

**GNAT** *Box*®

**SYSTEM  
SOFTWARE  
VERSION 3.3**

**Console Interface  
User's Guide**



**Global  
Technology  
Associates, Inc.**

## Copyright

© 1996-2002, Global Technology Associates, Incorporated (GTA). All rights reserved.

GTA acknowledges all trademarks appearing in this document. This product includes software developed by the University of California, Berkeley and its contributors. Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

### Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

### Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated. RoBoX is a trademark of Global Technology Associates, Incorporated. Netscape Navigator is a trademark of Netscape Communications Corporation. Internet Explorer is a trademark of Microsoft Corporation. Cerberian is a trademark of Cerberian, Inc. CyberNOT and SurfControl are trademarks of SurfControl, plc, and may be registered in certain jurisdictions. MAPS is a service mark of Mail Abuse Prevention System, LLC. WELF and WebTrends are trademarks of NetIQ.

All other products are trademarks of their respective companies.

### Technical Support

GTA includes 30 days installation support from the day you receive the initial shipment. GTA's direct customers in the USA should call or email GTA via the contact information listed below. Other customers should contact their local GTA authorized reseller.

### Contact Information

Global Technology Associates, Inc.  
3505 Lake Lynda Drive, Suite 109  
Orlando, FL 32817 USA

Main: +1.407.380.0220

Fax: +1.407.380.6080

Web: [www.gta.com](http://www.gta.com)

Email: [info@gta.com](mailto:info@gta.com)

Support: +1.407.482.6925

Email : [support@gta.com](mailto:support@gta.com)

### Document Information

GNAT Box System Software Version 3.3, Console Interface

October 2002

# Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	<b>About this Guide</b> .....	1
	Documentation .....	1
	<b>User Interface</b> .....	3
	Exclusive Features .....	3
	Console Access .....	3
	Console Interfaces .....	4
	Navigation .....	7
<b>2</b>	<b>CONFIG MENU</b>	<b>9</b>
	<b>Configuration Verification</b> .....	9
	<b>Reset to Factory Defaults</b> .....	10
<b>3</b>	<b>BASIC CONFIGURATION</b>	<b>13</b>
	<b>Preferences (Contact Information)</b> .....	13
	<b>DNS</b> .....	14
	DNS Proxy .....	14
	<b>Keyboard Layout</b> .....	15
	<b>Features</b> .....	16
	<b>PPP</b> .....	17
	PPPoE .....	17
	<b>Network Information</b> .....	19
<b>4</b>	<b>SERVICES</b>	<b>23</b>
	<b>Email Proxy</b> .....	23
	<b>Remote Logging</b> .....	25
<b>5</b>	<b>ROUTING</b>	<b>27</b>
	<b>RIP</b> .....	27
	<b>Static Routes</b> .....	29
<b>6</b>	<b>OBJECTS</b>	<b>31</b>
	<b>Address Objects</b> .....	31
	Creating Address Objects .....	32
	Default Address Objects .....	32
	<b>VPN Objects</b> .....	33
	Default VPN Objects .....	33
<b>7</b>	<b>FILTERS</b>	<b>37</b>
	<b>Outbound Filters</b> .....	37
	<b>Remote Access Filters</b> .....	40
	<b>Preferences</b> .....	40
	<b>Protocols</b> .....	43
	<b>Services</b> .....	44

<b>8</b>	<b>NAT</b>	<b>47</b>
	Aliases .....	47
	Inbound Tunnels .....	48
	Static Address Mapping .....	50
	Timeouts .....	51
<b>9</b>	<b>IP PASS THROUGH</b>	<b>53</b>
	IP Pass Through Filters .....	54
	Hosts/Networks .....	55
<b>10</b>	<b>AUTHORIZATION</b>	<b>57</b>
	Admin Accounts .....	57
	Content Filtering Preferences .....	58
	Proxy .....	59
	New SSL Certificate .....	61
	Remote Administration .....	61
	WWW Administration .....	62
	RMC (GBAdmin) .....	63
	VPNs .....	64
<b>11</b>	<b>ADMIN MENU</b>	<b>67</b>
	Archive .....	67
	Backup .....	68
	Restore .....	68
	Current Statistics .....	68
	Flush ARP Table .....	70
	Halt .....	70
	Interfaces .....	71
	Ping .....	71
	Reboot .....	72
	Set Date/Time .....	72
	Trace Route .....	73
<b>12</b>	<b>REPORTS</b>	<b>75</b>
	Configuration .....	75
	Email Configuration .....	76
	Hardware .....	77
	View Log Messages .....	78
	<b>INDEX</b>	<b>79</b>

# 1 Introduction

GTA Firewalls and GNAT Box System Software include two primary user interfaces: the platform-independent Web interface and Windows-only GBAdmin. A third user interface, the Console, allow the user to default filters in case of a configuration error; recover a GTA Firewall; reset a misconfigured firewall to defaults; and perform basic configuration tasks.

The Console interface is a GUI-based interface of hierarchical menus. It operates only on the GTA Firewall console; it cannot be accessed in any other way.

The Console interface has limited functions on a GB-Pro and GB-100 due to the increasing number of features offered in the software and the space limitations on floppy disks. For a list of these limited functions, see the User Interface section.

---

## About this Guide

This guide includes Console interface instructions, basic configuration options, description of fields and administrative tools. For instructions on how to use GBAdmin and the Web interface, as well as troubleshooting and relevant appendices, see the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**. For installation and product-specific questions, see product and feature guides.

The configuration and administration chapters after the Introduction describe each function in the order that they appear on the Console interface. After a brief explanation, there will be a table of field descriptions and illustrations.

Navigation, common keystrokes, menu items and buttons are explained in the User Interface section of this introduction.

## Documentation

For GNAT Box System Software version 3.3, the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** has been streamlined, with some information moving to the Installation CD and to the Web at [www.gta.com](http://www.gta.com). Look in your firewall's Product Guide for instructions on installation, registration and setup in default configuration; look in the Feature Guides for instructions on setting up GTA's optional features.

---

## Documentation Conventions

---

Typeface	Convention
SMALL CAPS	Field names.
<b>BOLD SMALL CAPS</b>	Names of publications.
<b><i>Bold Italics</i></b>	Emphasis.
Courier	Screen text.
<brackets>	Names of keyboard keys, e.g., <Return>, <F12>.

---

### Notes

are indicated by an indented, italicized headline and one rule line.

### “How to” sections

are indicated by an indented, bold headline and two rule lines.

---



---

## Documentation Map

---

Topic	Document Name	Location
Installation	Product Guides	Shipped w/product*
System Setup	Product Guides	Shipped w/product*
GNAT Box Concepts	Concepts	gta.com
Troubleshooting	User's Guide or Product Guides	Shipped w/product, CD*
Configuration examples	–	gta.com
Sample reports	–	gta.com
Ports & Services	User's Guide	Shipped w/product, CD*
Drivers & NICs (Pro, Flash)	Product Guides	Shipped w/product*
GTA Firewalls	Product Guides	Shipped w/product*
Content Filtering	Surf Sentinel Feature Guide	Shipped w/product*
High Availability	H <sub>2</sub> A Feature Guide	Shipped w/product*
VPN	GB-VPN Feature Guide	Shipped w/product*
VPN Examples	GB-VPN to VPN Tech Docs	gta.com
GBAdmin interface	User's Guide	Shipped w/product, CD*
GBAdmin Help	GBAdmin Online Help	Shipped w/product, CD*
Web interface	User's Guide	Shipped w/product, CD*
Console interface	Console Interface Tech Doc	gta.com

\* All documents for registered products can also be found on the [www.gta.com](http://www.gta.com) website.

Online and support documents are either in plain text (\*.txt), email, Microsoft Word format (\*.doc) or Adobe® Acrobat® Portable Document Format (PDF; \*.pdf) which requires Acrobat Reader 5.0 for viewing and downloading. A free copy of Acrobat Reader can be obtained at [www.adobe.com](http://www.adobe.com).

---

# User Interface

The Console interface is a GUI-based interface of hierarchical menus. As the name implies, the Console interface only operates on the GTA Firewall console; you can access it directly using the Video Console with a keyboard and monitor attached to your GTA Firewall (excluding RoBoX); or via the Serial Console on a workstation attached to the firewall through the serial port and using a terminal emulator such as TeraTerm.

The Console interface can be used to perform most configuration tasks, although it is best suited for initial configuration and administrative tasks when the other remote user interfaces (Web or GBAdmin) are not available.

## Note

Configuration data is read by the Console interface only once a session, when the administrator logs on. This means that if the configuration is modified via the Web interface or GBAdmin during a Console session, the new data will not appear on the Console interface, and subsequent changes made using Console will overwrite the changes made remotely.

## Exclusive Features

- Physical access control (one access point) when used as the only access to the firewall.
- Basic interface for routine configuration tasks.
- Reset capability.
- Fail-safe access to firewall.

## Console Access

The Console interface is always available on the GTA Firewall; access cannot be disabled. The Console interface is accessible using the serial port and a serial cable, whether in a direct video connection or using an emulator. See Product Guides for more information about connecting to the GTA Firewall.

## Characteristics

- Console interface changes take place when items are saved.
- Configuration data is read only at login.
- Blanking out data fields will delete information when items are saved.
- The factory set User ID and Password are both “gnatbox.”

## Console Interfaces

The two versions of the full Console interface, Video and Serial, use different methods to access the GTA Firewall and use different keystrokes. The Limited Video Console is a version of the Video Console with fewer functions.

### Serial Console

The Serial Console is available on GB-1000 and RoBoX, and as an installation option on the GB-Flash. Serial Console uses a terminal emulator such as TeraTerm on a workstation to connect to a GTA Firewall via the serial port.

To use the Serial Console, connect the GTA Firewall to a PC workstation using the serial port and boot up the firewall. Create a new connection by selecting the appropriate COM Port; setting the desired and available Terminal ID; and setting these parameters: Baud Rate = 38400; Data = 8 bit; Parity = None; Stop = 1 bit; Flow Control = none. Enter “gmatbox” for the user ID and password if logging on for the first time. If using TeraTerm, select the terminal type; your terminal emulator may vary. The configuration menu should appear.

Use the keystroke guide below for TeraTerm with a generic VT100 keymap; for other emulators, refer to the emulator documentation for key locations. To change TeraTerm's key map, see TeraTerm's Help menu.

---

#### Serial Console Keystroke Guide

---

Function	Keystroke
Cancel changes	<Esc> (twice)
Clear next space	<Space Bar>
Clear previous space	<Backspace>
Next field	<Tab> (in use order)
Next/previous field	Up & Down Arrow Keys
Next/previous space	Left & Right Arrow Keys
Delete line item	<Delete> <D>
Toggle field choices	<Space Bar>
Insert line item	<I> (the letter I key)
Select screen button	<Space Bar> <Return> (Enter)
Select/edit line item	<Return> (Enter)

---



```

Global Technology Associates, Inc.                GB-1000 3.3.0s
Config      Auth      Admin      Reports      Exit      Help
-----
Configuration Verification...
-----
Basic Configuration...
Services...
Routing...
Objects...
Filters...
NAT...
IP Pass Through...
-----
Reset To Factory Defaults...
-----
Check your GNAT Box software configuration for errors.

```

*Console Interface, TeraTerm*

## Video Console

The full Video Console, previously called the standard console, is available as an installation option on the GB-Flash. A limited Video Console version is installed with GB-Pro, GB-100, GNAT Box Light and GNAT Box Demo.

Three virtual modes operate on the Video Console: log messages, main interface and statistics. View log messages on the Video Console by pressing <ALT><F1>. Switch to the main Console interface by pressing <ALT><F2>. See firewall statistics by pressing <ALT><F3>. These keys are always active.

