Accessing Remote Devices via the LAN-Cell 2

Technote LCTN0017

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

This TechNote applies to LAN-Cell models:

LAN-Cell 2:

LC2-411 (firmware 4.02 or later)

Document Revision History:

Date	Comments
May 11,2012	Revised title
May 18, 2010	Added port translation comments
September 29, 2009	Initial Release

Introduction

One of the most common applications for the LAN-Cell 2 is to provide users anywhere on the Internet with access to one or more devices at a remote location. Devices such as IP Cameras, Networked Digital Video Recorders (NVR/DVR), Programmable Logic Controllers (PLC), Remote Telemetry Units (RTU), SCADA equipment, data loggers, and other IP-enabled devices can be easily accessed remotely via the LAN-Cell.

This TechNote provides an overview of how to configure the LAN-Cell and/or your equipment for direct remote access. An example using a DVR is presented for illustration purposes. The process is similar for all other types of equipment. An alternative approach is to create a Virtual Private Network (VPN) between a PC or a router at your main location and the remote LAN-Cell. The VPN approach is covered in the *LAN-Cell 2 Users Guide* and several VPN-related TechNotes.

Proxicast has also prepared a TechNote specifically for using PC remote-control software such as VNC, PC-Anywhere and Windows Remote Desktop with the LAN-Cell. Please see *LCTN0010: Using Remote Desktop Software with the LAN-Cell* for tips on configuring the LAN-Cell for these specific software packages.

Background

The procedure for establishing remote access to devices connected to the LAN-Cell is straightforward and can be broken down into these five steps:

1. Attach the equipment to the LAN-Cell's LAN subnet
2. Locate the LAN-Cell on the Internet
3. Determine the IP ports required for communication
4. Create firewall rules to allow the necessary traffic
5. Forward incoming traffic from the Internet to the equipment

We will configure the LAN-Cell 2 to permit access to a Digital Video Recorder (Figure 1) throughout this TechNote as an illustration of the LAN-Cell parameters that must be set to enable remote access.

Before attempting to configure the LAN-Cell, you should ensure that you have gathered all of the necessary configuration information (see Table 1). It is easiest to test remote access if you configure the LAN-Cell and your equipment before installing them in a remote location.

Table 1: Remote Access Parameters

Item	TechNote Example Values	Your System
LAN-Cell LAN IP	IP: 192.168.1.1 Subnet Mask: 255.255.255.0	IP: Subnet Mask:
DVR IP Settings	IP: 192.168.1.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1	IP: Subnet Mask: Default Gateway:
DVR Application Ports	TCP-3000 TCP-3001 TCP-8800	
ISP / APN	AT&T / "internet"	
LAN-Cell Public IP Dynamic DNS Name	166.139.37.167 (static) remote-office.prxd.com	

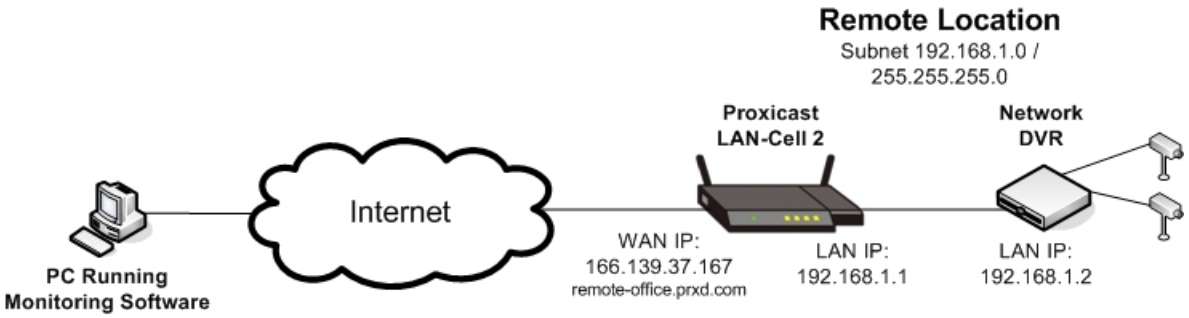

Figure 1: Remote Access to DVR Example

Prerequisites:

