USERGUIDE

Revised: 14-Nov-07

Inmarsat Fleet from Stratos

MPDS Firewall Service

Version 1.0

STRATOS®

BEYOND THE HORIZON®

This edition of the User Manual has been updated with information available at the date of issue. This edition supersedes all earlier versions of this manual.

This publication has been compiled with the greatest possible care, but no rights may be derived from its contents.

1 Introduction

This manual describes the web based MPDS Firewall Service.
The MPDS User is provided with a web interface in order to access your personal firewall profile on the MPDS Service. This interface of the MPDS Firewall Service allows you:

- To update your personal details, for example if an email address has changed.
- To access, adjust and maintain your Firewall and PPP Parameter settings for the Stratos MPDS Service.
- To change your passwords and security setting which will in turn affect the password you use to access the Stratos MPDS service.

Log In
You can log in using a standard web browser - from either a GAN or Fleet terminal equipped with MPDS or from a PC connected to the Internet. The MPDS Firewall Service is available via the following URL:
https://mpds.xantic.net

Automatic Log Out
If you have not used the MPDS Firewall Service for more than 20 minutes you will be automatically logged out. The following message will appear:

“You have been logged out because your session time has expired”

2 Advantages

Web based
The MPDS Firewall Service is easily accessible via the Web.
Cost control
With MPDS you pay for the amount of traffic you send and receive, the MPDS Firewall Service is an excellent way to control cost. You can avoid hackers from sending you unwanted traffic, and if you are a network administrator, make sure that employees only use the terminal to access relevant sites.

Ease of use
You can easily access your personal firewall via a Web browser, you don’t have to buy and install a firewall yourself.

Security
You can configure your own level of security to block any unwanted traffic to and from your terminal.

3 Access

The MPDS Firewall Service is available via the following URL: https://mpds.xantic.net

Username/Password
You must login using the same username and password when connecting to the MPDS service.

4 Configuration

The MPDS Firewall Service allows you:

- To edit your Personal Details, for example if an email address has changed.
- To set your Firewall Rules: access, adjust and maintain your Firewall and PPP parameter settings for the Stratos MPDS service.
- To change your password and security setting which will in turn affect the password you use to access the Stratos MPDS service.
- To get more information on Stratos's MPDS Service.
- To look for help on the MPDS Firewall settings.

To logout.

4.1 Edit Options

The Edit Options function allows you to change your own profile. By selecting one of the two options in the menu along the left hand side you can:

- Edit your Personal Details
- Set your Personal Firewall rules

4.1.1 Edit Customer Personal Details

The user may edit their personal details by clicking on the "Edit Customer Personal Details" option. The current details will be displayed and the user may edit these. Once all edits have been made the user should click the UPDATE button to save the changes.

In this screen you can alter the following information:

- First Name
- Surname
- Email Address
- Company

Once edited, the UPDATE button will commit the changes to the database. The CANCEL UPDATE button will restore the original settings.

4.1.2 Edit Service Profile

Each user has one or more services associated with their login. A service defines the type of network access a connection will have and includes the personal firewall settings. Click on a service title to view the details of that service.

The Edit Service Profile allows you to:

- Configure, add and remove Firewall Rules
- Change the PPP Parameter settings

Configuring Firewall Rules

You can access any service profiles associated with you. The firewall rules are the main part of the MPDS Firewall Service. These rules allow the definition or what traffic can flow into and out of your terminal and allow for a fine degree of control.

What is a Firewall?

A firewall is an application to be able to securely connect to the Internet. With the MPDS Firewall Service, you can easily specify what traffic is allowed between your Terminal and the Internet. You can for example:

- Block all traffic from the Internet to the terminal.
- Permit only email to and from your terminal, and block Web browsing and everything else.
- Permit only Web browsing to your corporate website from the terminal

How to use the Firewall Service

Click on 'Edit Options' on the top left hand side of the screen and then 'Edit Service Profile'.

