Changing the LAN-Cell 2's Remote Management Ports

Technote LCTN0015

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
September 11, 2009	Initial Release

Introduction

The LAN-Cell 2 can be managed using a variety of interfaces and applications including Web (HTTP/HTTPS), Terminal (Telnet/SSH), FTP and SNMP protocols. By default, the TCP/IP ports required for these interfaces are "open" through the LAN-Cell's firewall and assigned to the IANA-standard TCP/UDP port numbers for commonly used services.

In some instances, the standard TCP/UDP ports used for remote management applications must be changed to accommodate devices attached to the LAN-Cell which also require the use of the same port numbers. This TechNote describes how to change the LAN-Cell 2's Remote Management port configuration to avoid such conflicts.

This Technote is for illustration purposes only.

Background

By default, the LAN-Cell 2 uses the following TCP/IP ports for its remote management and other internal server applications:

Default 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)

The LAN-Cell also has a set of default Firewall Rules which allow traffic from public interfaces (CELL and WAN) to flow to the LAN-Cell's internal interface, but not any private interfaces (e.g. LAN/WLAN). This permits the user to manage the LAN-Cell from both the private and public interfaces immediately upon booting up the device.

The LAN-Cell's uses only 1 instance of each remote management application server, therefore the same TCP/IP service port numbers are used when communicating via the private or public interfaces. Changing the Remote Management port numbers will require you to use the new port numbers when communicating directly with the LAN-Cell over any interface.

proxicast®

Avoiding the Need to Change Remote Management Ports

Before changing the LAN-Cell's Remote Management port assignments, determine if either of the following alternatives are a viable option for your situation.

1. Change the ports used by your equipment/application
    Many devices and software applications can easily be modified to work on any TCP and/or UDP port assignment. For example, an IP Camera or DVR that defaults to use TCP port 80 may be able to use a different port number (e.g. TCP/81). See *TechNote LCTN0017: Accessing Remote Devices* for examples of how to configure the LAN-Cell for this scenario.

2. Use Port Translation and Port Forwarding
    If you cannot change the conflicting port number on your equipment/application, the LAN-Cell 2 can "translate" incoming requests on an unused port to the port required for your application and then forward this traffic onto the target device. For example the LAN-Cell can translate a request sent to its TCP port 81 into a request to your camera's port 80. See **Section 13.4** of the *LAN-Cell 2 Users Guide* and *TechNote LCTN0017: Accessing Remote Devices* for examples of how to configure port translation and forwarding.

Changing Remote Management Ports

In this example, we will change the LAN-Cell 2's default web (HTTP) management port from TCP/80 to TCP/7780.

Step 1: Define the new port as a new Service in the Firewall (SECURITY > FIREWALL > SERVICES)

Determine if the proposed new management port number is already a pre-defined port on the **Services** list (Figure 1). If so, consider using a different port for Remote Management to avoid future conflicts with commonly used TCP/UDP port assignments. Otherwise, click the **ADD** button on the Services page to define a new service (Figure 2).


Figure 1: Firewall Service List

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, the new service is called "Proxicast-HTTP" on TCP port 7780 only.
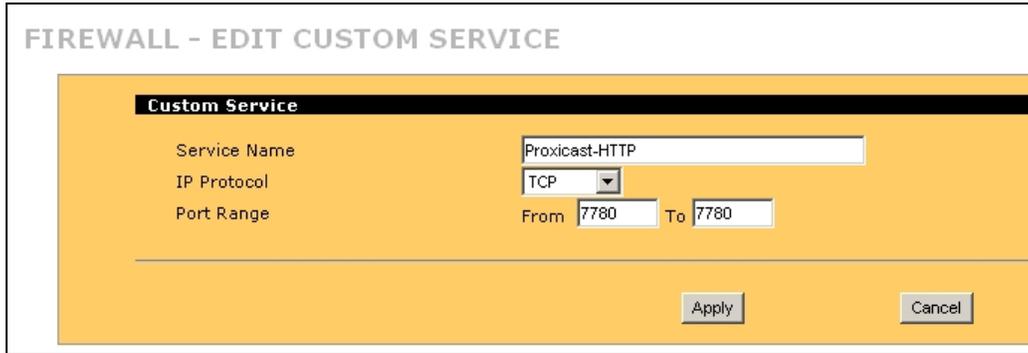
Figure 2: Adding a Custom Service Port

