

Introduction

This document is a quick user guide to configuring and managing the value added IP services found in the Orion & Dorado services packages within the ClearVision Management System.

The instructions and processes described in this document are presented from the end user perspective, i.e., in the way that an end user, which has signed up for a Dorado or Orion service package, would control the system through the Control Panel.

Need More Help?

If you run into a difficult task not covered in this reference guide you can get knowledgeable help from the ClearAccess support center.

Technical Support #	Technical Support @
866-894-4657	support@rconnects.com

The Control Panel

The Control Panel is a web-based portal to access a ClearAccess manageable gateway in order to configure and manage all of the following parameters and services:

1. Wireless LAN parameters:
 - a) WEP Key Management
 - b) Geographic Location
 - c) Channel Management
 - d) SSID
 - e) Encryption Level
2. Managed Firewall parameters
 - a) UPnP management
 - b) Automatic Port Forwarding settings via Templates
 - c) Manual Port Forwarding settings
3. Internet Filter (Parental Control)
 - a) Configure a *Kidz* sites only profile via Template
 - b) Allow or continue to block websites requested from different users behind the gateway
 - c) Manually add particular sites to the blocked list
 - d) Manually add particular sites to the allowed list
 - e) Track a history of blocked sites
4. Time Blocking
 - a) Manually configure a daily schedule allowing or blocking Internet Access for different time periods, e.g. allow Internet Access from 4:00 PM to 7:00 PM only Monday through Friday
 - b) Manually set a maximum daily time allowed
 - c) Manually set a maximum weekly time allowed
 - d) Manually trigger a timer (Egg Timer) to override the time blocking schedule for short periods of time.

Accessing the Control Panel

There are two ways for an end user to access the Control Panel:

1. Through a computer that is directly connected to the gateway following the steps below:
 - a) Open a Web Browser and type the IP address 192.168.50.1 (or <http://clearview.home>) into the navigation bar and hit the enter/return key.
 - b) A prompt for ClearView credentials will popup on the screen (see Figure 1)

ClearAccess™
The Clear Choice in Broadband Solutions™

Gateway Login

Please enter your ClearView user name and password.

User Name:

Password:

Login

ClearView

Copyright © 2006, ClearAccess, All Rights Reserved. www.clearaccess.com

Figure 1: ClearView login page

2. Once you have entered your ClearView credentials correctly (contact Reliance Connects Technical Support if you do not have this login information – Technical Support can give this information ONLY to the account holder, and no one else) , the main page of ClearView will show up on your screen. From this main page (see Figure 3) you will get a link to the Control Panel on the upper left corner.



Figure 2: ClearView Home Page

3. It is also possible to access a ClearAccess gateway's Control Panel from any computer connected to the Internet by following the steps below:
 - a) Open a Web Browser and type the following address in the navigation bar:
<https://clearvision100.clearaccess.com/user>
 - b) A prompt for Control Panel credentials will pop up. These are the same ClearView credentials described earlier.

Navigating the Control Panel

Once you have been granted access into the Control Panel, all the network elements connected to the ClearAccess gateway, as well as the available services for these devices will show up on your web browser screen in the form of icons, as shown on the list and figure (see Figure 4) below:

1. A **Gateway** icon
2. A **Reserve Static IP** icon
3. An **Internet Filter** icon
4. One icon per each device connected to the gateway