Now you can see your default active firewall settings, or in common firewall terminology, ‘Firewall Rules’ as shown in the screen

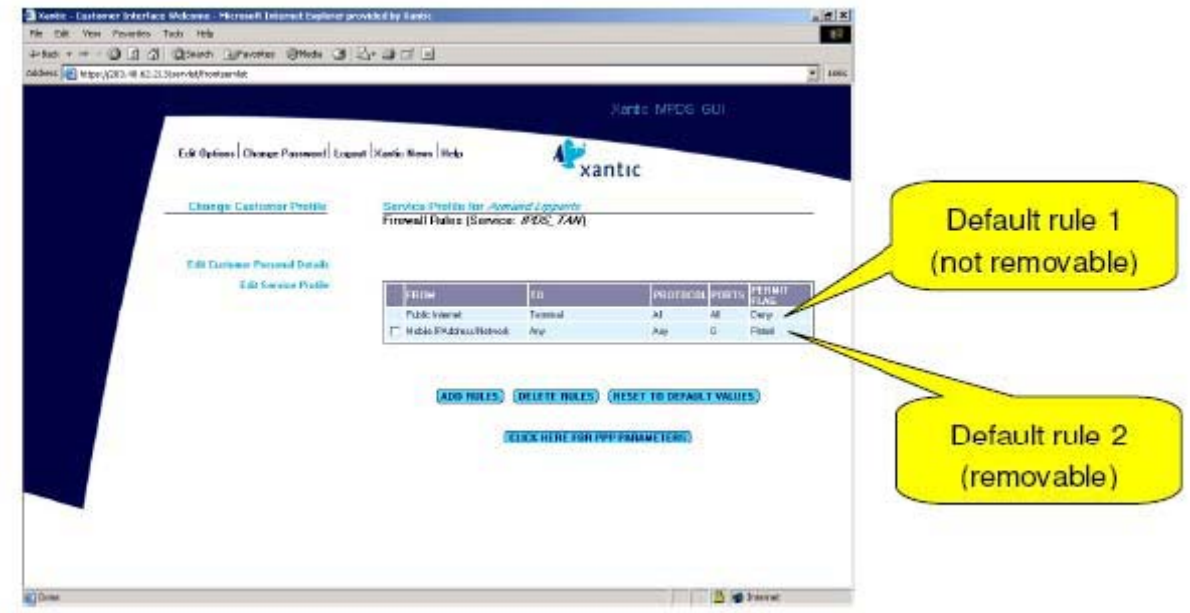


Figure 1: Default Firewall Rules

Default Firewall Settings

Every terminal is by default protected by the MPDS Firewall Service. The default setting is to permit all traffic from your terminal to the Internet, and only permit requested traffic back. For example, you can do Web browsing, but someone from the Internet will not be able to ‘ping’ you (send you unsolicited traffic). See Figure 2 and Figure 3.

Note: *Because a firewall is based on protection of the user, all traffic that is not explicitly permitted via a rule is denied.*