- The LAN-Cell is already configured for Internet access via its WAN and/or 3G Cellular modem.
- Devices attached to the LAN segment of the LAN-Cell are able to access the Internet (e.g. open a web page on a PC, etc) via the LAN-Cell.
- If there are any intervening firewalls between the monitor PC and the LAN-Cell, ensure that these firewalls permit the necessary IP ports (see Step 3).

1. Attach the equipment to the LAN-Cell's LAN subnet

Use the DVR's management software to set its IP address information. The DVR should be assigned a "static" IP address that is part of the LAN-Cell's LAN subnet[1]. The LAN-Cell's LAN IP address must be the DVR's Default Gateway. If this value is not set in the DVR, it will not be able to properly reply to remote access requests. In our example, the DVR IP settings would be:

DVR IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

After configuring the DVR's IP settings, attach the DVR to one of the 4 Ethernet LAN ports on the LAN-Cell.

2. Locate the LAN-Cell on the Internet

Static IP

If your LAN-Cell has been assigned a "static" IP address by your ISP (cellular carrier[2]), note this value. You will use this IP address to access the remote LAN-Cell and attached equipment. In our example, the LAN-Cell has a static IP address of 166.139.37.167.

Dynamic IP / DDNS

If you do not have a "static" IP address (or prefer to access your device by name rather than number) you must set up a Dynamic DNS (DDNS) account and configure the LAN-Cell to update your DDNS provider with its current

[1] You can optionally use the DHCP reservation technique to assign a specific IP address to the DVR's MAC address via DHCP. See the LAN-Cell menu NETWORK > LAN > STATIC DHCP

[2] Cellular carriers do not implement true "static IP" addresses. Instead, they use "Mobile IP" technology that is similar in function to the LAN-Cell's "static DHCP" feature where the same IP address is always assigned to the same device, but the device must make a dynamic IP address request. Configure the LAN-Cell's Cellular interface as "Get Automatically from ISP" not "static".

WAN and/or CELL IP address every time the IP address changes. In our example, we have defined the DNS name of *remote-office.prxd.com* to map to the LAN-Cell's current CELL IP address.

See *TechNote LCTN0016: Configuring Dynamic DNS* for more information and examples of setting up DDNS.

3. Determine the IP ports required for communication

Every TCP/IP-based application uses one or more numbered "ports" to communicate between devices. Each IP address has only a single instance of each port number. Many common network applications have "well-defined" port numbers assigned by convention and agreement via the Internet Assigned Numbers Authority (IANA).

Check with your equipment manufacturer and documentation for the list of port numbers required by your application software. Many applications require multiple ports or ranges of ports. The DVR and monitoring software in our example are using TCP ports 3000-3001 and 8800.

The LAN-Cell's internal remote management applications use several well-defined ports to support web (HTTP/HTTPS), terminal (Telnet/SSH) and other applications. If your equipment and software require **ANY** of the ports shown in Table 2, please refer to *TechNote LCTN0015: Changing the LAN-Cell 2's Remote Management Ports* for instructions on how to configure the LAN-Cell to avoid conflicts.

Table 2: LAN-Cell Default Remote Management Ports

Default LAN-Cell Service Port #	Application
20 & 21 – TCP	FTP
22 – TCP	SSH
23 – TCP	TELNET
53 – UDP	DNS (note: port # cannot be changed)
80 – TCP	HTTP
161 – UDP	SNMP
443 – TCP	HTTPS
500 – UDP	IKE (VPN)

Note on Embedded Web Servers:

Many devices now have embedded web servers that enable easy configuration of the equipment with no external software. Most of these web servers default to TCP port 80 which the LAN-Cell also uses for its web configuration interface. You must change either the web server port number on your equipment or the LAN-Cell in order for both to work.