The Video Console will start automatically when the GTA Firewall is booted up with an attached keyboard and monitor. The configuration menu (similar to the Serial Console screen) should appear; if not, press <ALT><F2>. Enter “gnatbox” for the user ID and password if logging on for the first time. Use the keystroke guide below for navigation and data entry.

---

### Video Console Keystroke Guide

---

Exit/Abort	<Esc>
Clear field	<F6>
Previous field	<F7>
Next field	<F8> or <Tab>
OK/Save	<F10>
Delete/Backspace	<Del> or <Backspace>
Toggle choice list	<Space Bar>
Display choice list	<F2>
Toggle color display	<F12>
Insert	<Insert Key>
Select a button	<Space Bar>

---

The interface was designed for use with a color display, but will also operate on grayscale and TTL displays. The function key <F12> will toggle the display mode between color and black & white.

## Limited Video Console

The GB-Pro, GB-100, GNAT Box Light and GNAT Box Demo utilize a limited console that contains only the functions necessary for basic configuration and reset. The Video Console had to be reduced on these platforms due to the difficulty of fitting the increasing number of GNAT Box System Software features on one floppy disk. For a list of items on the Limited Video Console, see the items emphasized in the Console functions list below.

---

## Console Menu Items

---

### **Config Menu**

#### **Configuration Verification**

#### **Basic Configuration**

#### **Preferences (Contact Information)**

DNS

#### **Keyboard Layout**

#### **Features**

PPP

#### **Network Information**

Services

Email Proxy

Remote Logging

Routing

RIP

Static Routes

Objects

Address Objects

VPN Objects

#### **Filters**

#### **Outbound Filters**

#### **Remote Access Filters**

Preferences

Protocols

Services

NAT

Aliases

Inbound Tunnels

Static Address Mapping

Timeouts

IP Pass Through

Filters

Hosts/Networks

#### **Reset to Factory Defaults**

#### **Authorization**

#### **Admin Accounts**

Content Filtering Preferences

New SSL Certificate

#### **Remote Administration**

VPNs

#### **Admin Menu**

#### **Archive**

#### **Backup**

#### **Restore**

#### **Current Statistics – also, press <Alt><3>**

Flush ARP Table

Halt

#### **Interfaces**

#### **Ping**

Reboot

#### **Set Date/Time**

#### **Trace Route**

#### **Reports**

#### **Configuration**

#### **Email Configuration**

#### **Hardware**

#### **View Log Messages – or press <Alt><1>**

---

**Emphasized items are on the Limited Video Console.**

## Navigation

All Console interface variations use the following menus, buttons, fields and lists in navigation.

### Menu

There are six top-level menus in the Console interface: Config, Auth, Admin, Reports, Exit and Help. The Exit menu item has only the exit function; Help contains information about the GNAT Box System Software version number and software licensing agreement.

Most configuration items are found under the Config menu. The Auth menu contains most functions for access definitions; Admin allows the user to perform various basic administrative tasks; reporting functions available on the Console are in the Reports menu. More reports and lists are available on the Web interface and GBAdmin.

Use the keyboard arrow keys to move through the menus and press the <Return> key to select the function currently highlighted.

Under the menus and functions, a small help system gives the user basic directions for each function using the Video Console; refer to the Serial Console keystroke guide for directions on working with a serial interface and a VT100 terminal emulator, or to the documentation for your terminal emulator.

### Buttons

Buttons, when referred to in the Console interface documentation, refer to fields which appear similar to Web and GBAdmin buttons; these Console button fields can be selected by pressing <Return> when the field is selected.

---

#### Console Buttons

---

Save	Save the section to the running firewall.
Cancel	Cancel changes and exit the screen or section.
OK	Exit the screen, or execute administrative action.
Default	Create configuration settings in the section that conform to the settings on the firewall; <b>not</b> factory settings.
Send	Send email.

---

[ SAVE ]

*Save Button*

[ CANCEL ]

*Cancel Button*

[ OK ]

*OK Button*

[ DEFAULT ]

*Default Button*

[ SEND ]

*Send Button*

## Entry, Choice, Check, and Item List Fields

Fields in the Console interface can be data or data entry fields, choice/selection fields, check fields and item list fields.

Data fields are represented by either a blank line \_\_\_\_\_ or a line with a default or placeholder entry 0.0.0.0/24 as a data format example. Some fields are pre-filled by the system and will be unavailable for data entry.

Choice fields offer the user a number of items from which to select the desired entry; scroll through the selections by pressing the <Space Bar>.

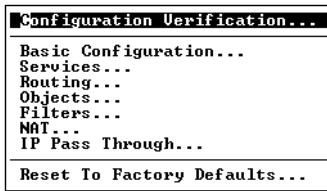
Check fields are either enabled [X] or disabled [ ]. Use the <Space Bar> key to toggle a check field.

Item List fields represent the items that have been entered in sections with more than one item. See the edit screen for these by pressing <Return>.

## 2 Config Menu

The Config Menu contains commands related to the setup and configuration of the GTA Firewall system. Some items in the Config Menu and its sub-menus are optional and need not be completed.

This section contains the two independent functions in the Config Menu: Configuration Verification and Reset to Factory Defaults.



*Config Menu*

---

## Configuration Verification

Configuration Verification will run a system configuration check of the GTA Firewall. The check will verify the following functional areas: IP addresses, netmasks, interface assignment, filters, tunnels, PPP/PPPoE and Static Address Mapping.

After you have configured your GTA Firewall, run a configuration verification to ensure that you have a valid configuration. Run a check each time after making changes to the system.

Verification happens every time a section or configuration is saved. These automatic verification checks will prompt the administrator to change the section if there is an error.

Verify Configuration at the bottom of the menu in the Web interface. Verify Configuration is the last item in the Reports section in GBAdmin.

```

Basic Configuration
DNS
Features
Network Information
PPP
  WARNING: PPP1. No user id.
  WARNING: PPP1. No password.
  WARNING: PPP1. No phone number.
Preferences
  WARNING: Administrator's email address is missing.
Services
DHCP Server
DNS Server
  WARNING: Domain "gta.com", mail exchanger "postserver.gta.com" not found.
Email Proxy
Enterprise Server
High Availability
Network Time Service
Remote Logging
SNMP
Authorization
Admin Accounts

Use <PAGE-UP> and <PAGE-DOWN> keys to move or <ESC> to quit.

```

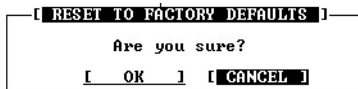
*Configuration Verification Example*

## Reset to Factory Defaults

Reset to Factory Defaults will reset all GTA Firewall configuration parameters back to their original factory settings. This function is exclusive to the Console interface for ultimate security.

Once you have used Reset to Factory Defaults, you must configure your firewall again. See your Product Guide for information on initially configuring your firewall.

When the menu item is selected, a pop-up window is displayed which requests confirmation of the reset request. Select the OK button and then press <Return> to reset.



*Reset to Factory Defaults*

### Why Reset?

The Reset to Factory Defaults option is used when all other options to rectify the configuration are exhausted, or when an old configuration is no longer useful, e.g., a mis-configuration locks out access to the firewall, or an existing firewall is inserted into a new system configuration.

If the Administrator user name and/or password (Auth/Admin Accounts, Index 1) are irretrievably lost, you will have to perform a disaster recovery installation, re-entering all configuration information. You will only be able to use a back up configuration with a valid user name and password. This can be the Administrator user name and password

### ***Caution***

---

Don't use the Reset to Factory Defaults option until all other options have been exhausted. Using Reset to Factory Defaults will permanently erase all modified configuration information from the system!

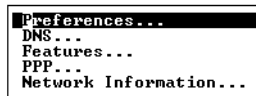




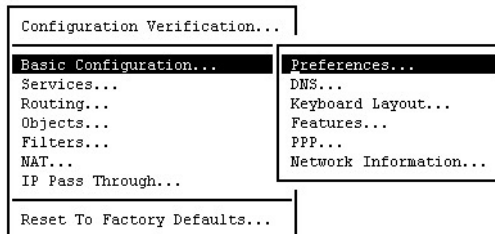
## 3 Basic Configuration

Basic Configuration contains functions that address basic GTA Firewall setup and configuration. Not all GTA Firewall configurations require all functions, so some sections may not be relevant to your configuration.

This chapter is organized in order of a function's appearance on the menu in the Console interface. After a brief explanation of the function, there will be a table of field descriptions and screen illustrations from the Serial Console run using the TeraTerm terminal emulator supplied with system software.



*Basic Configuration Menu (Serial)*



*Basic Configuration Menu (Video)*

## Preferences (Contact Information)

The Preferences facility stores information about the firewall administrator and the GTA Firewall, including contact information and serial number. This information is used by email, report and list functions. The serial number must be entered in order to use the GTA Firewall, and before activation codes will work. The serial number is pre-installed on hardware appliances.

## Preferences Fields

Administrator Contact Information	
Name	Primary contact name.
Company	The company or organization name.
Email address	The email address of the contact.
Phone number	The phone number of the contact.
Serial number	The GTA Firewall serial number, which can be found: on the shipping box that came with your software and User's Guide and on the license (activation code) certificate.
Support email	Email support address, supplied by GTA or your Authorized GTA Firewall Reseller.
Default character set	(Web Only) If the default character set is not correct, select the appropriate character set.

**[ ADMINISTRATOR CONTACT INFORMATION ]**

Name: Mary Tester

Company: ACME

Email address: mtester@gta.com

Phone number: 407-380-0220

Serial number: XXXXXXXX36

Support email address: gfb-config@gta.com

**[ SAVE ] [ CANCEL ]**

*Preferences (Contact Information)*

## DNS

The DNS (Domain Name System) function is used by the networks behind the GTA Firewall to resolve host names into IP addresses. The DNS function is used to specify the IP addresses of internal and external DNS, and to enable DNS Proxy and specify which hosts on the network will be allowed to use it.

Use an internal DNS server if one is available; use a DNS server from outside your network, e.g., a name server accessed through your ISP, as your external DNS server.

## DNS Proxy

DNS Proxy is enabled by default, except when upgrading from a software version that does not have DNS Proxy. A Remote Access Filter to allow DNS proxy replies is also enabled, except when upgrading from a version previous

to 3.3. DNS proxy specifies which hosts on a network will use the firewall as a DNS proxy. The hosts will be represented either by an IP address or an Address Object. The DNS proxy sends a request to all available DNS servers (those listed and those acquired dynamically) to resolve a host name. The first reply will be sent to the requestor.

## DNS Fields

Primary Domain Name	The primary domain name used for the network, e.g., gta.com.
External name server	Check to enable an external name server.
IP address	Enter the IP address of an external DNS server.
Internal name server	Check to enable an internal DNS.
IP address	IP address of an internal DNS server.
DNS Proxy	Check to enable DNS Proxy.
Hosts allowed to use	Select the object that represents the hosts that will use the proxy.
IP address	If Use IP address was selected in the previous field, enter the selected IP address and netmask.

## Note

Enabling DNS Server (in the Services section) will override DNS Proxy.

```

[ DOMAIN NAME SERVER <DNS> INFORMATION ]
[ ] External NS: 0.0.0.0      0.0.0.0
[ ] Internal NS: 0.0.0.0    0.0.0.0
Domain name: gta.com
[ DNS Proxy ]
Enable: [ ]
Allowed: Protected Networks
[ SAVE ] [ CANCEL ]

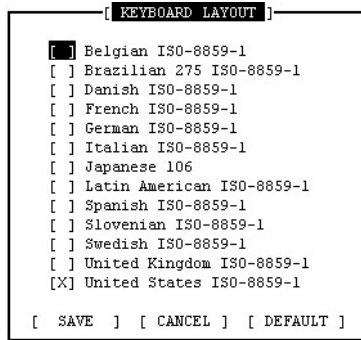
```

DNS

## Keyboard Layout

The Keyboard Layout item is only used on the Video Console (previously known as the standard console), which is accessed using a monitor and keyboard. Keyboard Layout allows the administrator to select a localized keyboard layout for operations on the console. This facility only provides a

means to map the standard ASCII characters to their correct locations on the keyboard; it does not enable support for localized characters, such as Japanese Kanji and Swedish characters.