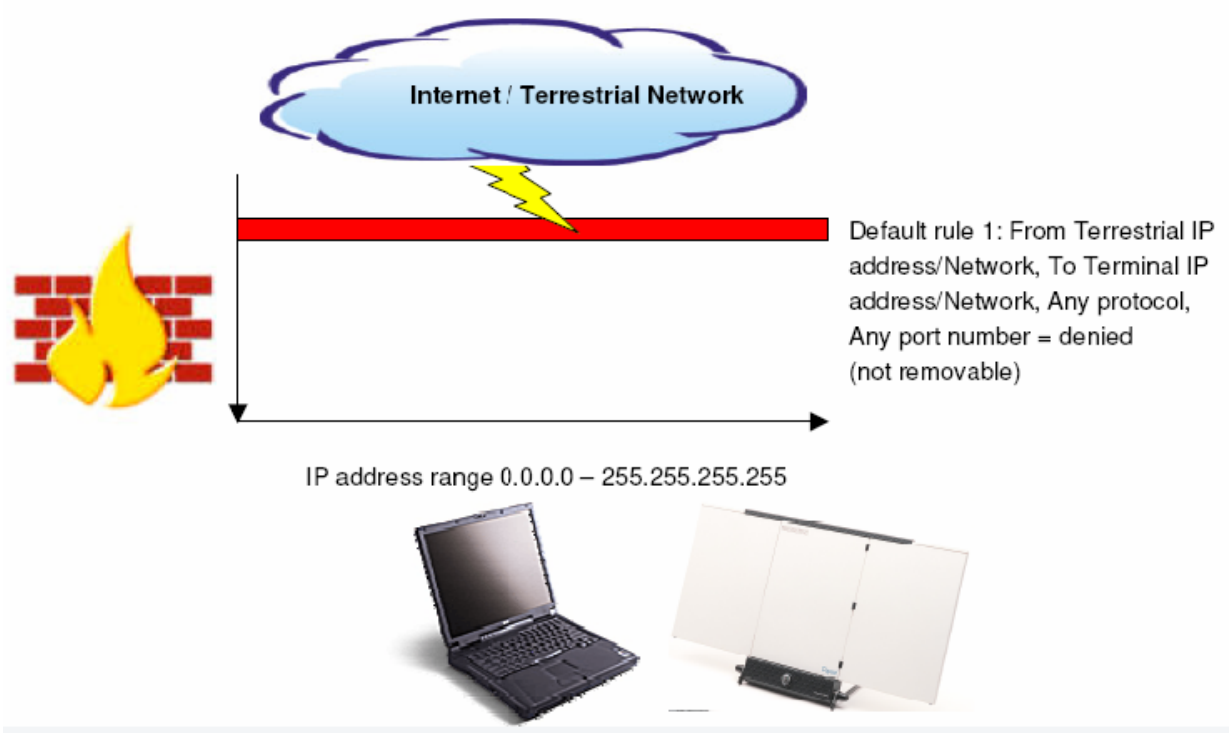


Figure 2: Default Rule 1

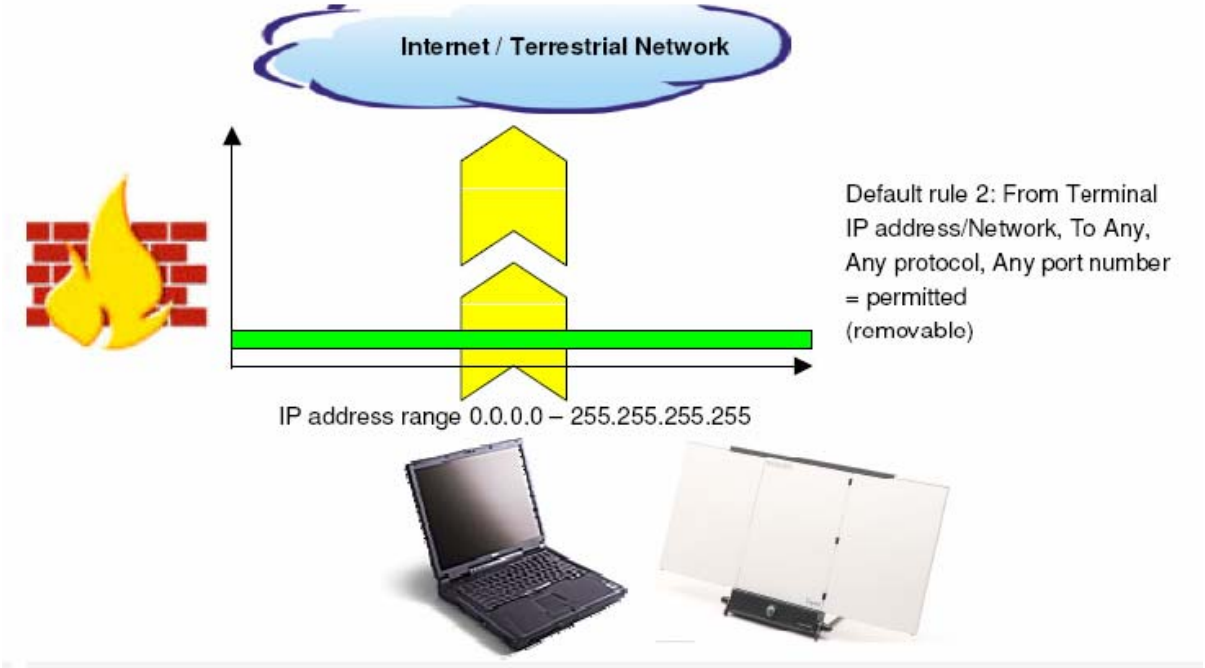


Figure 3: Default Rule 2

Understanding the Settings
The rules in the firewall specify which IP addresses and which upper layer communication protocols are permitted or denied.

- The FROM field specifies what the source (sender) of the traffic is.
- N/W BITS specifies the network mask by the number of (binary) ones in the mask. A network mask is used to indicate a range of IP addresses. See Table 1 for an example of a network mask to N/W bits conversion.

Table 1: Network Mask to Bits Conversion

Mask	Bits	Mask	Bits	Mask	Bits
255.255.0.0	16	255.255.248.0	21	255.255.255.192	26
255.255.128.0	17	255.255.252.0	22	255.255.255.224	27
255.255.192.0	18	255.255.254.0	23	255.255.255.240	28
255.255.224.0	19	255.255.255.0	24	255.255.255.248	29
255.255.240.0	20	255.255.255.128	25	255.255.255.252	30

- The TO field specifies what the destination (receiver) of the traffic is.
- PROTOCOL specifies ICMP, UDP, TCP, GRE, ESP (IPSEC), AH (IPSEC), SKIP or any.

Table 2: Used Protocols

ID	Name	Protocol
1	ICMP	Internet Control Message
6	TCP	Transmission Control
17	UDP	User Datagram
47	GRE	General Routing Encapsulation
50	ESP	Encapsulating Security Payload
51	AH	Authentication Header
57	SKIP	SKIP

- PORT NUMBER indicates the port number of the specified protocol. This specifies the application (such as FTP, HTTP, etc) See Chapter 7 for a overview of well-known protocol numbers and description.

Add Rules
A Firewall Rule can be added by clicking the ADD RULES button. This prompts for the following fields to be entered:

- From
  Terminal IP Address : IP Address of the mobile user
  Terrestrial IP Address : Any IP Address
  Terminal Network : Mobile LAN (MLAN) Address
  Terrestrial Network : Network Address.
  Any : Allows any IP Address / Network

- To
  Terminal IP Address : IP Address of the mobile user
  Terrestrial IP Address : Any IP Address
  Terminal Network : Mobile LAN (MLAN) Address
  Terrestrial Network : Network Address
  Any : Allows any IP Address / Network

- **N/W Bits:** NetWork Bits are required when a Terminal or Terrestrial Network is selected in the From or To field. It provides a range of IP addresses the firewall rule can apply to. (For example: 192.168.0.1 /16 means: allow any IP address between 192.168.0.1 and 192.168.255.255)