Note on Cellular Carriers & ISP's:

Your ability to access specific port numbers depends on the service you have with your ISP (cellular carrier) and any network restrictions they have in place. Contact your ISP with the list of required application port numbers to ensure that you have the proper type of service that permits "inbound" access to these ports.

As of the time of this writing, the major U.S. cellular carriers have the following policies in effect:

Table 3: U.S. Cellular Carrier Port Restrictions

Carrier	Port Restrictions
Verizon Wireless	All ports open
AT&T isp.cingular internet & I2GOLD	Depends on APN used: All ports blocked All ports open[3]
Sprint	Most ports open. Port 80 blocked.
T-Mobile	All ports blocked Contact third-party M2M service providers for alternate APNs

4. Create firewall rules to allow the necessary traffic

Once you have gathered all of the necessary information, you must configure the LAN-Cell to permit "inbound" traffic to flow from the Internet to the LAN through the firewall on your designated ports. Begin by defining the list of required port numbers as new Custom Services (unless the ports are already on the Predefined Services list).

Define Custom Services

Go to SECURITY > FIREWALL > SERVICES (Figure 2).

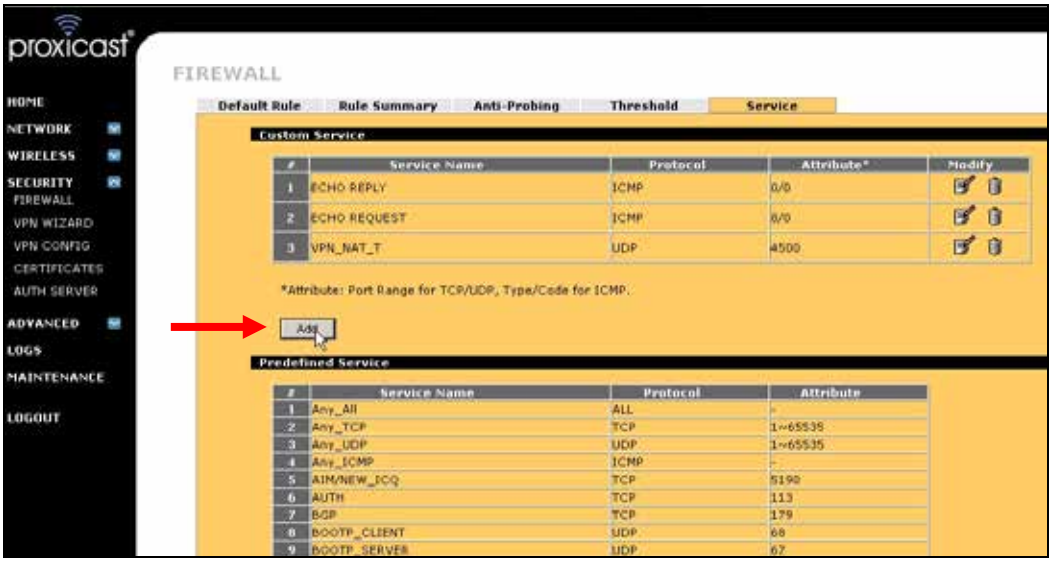

Figure 2: Firewall Service List

[3] Access to these APN's requires the *Mobile Terminated Data Service* feature on your AT&T account. Contact your AT&T representative about this service and access to "open" APN's.

This screen shows both the Predefined and Custom TCP/IP services that can be applied to the LAN-Cell firewall rules. To add a new Custom service, click the Add button.