*Keyboard Layout (Video only)*

## Features

In Features, the administrator enters GTA Firewall software and optional feature activation codes for options such as H<sub>2</sub>A, Surf Sentinel, Multi-Interface and VPN Client in Features. System activation codes entered during installation or pre-installed with hardware appliances will also appear. Activation codes will not function without the system serial number entered in the Preferences screen. Hardware appliances have this number pre-installed.

Enter GTA Firewall activation codes (hexadecimal characters only – 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) provided with software or feature registration. Select Save. The system will display a description of what has been activated. If this description does not appear, the code has either been entered incorrectly or is not correct for the current system or version. Up to twenty (20) activation codes may be entered in the Features screen.

If you would like to revert to the previously saved codes, select Cancel to *before* saving. Once you have selected Save, you cannot revert to saved codes.

---

# PPP

In the Console interface, only the first (PPP0) of the five available PPP (Point-to-Point Protocol) and PPPoE (PPP over Ethernet) connections may be configured. *After* creating the configuration in the PPP section, enable the PPP/PPPoE connection in the Network Information section by associating the configuration with the chosen logical interface.

The fields will vary depending on whether standard PPP or PPPoE is selected. Some PPPoE options are not used by standard PPP, therefore they will be absent when PPP is selected. PPP has fields not found in PPPoE; these fields are indicated in the fields table by “\*” (one asterisk).

## Note

The five PPP/PPPoE connections are named PPP0, PPP1, PPP2, PPP3, PPP4, in list order. If you delete a configuration in the PPP section, each of the remaining configurations will be renamed to maintain the list order. Therefore, any logical interface which references a connection with a renamed designation will have to be changed to reflect the new name.

# PPPoE

PPPoE has become widely deployed as a method of assigning IP addresses for DSL service providers. Some standard PPP options are not used by PPPoE, therefore they will be absent from the configuration screen when PPPoE is selected. PPPoE has a few fields not found in PPP; these are indicated in the fields table by “\*\*” (two asterisks). GNAT Box System Software automatically detects connection preferences so that the user is no longer required to enter chat or dial scripts, select CHAP or PAP, or set parity and flow control.

## How to Enable PPP in Network Information

After completing the PPP or PPPoE configuration in the PPP section, go to the Network Interface section and select the NIC number (PPP0, 1, 2, 3, or 4) on the logical interface for the External Network interface you have selected for the PPP connection. Next, select the logical interface as the Gateway. Once these have been selected, the system will dynamically negotiate the IP address of the Gateway. The DHCP selection will be unavailable.

---

---

## PPP/PPPoE Fields

---

Connection Type	<p><b>Dedicated</b> Establishes a link when the firewall boots up. The link will remain until the interface is manually disabled, or the system is halted. Use "Dedicated" to test a configuration.</p> <p><b>On-demand</b> Establishes a link with the remote site when a packet destined for the External Network arrives on a Protected or PSN. A link remains as long as packets are received.</p> <p><b>On-enabled</b> When the External Network interface is manually enabled, this connection type establishes a link with the remote site. The link will stay established until disabled. Interfaces can be disabled in Admin &gt; Interfaces.</p>
PPPoE	Enable to create a PPPoE connection.
NIC**	Network interface on which PPPoE will run.
PPPoE Provider**	Designation for the PPPoE Provider. Leave this field blank if you do not know the <b>exact</b> designation; the value is not required for the connection, and an incorrect setting can prevent the connection.
COM Port*	Select the COM Port used for the PPP interface. COM 1-4 are allowed on GB-Pro and GB-Flash. The GB-1000 is set to COM 2, and the RoBoX to COM 1.
Phone Number*	The number used to dial the remote site. This field should contain any required access codes, e.g., "9" to dial out. Characters used for pauses and secondary dial tones can be used. Consult your modem or ISDN TA manual for dialing codes.
User Name	User ID and password for remote PPP/PPPoE access.
Password	The password is obscured in the data entry field.
Local IP address	A PPP/PPPoE link uses a local and remote IP address.
Remote IP address	If the remote site supports <b>dynamic</b> address assignment (as for most ISPs and remote sites), leave the local address set to 0.0.0.0. Set the remote address to an IP address on the remote network; PPP will negotiate the actual value. If the Remote IP address is <b>static (dedicated)</b> , enter the address and leave the Local IP address set to 0.0.0.0. If <b>both addresses are static</b> , set both fields to the appropriate IP address.
Connection time out	Number of seconds during which a connection will stay connected when inactive. The default is 600 (10 minutes). To prevent timing out, enter "0."

\* PPP screens only.

\*\* PPPoE screens only.

```

[ PPP CONFIGURATION ]
Connection type: Dedicated
Use PPPoE: [X]
NIC: fxp3
Provider: _____

User name: _____
Password: _____

Local IP number: Default      Negotiated
                  0.0.0.0      0.0.0.0
Remote IP number: 0.0.0.0      0.0.0.0

Connection time out: 600 seconds

[ SAVE ] [ CANCEL ]

```

*PPPoE*

## Network Information

Much of the Network Information data will have been entered during installation, including the required Protected Network and External Network.

### Warning

Use caution when changing the logical names of interfaces; if a logical name does not match a filter, you may lose access to the firewall.

### Network Information Fields

Name	The Logical Name of the Interface.
Type	Interface type: Protected, External and PSN.
IP address	All active network interfaces that do not use PPP/PPPoE or DHCP configurations require an IP address and netmask. If a netmask is not entered, the system will attempt to create one based on the network class: Class C = /24, Class B = /16, Class A = /8. This helps to prevent mis-configuration.
NIC (& PPP/PPPoE)	Network Interface, including PPP/PPPoE. The GTA Firewall requires two network interfaces, a Protected and an External. Select the device to associate with the logical name. The field contains a list of all devices present on the GTA Firewall, including PPP/PPPoE configurations. To configure PPP or PPPoE, first configure a PPP or PPPoE connection, then select the connection configured – PPP0, 1, 2, 3 or 4 – in this field.

*Network Information Fields cont'd...*

Host Name	The system name assigned to the GTA Firewall and used to tag log messages. It is not a DNS host name. If your network DHCP servers make IP address assignments based on the system name, enter the host name, often assigned by an ISP.
Default Gateway (Route)	On a static interface, enter the IP address of the selected default route. This value is usually the IP address of the router connecting the network to the Internet and must be on the same logical network as the associated External interface, except when using PPP/PPPoE. The gateway value will be set automatically if it is on a dynamically negotiated interface. When the interface is static, the IP address must be entered in the DEFAULT GATEWAY field.

NETWORK INFORMATION

Name	Type	IP address/Netmask	NIC
1 EXTERNAL	EXT	192.168.71.84/24	fxp1 ^
2 PROTECTED	PRO	10.10.1.84/24	fxp0
3	EXT		fxp2
4	EXT		fxp3
5	EXT		PPP0
6	EXT		PPP1
			v

Host name: doc1000.gta.com  
Default route: 10.10.1.1

[ SAVE ] [ CANCEL ]

*Network Information***How to Use CIDR-based or Slash (/) Notation**

Calculate a CIDR-based notation netmask by converting the dotted decimal netmask to binary and count the ones. For a Class C network, the dotted decimal netmask is: 255.255.255.0. The binary notation is: 11111111.11111111.11111111.00000000. There are 24 ones, so the notation would be "/24". Using a 255.255.255.240 netmask, the binary representation would be: 11111111.11111111.11111111.11110000. The notation would be "/28".

You may also enter a host address which is defined by not including a mask; e.g., 192.168.123.1. (Equivalent to /32.) To enter a range of addresses, use a hyphen (-) between the two extremes of the range; e.g., 192.168.123.0-192.168.123.255

Dotted decimal can be used by entering a forward slash and then the dotted decimal netmask.



---

## Network Information Add/Edit Fields

---

Name	Assign a logical name to suit company convention. Interface Object names may not use a number as the first character. See Warning Note, above.
Gateway (Web and Console)	On dynamic interfaces, i.e., PPP, PPPoE and DHCP, select the Gateway checkbox to make the interface the Internet gateway (default route). If Gateway is selected, any value entered in the Default Gateway field will be removed (replaced by 0.0.0.0). The Gateway checkbox is not used with a static interface.
NIC (& PPP/PPPoE)	The name of a supported and configured network interface device detected by the system. Configured PPP/PPPoE connections will appear here.
Connection	AUTO is generally recommended. Selections are:
AUTO	Auto-select the active network connection.
UTP_10	Use the unshielded twisted pair interface at 10Mbps.
TX_100	Use the unshielded twisted pair interface at 100Mbps.
Option	Select default (full- <b>or</b> half-duplex) or full duplex.
MTU	Maximum Transmission Value. Default is 1500. Incorrect MTUs can cause poor performance. However, it may be beneficial to increase MTU for a Gigabit Ethernet interface when jumbo packets are to be used.
Interface Type	Select the interface type: Protected, External and PSN.
DHCP	Dynamic Host Configuration Protocol. DHCP is typically required for cable modem connections. When selected, the system uses DHCP to obtain an IP address for the specified interface. DHCP may be used on any and all network interfaces.
MAC Address	If the device is an Ethernet card, its MAC address will be displayed in this section. Use to assign a physical interface to a particular logical interface. Record MAC addresses before installation into GB-Flash or GB-Pro hardware.

---

```

[ EDIT NETWORK INTERFACE ]
Name: EXTERNAL          [ ] Gateway
NIC: fxp1  Connection: AUTO      Option: default      MTU: 1500

[ Interface Type ]
[X] External [ ] Protected [ ] PSN

[ Network Address ]
[ ] DHCP
IP address: 192.168.71.84/24

Network Interface Cards


|   | NIC  | MAC address       | Name      | Connection   |
|---|------|-------------------|-----------|--------------|
| 1 | fxp0 | 00:D0:68:00:47:D1 | PROTECTED | AUTO default |
| 2 | fxp1 | 00:D0:68:00:47:D2 | EXTERNAL  | AUTO default |
| 3 | fxp2 | 00:D0:68:00:47:D3 |           | AUTO default |
| 4 | fxp3 | 00:D0:68:00:47:D4 |           | AUTO default |


[ OK ] [ CANCEL ]

```

*Network Information Add/Edit*

## How to Change an Object Name without Losing Connectivity

To change an object name without losing connectivity:

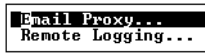
1. Copy the object.
2. Change the object name in the copy.
3. Enable the object.
4. Change the configuration section fields that reference it.
5. Delete the original object (if desired).

Alternatively, to change logical names:

1. Create filters using the new interface names
2. Change the LOGICAL NAMES in Network Information.
3. Remove the filters referring to the old logical names.

## 4 Services

The Services section on the Console interface consists of the Email Proxy and the Remote Logging facility. These services and others available using the Web interface and GBAAdmin can enhance functionality, but are not required when running the GTA Firewall. However, GTA recommended running Email Proxy, as it increases the security of your network and helps reduce unsolicited email.



