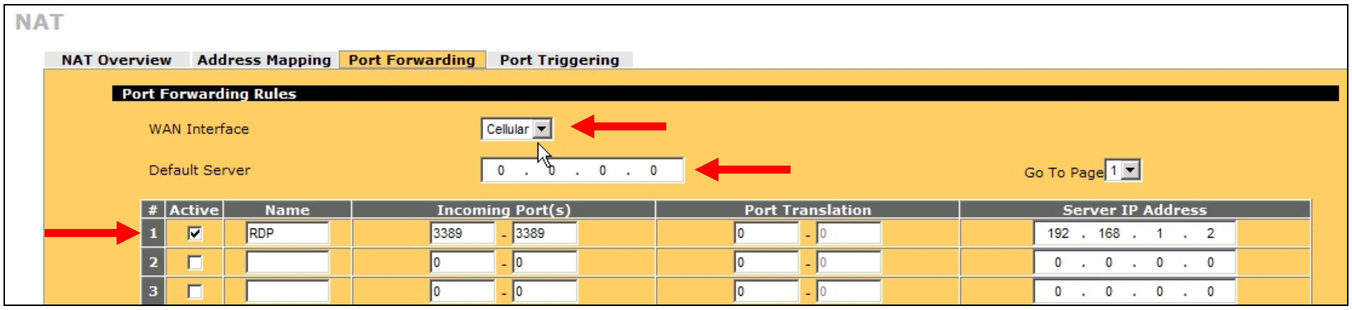
- Microsoft RDP(TCP:3389)

Figure 7: Firewall Rule Edit Screen (RDP TCP/3389 Selected)

The remaining sections of the Firewall Edit Rule screen define when this rule should apply (default is always) and what to do with an incoming packet that matches the rule (permit it to pass to the LAN). These settings are appropriate for our application, so click the Apply button to define the new Firewall Rule.

Step 3:

Now go to the NAT Port Forwarding Rules screen (ADVANCED->NAT) as shown in Figure 8.



NAT

Port Forwarding Rules

WAN Interface: Cellular

Default Server: 0 . 0 . 0 . 0

Go To Page 1

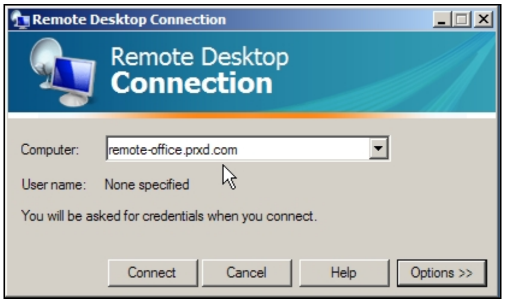
#	Active	Name	Incoming Port(s)		Port Translation		Server IP Address
1	☑	RDP	3389	3389	0	0	192 . 168 . 1 . 2
2	□		0	0	0	0	0 . 0 . 0 . 0
3	□		0	0	0	0	0 . 0 . 0 . 0

Figure 8: NAT Port Forwarding Rules Screen

Ensure that the WAN Interface selected is “Cellular” (or “WAN” if your LAN-Cell has a wired WAN or serial modem connection) and that the Default Server address is 0.0.0.0.

Create a new Port Forwarding Rule by marking the first line as Active and giving it a descriptive Name. For Microsoft Remote Desktop, you need to forward Incoming Port 3389 to the remote PC (“server”) which has a static LAN IP address of 192.168.1.2. You do not need to do Port-Translation in this example. Click Apply to save this rule.

Configuration of the LAN-Cell is now complete. Use the Microsoft Remote Desktop software on your HQ PC to initiate a connection to the remote PC using either its WAN IP address or FQDN (if defined). See Figure 9.