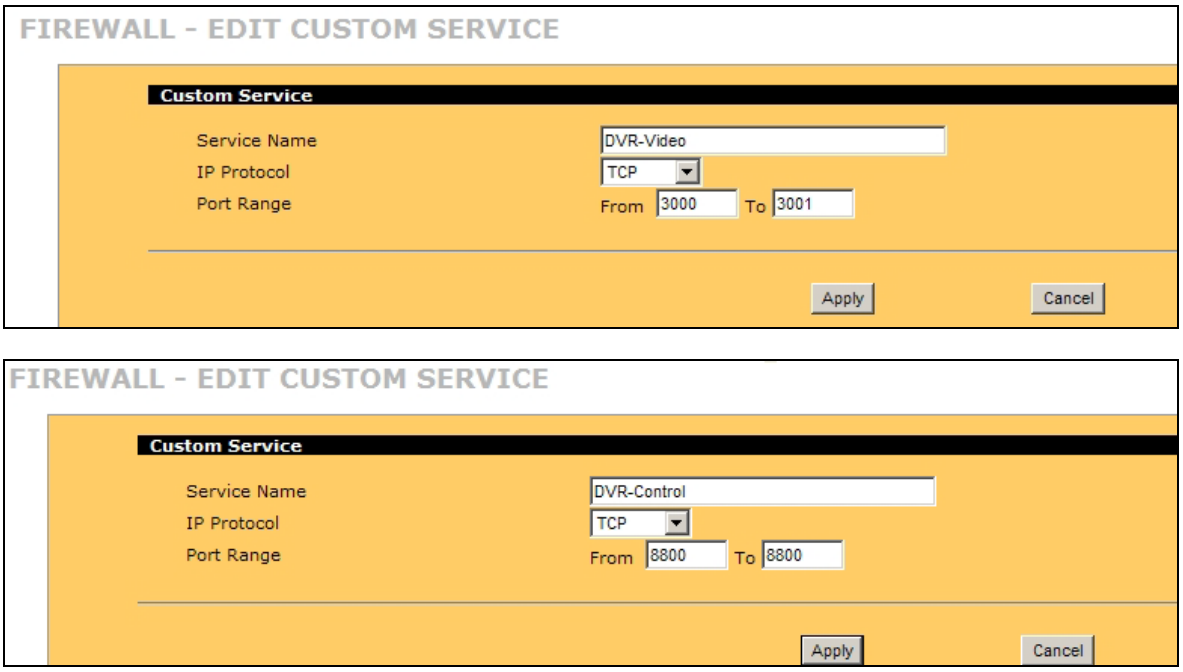

Figure 3: Adding Custom Service Ports

You may assign any meaningful Name to the new service. Select the desired IP Protocol(s) and the Range of Ports used by this service. If only 1 port is used, enter the same port number for the "From" and "To" fields. In our example, two new services are required: "DVR-Video" on TCP ports 3000-3001 and "DVR-Control" on TCP port 8800 (Figure 3).

The newly added services will appear at the top of the Custom Service list (Figure 4).