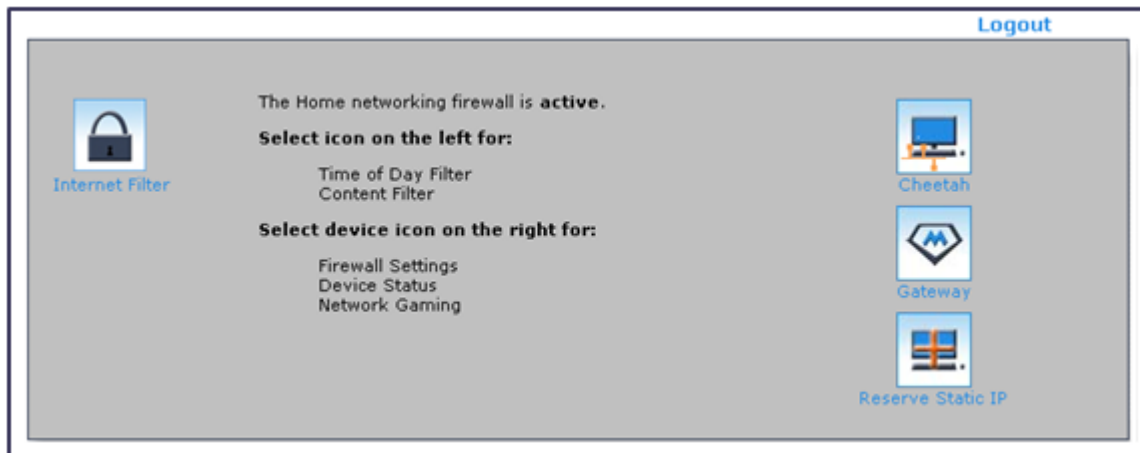


Figure 3: Control Panel main page

Managing Internet Access Rules

If the customer has time blocking and content filtering enabled in their subscription, then you can manage those features using the **Internet Filter**.

Configuring Time Blocking

The time blocking feature in the control panel allows customers to set time blocking rules and monitor how much time the internet has been used.

Customers can set individual blocks of time throughout the week to be blocked, they can limit the amount of time the internet can be accessed each day, and they can limit the amount of time it can be accessed each week. They can also use the 'Egg Timer' feature to override the normal schedule and add timed access starting immediately for a set amount of time.

As an example lets block a section of time every Wednesday from 6 a.m. to 10:30 p.m., as well as limit internet access to 2 hours per day and 20 hours per week.

How to Add Blocked Time

1. From the Control Panel main menu, open the **Internet Filter** toolbox (see Figure 5)
2. Select **Time Blocking** this will open a time calendar
3. Under Start select the day – **Wednesday**
4. Set the time to **6 a.m.**
5. Under **Stop** set the ending time to **10:30 p.m.**
6. If you want to block Internet access during this period of time, then click on the **Block** button. If you want to allow Internet access during this period of time **AND** block Internet access for the rest of that day, then click on the **Allow** button.



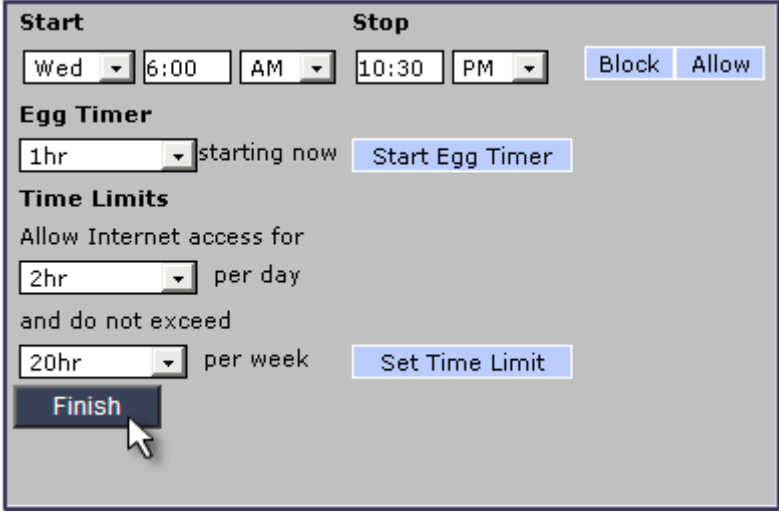
Figure 4: Click to open the Internet Filter toolbox

How to Add Time Limits

Once you have configured a time window to be blocked or allowed for Internet Access, it is possible to complement the schedule with additional Time Limit settings on a per day or weekly basis. In order to add these parameters, follow the extra steps below:

1. Within the **Time Limits** section, select the maximum amount of time allowed on a given day. For example, we set the daily limit to **2hr** and the weekly limit to **20hr** (see Figure 6)
2. Click **Set Time Limit**
3. Click **Finish** - This action will take you back to the Control Panel main menu