Remote Desktop Connection

Computer: remote-office.prxd.com

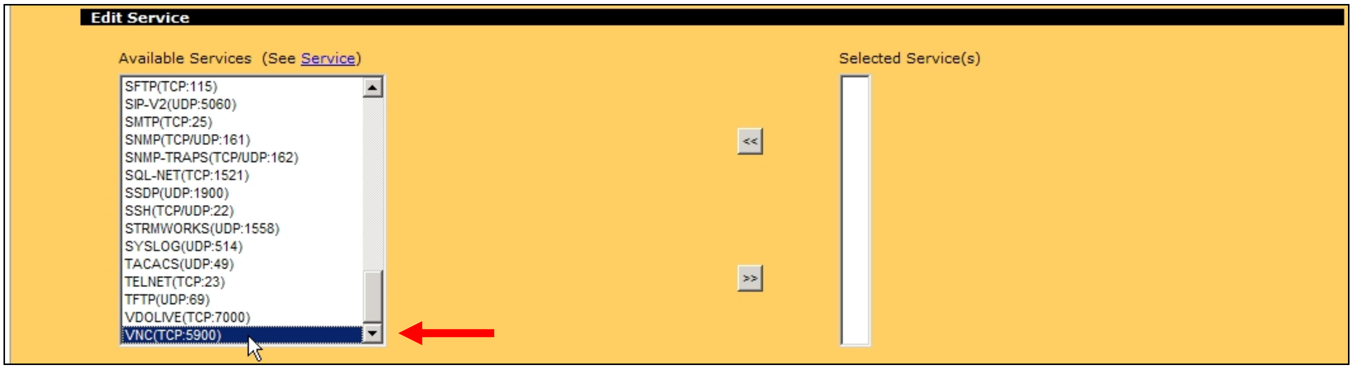
User name: None specified

You will be asked for credentials when you connect.

Figure 9: Initiating a Remote Desktop Connection

VNC Example

Configuring VNC / RealVNC is the same as configuring Microsoft Windows Remote Desktop, except that VNC uses TCP port 5900 instead of 3389. Follow the Microsoft RDP example but substitute the VNC port number in the Firewall Rule and NAT Port Forwarding Rule screens. See Figures 10 & 11.



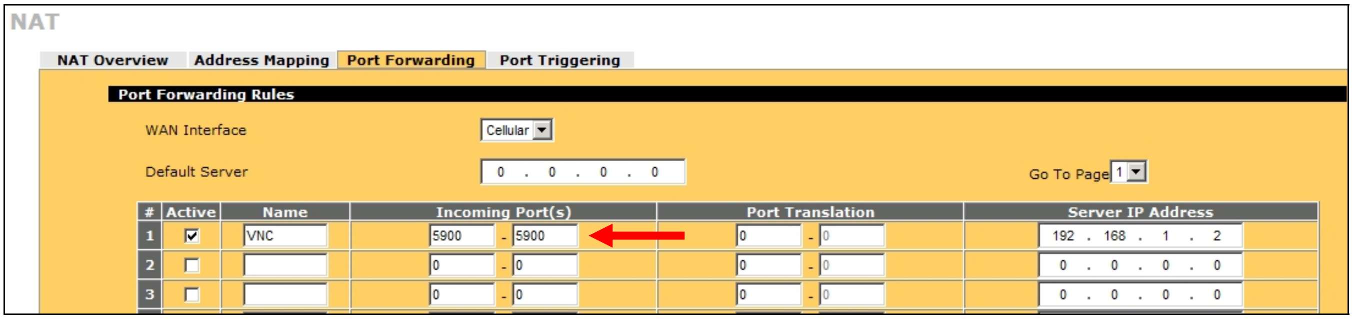
Edit Service

Available Services (See Service)

- SFTP(TCP:115)
- SIP-V2(UDP:5060)
- SMTP(TCP:25)
- SNMP(TCP/UDP:161)
- SNMP-TRAPS(TCP/UDP:162)
- SQL-NET(TCP:1521)
- SSDP(UDP:1900)
- SSH(TCP/UDP:22)
- STRMWORKS(UDP:1558)
- SYSLOG(UDP:514)
- TACACS(UDP:49)
- TELNET(TCP:23)
- TFTP(UDP:69)
- VDOLIVE(TCP:7000)
- VNC(TCP:5900)

Selected Service(s)

Figure 10: VNC Firewall Rule



NAT

Port Forwarding Rules

WAN Interface: Cellular

Default Server: 0 . 0 . 0 . 0

Go To Page 1

#	Active	Name	Incoming Port(s)		Port Translation		Server IP Address
1	☑	VNC	5900	5900	0	0	192 . 168 . 1 . 2
2	□		0	0	0	0	0 . 0 . 0 . 0
3	□		0	0	0	0	0 . 0 . 0 . 0