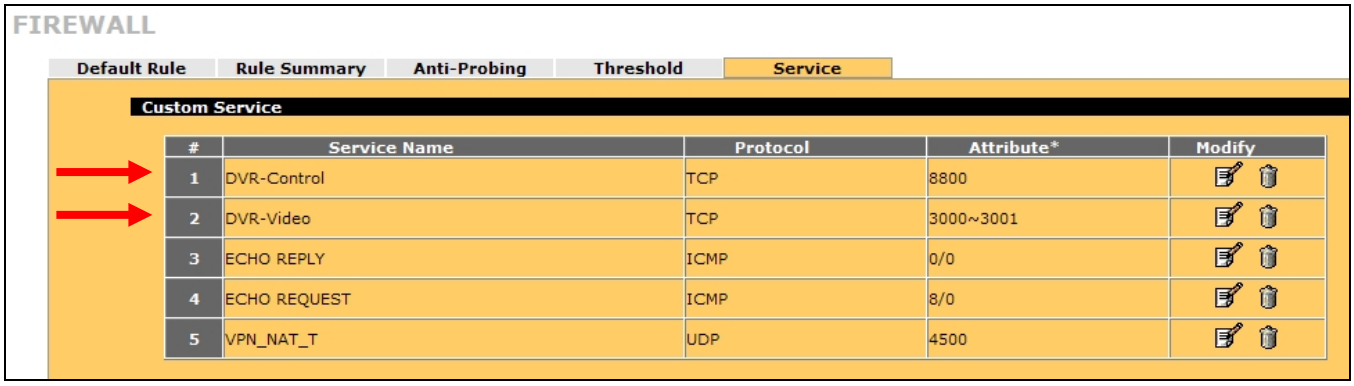

Figure 4: New Custom Services

Define Inbound Firewall Rule

Go to SECURITY > FIREWALL > RULE SUMMARY

You must permit the new service port traffic to flow from one or more of the public interfaces (CELL, WAN) through the firewall into the LAN-Cell's private LAN interface. On the **Firewall Rule Summary** screen, select the

packet source zone (interface) and the destination zone as the LAN interface. For example CELL-to-LAN, then click the Refresh button (Figure 5).

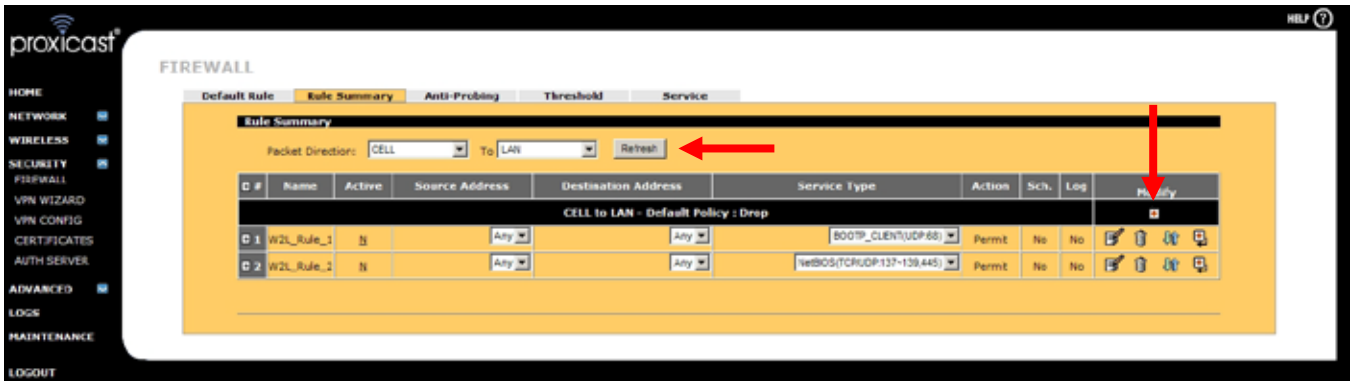

Figure 5: Firewall Rule Summary

There may be existing firewall rules for the packet direction you have selected. Click the small red plus sign under the Modify column to insert a new firewall rule for this packet direction.