4. From the icons on the right hand side of the screen, select a computer to assign a Time Blocking schedule to
5. Click on that particular computer and check the **Time Limit** box
6. Click **Apply**
7. Click **Logout** on the upper right corner of the Control Panel



The screenshot displays a control panel for configuring time blocking. It features two columns for 'Start' and 'Stop' times, with dropdown menus for days of the week, times, and AM/PM. There are 'Block' and 'Allow' buttons. Below this is an 'Egg Timer' section with a dropdown for duration (set to 1hr) and a 'Start Egg Timer' button. The 'Time Limits' section includes 'Allow Internet access for' with a dropdown (set to 2hr) and 'per day', followed by 'and do not exceed' with a dropdown (set to 20hr) and 'per week'. There is a 'Set Time Limit' button and a 'Finish' button at the bottom left with a mouse cursor pointing to it.

Figure 5: Enter time blocking parameters

The blocked time will be reflected on the weekly chart on the screen. You can also click this chart to view what time limits have been set and have the option to remove them.

The **Set Time Limit** button allows you to reset how much time is available this week for internet usage. For instance, if there has already been 1 hour used out of the 2 hours available, you can press **Reset** to reset the amount of time available to 2 hours.

How to Delete Time Blocking Rules

1. From the Control Panel main menu, open the **Internet Filter** toolbox
2. Select **Time Blocking**
3. In the calendar on the left hand side, click on the colored block representing the time schedule that you want to remove. This will show the details for that rule and will present a **Remove** option on the right hand side of the screen (see Figure 7)

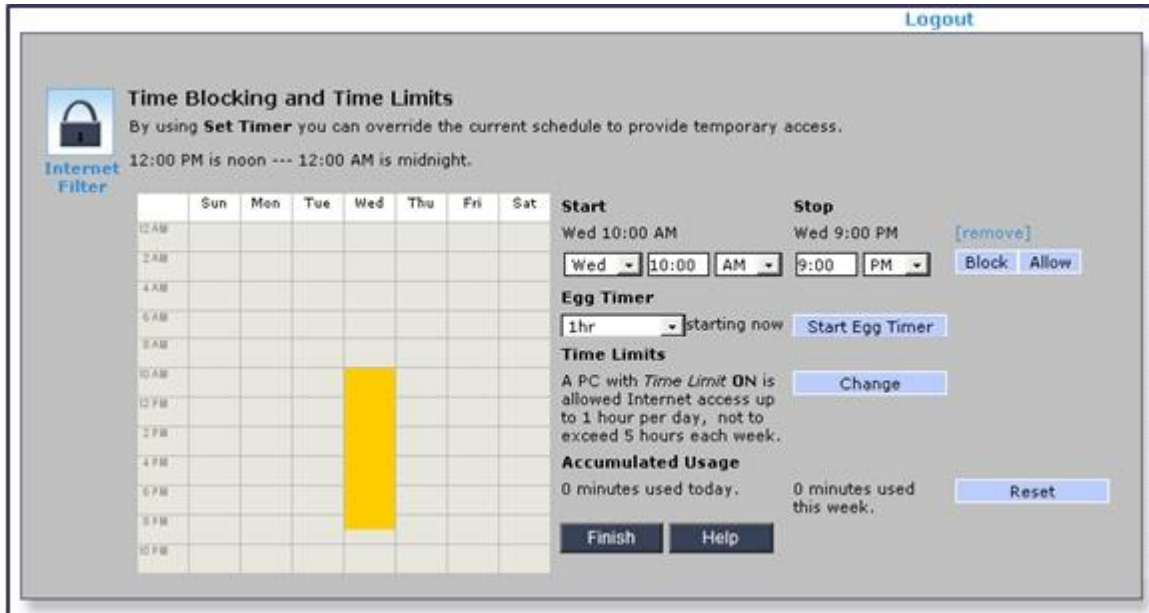


Figure 6: Removing time blocking rules

4. Click on the **Remove** button associated with the Time Blocking rule on the right hand side of the screen.
5. Click **Finish**

Configuring Content Filtering Rules

In order to access and manage Content Filtering rules, you need to click on the Internet Filter icon on the upper left corner on the Control Panel main page.