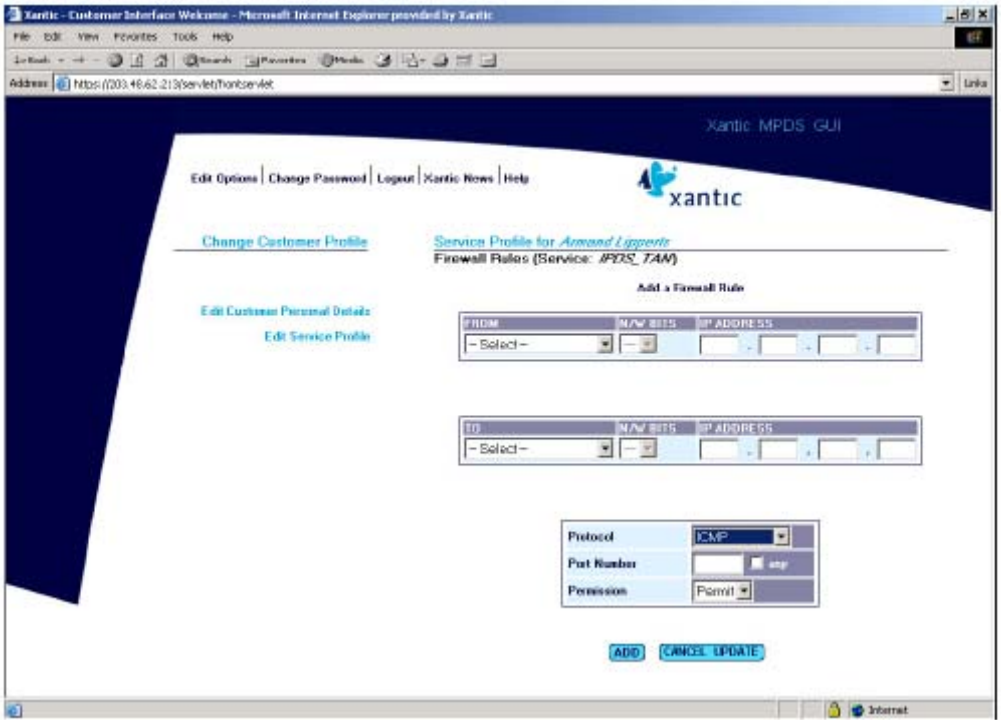
- **Protocol:** Select a protocol from the existing list. Listed protocols are: ICMP, UDP, TCP, GRE, ESP (IPSEC), AH (IPSEC), SKIP. If a Firewall Rule must apply for all protocols, “Any” must be selected.

- **Port Number:** This is a number identifying the port used by the network application. Some common ports are (See Chapter 7 for more commonly used ports):
  - o 21 : FTP
  - o 23 : Telnet
  - o 25 : Sending email (SMTP)
  - o 80 : HTTP or web traffic
  - o 110 : Retrieving email (POP3)
  - o 443 : HTTPS or secure web traffic

- **Permission:**
  Choose the permission for the rule (Permit / Deny).

  After entering all the fields, click on the ADD button. This adds the requisite customer firewall rule.

  Remember, all traffic that is not explicitly permitted via a rule, is denied (blocked).



Note: If you are adding a rule for the first time, you first need to delete the default Rule 2 (See Figure 6). The default rule can be deleted by ticking the box of the rule, and then clicking ‘Delete Rules’.

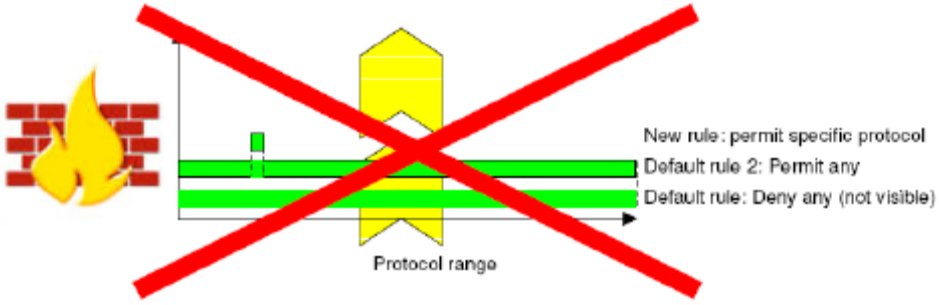
Delete Rules
Ticking the check boxes of the rule and clicking the DELETE RULES button can delete a firewall Rule.