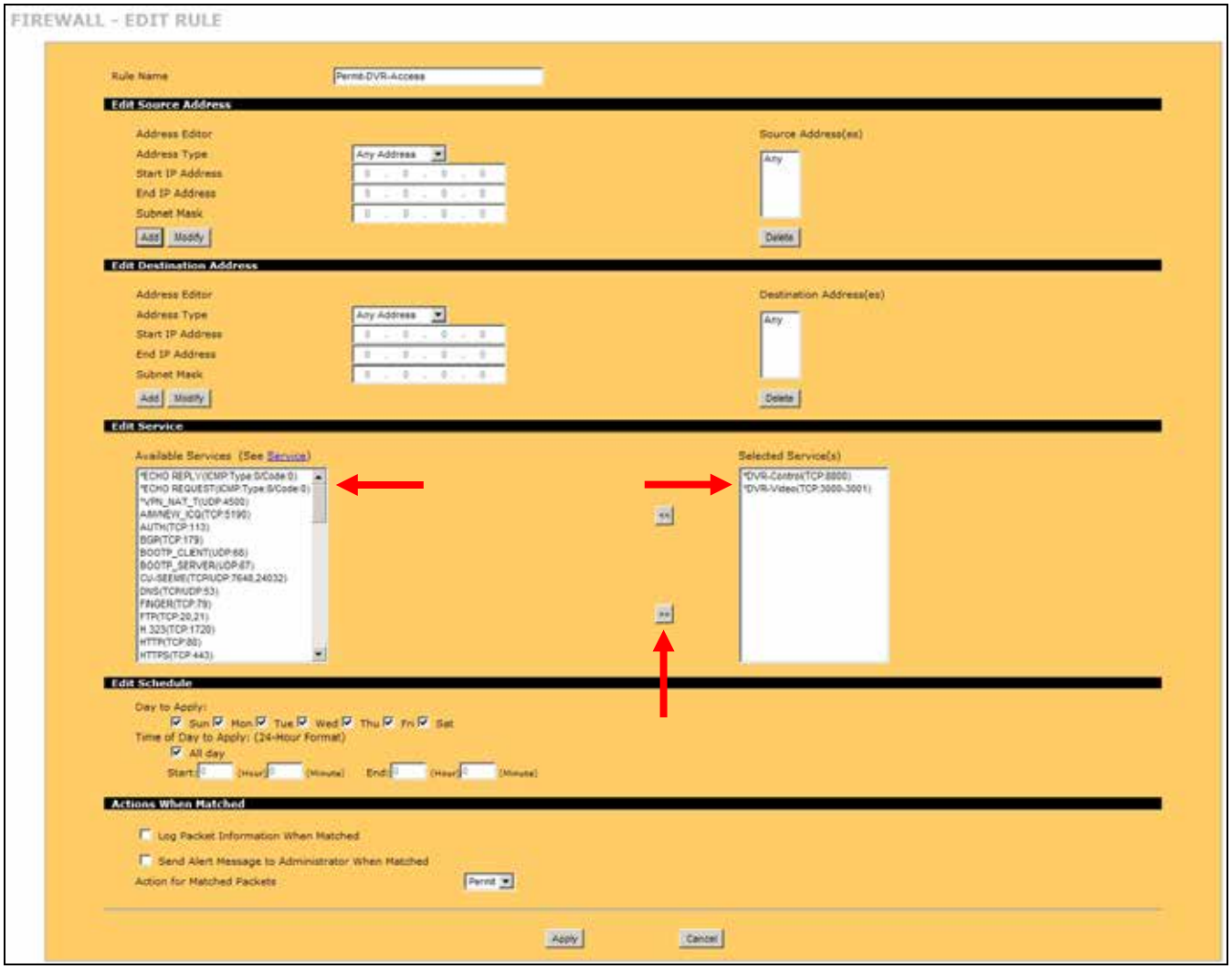

Figure 6: Adding a New Firewall Rule

You may give the new firewall rule any meaningful Name (no spaces). The Edit Source Address section allows you to limit which IP addresses are able to use this rule. If you choose to make this restriction, select the IP address range carefully to avoid locking yourself out if your IP address changes. The Edit Destination Address can limit which LAN devices may receive traffic via this rule.

In the Edit Service section, highlight the newly created service (an asterisk will be to the left of the name) and click the right arrow button to move the new service into the Selected Services listbox (Figure 6).

Accept the default settings for the remainder of the fields on this screen and click Apply. Your new rule will be displayed in the **Firewall Rule Summary** table (Figure 7).