The rules configured through this functionality can be enabled or disabled on each computer connected to the gateway through the Internet Filter functionality, found on each particular device.

By clicking on the Content Filter button (see Figure 8), the Content Filtering parameters will pop up on a new page (see Figure 9).

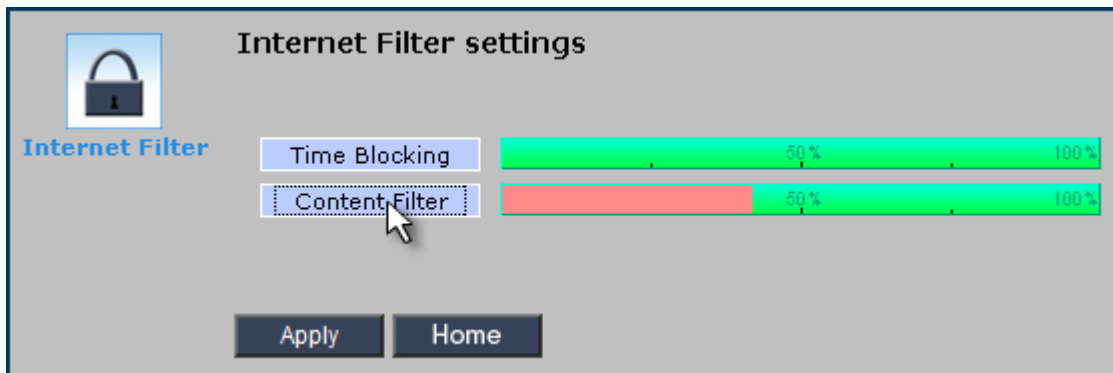


Figure 7: Internet Filter Settings



Figure 8: Content filter settings page

There are two ways to block content using the Content Filter:

- **Enable Content Filtering** – This option is the default content filtering option. This option blocks inappropriate sites as well as sites explicitly identified in the **Blocked Site List**.
- **Disable Content Filtering** – This option disables all content filtering except for sites that have been explicitly chosen in the **Blocked Site List**.
- **Allow Only Kidz Sites** – This option only allows sites known to be safe for kids. These sites are presets managed by ClearAccess. This option also blocks sites chosen in the **Blocked Site List**.

Through the content filtering tool you can track which websites were blocked as well as set which websites should be allowed past the filter policy. By using check-boxes it is possible to enable or disable the filter settings, blocked list, allowed list, and blocked site tracking.



Important Note: If the new content filtering settings being applied are set for the same computer you are currently using, then the new settings will be applied once the user clicks **Logout** from the ClearView main menu, or after the computer is restarted.

Creating a Static IP Address

Your ClearAccess gateway will hand out IP addresses on the LAN side dynamically by default. For some network elements that cannot receive an IP address via DHCP, it is possible to create and assign a static IP address through the Control Panel as well.

How To Assign a Static IP Address

1. Open the Control Panel of your gateway
2. Open the **Reserve Static IP** toolbox on the bottom right corner
3. Choose a name for the computer or network element that you will assign the fixed IP address to.
4. Assign a static IP Address – **Ex. 192.168.50.xxx**, XXX must be greater than 1
5. Assign the MAC Address the computer or network element that you will assign the fixed IP address to – **Ex. 00:0e:12:45:a2:6b**
6. Click **Finish**



Figure 9: Click to open the Reserve Static IP toolbox

You can now access your new network element from the Control Panel's main menu to view its connection status, settings, and modify filtering/time blocking parameters as described in the previous sections.