*Services Menu*

---

### Email Proxy

The Email Proxy shields an internal email server from unauthorized access through SMTP exploits. It also provides facilities to reduce or eliminate “spam” (unsolicited email). The Email Proxy facility is used to configure an SMTP (Simple Mail Transfer Protocol) TCP/25 proxy for inbound email connections. It will respond on any IP address assigned to the External Network interface unless a tunnel is created on port TCP/25. This tunnel would override the proxy startup on the IP address.

---

#### Email Proxy Fields

Enable	Select to enable the Email Proxy.
<b>Connection</b>	
Timeout	Default is 120 seconds. Timeout is the time to wait between each SMTP command exchange.
Maximum Connections	Enter the largest number of SMTP connections allowed to occur simultaneously. Additional connections are deferred until a connection becomes available. Each connection invokes a copy of the SMTP proxy facility.
Primary server	Enter the host name (if using an internal DNS server) or IP address of your email server. The primary email server must reside either on the PSN or Protected Network. If it doesn't, the Email Proxy will not operate.

---

**Email Proxy Fields, cont'd...**

---

Alternate server	Enter the host name (if an internal DNS server has been configured) or IP address of any alternative email server.
------------------	--

---

**Domains to Accept**

---

Domain List	Enter domains from which you wish to accept email. Separate domains with a white space (blank or tab) or a comma. May be used in conjunction with the MX option. When using the option, connections are only accepted for domains specified in this list and/or that rely on DNS MX records assigned to IP addresses on the External interface.
-------------	---

Match against MX	Makes a DNS MX (Mail Exchanger) record query that tries to match the domain in the "To:" portion of an email header to a domain assigned to the proxy's IP address. The email is rejected if there is no match, preventing the site from being used to relay email to other sites.
------------------	--

---

**Email to Block**

---

RDNS will not function correctly without a defined DNS Server. Some legitimate hosts may have mis-configured DNS entries; these hosts will not be able to deliver to your domain.

Verify RDNS	Performs a Reverse DNS lookup on the IP address of the remote host trying to make an SMTP (Simple Mail Transfer Protocol) connection, and then compares it to a DNS lookup of the returned host name. If the lookups fail or don't match, the connection is refused.
-------------	--

Maximum size	Enter the maximum size (in kilobytes) of email message that will be accepted by the proxy. A value of zero (0) means the email proxy will have no size restrictions. This facility is designed to prevent "email bombs" (extremely large attachments that consume disk space and cause problems for email clients).
--------------	---

---

**Mail Abuse Prevention**

---

These providers maintain a list of hosts and domains that have been documented as transmitting or generating spam. Use these lists to block known spam sites, or enter a different provider's list.

For more information about these lists, go to the server websites.

MAP1	relays.orbd.org. Open Relay DataBase: <a href="http://www.orbd.org">www.orbd.org</a>
------	--

MAP2	list.dsbl.org. Distributed Server Boycott List: <a href="http://www.dsbl.org">www.dsbl.org</a>
------	--

MAP3	blackholes.mail-abuse.org** <a href="http://www.mailabuse.org">www.mailabuse.org</a>
------	--

MAP4	relays.mail-abuse.org** <a href="http://www.mailabuse.org">www.mailabuse.org</a>
------	--

---

\* Mail Abuse Prevention System LLC lists require a subscription.

[ EMAIL PROXY ]	
Enable email proxy: <input type="checkbox"/>	[ CONNECTION ]
Timeout: 120 seconds	Maximum connections: 50
Primary server: mailhost	
Alternate server:	
[ DOMAIN(S) TO ACCEPT ]	
Domain(s): networkcomputing.com infosecnews.com	
Match MX: <input checked="" type="checkbox"/>	
[ EMAIL TO BLOCK ]	
Verify RDNS: <input type="checkbox"/>	Maximum size: 0 kilobytes
[ Mail Abuse Prevention Systems (MAPSs) ]	
<input checked="" type="checkbox"/> MAPS 1: relays.ordb.org	
<input checked="" type="checkbox"/> MAPS 2: list.dsbl.org	
<input type="checkbox"/> MAPS 3: blackholes.mail-abuse.org	
<input type="checkbox"/> MAPS 4: relays.mail-abuse.org	
[ SAVE ] [ CANCEL ] [ DEFAULT ]	

*Email Proxy*

## Remote Logging

Remote Logging provides a means to configure how and where log information is sent. GNAT Box System Software uses the syslog TCP/IP protocol, a standard Unix service, for recording logs remotely. All of the standard Unix facilities and priority designations are available. A server for use under Windows NT, 98, 2000 or XP is also provided with installation.

Enable Remote Logging by entering values in the IP ADDRESS and PORT NUMBER fields and saving the function. The resulting log will be formatted in WELF (WebTrends Enhanced Log Format). See the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more information about WELF.

### Remote Logging Fields

Syslog server IP address	The IP address of a host system that will accept the remote logging data. Remote logging data can be accepted by the standard Unix syslog program, the supplied Windows syslog client or any program that accepts the syslog protocol.
Syslog server port number	Port used to connect with the Syslog server IP address. This is port 514 by default.
Use old log format*	Select this to choose the GTA log format used prior to version 3.3 in lieu of WELF.

*Remote Logging Fields, cont'd...***Facilities**

Unix syslog facilities: auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, news, ntp, security, user, uucp, and local0 - local7

**Filter Facility** The Filter Facility logs information associated with any filter that has logging enabled. The default logging configuration records any rejected packets to this log stream. Any attempts at unauthorized access will be logged to the Filter Facility log stream. Disable by selecting None from the list.

**NAT Facility** The NAT facility logs information associated with any Network Address Translation process: essentially, outbound packets. Select None from the list to disable.

**WWW Facility** The WWW facility is the syslog stream which logs all URLs accessed through the GTA Firewall. Disable by selecting None from the list.

**Priorities**

Unix syslog priority designations: 0=emergency; 1=alert; 2= critical; 3=error; 4=warning; 5=notice; 6=information; and 7=debug.

**Priority to log tunnel opens** Set to None by default. When a network connection is initiated, an Open record is generated. Select None to disable Open log records.

**Priority to log tunnel closes** Set to 5 (notice) by default. When a network connection is terminated, a Close record is generated which contains the number of packets and bytes sent and received. Select None to disable Close log records.

**Priority to log WWW pages accessed** Set to 5 (notice) by default. When an Internet connection is initiated, a log record listing the URL accessed will be generated. Select None to disable WWW log records.

\* GTA's previous log format has been deprecated and will be phased out in future releases of GNAT Box System Software.

```

[ REMOTE LOGGING ]

Syslog server IP address: 192.168.101.2
Syslog server port number: 514
Use old log format: [ ]

Filter facility: local1
NAT facility: local0
WWW facility: local2

Priority to log tunnel opens: none
Priority to log tunnel closes: 5 - notice
Priority to log WWW pages accessed: 5 - notice

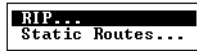
[ SAVE ] [ CANCEL ] [ DEFAULT ]

```

*Remote Logging*

# 5 Routing

The Routing section provides facilities for routing data to its destination: RIP (Routing Information Protocol) and Static Routes.



*Routing Menu*

## RIP

The RIP (Routing Information Protocol) facility provides a means to configure RIP on any network interface. RIP is a TCP/IP routing protocol defined by RFC 1058 that allows broadcasting and/or listening to routing information in order to choose a route for a packet that uses the fewest hops. RIP allows the system to select the routes that use the fewest hops, or to select an alternate path if a route is down or has been slowed by high traffic. RIP is limited to 15 hops; more than that, and the route is flagged as unreachable.

RIP is disabled by default on the GNAT Box System Software, meaning that routing information to redirect packets is not accepted from external sources.

### Note

Most smaller network configurations do not require RIP. Before using RIP, be aware that the protocol adds overhead to networks.

By enabling the RIP facility on an individual interface, the GTA Firewall can receive and/or broadcast routing information. The GNAT Box System Software supports both RIP version 1 and RIP version 2.

### RIP Fields

Enable	Enables the RIP facility on the selected interface. If connected to a remote GTA Firewall, the RIP facility will not begin operation until the section is saved.
Advertise Default Route?	Advertise the default route (default gateway) on any Protected Network or PSN on which RIP is enabled.
Interface	Lists all configured network interfaces available for RIP.

## RIP Edit Fields

**Enable** Enables RIP on the specified network interface. Each interface may be independently configured to accept/export RIP information.

**Input/Output** Controls how RIP is implemented. Input determines whether any version of RIP will be accepted from other routers. Output determines whether any version of RIP will be exported or broadcast.

The choices are:

**None** RIP is not accepted or exported.  
**V1** Version 1 RIP is accepted or exported.  
**V2** Version 2 RIP is accepted or exported.  
**Both** Both version 1 and 2 are used.

### Password Fields

The Password field is used in conjunction with RIP version 2.

**Password Type** If using RIP version 2, which uses a password, select the type of encryption that will be used. If an encryption type is selected, the password field is enabled. Encryption types are: None, Clear and MD5.

**Password** Enter the password that must be used to collect routing information through RIP.

**Key ID** Enter the Key ID for the Password.

```

ROUTING INFORMATION PROTOCOL (RIP)
[ ] Enabled?

Interface  Enabled  Input  Output  Password
1  ext2      no     none   none   none
2  ext3      no     none   none   none
3  EXTERNAL  no     none   none   none
4  PROTECTED yes     v2     v2     none

[ ] Advertise default route?

[ SAVE ] [ CANCEL ] [ DEFAULT ]
  
```

*RIP*

```

EDIT RIP INTERFACE
[ ] Enabled?

Interface: EXTERNAL
Input: none Output: none

Password: none _____ 0

[ OK ] [ CANCEL ]
  
```

*RIP Edit*



# Static Routes

The Static Routes facility allows the administrator to define static (fixed) routes used to create a path between one part of a network and another. By default, a GTA Firewall does not listen to routing protocols such as RIP, so a static route allows information to move in a specific path across the network without the use of broadcasted routing information. See product guides for the number of Static Routes available on a specific GTA Firewall.

A static route tells the system, “Use *this* route for packets traveling from this network to that location instead of the Default Gateway defined in Network Information,” (or in Gateway Selector, if that facility is enabled – on GBAAdmin or the Web interface).

## Static Routes Fields

Index	Number used to identify the static route.
Network IP address	Enter the Destination IP address which will be the target of the static route, either by selecting the appropriate Interface Object in the dropdown box or by selecting Use IP address and entering the address and netmask, either in CIDR-based (slash /) notation or dotted decimal.
Gateway	Enter the IP address of the gateway (default route) to the Destination IP address selected for this static route.

*Static Routes, Add/Edit*

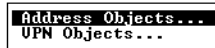


# 6 Objects

Using Objects increases speed and consistency when creating a configuration with GNAT Box System Software. With the Objects function, a user need only define an address or group of addresses, an interface, or a configuration once, then select the object in each screen where that definition is required. Once the object is created the user will only need to change the object to change the definition in all the locations where it is used.

## Note

Object names may *not* have a number as the first character, except host names in the Network Information and DNS Server screens.



*Objects Menu*

## How to Change an Object Name without Losing Connectivity

1. Copy the object.
2. Change the object name in the copy.
3. Enable the object.
4. Change the configuration section fields that reference it.
5. Delete the original object (if desired).

## Save a Configuration Copy

GTA recommends **always** copying the active configuration to a file (\*.GBcfg) or printing the Configuration Report before making changes. See the **GNAT Box SYSTEM SOFTWARE USER'S GUIDE, Chapter 13 – Administration, Download Configuration.**

# Address Objects

The Address Object list displays the name and description of all defined Address Objects. An Address Object may have a maximum of 10 members. The members may be either a single IP address (host), a range of IP addresses, a subnet specified by an IP address and netmask, or another Address Object. See product guides for the maximum number of Address Objects available on a specific GTA Firewall.