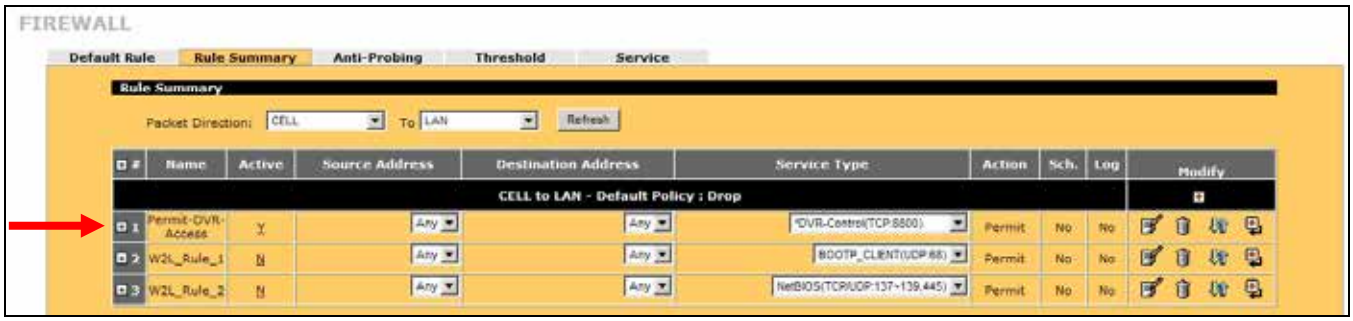

Figure 7: DVR Access Rule via 3G Cellular

Note 1: If you will be accessing the remote equipment from more than one public interface, repeat this step for each public interface (e.g. CELL-to-LAN, WAN-to-LAN).

Note 2: If you are "translating" port numbers (see below), the "translated" port number must be included in the permitted firewall rules.

5. Forward incoming traffic from the Internet to the equipment

Now that the inbound traffic from your TCP/IP ports is allowed onto the LAN, you must tell the LAN-Cell which device(s) on the LAN are to receive the data on each port.

Go to ADVANCED > NAT > PORT FORWARDING

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** for each set of Service ports required by your application by marking the first line as Active and giving it a descriptive Name. For our DVR example, 2 port forwarding rules are required. Both rules will forward incoming traffic on the specified ports to the static LAN address of our DVR (192.168.1.2). Click Apply to save the rules.

In some instances, you may need to "translate" externally visible TCP/UDP port numbers to other port numbers used on your private LAN if you cannot modify a port number that your equipment is using and it conflicts with other devices or the LAN-Cell. You may also need to use port translation if you have more than 1 LAN device that must use the same port number. For example, you could translate incoming port 8002 to port 80 on 192.168.1.2 and incoming port 8003 to port 80 on 192.168.1.3. The "translated" port number (80) must be included in the LAN-Cell's CELL-to-LAN or WAN-to-LAN firewall rules. Port translation is not used in our example.