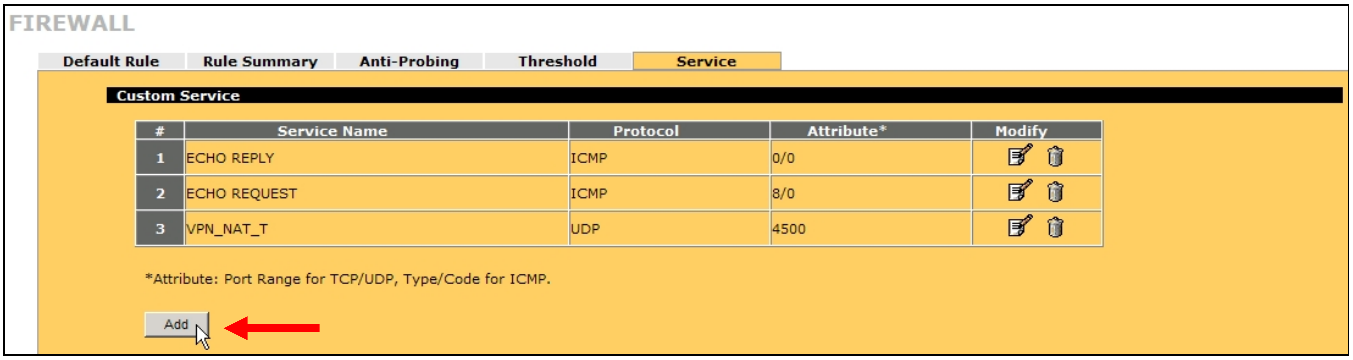
Figure 11: VNC Port Forwarding

pcAnywhere Example

pcAnywhere is similar to the other remote desktop applications, except that it uses 2 ports: a TCP port for data and a UDP port for status messaging. Recent versions of pcAnywhere use TCP/5631 and UDP/5632. Older versions use other ports (see Figure 16 below).

The pcAnywhere ports are not predefined services on the LAN-Cell, so you will have to define these ports before creating the Firewall Rule.

Go to SECURITY->FIREWALL->SERVICE and add a new service for each pcAnywhere port (Figures 12-14).



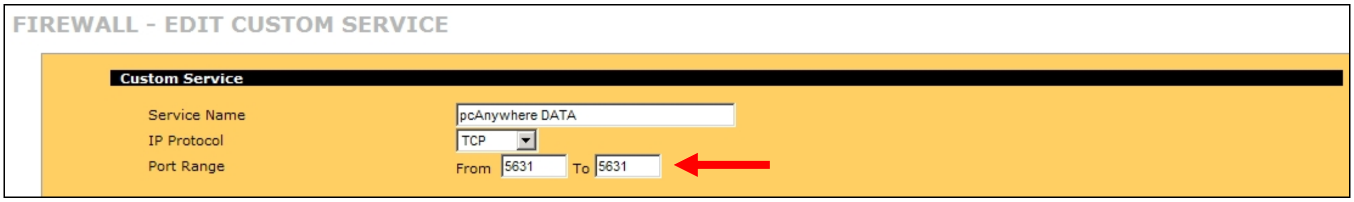
FIREWALL

Custom Service

#	Service Name	Protocol	Attribute*	Modify
1	ECHO REPLY	ICMP	0/0	✎ 🗑
2	ECHO REQUEST	ICMP	8/0	✎ 🗑
3	VPN_NAT_T	UDP	4500	✎ 🗑

*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Figure 12: Adding a Custom Service

