

GlobeSurfer® III

Port Forwarding

About this document

Overview and Purpose

This document provides a description of how to configure Port Forwarding rules on the GlobeSurfer® III (GS3).

Confidentiality

All data and information contained or disclosed by this document is confidential and proprietary of Option NV, and all rights therein are expressly reserved. By accepting this document, the recipient agrees that this information is held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without prior and written permission of Option NV.

Version History

Date	Version	Author	Revision	Remarks
Dec 15, 2008	v001draft	F. Arboleda		Initial version
Dec 16, 2008	v002ext	F. Arboleda	<i>P. Vandeneede</i>	Revision

Author: F. Arboleda
Creation Date: Dec 16, 2008

Version: v002ext
Page: 1 of 9

Option Confidential: This document is Option Confidential - it may not be duplicated, neither distributed externally without prior and written permission of Option NV.

Table of contents

1	INTRODUCTION	3
2	PORT FORWARDING CONFIGURATION	4
2.1	A Port Forwarding Example	7

1 INTRODUCTION

In its default state, the GS3 blocks all external users from connecting to or communicating with the local network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, there is a possibility to expose the local network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities.

The 'Port Forwarding' screen enables the user to define the applications that require special handling by the GS3. The only thing that has to be done is select the application's protocol and the local IP address or name of the computer that will be using or providing the service. If required, the user may add new protocols in addition to the most common ones provided by the GS3. For example, if the user wanted to use a File Transfer Protocol (FTP) application on one of the local PCs, the user would simply select 'FTP' from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at GS3 from the Internet will henceforth be forwarded to the specified computer.

Similarly, Internet user's access to servers inside the home network can be granted, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside the home network. When an Internet user points his/her browser to the GS3's external IP address, the gateway will forward the incoming HTTP request to the internal Web server.

However, there is a limitation that must be considered. With one external IP address (the GS3's main IP address), different applications can be assigned to the LAN computers, however each type of application is limited to use one computer. For example, you can define that FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail.

Additionally, port forwarding enables the user to redirect traffic to a different port instead of the one to which it was designated. For example, a Web server running on a LAN PC on port 8080 and the user wants to grant access to this server to anyone who accesses GS3 via HTTP (Port 80). To accomplish this, you will have to define a port forwarding rule for the HTTP service, with the PC's IP or host name, as well as specify 8080 in the 'Forward to Port' field. All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080.

Author: F. Arboleda
Creation Date: Dec 16, 2008

Version: v002ext
Page: 3 of 9

Option Confidential: This document is Option Confidential - it may not be duplicated, neither distributed externally without prior and written permission of Option NV.

When setting a port forwarding service, the user must ensure that the port is not already in use by another application, which may stop functioning.

2 PORT FORWARDING CONFIGURATION

To add a new port forwarding service, perform the following:

1. In the web interface, select the 'Firewall' menu item under the 'Services' tab, and click the 'Port Forwarding' link. The 'Port Forwarding' screen appears.



Figure 1: Port Forwarding

2. Click the 'New Entry' link. The 'Add Port Forwarding Rule' screen appears.



Figure 2: Add Port Forwarding Rule – Basic

- Click the 'Advanced' button at the bottom of the screen. The screen expands.



Firewall

Add Port Forwarding Rule

Overview | Access Control | **Port Forwarding** | DMZ Host | Port Triggering | Website Restrictions | NAT | Connections | Advanced Filtering | Log

Local Host: Add... ▼

Protocol: Any ▼

Specify Public IP Address

Forward to Port: Same as Incoming Port ▼

Schedule: Always ▼

OK Cancel Basic <<

Figure 3: Add Port Forwarding Rule – Advanced

- The 'Local Host' drop-down menu lists your available LAN computers. Select a computer that will provide the service (the "server"). If you would like to add a new computer, select the 'User Defined' option in the drop-down menu and fill in the values of your new LAN computer. Note that only one LAN computer can be assigned to provide a specific service or application.
- The 'Protocol' drop-down menu lets you select or specify the type of protocol that will be used. Selecting the 'Show All Services' option expands the list of available protocols. You can either select a pre-defined protocol or add a new one using the 'User Defined' option.
- By default, GS3 will forward traffic to the same port as the incoming port. If you wish to redirect traffic to a different port, select the 'Specify' option in the 'Forward to Port' drop-down menu. The screen refreshes, and an additional field appears, enabling you to enter the port number.



Forward to Port: Specify ▼

Figure 4: Forward to a Specific Port

Author: F. Arboleda
Creation Date: Dec 16, 2008

Version: v002ext
Page: 5 of 9

Option Confidential: This document is Option Confidential - it may not be duplicated, neither distributed externally without prior and written permission of Option NV.

7. By default, the rule will always be active. However, you can configure scheduler rules by selecting 'User Defined', in order to define time segments during which the rule may be active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules.
8. Click the 'OK' button to save your changes. The 'Port Forwarding' screen displays a summary of the rule that you have just added.