Change Rules
To change a rule you must first delete the rule and then add a new rule (modifying a rule is not possible in this version of the MPDS Firewall Service). Remember that the order in which rules are placed is important because the new rule will be added at the bottom. In case a newly added rule is in conflict with a rule that is already there it will give the message: **“Rule not added. Clashes with the following rule”.**

Reset Firewall Rules
The user's Firewall Rules can be reset to the default rules by clicking the RESET TO DEFAULT RULES button.

Automatic Checking of the Firewall Rules
The MPDS Firewall Service automatically checks the firewall rules as set up by you to verify if the rule can be applied. The verification is based on the following logics:

1. If the default rule 2 is present then a rule allowing a specific protocol From the Terminal To for example Any is NOT allowed (To do that delete default rule 2 first).



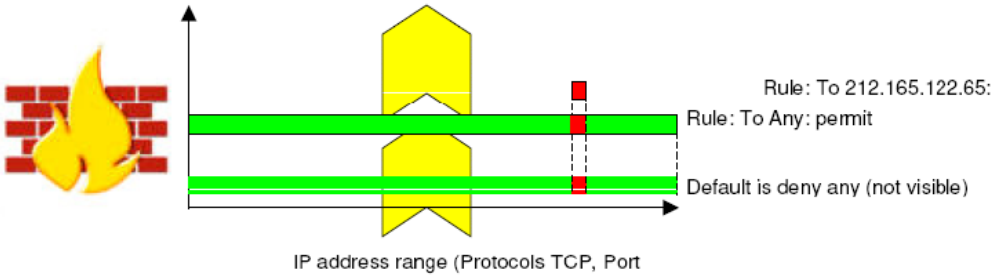
2. A rule denying From Terminal, To Terrestrial Network/IP address, for specific Port number, is ONLY allowed if there is a similar permit rule with destination To Any. An example:

   - Permit From Terminal IP address, To Any, Protocol TCP, Port number 80
   - Deny From Terminal IP address, To 212.165.122.65, Protocol TCP, Port number 80

   or

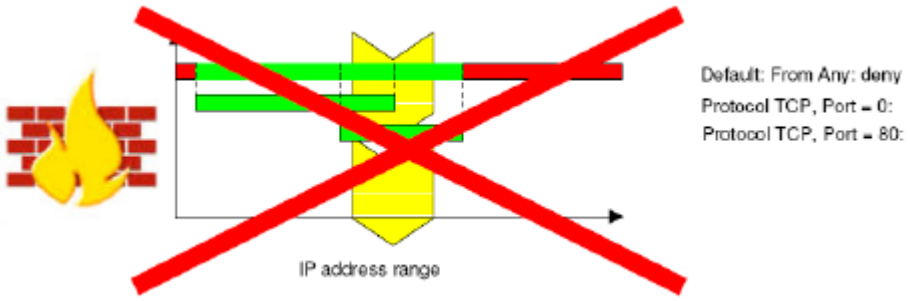
   - Permit From Terminal IP address, To Any, Protocol TCP, Port number 0 (any)
   - Deny From Terminal IP address, To 212.165.122.65, Protocol TCP, Port number 0

   See example below:



3. A rule denying a specific Port number To Any is not possible.

4. If a rule already exists permitting Port number = 0 (any) for a certain Protocol, then adding a new rule denying or permitting a specific Port number (for example 80) for this Protocol is not allowed when the IP addresses overlap. See example below.



5. If a rule already exists permitting a specific Port number (for example 80) for a certain Protocol, then adding a new rule denying or permitting any Port number for the same Protocol is not allowed when the IP addresses overlap

Table 3: Sample Applications

Common Name	Protocol	Application	Port Number
Web Browsing	TCP	HTTP	80
File Transfer (with FTP)	TCP	FTP	21
Secure Browsing	TCP	HTTPS/SSL	443
Telnet	TCP	Telnet	23
Sending E-mail	TCP	SMTP	25
Retrieving E-mail (I)	TCP	POP3	110
Retrieving E-mail (II)	TCP	IMAP4	143

Configuring PPP Parameter Settings

On click of CLICK HERE FOR PPP PARAMETERS button the PPP Parameters for the customer can be viewed,updated or reset.