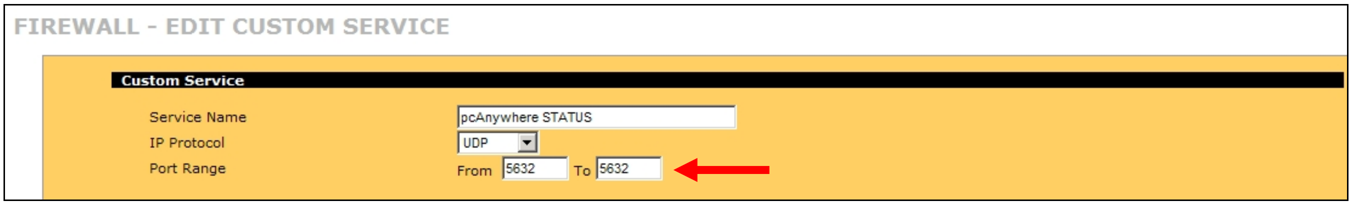


FIREWALL - EDIT CUSTOM SERVICE

Custom Service

Service Name	pcAnywhere DATA
IP Protocol	TCP
Port Range	From 5631 To 5631

Figure 12: pcAnywhere Data Port



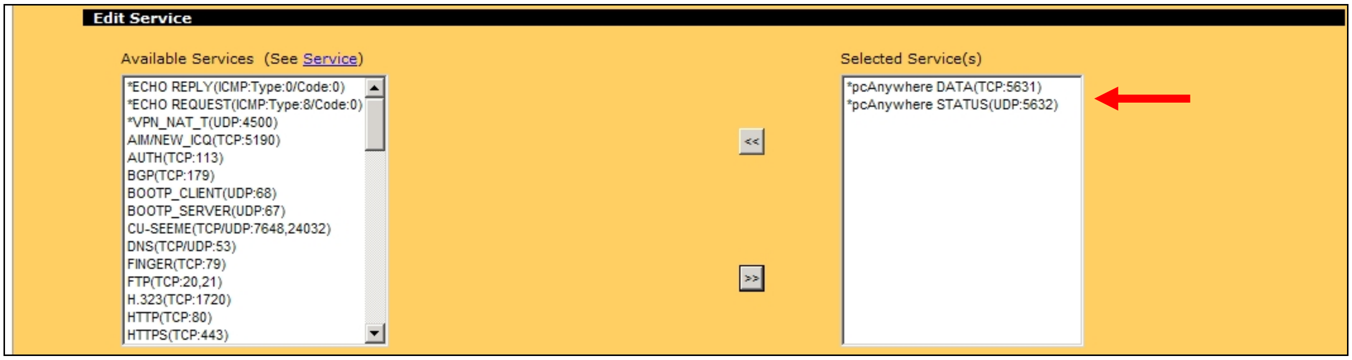
FIREWALL - EDIT CUSTOM SERVICE

Custom Service

Service Name	pcAnywhere STATUS
IP Protocol	UDP
Port Range	From 5632 To 5632

Figure 13: pcAnywhere Status Port

When defining the Cell-to-LAN Firewall Rule, include both new pcAnywhere service ports in the Selected Services list (Figure 14).



Available Services (See Service)

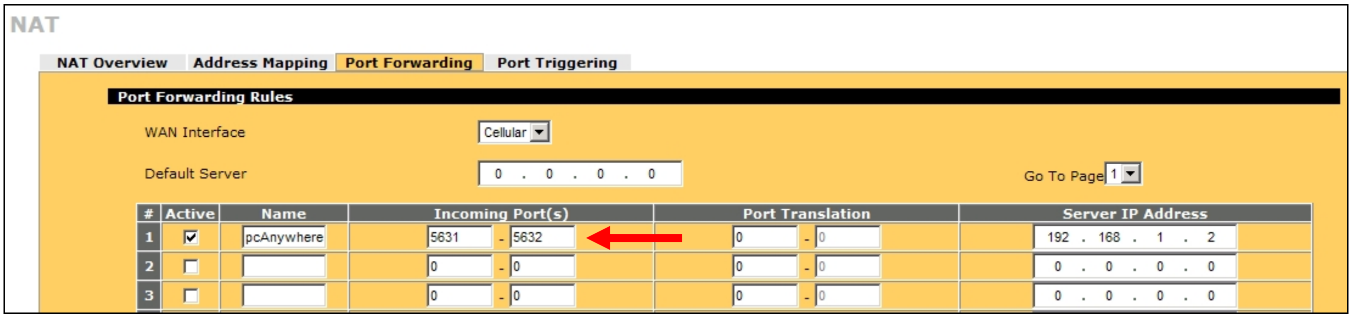
- *ECHO REPLY(ICMP:Type:0/Code:0)
- *ECHO REQUEST(ICMP:Type:8/Code:0)
- *VPN_NAT_T(UDP:4500)
- AIM/NEW_ICQ(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)
- BOOTP_SERVER(UDP:67)
- CU-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)
- FTP(TCP:20,21)
- H.323(TCP:1720)
- HTTP(TCP:80)
- HTTPS(TCP:443)