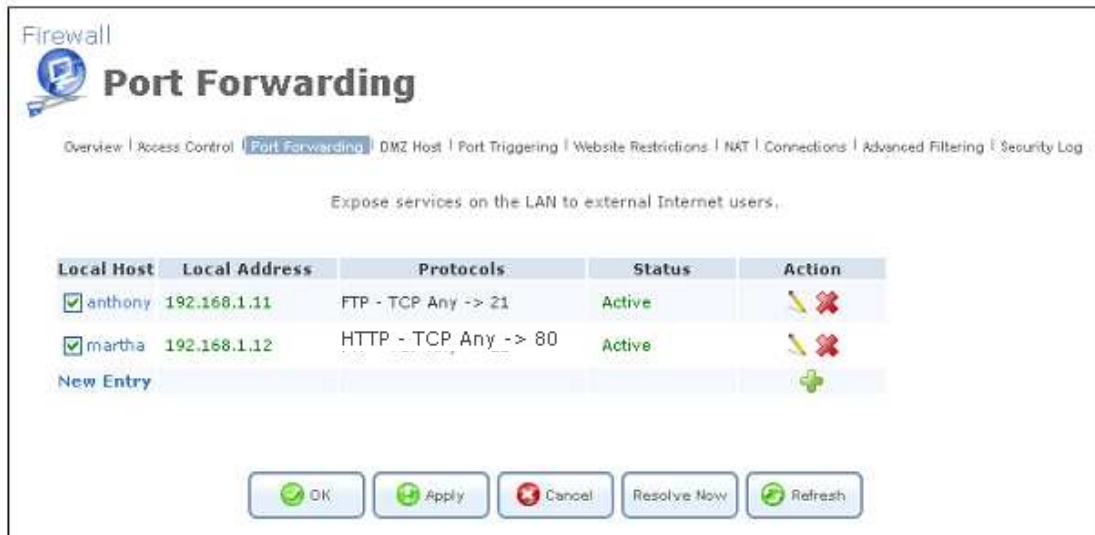



Figure 5: Port Forwarding Rule

You may edit the port forwarding rule by clicking its entry under the 'Local Host' column in the 'Port Forwarding' screen. You can disable the rule in order to make a service unavailable without having to remove the rule from the 'Port Forwarding' screen. This may be useful if you wish to make the service unavailable only temporarily and expect that you will want to reinstate it in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the  action icon for the service. The service will be permanently removed.

2.1 A Port Forwarding Example

In order to allow outside access (from the WAN) to a server inside your LAN, you must configure GS3's firewall, by adding a port forwarding rule. The following exercise demonstrates how to allow such access to an HTTP server located inside GS3's LAN.

When remote administration is enabled on GS3, an attempt to browse to GS3's web interface from a WAN PC will yield the web interface's 'Home' page. However, when the following port forwarding rule is defined on GS3, an attempt to browse to GS3's web interface from a WAN PC will yield the HTTP server located on the LAN.

To enable remote administration, perform the following:

1. From a LAN PC, browse to GS3's web interface and click 'Advanced'. Click the 'Remote Administration' icon, and check the 'Using Primary HTTP Port (80)' check box.

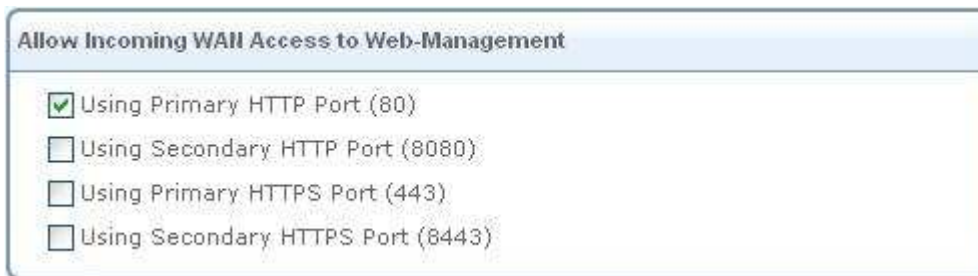


Figure 6: Allow Incoming WAN Access to Web-Management

2. Click 'OK' to save the settings.
3. Verify that remote administration is enabled, by accessing GS3's web interface from a WAN PC.

To define a port forwarding rule, perform the following:

1. From a LAN PC, browse to GS3's web interface and select the 'Firewall' menu item under the 'Services' tab. In the links bar, select 'Port Forwarding', and click 'New Entry'.
2. From the 'Local Host' drop-down menu, select the server's LAN PC name or IP address. In the 'Protocol' drop-down menu, select the 'HTTP' protocol. The screen refreshes after each change.



Figure 7: Add Port Forwarding Rule

3. Click 'OK' to save the settings.
4. To verify that port forwarding takes place, access GS3's web interface from a WAN PC. You should be redirected to the LAN HTTP server.

You may disable the port forwarding rule by deselecting its check box in the 'Port Forwarding' screen. If you try to access the local server from the WAN, the HTTP server will not be accessible, and GS3's web interface 'Home' page will appear instead.

References

Ref	Document
1	user_manual.pdf Jungo