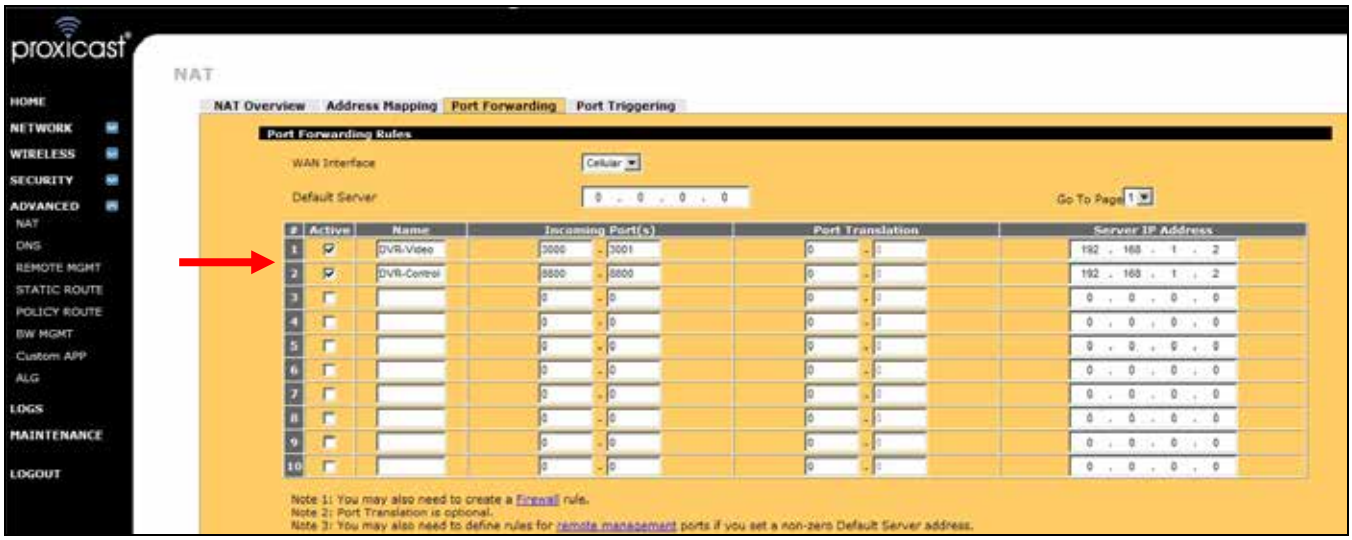

Figure 8: NAT Port Forwarding Rules

You are now ready to access your remote equipment over the Internet via the LAN-Cell.

Usage Notes

- You may repeat this process to define the parameters for any other remote LAN devices to which you need access.
- Backup your LAN-Cell's configuration before and after configuring remote device access.
- You cannot directly "ping" the devices on the LAN-Cell's LAN since ICMP cannot not flow through the Network Address Translation (NAT) feature of the firewall. If you ping the LAN-Cell's WAN IP address or DDNS name, the LAN-Cell itself will respond to the ping (if this feature is not disabled and your ISP does not block ICMP traffic). Use your application software to test the connection to your remote equipment.

Troubleshooting

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

1. *Incorrect IP addressing on the remote equipment*
   Ensure that the remote equipment has the LAN-Cell's LAN IP address as its Default Gateway and that the subnetting is correct.

2. *Not being aware of all of the ports used by your application*
   Please consult your documentation or contact the software/equipment manufacturer.

3. *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). Verizon Wireless has no inbound restrictions. Sprint blocks some ports including port 80.

   If you are unable to have the necessary ports opened and cannot change your remote equipment configuration, use the Port Translation feature to map an open port to the required port for your application (e.g. public port 7780 translates to private port 80). You may also be able to set up a VPN to get around carrier-imposed port restrictions.

4. *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.

5. *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.

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 your management software to communicate.

The LAN-Cell has extensive error logging features that you can use to help troubleshoot connectivity issues. On the Firewall Rule screen, check the Log option (Figure 9) 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 10). If no log entries are recorded, then packets are being blocked by the carrier, corporate firewall or your HQ PC's firewall.

Figure 9: Logging Matched Firewall Rules

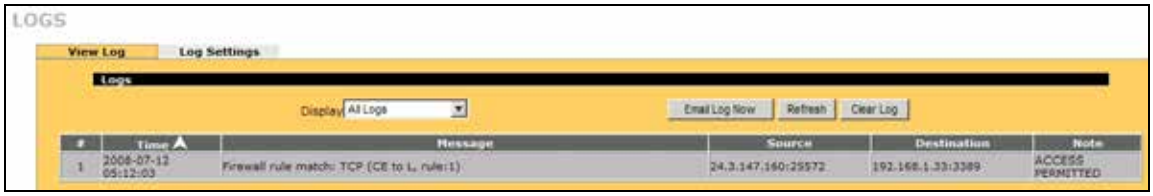

Figure 10: Matched Firewall Rule Log Entry

# # #