Selected Service(s)

- *pcAnywhere DATA(TCP:5631)
- *pcAnywhere STATUS(UDP:5632)

Figure 14: pcAnywhere Firewall Rule

For the NAT Port Forwarding Rule, include both incoming ports 5631 and 5632 as shown in Figure 15 (both TCP and UDP packets are forwarded).



WAN Interface: Cellular

Default Server: 0 . 0 . 0 . 0

Go To Page 1

#	Active	Name	Incoming Port(s)		Port Translation		Server IP Address
1	☑	pcAnywhere	5631	5632	0	0	192 . 168 . 1 . 2
2	□		0	0	0	0	0 . 0 . 0 . 0
3	□		0	0	0	0	0 . 0 . 0 . 0

Figure 15: pcAnywhere NAT Port Forwarding Rule

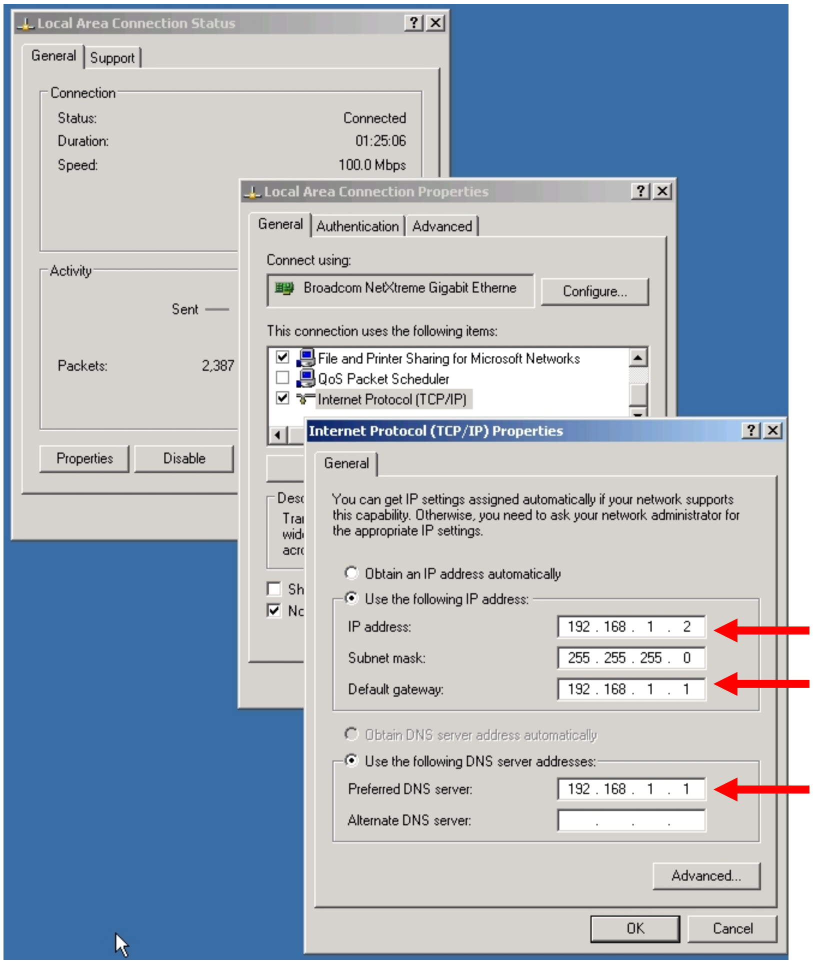
pcAnywhere version	TCP (data) port number	UDP (status) port number
2.0	65301	22
7.0	65301	22
7.50, 7.51	65301	22
CE	65301	22
7.52	5631	5632
8.x, 9.0	5631	5632
9.2	5631	5632
10.0, 10.5, 11.0, 11.5, 12.0	5631	5632

Figure 16: pcAnywhere Port Usage

Appendix A: Static IP Addressing For LAN Devices

Your remote PC must have a static (fixed) IP address so that the NAT Port Forwarding rules can send data to the correct device. You can either configure your PC with a static IP address or let the LAN-Cell's DHCP server assign the same address to the PC every time it connects.