PPP Parameters of the customer displays the values for:

- **Idle Timeout** - This defines the number of seconds with no network activity before the user's connection is closed. If this is set to zero the user will not be timed out.
- **Session Timeout** - This defined the maximum length in seconds of a connection. After this length of time the connection will be closed.
- **Maximum Transmission Unit (MTU)** - This defines the maximum size in bytes of the packets of information sent from the user's computer. This can effect performance of the connection but unless there is a very good reason it should not be changed from the default.

Important Note: Changing the MTU can have impact on the MPDS performance.

Updating PPP Parameters
The PPP parameters can be updated by modifying the values and clicking the UPDATE button.

Reset PPP Parameters
The PPP parameters can be reset to the default values by clicking the RESET TO DEFAULT VALUES button.

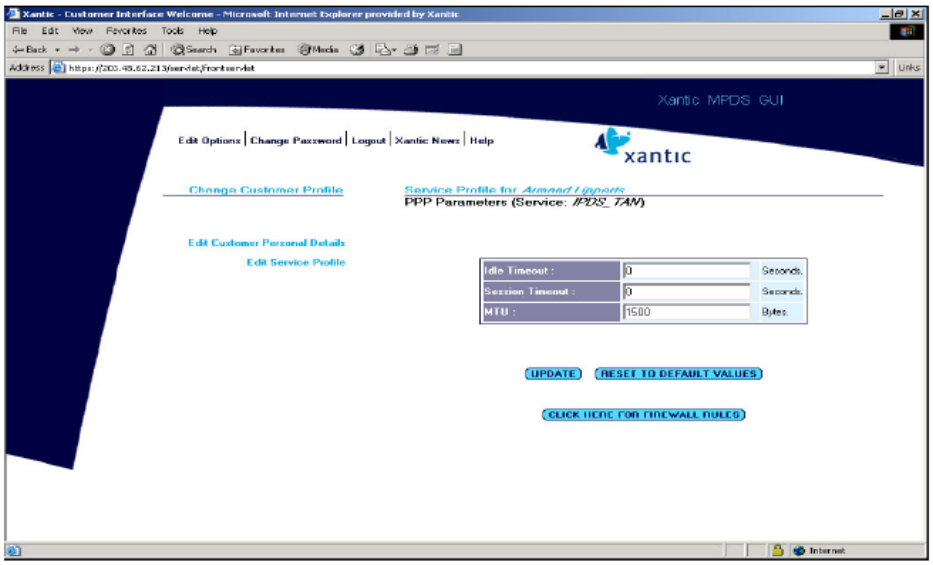


Figure 8: Default PPP Parameters Screen

4.2 Change Customer Password

In the menu on the top of your screen you have the option to change your password. The Password field excepts: 6 till 15 amount of characters, numbers (0 to 9), alphabets (a to z and A to Z), dot(.) and underscore (_).

The new password is active after clicking the UPDATE button.

4.3 Logout

You can select the Logout button in case you want to log out of the MPDS Firewall Service.
Automatic log out: If you have not used the MPDS Firewall Service for more than 20 minutes you will be automatically logged out. The following message will appear:
“You have been logged out because your session time has expired”.

4.4 Stratos News

When you click on Stratos News you will be redirected automatically to the Stratos homepage.

4.5 Help

This Help Page opens a new window and provides an explanation of the different options of the MPDS Firewall Service.