## Creating Address Objects

Click Add (+) in the Address Object list. Enter a unique name for the object in the NAME field and a description in the DESCRIPTION field, then click OK.

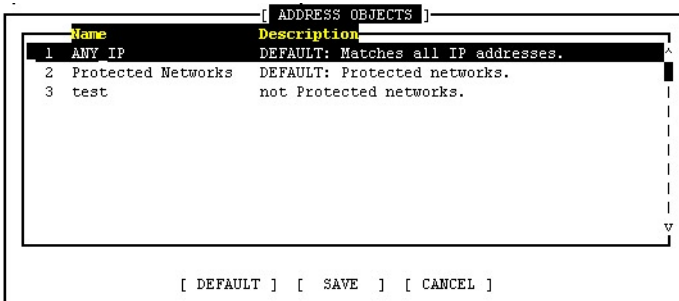
To add members to the object, select a previously defined Interface or Address Object from the OBJECT field dropdown box, select Use IP address and enter the IP address in the IP ADDRESS field, or select ANY\_IP. The IP address can be a single IP address or host, a range of addresses, or an IP address/netmask.

## Default Address Objects

The GNAT Box System Software has two default address objects, ANY\_IP and Protected Networks. The ANY\_IP address object can be viewed, but not deleted. The Protected Networks object contains the IP addresses of each interface with a Protected TYPE field. Defaulting the Address Objects screen displays only these default address objects in their default configuration. To use the defaulted objects, click Save at this point. To return to the previously saved settings, click on another section of the menu. When you return to Address Objects, your saved objects will be displayed.

### Address Object Fields

Name	Unique name by which the object will be referenced.
Description	Describe the address object.
Object	Select a previously defined Interface or Address Object as a member of this object.
IP address	Enter an IP address/netmask to be included in this address object. Use this field if Use IP address was selected in the Object field.



*Address Objects*

[ EDIT ADDRESS OBJECT ]

Name: ANY IP  
 Description: DEFAULT: Matches all IP addresses.

---

Object/Address

1	0.0.0.0/0
---	-----------

[ OK ] [ CANCEL ]

*Default Address Object*

[ EDIT ADDRESS OBJECT MEMBER ]

Object: <USE IP ADDRESS>  
 Address: 0.0.0.0/0

[ OK ] [ CANCEL ]

*Address Object Add/Edit*

## VPN Objects

The VPN Objects list displays the name and description of all defined VPN Objects. VPN Objects are defined primarily in the LOCAL GATEWAY and LOCAL NETWORK fields. Other fields define how the connection will be protected and how the phases of the connection will be encrypted.

### Default VPN Objects

Three VPN objects are created by default: one each for IKE VPNs, Manual VPNs and Mobile VPNs. These three objects, tailored to suit your organization, can usually replace the extensive VPNs built prior to version 3.2.2.

When the firewall is reset to factory settings, the default VPN objects will be created, replacing all other objects.

#### ***Exception***

GB-Pro systems have only the Manual Key Exchange default VPN object.

---

## VPN Objects Fields

---

Disable	Check to disable all access for the selected object.
Name	Enter name by which the objects will be referenced.
Description	Enter a description of the object.
Mobile Authentication Required	Enabling this option requires a user to pre-authenticate using the <b>GBAuth</b> utility. (The User ID and Password are set in User Authorization.) A Remote Access Filter must also be defined and enabled. See the <b>VPN CLIENT USER'S GUIDE</b> for more information.
Local Gateway	An IP address, alias or H <sub>2</sub> A group assigned to an External Network interface on the local GTA Firewall. The encapsulated packets will appear at the remote gateway with this IP address listed as the source, therefore the IP address should be used as the remote (destination) gateway when Remote Access Filters are created for the VPN. After saving a VPN, defaulting Remote Access Filters will create an appropriate filter.
Force Mobile Protocol	Select Force Mobile Protocol if you are using dynamic IP addresses that require the system to use dynamic protocol negotiation; deselect for static IP addresses.
Local Network	If you have defined an Address Object for the local network that is to be accessible via the VPN, select that object from the list. If not, enter the network IP address and mask of the local network, typically a Protected Network, PSN or a subnet of either.

### Phase I

In IKE, a Phase I exchange establishes a security association by negotiating the VPN terms, authenticating the validity of the VPN peer and setting connection parameters. Manual Key Exchange is not user-configurable in Phase I. For mobile connections, Phase I will default to Aggressive, 3DES, SHA-1 and Diffie-Hellman Group 2.

---

Exchange Mode	<p><b>Main: Static IP to Static IP</b> Set to Main when the connection is from one gateway with a static IP address to another, e.g., a VPN between two GTA Firewalls or a GTA Firewall communicating with another vendor's VPN device/software.</p> <p><b>Aggressive: Static IP to Dynamic IP</b> Set to Aggressive when the connection is from a gateway with a dynamic IP address to one with a static address, i.e., in all VPN mobile connections, and in most connections using PPP/PPPoE or DHCP. <b>In either mode</b>, if the vendor's VPN device has a setting or identification method, always set it to the IP address.</p>
---------------	---

---

Encryption Method	3DES, AES, Blowfish, DES, and Strong (Any). The encryption method that the GTA Firewall will accept from a connection initiator during Phase I. Blowfish will be used when the GTA Firewall initiates the connection.
Hash Algorithm	All, HMAC-MD5, HMAC-SHA1; HMAC-SHA2. The method that will be used for the Phase I authentication transformation. “All” allows the GTA Firewall to accept any of the hash algorithm encryptions for the Authentication Header (AH). MD5 will be used when the GTA Firewall initiates the connection.
Key Group	Any, Diffie-Hellman Group 1, 2 or 5. Select the key group for Phase I. Diffie-Hellman is a crypto-graphic technique that enables public keys to be exchanged in a way that derives a shared, secret (private) key at both ends. GNAT Box System Software uses Group 2 by default.

### Phase II

In IKE, a Phase II exchange establishes security associations for other protocols, providing source authentication, integrity, and confidentiality.

Encryption Method	3DES, AES, Blowfish, CAST128, DES, None, Null, Strong, Twofish. Select the method for the Encapsulating Security Payload (ESP) transformation. When Strong is selected, any of the algorithms except None and Null will be accepted from the remote initiator. AES will be used when the GTA Firewall is the initiator. Null is a special case where there is only IP encapsulation. The Null method has little impact on performance. Null is useful when unsupported protocols are used in NAT mode between two firewalls.
Hash Algorithm	All, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, None. Select method for the Phase II authentication transformation. Selecting None will result in no AH (Authentication Header) transformation being applied to the packet.
Key Group	Any, Diffie-Hellman Group 1, 2 or 5. Select the key group for Phase II. On the GNAT Box VPN Client, this value is defined in the Security Policy section and is labeled PFS (Perfect Forward Secrecy) Key Group. With PFS, the compromise of a key exposes only the data protected by that key to unauthorized access.

### Note

The GNAT Box IPsec VPN always has PFS and Replay Detection enabled. When communicating with another vendor's VPN device, enable PFS and Replay Detection on the other device. The anti-replay protocol prevents the insertion of changed packets into the data stream.

[ GNAT Box VPN Objects ]

Description	
1	DEFAULT: IKE VPNs
2	DEFAULT: MANUAL VPNs
3	DEFAULT: MOBILE VPNs

[ SAVE ] [ CANCEL ]

### *VPN Objects*

[ EDIT VPN OBJECT ]

Disable:

Description: DEFAULT: IKE VPNs

Name: IKE  Mobile authentication required

Local gateway: EXTERNAL  Force mobile protocol

Object: Protected Networks Address:

[ Local Network ]

[ Phase I ]

Mode: main

Method: 3des

Hash: hmac-shal

Key group: Diffie-Hellman Group 2

[ Phase II ]

Method: aes

Hash: hmac-shal

Key group: Diffie-Hellman Group 2

[ OK ] [ CANCEL ]

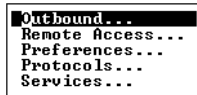
### *VPN Objects Add/Edit*



# 7 Filters

Filters control access to and through the GTA Firewall; Outbound and Remote Access Filters are created in functions under the Filters chapter, while IP Pass Through Filters are created in the first IP Pass Through function. The Filters configuration section includes Outbound Filters, Filter Preferences, Protocols, Remote Access Filters and Time Groups.

Outbound, Remote Access and IP Pass Through Filters are defined using the same screen layout and process. Use the information on filter management and fields in the Outbound Filters section to create Remote Access and IP Pass Through Filters.



*Filter Menu*

## Note

Changes to filters will not be effective until the section is saved. If you leave the filter or filter set displays without saving, changes will be lost.

---

## Outbound Filters

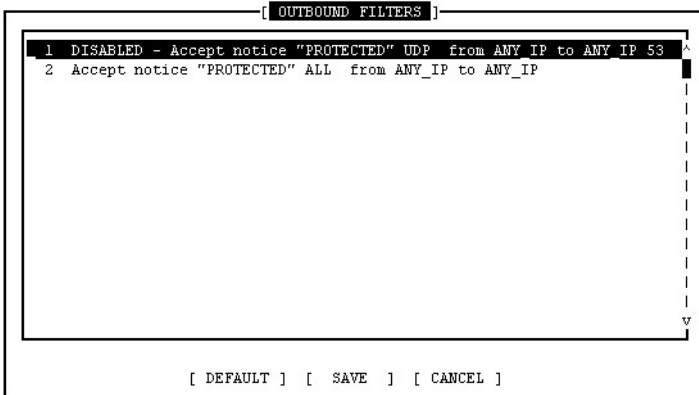
Outbound Filters control access to IP addresses that reside in an External Network from hosts on Protected and PSNs, and those that reside external to a PSN from hosts on a Protected Network. Outbound Filters support only the IP protocols: TCP, UDP and ICMP. The implicit rule, “that which is not expressly permitted is denied,” applies to both outbound packets and inbound packets. The default Outbound Filter set allows all IP addresses on the Protected Network to access any IP address and any service external to the Protected Network. If a PSN interface exists, a similar default Outbound Filter will be created that allows all access to the External Network. These filters can be modified or deleted according to local network security policy.

For information about managing filters, see the **GNAT BOX SYSTEM SOFTWARE USER’S GUIDE**.

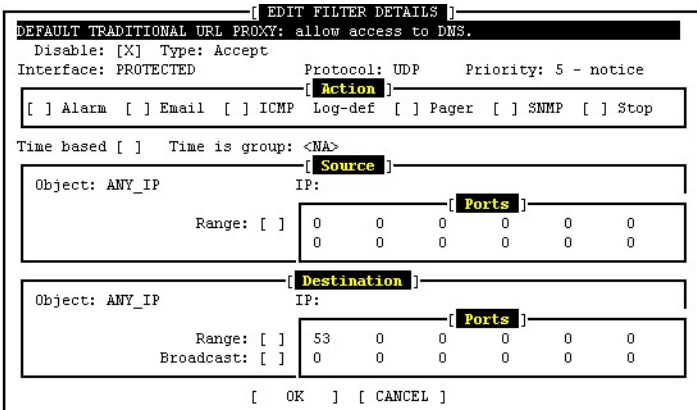
## Filter Fields

Description	Enter a description of the filter for reference. Any filters generated by the system will have descriptions with a label tag such as: Email Proxy, No RIP (RIP is disabled), and Stealth (Stealth mode is enabled).
Disable	Check to disable the selected filter.
Type	Accept or Deny the packet type.
Interface	Logical interfaces. The specified Interface is matched against the interface on which the IP packet arrived. <ANY> will match any interface.
Protocol	TCP, UDP, ICMP, IGMP, ESP, AH, ALL, or any other protocol defined in the Protocols section can be selected to match against the packet. If ALL is selected, no destination or source ports may be specified. Using NAT, only TCP, UDP, ICMP can be used with a Deny filter. Specified protocols can be used to suppress the logging of noisy "benign" protocols which are implicitly blocked by creating a Deny filter with "nolog" selected. Using IP Pass Through, all protocols can be used with either an Accept or a Deny filter.
Priority	A notice sent with the alarm event. Defined by the user.
Actions	Select one or more events to notify the administrator about a filter alarm. Alarm, Email, ICMP, Pager, SNMP, Stop Interface
Log	Yes, No, and Default. Default is the value defined in the Filter Preferences section.
Time based	Click to make the filter operate at a specified time.
Time Group	Select the previously created time parameters from the dropdown box.
Source Address	IP address of the packet. The selected IP address or object will be matched against the source IP address of the packet.
Range	Select to choose a range of ports.
Source Ports	Leave empty for any source port to be accepted. The source port for most client protocols is a random value above 1024. The source port can be a single port, multiple ports or a range of ports. Specified Source Ports are matched against the source port of the IP packet.
Destination Address	IP address of the packet. The selected IP address or object will be matched against the destination IP address of the packet.