In Windows XP, you can assign a static IP address using Control Panel -> Network Connections -> Local Area Connection and setting the properties of the TCP/IP protocol to be a fixed IP address. Do not select a static IP address that falls within the LAN-Cell's DHCP server range (.33 to .161 by default). Set the Default Gateway and Primary DNS values to the LAN IP address of the LAN-Cell (Figure A-1).



Local Area Connection Status

General | Support

Connection

Status: Connected

Duration: 01:25:06

Speed: 100.0 Mbps

Activity

Sent —

Packets: 2,387

Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Broadcom NetXtreme Gigabit Etherne

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks

☐ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

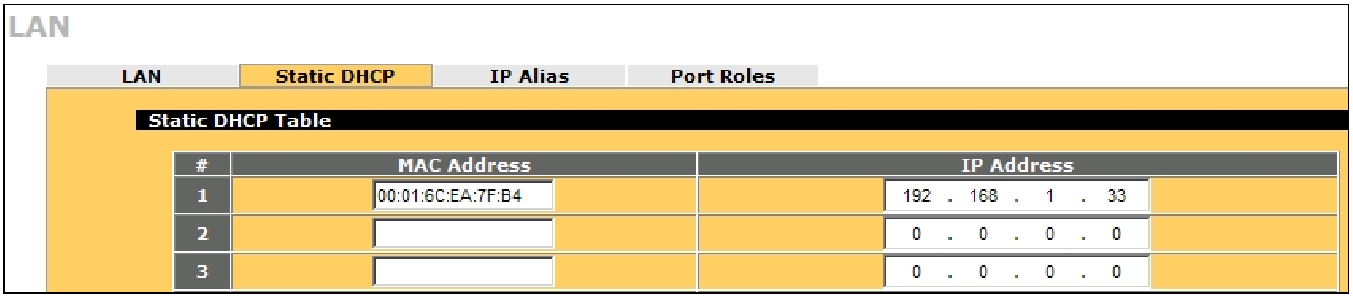
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

Figure A-1: Static IP Addressing in Windows XP

Alternatively, you can use the "static DHCP" feature (also known as DHCP reservation) in the LAN-Cell's DHCP server to assign the same IP addressing parameters to a given MAC address every time that MAC address must renew its DHCP lease. Go the NETWORK->LAN-STATIC_DHCP (Figure A-2).



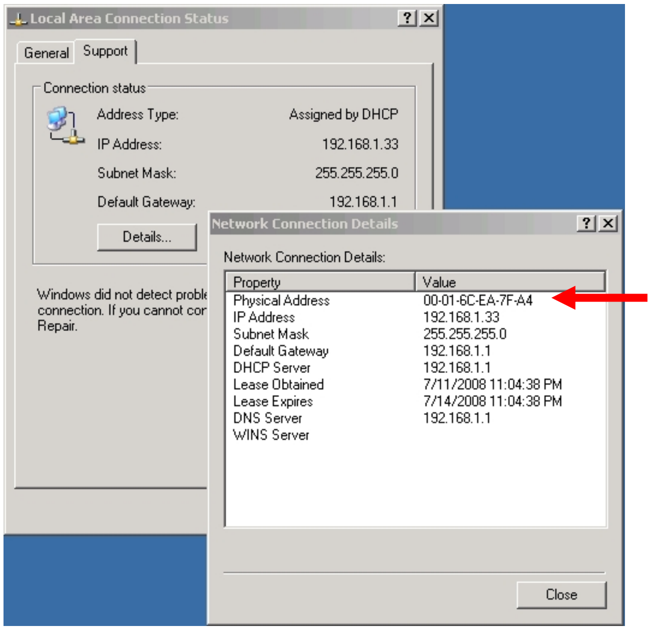
Static DHCP Table

#	MAC Address	IP Address
1	00:01:6C:EA:7F:B4	192 . 168 . 1 . 33
2		0 . 0 . 0 . 0
3		0 . 0 . 0 . 0

Figure A-2: Static DHCP Addressing in the LAN-Cell

Enter the remote PC's Ethernet MAC address in the format 11:22:33:44:55:66. Enter the desired "static" IP address for this PC. The selected IP address to be assigned must be within the defined DHCP pool range.