The newly added service will appear at the top of the **Custom Service** list (Figure 3).
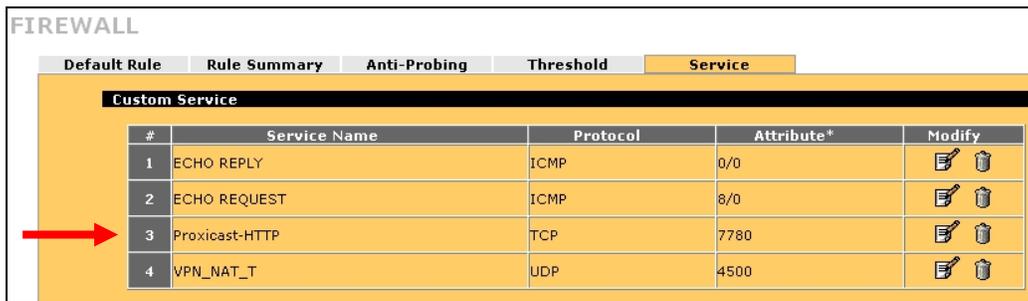
Figure 3: New Custom Service

Step 2: Permit traffic on the new port through the Firewall and into the LAN-Cell
(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 internal management interface. On the **Firewall Rule Summary** screen, select the packet source zone (interface) and the destination zone as the same public interface. For example CELL-to-CELL, then click the **Refresh** button (Figure 4).
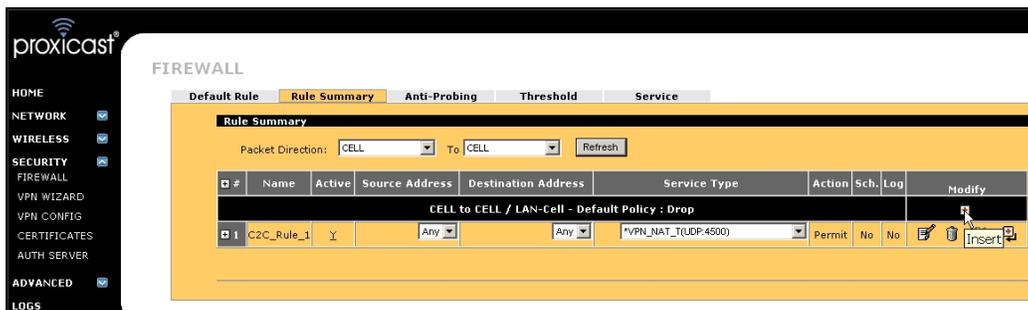
Figure 4: Firewall Rule Summary

proxicast®

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 4).

Figure 5: 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 of the LAN-Cell. The **Edit Destination Address** can limit which devices may receive traffic via this rule. Since we are editing a rule for LAN-Cell's internal address, this section does not apply.

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 5).