Viewing and Modifying Wireless Settings

The **Gateway** toolbox allows you to view a gateway's parameters as well as modify its wireless settings. Through the **Gateway** toolbox you can view:

- **Gateway Model** – Ex. ClearAccess AG10W
- **Gateway Type** – This field indicates the hardware that the gateway uses. Ex. **6348gw11_CAP**:
 - **6348** – Broadcom chip product number
 - **gw** – Indicates a 'gateway wireless'
 - **11** – Uses 802.11
- **MAC Address**
- **External Name**
- **External IP** – IP address seen by the WAN
- **Internal IP** – IP address seen by the LAN
- **WEP** – Indicates the status of WEP security (Ex. On/Off)
- **ESSID** – A unique name to identify the gateway to any client which would want to wirelessly connect to it (Ex. Jack's Wireless)
- **WEP Key** – If WEP is enabled the key will be displayed here. This is useful if the customer forgets their WEP key and needs it recovered.

Using the **Gateway** toolbox you can modify your wireless settings, such as changing your WEP Key, enabling/disabling wireless, changing the wireless broadcast channel, and enabling/disabling the broadcast of your SSID.

Let's enable some security settings to make the gateway more secure. Let's change the network name to SpeedyISP, change the WEP Key to a 13 digit password - Sp33dee123456, and disable the broadcast of the wireless SSID.

How To change Gateway Security Settings

1. Open the **Gateway** toolbox, by clicking the Gateway icon on the Control Panel.
2. Click **Wireless Setup**.
3. Click **Advanced**.
4. Select the **Network Name** of your preference. This name will show up on wireless computers as an available secured wireless network. In the example below, we set the Network Name to **SpeedyISP**.
5. In order to change the WEP key value to one other than what is automatically generated by the gateway, type the new WEP key into the WEP Key field. Please note that if using 128 bit encryption, the length of the WEP keys must be 13 characters long (alpha-numeric), if the encryption level has been set to 64, then the WEP key has to be 5 characters long. In this example type **Sp33dee123456** into the WEP Key field (see Figure 12).

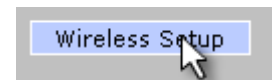


Figure 10: Click Wireless Setup

Gateway Wireless LAN settings
This page displays and edits settings for the **wireless lan** access integrated into the gateway.

Enable Wireless **Network Name** SpeedyISP

Enable WEP On

WEP Key Sp33dee123456
13 Chars if Length=128
5 Chars if Length=64

Key Length 128-bit, 13 Characters

Country Local UNITED STATES

Channel 11

Auth Method Auto

Hide SSID

Apply Help Less <<

Figure 11: Enter security settings

6. In order to change the channel on which the radio broadcasts its signal, please choose a channel number from **1** to **14** by clicking on the scroll down menu. This functionality is useful if the gateway's radio is interfering with other wireless devices in your environment or vice versa (other wireless devices affecting the gateway's ability to transmit wireless signals properly).
7. Check the **Hide SSID** check-box to disable broadcasting the wireless SSID. This functionality adds greater security to your wireless connection by hiding the wireless network name. Once you have your computer connected to the secure wireless network you can add this extra security step.
8. Click **Apply** to save your gateway security settings.
9. Logout from the Control Panel.

Configuring Port Forwarding Rules

A powerful feature of the Control Panel is the ability to remotely configure port forwarding settings for specific network elements connected behind the gateway on the local area network (LAN).

In a Network Address Translation (NAT) environment, where multiple network elements connect to the WAN (outside network) by sharing one public IP address belonging to the gateway (using NAT), it is sometimes necessary to configure Port Forwarding rules in order for external hosts to be able to communicate with devices behind the gateway on the local area network (LAN). A 'port forward' command consists of a rule which configures the gateway's firewall to map a particular TCP or UDP port (or range of ports) to one particular device on its LAN side. This enables the gateway to know which private IP address on the LAN to send certain data packets to when it receives data from the WAN over a specific logical port.

Port forwarding is usually necessary to play online games or deploy VoIP services behind a NAT enabled gateway. In this section you will learn how to configure Port Forwarding rules through the Control Panel.