You can obtain the Ethernet card's MAC address in Windows XP by examining the properties of your LAN connection (Figure A-3). The MAC address is also called the Physical Address.



Connection status

Address Type:	Assigned by DHCP
IP Address:	192.168.1.33
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

Windows did not detect probl
connection. If you cannot cor
Repair.

Network Connection Details:

Property	Value
Physical Address	00-01-6C-EA-7F-A4
IP Address	192.168.1.33
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	192.168.1.1
Lease Obtained	7/11/2008 11:04:38 PM
Lease Expires	7/14/2008 11:04:38 PM
DNS Server	192.168.1.1
WINS Server	

Figure A-3: Obtaining the MAC Address in Windows XP

Now, every time the remote PC is assigned an IP address by the LAN-Cell's DHCP server, it will receive the address you defined. If you change the Ethernet card in your remote PC (or switch to a different PC) you must update the Static DHCP table with the new MAC address.

Appendix B: Troubleshooting

The most common difficulties encountered when setting up remote desktop access via the LAN-Cell involve:

1. *Not being aware of all of the ports used by your remote desktop application*
   Please consult your documentation or contact the software manufacturer.

2. *Carrier blocking the ports necessary*
   Consult with your cellular operator on what features are necessary on your account to allow inbound access to the necessary ports. For example, AT&T requires a feature called “mobile terminated data service” on your account and the use of either the “internet” APN or a custom APN for your company (the APN “isp.cingular” blocks inbound connections and cannot be used to host remote servers). Alltel requires you to define the necessary ports and rules in their firewall. Verizon Wireless has no inbound restrictions. Sprint blocks some ports including port 80 but common remote desktop ports are open.

   If you are unable to have the necessary ports opened and cannot move your application ports or use Port Translation, please refer to the Proxicast Support web site for more information on configuring the LAN-Cell for VPN access.

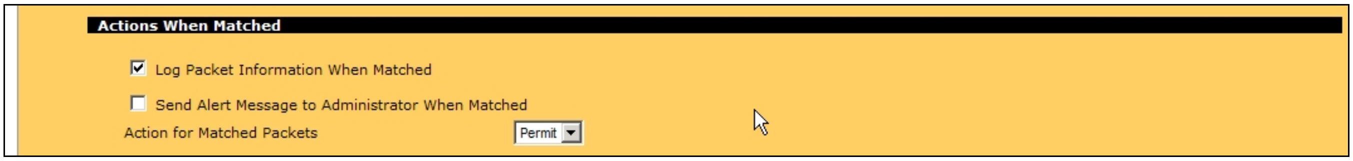
3. *Incorrect firewall rules*
   Double check the packet direction and allowed services. You can also temporarily disable the firewall if you feel that a configuration error in the rules is causing the problem.

4. *Incorrect port forwarding*
   Double check the port range defined as well as the destination server IP address. Do not define a “default server” IP address. Do not map the same ports to more than one server IP address unless you are using Port Translation with different incoming (public) ports.

5. *Incorrect IP addressing on the remote PC*
   Ensure that the remote PC has the LAN-Cell’s LAN IP address as its default gateway and that the subnetting is correct.

6. *Corporate or PC-level firewalls blocking the necessary ports*
   Disable any software firewalls on the remote or HQ PCs. Ask your firewall administrator to open the necessary ports in your corporate firewall to allow the remote desktop software to communicate.

The LAN-Cell has extensive error logging features that you can use to help troubleshoot connectivity issues. On the remote desktop Firewall Rule, check the Log option (Figure B-1) to have all matched packets written to the LAN-Cell’s log (dropped packets are already automatically logged). After attempting a connection, check the log for a record of the attempt. If packets are reaching the LAN-Cell, they will be recorded (Figure B-2). If no log entries are recorded, then packets are being blocked by the carrier, corporate firewall or your HQ PC’s firewall.