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 6).
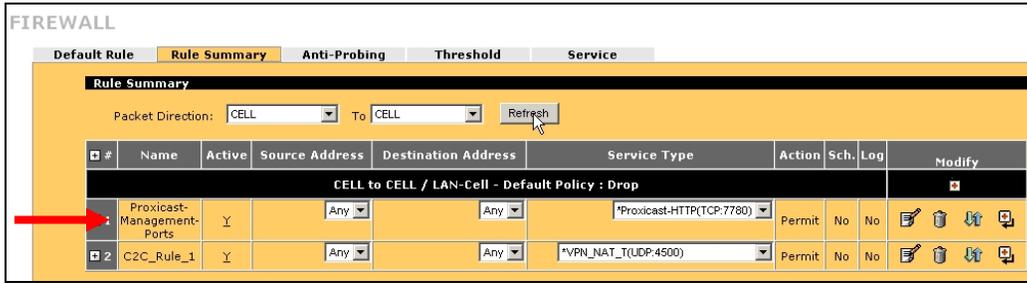

Figure 6: LAN Access via 3G Cellular

Important Note: If you will be accessing the LAN-Cell's Remote Management features from more than 1 public interface, repeat this step for each public interface (e.g. WAN-to-WAN).

Step 3: Change the Remote Management Port Assignment (ADVANCED > REMOTE MGMT)

Go to the **REMOTE MGMT** section under the **ADVANCED** menu and select the tab for the type of remote management interface you need to change (Figure 7). Enter the new created port number in the **Server Port** field and click **Apply**.

NOTE: If you are changing the port number of the remote management interface that you are currently using to manage the LAN-Cell, your session will be disconnected. Close your application and reconnect to the LAN-Cell using the new port number (e.g. http://192.168.1.1:7780)
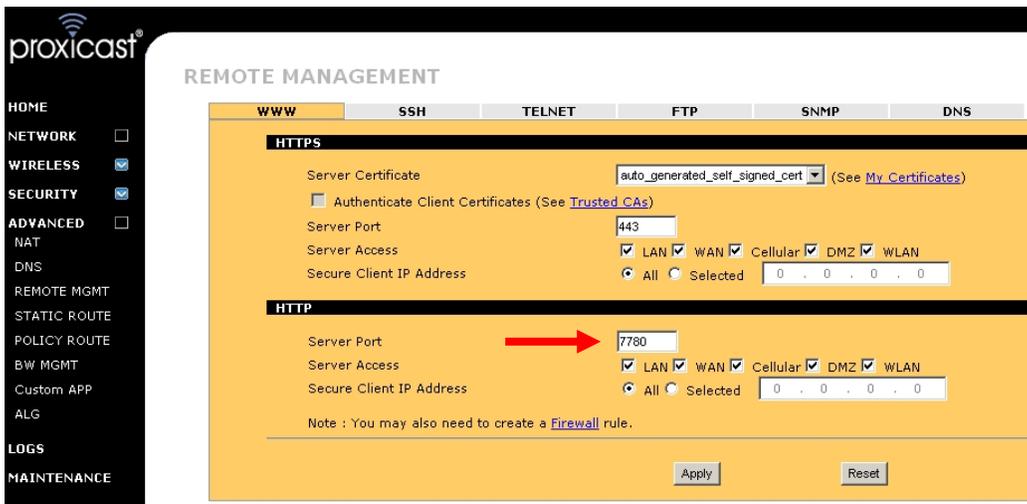

Figure 7: Changing Remote Management Port Numbers

Usage Notes

- You may repeat this process to redefine any or all of the LAN-Cell's Remote Management ports.

- To access the LAN-Cell via the new management port numbers, you will need to change the settings on your application, or open the connection with a specific port. In our example, the Web GUI is now accessible by appending ":7780" to the end of the URL (http://192.168.1.1:7780)

- The new port numbers must be used when connecting to the LAN-Cell from either the public (WAN, CELL) or private (LAN, WLAN) interfaces.

- When selecting new port numbers, IANA recommends using port numbers greater than 1024 and preferably between 49152 through 65535. See http://www.iana.org/assignments/port-numbers for the current list of IANA assigned port numbers

- Backup your LAN-Cell's configuration before and after making changes to the Remote Management ports (MAINTENANCE > BACKUP&RESTORE)

- Make note of the new Remote Management port numbers and inform anyone else who may need to access the LAN-Cell's management interface.

# # #

proxicast®