How to configure Port Forwarding via the Control Panel

1. Login to the Control Panel
2. Click on the computer or network element of interest on the right hand side of the screen
3. Click on **Manage Firewall** - A new page with the firewall parameters will pop up (see Figure 13)

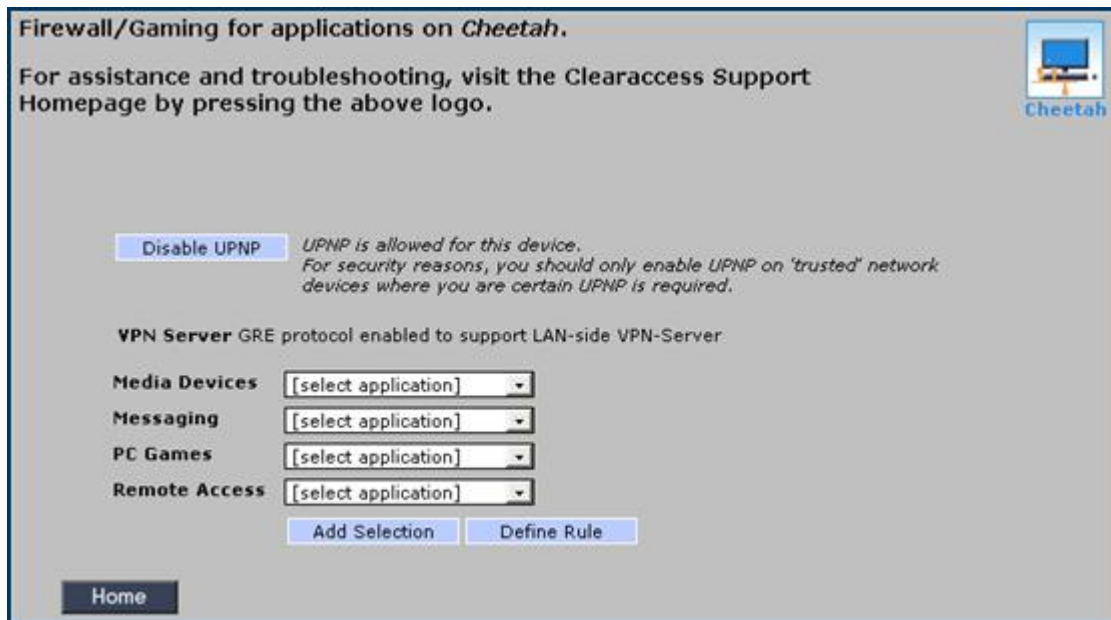


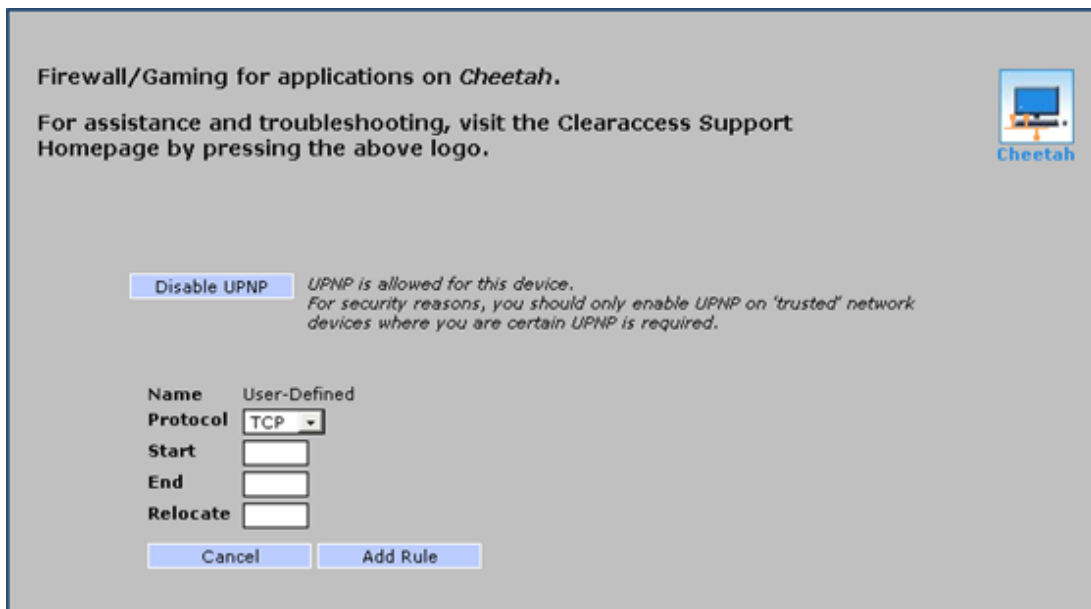
Figure 12: Port forwarding templates

4. Port Forwarding rules can be automatically configured for this network element by selecting the appropriate template from any of the four categories listed:
 - **Media Devices** – A list of media related devices that can be configured to be forwarded through the gateway, such as a Playstation2, or Net2Phone
 - **Messaging** – A list of instant messaging applications which can be forwarded through the firewall, such as AOL Instant Messenger, MSN Messenger, and ICQ Messenger
 - **PC Games** – This contains a list of games which can be forwarded through the firewall
 - **Remote Access** – Remote access applications that would need to be forwarded through the firewall, such as VPN and SSH applications
5. Select the particular template of interest and click the **Add Selection** button
6. Click the **Home** button
7. Click the **Apply** button

8. Logout from the Control Panel
9. The Port Forwarding setting will start working immediately for that particular device

If an application is not listed in the one of the four templates' scroll down menus, then you can set the port forwarding for that application manually by following the steps below:

1. From the Manage Firewall page from step 3 above, click on **Define Rule** (see Figure 15)



Firewall/Gaming for applications on *Cheetah*.

For assistance and troubleshooting, visit the Clearaccess Support Homepage by pressing the above logo.

UPNP is allowed for this device.