Range	Select this to choose a range of ports.
Broadcast	Select Broadcast if this is a Broadcast IP Address. Usually, a broadcast address is the last IP address in a subnet. Broadcast packets are not accepted by GTA Firewalls, so when they are blocked, a message is generated by default. To prevent these repetitive block messages, select Broadcast on a Deny filter to explicitly block, but not log, these packets.
Destination Ports	Often called well-known services, originally assigned dedicated port numbers ranging from 1 to 1024; other services have since been assigned outside this range. See Source Ports, above, for more information.



*Outbound Filters*



*Outbound Filters Add/Edit*

# Remote Access Filters

Remote Access Filters control inbound access, primarily tunnel access, but is also inbound access from any attached network to any interface on the GTA Firewall. A Remote Access Filter must be in place before a Tunnel can be accessed. Remote Access Filters support only the protocols TCP, UDP and ICMP.

Generally, it is best to select and configure system Preferences (in Basic Configuration) and Inbound Tunnels before Remote Access Filters. This allows the creation of a set of Default filters that reflect the system's configuration. These filters can be used as is, or modified, disabled or deleted to suit the local network security policy.

See Outbound Filters in this section for set information, tips and fields for Remote Access Filters.

## Preferences

The Preferences section allows the administrator to define preferences for the manner in which filters are applied and recorded.

### Preferences Fields

#### Default Logging

Every filter has a log action. A 'Yes' in the filter action field for the filter explicitly logs the packet, a 'No' explicitly does not log the packet.

The Default option requires the filter to take the action defined here.

By default, all rejected packets for all protocols are logged.

Protocol	Protocol to log: ALL, TCP, UDP, ICMP or NONE.
Packet Types	Packet type choices are not mutually exclusive. However, selecting multiple types may result in excessive logging.
Received	Log packet that is compared to the filter.
Rejected	Log packet that is rejected by the filter.
Accepted	Log packet that is accepted by the filter.
Matched	Log packet that matches the filter criteria.

## Alarms

This section allows the parameters for alarm notifications to be set. When a filter (Remote Access, Outbound, or IP Pass Through) is matched, an alarm event is activated. Each alarm event increments the alarm count by one. If either the time or number of alarms threshold is exceeded, a notification will be sent documenting all the events that contributed. Multiple messages will be sent if the number of events exceeds the maximum alarm count.

Threshold for generating email	Number of alarms above which a notification is sent.
Threshold interval	Length of time after which to send alarms.
Maximum Alarms per Email	Maximum number of alarm messages included in a message. An alarm message is generally 200 bytes.
Attempt to Log Host Names	Attempt to resolve the host name of the IP address that generated the alarm. This increases processing time.
Page When Threshold Reached	If Pager is enabled, a pager notification is sent when an alarm threshold is exceeded.

## General

The administrator may generate an Alarm; send an email message to the address in Email Server: generate a Log Entry; or generate an ICMP “service not available” message to send to the source IP address of the attempted connection. (ICMP is for a doorknob twist only.)

Stealth Mode	In stealth mode, the GTA Firewall will not respond to ICMP ping and traceroute requests, or to UDP traceroute requests, and will not reply with an ICMP message when a packet arrives for a port without a service or tunnel. Stealth Mode is enabled by default on version 3.3.1 and up.
Actions to generate doorknob twist	Controls the response to “doorknob twists.” A doorknob twist occurs when a connection is attempted on a port for which there is no service or tunnel in place and a filter has accepted the packet. A Doorknob Twist usually indicates that the firewall is mis-configured.
Actions to generate for Address Spoofs	Controls the response to address spoofs. A spoof occurs when a packet arrives at one interface and its return path is through a different interface. Possible causes: <ol style="list-style-type: none"> <li>1. Firewall is mis-configured: networks, subnets or hosts located on, or connected to the internal side of a firewall have not been defined. (A GNAT Box system assumes that IP addresses not defined on the Protected Network, in Static Routes or learned via RIP, should appear only on the external side.)</li> <li>2. An intrusion attempt is made by altering the source IP address of a packet directed at a network interface.</li> </ol>

```

[ FILTER PREFERENCES ]
[ DEFAULT LOGGING ]
Protocol: <ALL>
Packets: [ ] Received [X] Rejected [ ] Accepted [ ] Matched

[ ALARMS ]
Send email for alarms when 10 alarms send in 120 seconds.
Maximum alarms per email: 500

[ ] Attempt to log host names (reverse DNS).
[ ] Send page when alarm threshold reached.

[ GENERAL ]
[ ] Stealth mode.
          ALARM  EMAIL  ICMP  LOG
Doorknob twist: [X] [ ] [ ] [X]
Address spoof: [X] [ ] [ ] [X]

[ SAVE ] [ CANCEL ] [ DEFAULT ]

```

*Filter Preferences*

# Protocols

The Protocols function provides a means to define IP protocols to make available in the protocol list used when defining filters. The protocols may only be used with a Deny filter, since the system can only process TCP, UDP and ICMP IP packets. Using the Protocols function, the administrator can explicitly deny a protocol on a certain port in order to generate specific log entries.

The implicit rule of GNAT Box Systems, “that which is not explicitly allowed is denied,” combined with the default in which all rejected packets are logged, can make the “unknown protocol” log events too numerous. Identifying a protocol is useful in reducing these extraneous events.

To define a protocol, enter the acronym of the protocol in the Name field and the port number of the protocol in the Number field.

After the protocol has been defined, the administrator must create and enable an appropriate Remote Access Filter to deny the protocol on that port, and log it in a specific manner, or explicitly prevent it from being logged.

By default, the Protocols section contains the protocols IGMP/2, ESP/50 and AH/51. Defaulting the Protocols section will delete customization of protocols. Remove protocols by deleting the fields and saving the section.

	Name	Number
1	IGMP	2
2	ESP	50
3	AH	51

[ SAVE ] [ CANCEL ] [ DEFAULT ]

*Protocols*

[ EDIT IP PROTOCOL ]

Name:

Number: 0

[ OK ] [ CANCEL ]

*Protocols Add*

# Services

The Services screen allows the administrator to define available filter services.

## Filter Services Fields

### Email Server

This Email Server need not be the same as the one used in the Email Proxy.

Enable	Send email and alarm notifications. If alarms and/or email notifications are set on a filter, and the email server is not enabled, a warning message will be sent to the log.
Server	DNS host name or IP address of the email server where alarms and notification messages will be sent. Although the email server is typically a host on the Protected Network or PSN, it can be an external host or any valid and accessible email address. In order to use a host name for the email server, you must have defined a DNS server for lookups on the GTA Firewall. If the name is an internal host, the DNS server must also be internal. If the DNS server is an external host and the target server is an internal host, you will have to use the IP address. If you are unsure about the name, use the host's IP address.
From	Email address that will appear in "From" field of the email. An invalid address or a server that does not allow email with an empty From field can cause an email loop. The address can be a fully-qualified address, such as <code>jdoe@gta.com</code> , or the mailbox name on the specified email server: <code>jdoe</code> .
To	Email address where notifications should be sent. The address can be a fully-qualified address, such as <code>jdoe@gta.com</code> , or the mailbox name on the specified email server: <code>jdoe</code> .

### SNMP

Simple Network Management Protocol (SNMP) is a standard for managing IP devices, retrieving data from each device on a network, and sending it to designated hosts.

Enable SNMP	Enable the SNMP alarm facility. Upon selection, the SNMP Manager IP field will allow data entry. If SNMP is not enabled, selecting SNMP filter actions on the filter definition screen has no effect.
-------------	---



**Manager IP** Enter the IP address of the host that should receive SNMP trap messages. If SNMP is checked as an action, the GTA Firewall will generate an enterprise-specific generic trap on a filter definition when the filter is matched. The SNMP manager is typically on the Protected Network, though it may reside on any network.

### Pager

Connect a modem to one of an available serial ports on your GTA Firewall or use an internal modem card (GB-Flash and GB-Pro). The modem is only used for dialing and sending DTMF tones, so a basic model will suffice.

<b>Enable</b>	Enables the Pager alarm facility.
<b>COM Port</b>	Select the COM port to which the modem used for paging is attached or assigned. Choice of COM ports 1 through 4, except for GB-1000 (COM 2) and RoBoX (COM 1).
<b>Speed</b>	Enter the DTE speed at which the firewall will communicate with the modem.
<b>Phone number</b>	Telephone number for the target numeric pager. You should enter all numbers and dialing codes that are required to make a call.
<b>Code</b>	Numeric value that will be displayed on the pager. This code may include any valid numbers or symbols used by your numeric pager may use. Commas represent pauses and are typically required while the pager announcement is played. Most pagers have the message terminated by a # symbol. Please consult your pager service for the specifics of your pager.

```

[ FILTER SERVICES ]
[ Email Server ]
Enabled: [ X ]
Server: mailhost
From:
To: postmaster

[ SNMP Traps ]
Enabled: [ ]
Manager:

[ Pager ]
Enabled: [ ]
COM port: 2      Speed: 4800
Number:
Code: ,,,,,,1234#

[ SAVE ] [ CANCEL ] [ DEFAULT ]

```

### Filters Services



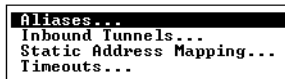
## 8 NAT

Functions in the NAT (Network Address Translation) section are used to configure certain aspects of the NAT facility. These facilities are Aliases, Inbound Tunnels, Static Address Mapping and Timeouts.

Network Address Translation translates an IP address behind the firewall to the IP address of the External Network interface, effectively disguising the original IP address and making it possible to use a non-registered IP address within the Protected Networks and the PSNs, while still presenting a registered IP address to the External Network (typically the Internet).

The NAT facility used in GNAT Box System Software is active by default. NAT is applied to outbound packets from a Protected to an External Network; from a Protected Network to a PSN; from a PSN to an External Network; from one Protected Network to another Protected Network; and from one PSN to another PSN.

NAT is available in two forms: dynamic and static, referred to as Default NAT and Static Address Mapping. NAT can be bypassed using IP Pass Through.



*NAT Menu*

---

## Aliases

The Alias facility allows a network interface to be represented by multiple IP addresses. An IP alias may be assigned to any network interface. This facility is useful on the External Network interface, or if multiple targets on the PSN or Protected Network are required for the same service (port) via the Tunnel facility (e.g., multiple web servers). See individual product guides for the maximum number of IP aliases available on a specific GTA Firewall.