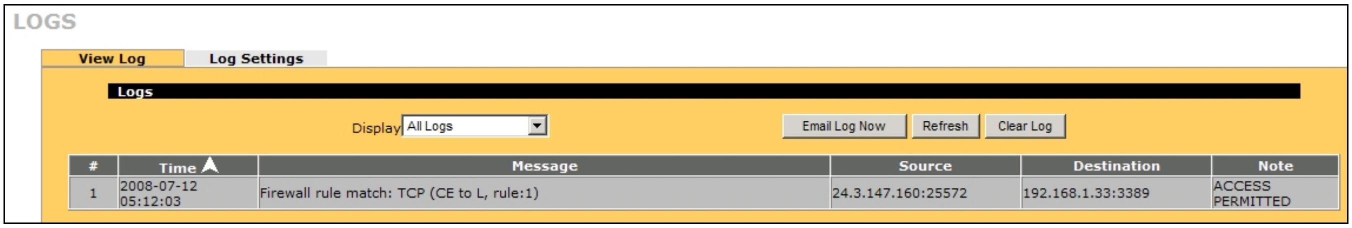
Actions When Matched

☑ Log Packet Information When Matched

□ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

Figure B-1: Logging Match Firewall Rules



Logs

Display: All Logs

#	Time	Message	Source	Destination	Note
1	2008-07-12 05:12:03	Firewall rule match: TCP (CE to L, rule:1)	24.3.147.160:25572	192.168.1.33:3389	ACCESS PERMITTED

Figure B-2: Match Firewall Rule Log Entry

Appendix C: Frequently Asked Questions

Q: Can I access more than 1 remote PC attached to the LAN-Cell?

A: Yes. Configure the first PC as described in this TechNote. For other PC's either change the port(s) used by the remote desktop software or use Port Translation to map different "public" port(s) to the necessary private port(s). You will also need to define a Firewall Rule for the new port(s). To access the secondary PC, you must append a colon and the port number to your remote desktop connection request, e.g. 166.139.37.167:3390

Q: What are my options if the cellular carrier is blocking the ports I need?

A: Check to see if they allow inbound traffic on any port. If so, change the remote desktop software to use this port, or use Port Translation to map the public port to the necessary private port. You will also need to define a Firewall Rule for the new port(s). If no ports are available, then you must implement a VPN connection to the LAN-Cell. See the Proxicast Support web site for examples of configuring site-to-site and client-to-site VPNs.

Q: How is the configuration different if I'm using both the wired WAN and 3G Cellular WAN interfaces (e.g. fail-over/backup)?

A: Follow the examples in this TechNote for the setting up access via the Cellular interface. Create the same Firewall Rule(s) for the **WAN-to-LAN** packet direction. On the NAT Overview screen, use the **Copy to WAN** button to copy the Port-Forwarding/Translation rules from the Cellular interface to the WAN interface.

Q: Do I need to configure the Firewall and NAT/Port-Forwarding if I'm using a VPN?

A: No. A properly configured IPSec VPN tunnel will make the LAN-Cell's LAN attached devices appear as if they are part of the HQ network. You can access the remote desktop PC just as if it were on the same network.

Q: What if my remote PC is connected to the LAN-Cell via Wi-Fi?

A: The configuration is the same as shown in these examples if the WLAN (Wi-Fi) access point is bridged to the LAN-Cell's LAN subnet. If you've implemented a separate WLAN subnet, create the necessary Firewall Rules in the Cell-to-WLAN direction.

Q: What if my remote PC is connected to the LAN-Cell's DMZ subnet?

A: The Firewall Rules are unnecessary in this case since the DMZ permits all inbound traffic by design. Set up port-forwarding and use the remote PC's DMZ IP address as the server for the necessary port(s).

Q: What if my remote desktop software uses ports TCP/20, TCP/21, TCP/22, TCP/23, UDP/53, TCP/80, UDP/161, TCP/443, or UDP/500?

A: By default, these ports are used by the LAN-Cell's management features. You can either change your remote desktop software to use a different port, or change the LAN-Cell's management utilities to use a different port. See ADVANCED->REMOTE_MGMT to change or disable the ports that the LAN-Cell uses. Remember to append the new port numbers to all future LAN-Cell device management requests.

# # #