5 Remarks and recommendations

- To make a Firewall Rule change effective, you need to log off from the network (the user terminal, not only from the MPDS Firewall Service) and log on again.
- If you would deny yourself access to all websites, you can still access the MPDS Firewall Service website.
- You don't need to put the DNS (Domain Name Server) in the rules.
- Some applications such as Microsoft Internet Explorer can incur additional satellite airtime charges by repeatedly sending/receiving updates. You can install an additional firewall between your Terminal and Laptop to prevent your applications from sending unwanted traffic.
- A firewall doesn't protect you against viruses in emails and web pages. An up to date virus scanner is also recommended, as well as applying the latest fixes to your web browser and email program.
- To be able to use an IPSec VPN you must either:
- Have only the default rules in place or
- Put your VPN traffic in UDP ("NAT traversal") and allow this through.
- If you don't know the IP address(es) of a specific website or server, only the domain name (for example www.Stratos.net), you can use a Web based "nslookup" utility. Use http://www.zoneedit.com/lookup.html. to find the IP address(es). Notice that sometimes one name can have multiple IP addresses, and that the IP addresses sometimes change.
- A useful tool for calculating the IP network mask bit conversion can be downloaded from http://www.pkostov.de/ipcalc.html.

More information on MPDS can be found on www.stratosglobal.com.

Stratos Customer Services can be reached via:

Customer Care:
Tel: 1 800-563-2255 Toll free in N. America
Tel: 1 709-748-4226 Worldwide
Tel: + 800-1313-1313 Intl. Free Phone
Tel: 33# Toll free when dialed from handset

Fax: 1 877-748-4320 Toll free in N. America
Fax: 1 709-748-4320 Worldwide E-mail: support@stratosglobal.com

6 Sample settings

Before applying these settings, delete all the existing rules in your profile. It is important to enter the suggested rules in the given order.

- **Permit only e-mail:** permit only sending (SMTP) and retrieving of email (POP3 and IMAP4) to and from a mail server.

From	N/W bits	IP Address	To	N/W bits	IP Address	Protocol	Port Number	Permission
Terminal IP Address	-		Terrestrial IP Address	-	212.165.122.65	TCP	25	Permit
Terminal IP Address	-		Terrestrial IP Address	-	212.165.122.65	TCP	110	Permit
Terminal IP Address	-		Terrestrial IP Address	-	212.165.122.65	TCP	143	Permit

- **Permit only access to your network and your web site:** permit unlimited access to your intranet (10.1.0.0; 255.255.0.0) and browsing to your company website on 213.244.173.52, and nothing else.

From	N/W bits	IP Address	To	N/W bits	IP Address	Protocol	Port Number	Permission
Terminal IP Address	-		Terrestrial IP Network	16	10.1.0.0	Any	Any	Permit
Terminal IP Address	-		Terrestrial IP Address	-	213.244.173.52	TCP	80	Permit

7 Port-numbers

In TCP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Port numbers range from 0 to 65536, but only ports numbers 0 to 1024 are reserved for privileged services and designated as well-known ports. This list of well-known port numbers specifies the port used by the server process as its contact port.
Reference: http://www.webopedia.com/quick_ref/portnumbers.asp

Port	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP – Data
21	FTP - Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	Whois
49	Login Host Protocol (Login)
53	Domain Name System (DNS
69	Trivial File Transfer Protocol (TFTP)

Port	Description
70	Gopher Services
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP

Port	Description
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

About Stratos
Stratos is the world's trusted leader for vital communications. With more than a century of service, Stratos offers the most powerful and extensive portfolio of remote communications solutions including mobile and fixed satellite and microwave services. More than 20,000 customers use Stratos products and industry-leading value-added services to optimize communications performance. Stratos serves U.S. and international government, military, first responder, NGO, oil and gas, industrial, maritime, aeronautical, enterprise, and media users on seven continents and across the world's oceans. For more information visit www.stratosglobal.com.

For more information please contact Stratos:
Toll Free (N. America): 1 800 563 2255
Worldwide: +1 709 748 4226
TTY: +1 709 748 4884
Fax (Worldwide): +1 709 748 4320
E-mail: info@stratosglobal.com
Web Site: www.stratosglobal.com

STRATOS®
BEYOND THE HORIZON®