The NAME field in Aliases allows the user to enter a logical name for the IP alias. Logical names can be used as Interface Objects.

### Note

User-defined names may **not** use a number as the first character.

IP aliases used on an External Network interface attached to the Internet must be registered (legitimate) IP addresses. An IP alias need not be from the same network as the real IP address, since the GTA Firewall will route packets between all networks to which it is logically attached.

The screenshot shows a console window titled 'ALIASES'. It contains a table with three columns: 'Name', 'Interface', and 'IP address/Netmask'. The table lists two entries: '1 Test Alias' on 'EXTERNAL' interface with IP '10.10.1.151', and '2 alias2' on 'EXTERNAL' interface with IP '10.10.1.152'. Below the table is an 'EDIT ALIAS' dialog box with fields for 'Name', 'Interface', and 'IP address/Netmask'. The 'Interface' field contains '???' and the 'IP address/Netmask' field is empty. At the bottom of the dialog are 'OK' and 'CANCEL' buttons.

Name	Interface	IP address/Netmask
1 Test Alias	EXTERNAL	10.10.1.151
2 alias2	EXTERNAL	10.10.1.152

*IP Alias, Add/Edit*

### Note

If the IP alias is on the same logical network as the network interface's primary IP address, use a netmask of /32 (255.255.255.255).

## Inbound Tunnels

The Inbound Tunnels facility allows a host on an external network to be able to initiate a protocol from the Protocol List, e.g., TCP, UDP, ICMP, IGMP, ESP or AH session, with an otherwise inaccessible host, for a specific service. Tunnels can be defined for both the External Network and the PSN; tunnels are only associated with inbound connections, so they are not used on a Protected Network interface. See product guides for the number of tunnels available on a specific GTA Firewall.

Tunnels can be created only for these inbound connections:

1. From the External Network interface to a host on the PSN.
2. From the External Network interface to a host on the Protected Network.
3. From the PSN interface to a host on the Protected Network.

### Caution

A tunnel with a source and destination port of zero means "tunnel all ports for the specified protocol." It is possible to expose a host by creating a zero tunnel with the protocol type set to ALL. It is not recommended to expose a host in this way, especially a host on a Protected Network.

## Creating Inbound Tunnels

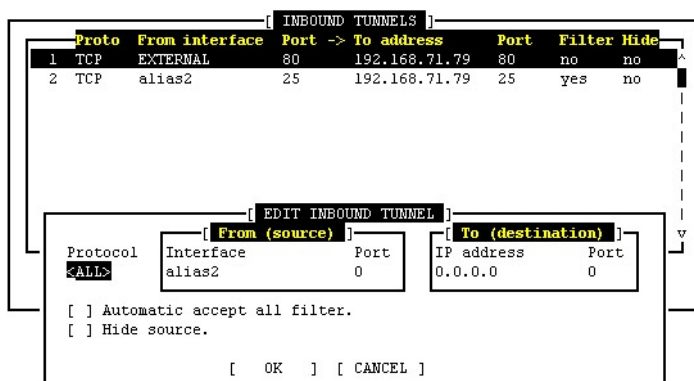
To create a new tunnel, first select the protocol the tunnel will use from the dropdown list. In the `INTERFACE` field, select the Interface Object that represents the source of the tunnel, and in the Port field, enter the number of the port through which this tunnel will operate on the source side.

For the destination of the tunnel, enter the IP address of the selected destination and then select the port through which the tunnel will operate on the destination side.

The tunnel source will not be usable unless an appropriate Remote Access Filter has been defined to allow access. The Default button on the Remote Access Filter set screen will generate default filters for all defined tunnels. The filters generated by this method are broad in scope and may require modification to meet your security policy.

### Inbound Tunnel Fields

Protocol	Select from the Protocol List: ALL, TCP, UDP, ICMP, IGMP, ESP, AH, etc.
From IP address	Select an interface object representing a network interface, an IP alias or a H <sub>2</sub> A (high availability) group for the source side of the tunnel.
From Port	Enter the port value which users will access. For an exhaustive and up-to-date list of port number and services, see <a href="http://www.iana.org/assignments/port-numbers">www.iana.org/assignments/port-numbers</a> .
To IP address	Enter the IP address of the target host. The host may reside on either the PSN or the Protected Network (including subnets routed behind either network).
To Port	Enter the port value which will be the destination of the tunnel. This is the port value of the service being offered on the target host.
Automatic Accept All Filter	Select to make the inbound tunnel connection ignore any conflicting filters. When activated, the Automatic filters will appear under the System Activity section in the Active Filters table.
Hide Source	Select to hide the source of the inbound tunnel connection. Hide Source is useful when the GTA Firewall is used on an intranet.



*Inbound Tunnels, Add/Edit*

## Static Address Mapping

Static Address Mapping, also known as Static Mapping, Mapping or Outbound Mapping, allows an internal IP address or subnet to be statically mapped to an external IP address during Network Address Translation. By default, all IP addresses on the Protected Networks and PSNs are dynamically assigned to the primary IP address of the outbound network interface. Static Address Mapping is used when it is desirable to statically assign the IP address used in the Network Address Translation. It is allowed:

- From a host or subnet on the Protected Network to an IP alias assigned to the PSN interface.
- From a host or subnet on the Protected Network to an IP alias assigned to the External Network interface.
- From a host or subnet on the PSN to an IP alias assigned to the External Network interface.

To use the Static Address Mapping facility, you must first assign at least one IP alias to the desired outbound network interface (External Network interface or PSN interface).

1. The target of a map definition must be an IP alias.
2. Mapping is only associated with outbound packet flow.
3. Map definitions may be for a single host or a subnet.

See individual product guides for the number of Static Address Maps available on a specific GTA Firewall.

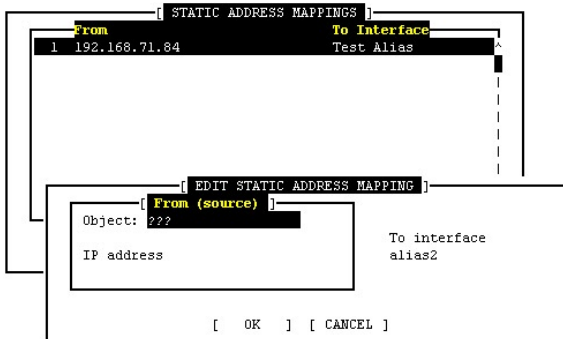
---

## Static Address Mapping Fields

---

Object	Select the Interface Object that will be mapped.
IP address	If an Interface Object cannot be used, enter the IP address and netmask that will be mapped, e.g., to map a single IP address, use a netmask of /32 (255.255.255.255).
To Interface	The Interface Object representing the IP address to which the source will be mapped.

---



*Static Address Mapping, Add/Edit*

---

## Timeouts

Timeouts define how long a connection should be idle before it is marked ready to close. The result of a connection reaching timeout differs for each protocol. For example, TCP has enough information for the GNAT Box System to determine when the connection is ready to close, but it is generally impossible to determine when an ICMP or UDP connection is ready to close.

---

### Timeout Fields

---

Wait for close	Default value is 20 seconds. If your firewall experiences spurious Remote Access Filter blocks from reply packets, typically from port 80, you may want to increase this value to give packets from slow or distant connections more time to return before the connection is closed.
----------------	--

---

#### Timeout in seconds

---

TCP	Default is 600 (10 minutes).
UDP	Default is 600 (10 minutes).

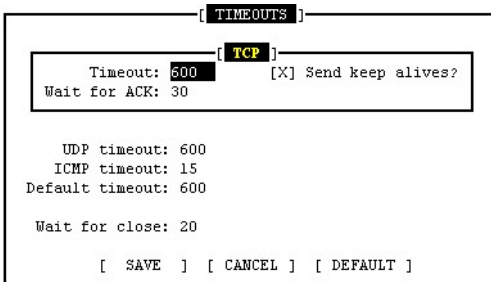
---

*Timeout Fields, cont'd...*

ICMP	Default is 15.
Default	Default is 600 (10 minutes). This is the timeout for any supported protocol other than TCP, UDP or ICMP. After a connection is marked ready to close, the firewall will wait five seconds before it closes it, giving redundant IP packets a chance to clear the firewall without causing false doorknob twist error messages.

**TCP Specific**

Wait for ACK	Default is 30 seconds. When creating a TCP connection, the client and server exchange several IP packets. All packets sent from the server will have a bit indicating ACK (acknowledgement) in the header. As part of Stateful Packet Inspection, a GTA Firewall records seeing this bit. If it is not seen, the remote server is probably down. If idle time is reached without an ACK from the server, the connection is marked ready for close.
Send keep alives?	Enabled by default. If this field is enabled, a Keep Alive packet is sent. If the connection is still valid, the firewall will set the connection idle time to zero. If the connection is invalid, the GTA Firewall will see a reset packet indicating this, sent by the client to its server, and will mark the connection ready to close. If no response is received within five minutes, the GTA Firewall will mark the connection ready to close. If a successfully created TCP connection remains idle for the timeout period and this field is disabled, it is marked ready to close.



*Timeouts*



## 9 IP Pass Through

IP Pass Through is the GTA term for “no NAT.” The IP Pass Through section allows the administrator to define a host, subnet or network that will not have NAT applied to packets from specified IP addresses. IP Pass Through supports all IP protocols.



### *IP Pass Through Menu*

IP Pass Through can be defined for packets from a host on a Protected Network outbound through PSN and External NICs; a host on a Protected Network outbound through a PSN NIC only; a host on a Protected Network outbound through an External NIC only; a host on a PSN outbound through an External NIC only; and for packets on a host on a Protected Network to a host on another Protected Network.

Two items must be in place for an IP Pass Through to operate correctly:

1. The IP address must be defined on the Network/Host form.
2. An IP Pass Through filter must be created to allow packets to flow from and/or to the IP Pass Through IP address.

### **Note**

If an IP Pass Through address is configured to use the External Network interface and the GTA Firewall is connected to the Internet, the IP Pass Through address must be registered.

By default, IP Pass Through-designated IP addresses are configured for outbound only. Stateful packet inspection information is maintained about sessions that originate from hosts on a PSN or a Protected Network outbound to guarantee that only IP packets that are replies to the initiated connections are accepted. If the connection protocol calls for a secondary inbound connection from an external host to the originating internal host, *virtual cracks* are created to allow the secondary connection. This allows protocols such as FTP to be used without arbitrary, semi-permanent inbound connections.

IP Pass Through provides great flexibility. For example, an IP address on the Protected Network can be defined so that no NAT is applied to packets with a destination on the Private Service Network, but packets from the same IP address which are going to the Internet will have NAT applied.

# IP Pass Through Filters

IP Pass Through Filters control access to and from IP addresses that have been specified as IP Pass Through addresses. IP Pass Through Filters are different from Remote Access and Outbound Filters in that they control both inbound and outbound access to/from the designated IP Pass Through addresses. Since IP Pass Through addresses are not translated, the GTA Firewall functions as a gateway for these addresses. IP Pass Through Filters utilize IP Pass Through addresses in the definitions, not GTA Firewall network interface addresses.

Typically, two filters are required for each different Host/Network IP Pass Through IP address: one for outbound access and the other for inbound access. IP Pass Through Filters are defined in the same manner as Remote Access or Outbound filters. The rules concerning filter order also apply.

If IP Pass Through hosts/networks are defined, defaulting filters will create a filter set based on the addresses defined on the Hosts/Networks screen. Since IP Pass Through hosts/networks can be defined in a variety of different combinations, the default filters will vary according to options selected. These system-generated filters can be modified to match your security requirements.

The IP Pass Through filter screen has the same fields as Outbound and Remote Access Filters. See Outbound Filters.