For security reasons, you should only enable UPNP on 'trusted' network devices where you are certain UPNP is required.

Name User-Defined

Protocol

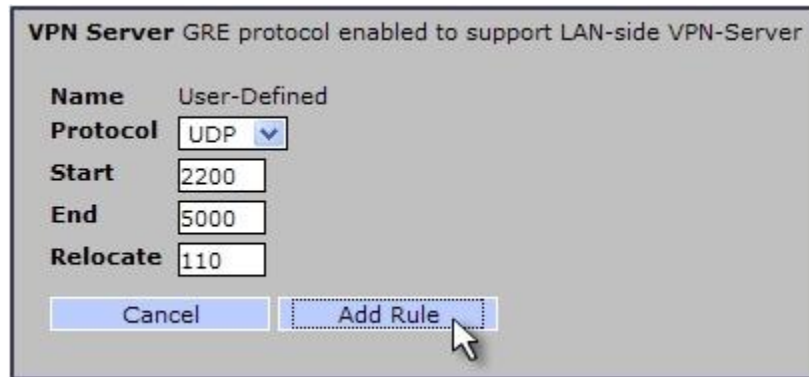
Start

End

Relocate

Figure 13: Adding a manual port forwarding rule

2. Choose **UDP** or **TCP** from the Protocol drop-down menu
3. Enter the Port number (or first port in the range of ports you are trying to forward) as the Start port. e.g. 2200
4. If you are configuring port forwarding for just one port, then enter the same **Start Port** as **End Port**. If you are configuring a range of ports, then enter the final port on the range as the **End Port**, e.g. 5000
5. If you are trying to configure the ports on the LAN side of the gateway to be mapped into the same Port number on the WAN side, then enter the **Start Port** number as the **Relocate** value. If you are trying to relocate the port or range of ports into another port or range of ports in the WAN side, then select the first port of the new range as the Relocate value. For example, if you would like to configure a port forwarding rule for all the UDP Ports between 2200 and 5000 on the LAN side, and map them starting on port 110 on the WAN side (which will run from port 110 to port 2911) then the configuration will look as depicted below:



VPN Server GRE protocol enabled to support LAN-side VPN-Server

Name User-Defined

Protocol UDP

Start 2200

End 5000

Relocate 110

Cancel Add Rule

Figure 14: Configuring parameters for manual port forwarding

6. Click the **Add Rule** button
7. Click on **Home**
8. Click on **Apply**
9. **Logout** from the Control Panel



Important Note: It is NOT possible to program the same port forwarding rule to more than one computer or network element behind the same gateway.

Make sure you do not forward ports to already designated ports. Programs using those ports will not function correctly