## **How to Create a Pair of Filters for a Defined IP Pass Through Host**

---

1. Create an empty filter definition, or edit an existing filter.
  2. An IP Pass Through address must have two filters, inbound and outbound. First create the Outbound filter. Complete the filter definition in the same manner as an Outbound filter, specifying the same source IP address as that of the IP Pass Through address. Save the filter.
  3. Create another filter for the inbound connection. Define the filter as you would a Remote Access Filter except that the destination IP address will be the IP Pass Through address, not the IP address on the GTA Firewall network interface. Save the filter.
  4. Once you have completed all the desired IP Pass Through Filters, click the Save button on the filter set to save the filters and apply them to the system.
-

# Hosts/Networks

The IP Pass Through Hosts/Networks definition form is used to specify an IP address, subnet or network that will not have NAT applied to packets.

## How to Create a New Host or Network

1. In an empty row in the Network/Host table, select an object or <Use IP address>.
2. If you are using an IP address, enter a host IP address/netmask (for a single host), subnet, or network (for multiple hosts) in the IP ADDRESS field. Single IP addresses should use /32 or /255.255.255.255.
3. Use the Interface dropdown menu to select which network interface will have no NAT applied to the specified IP packets when they pass outbound through the interface.
4. If unsolicited IP packets should be accepted for the specified IP Pass Through address, select the Inbound checkbox. If you wish to allow only IP Pass Through reply packets to return, leave the Inbound option deselected.

See individual product guides for the number of IP Pass Through Hosts/Networks available on a specific GTA Firewall.

## Note

The netmask has no relation to the network netmask. It is a means to specify a single IP address or a group of contiguous IP addresses.

The image shows a configuration window titled "IP PASS THROUGH HOSTS/NETWORKS". It features a table with three columns: "Address", "Interface", and "Direction". The "Address" column contains the text "<empty list>". Below the table is a button labeled "EDIT IP PASS THROUGH HOST/NETWORK". A secondary dialog box is open in front of it, containing the following fields: "Object: ???", "Address:" (empty), "Interface: <ANY>", and "Allow inbound: [ ]". At the bottom of this dialog are buttons for "[ OK ]" and "[ CANCEL ]".

*Hosts/Networks, Add/Edit*



# 10 Authorization

The Authorization section consists of administrative authorization, SSL certificate renewal, remote administration, GTA Firewall user definitions and VPN definitions using previously defined VPN objects.

```
Administration Accounts...
Content Filtering Preferences...
New SSL Certificate...
Remote Administration...
VPNs...
```

*Auth Menu*

## Admin Accounts

The Admin Accounts section provides a means to manage the administration accounts used to access the GTA Firewall. The primary account is the one initially used to log on to the firewall, with the default user ID and password “gnatbox.” Up to five (5) additional accounts can be defined. Each account is assigned a unique user ID and password with selected access privileges. The primary account is the only one that can log in on the GTA Firewall console.

### Note

GTA strongly recommends changing the default user ID and password.

### Admin Account Fields

Enable lockout	Lock out a user if the password is incorrect.
Lockout threshold	Number of tries a user can make before lockout.
Lockout duration	Number of seconds a user is locked out.
Email notification	Send email to administrator if user is locked out.
User ID	Administration account name and password for login.
Password	Any character generated from the keyboard is valid, except leading and trailing spaces. User ID and password may be up to 39 characters long.
Admin	Enable to give this account user update authority.
Console	Only the primary account user can log on to the Console.
WWW	Allow this user authority to log on via the Web interface.
RMC	Enable to give user authority to log in via GBAdmin.

```

[ GNAT Box ADMINISTRATION ACCOUNTS ]
[ LOCKOUT ]
Enable: [X] Threshold: 5
Notification: [ ] Duration: 300 seconds

User ID      Password  Admin  Console  WWW  RMC
gnatbox     [ CHANGE ] [X]    [X]    [X]    [X]
            [ CHANGE ] [ ]    [ ]    [ ]    [ ]
            [ CHANGE ] [ ]    [ ]    [ ]    [ ]
            [ CHANGE ] [ ]    [ ]    [ ]    [ ]
            [ CHANGE ] [ ]    [ ]    [ ]    [ ]
            [ CHANGE ] [ ]    [ ]    [ ]    [ ]

[ SAVE ] [ CANCEL ]

```

*Administration Accounts*

```

[ CHANGE GNAT Box PASSWORD ]
User ID: gnatbox
New password: ████████████████████
Retype new password:
[ OK ] [ CANCEL ]

```

*Password Change*

## Content Filtering Preferences

Content Filtering provides the administrator with the ability to control web site access based on the content of the site. The GTA Firewall has three primary functional areas for website access control: Access Control Lists (ACL), Local Content Lists (LCL) and Preferences.

### Note

Content Filtering relies on an efficient DNS server. Define a DNS server (under Basic Configuration) to access the selected list server.

Only the Preferences functional area is available on the Console interface. Refer to the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more about Content Filtering on GBAAdmin and the Web interface.

The Preferences section for content filtering enables the administrator to specify whether to use the Traditional Proxy mechanism and associated port or the Transparent Proxy; and to specify Mobile Code Blocking preferences.

## Proxy

A proxy breaks the connection between sender and receiver. Proxy servers are available for common Internet services; e.g., an HTTP proxy is used for Web access, and an SMTP proxy is used for email.

An HTTP proxy allows Web requests to be managed by funneling all user Web requests through the proxy, where content can be filtered.

Once Access Control Lists have been created, the Proxy has been selected, and Remote Access Filters have been created and enabled, content filtering will be activated and functional. Your Remote Access and Outbound Filter choices may require adjustment to conform to your company internet access policy by allowing or denying access to specific sites or groups of users.

### Note

ACLs must be created before the proxy is enabled. Enabling the proxy is the “on switch” for content filtering: without ACLs, users will be blocked from HTTP access to the Web using TCP port 80.

## Traditional Proxy

Traditional Proxy requires users located on Protected Networks to have their browsers configured with the port number and IP address of the proxy. This method allows the most control over web requests by funneling all requests through a specific port, and allowing the administrator to disallow all other ports for access.

When a traditional proxy is used for HTTP, it runs on TCP port 2784 by default. To run the proxy on a different port, enter the value in the PORT field.

A Remote Access Filter (RAF) must be in place to use Traditional Proxy. Use the example filter below as is, or as a pattern for more restricted access.

### How to Set Up an RAF for Traditional Proxy

This RAF allows access from the Protected Network to the Internet.

1. Create a new RAF and enter a description.
2. Type: Accept; Interface: Protected; Protocol: TCP.
3. Priority: (any); Action: (any).
4. Source Address Object: ANY\_IP; Range (deselect); Source Ports (none).
5. Destination Address: <USE IP ADDRESS>; IP Address: 0.0.0.0/0; Range, Broadcast: (deselect); Destination Ports: 2784.
6. Save Remote Access Filters.

Defaulting the RAF list also creates this filter, automatically disabled for security.

## Transparent Proxy

This method is transparent to users located on the Protected Network; no modification to browsers is required, and there is no PROXY PORT field.

Transparent Proxy is the most common method of HTTP proxy because it is easier to implement than Traditional Proxy, especially when a network is very large or widespread.

Transparent Proxy does not require that each user's browser be set to the proxy port individually. However, some browsers may already be set to Traditional Proxy, or the administrator may want to direct some users' web requests through a specific port. In these cases, both the Transparent and the Traditional Proxy may be enabled.

## Content Filtering Preferences Fields

### Traditional Proxy

Enable	Select this checkbox to enable the traditional proxy.
Proxy Port	Default is 2784. Port through which the proxy will run.

### Transparent Proxy

Enable	Select this checkbox to enable the transparent proxy.
--------	---

### Mobile Code Blocking

The built-in facility blocks JAVA, JAVA Script, or ActiveX objects. These appear in the inbound HTML streams on TCP port 443, 80, 8000, and 8080.

[ Content Filtering Preferences ]

[ TRADITIONAL PROXY ]

Enable:	<input type="checkbox"/>	Port: 2784
---------	--------------------------	------------

[ TRANSPARENT PROXY ]

Enable:	<input type="checkbox"/>
---------	--------------------------

[ MOBILE CODE BLOCKING ]

JAVA:	<input type="checkbox"/>
JAVA Script:	<input type="checkbox"/>
ActiveX Objects:	<input type="checkbox"/>

[ SAVE ] [ CANCEL ] [ DEFAULT ]

*Content Filtering Preferences*



---

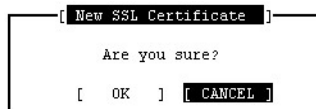
## New SSL Certificate

The New SSL Certificate feature, available on the Web and Console interfaces, allows the user to create a new SSL certificate for the currently loaded GTA Firewall. The SSL certificate must be generated after the firewall has been installed and the host name entered in the `HOST NAME` field in the Network Information screen under Basic Configuration. An SSL certificate is valid for one year.

The SSL certificate includes three levels of validity: the self-issued certificate authority; the date of certificate generation; and the firewall's host name.

Before generating a certificate, you must have installed the firewall and entered the correct host name in Network Information. To create a certificate in which the name on the security certificate matches the name on the site, make sure that the host name entered into the `HOST NAME` field in the Network Information screen matches the name given to the GTA Firewall in the DNS Server. If you cannot match the host name, you may instead add the host name to the Host file in your Windows workstation.

Once the certificate is installed and the host name has been matched to the firewall name in the DNS server, no more warnings should appear until the certificate expires. However, you can create a new certificate at any time. See the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more information about SSL certificates.



*SSL Certificate, New*

---

## Remote Administration

Remote Admin/Authentication provides a means to control remote administration via the Web interface or GBAdmin (Remote Management Console), and whether a VPN connection requires User Authentication. The default settings enable remote administration and the ability to apply updates. The Web interface is served on standard TCP port 443 for SSL encryption, non-SSL encryption is port 80. The GBAdmin (RMC) is the interface on TCP port 77 and user authentication is the interface on TCP port 76 by default.

## How to Change the Server Port

---

Implement a port number change for the Web interface in this order:

1. On the Remote Access Filters screen, find the filter that controls access and add the new port number value. The Remote Access Filter port must match the port set in Remote Administration. The default port for SSL is 443. The default port for no SSL is 80. Setting up your port and then defaulting filters will correct any port mismatch. Save the section.
  2. On the Remote Admin/Authentication screen, change the port to the new value and save the section.
  3. On the Remote Access Filters screen, return to the access filter and delete the old port. Save the section. Your firewall will now use the new port value for access
- 

## WWW Administration

In this section, the user can select access, update and SSL encryption preferences for the Web interface. A Remote Access Filter must be in place and enabled to use Web Administration.

---

### WWW Administration Fields

---

WWW Admin	
Enable	Enable remote administration via the Web interface.
Server Port	The SSL encryption Web interface default is 443. Port 80 is the standard for non-SSL HTTP, but GTA suggests using an alternate such as 8000 or 8080 to protect the Web interface even if a filter is mis-configured. Follow the procedure described above for port change.
Allow Updates	By default, updates are allowed.
Encryption	All levels of SSL encryption (Low, Medium and High) are enabled by default. SSL may also be set to None.

---

## RMC (GBAdmin)

The RMC (Remote Management Console) establishes an encrypted network connection to the GTA Firewall on port 77/TCP. By default, the GTA Firewall is only configured to allow this access on the Protected Network interface. Since the RMC network connection is encrypted, it is suitable for secure management from both External Networks and PSNs. A Remote Access Filter must be in place and enabled to use RMC.

---

### RMC Fields

---

Enable	Enable access via GBAdmin (RMC).
Server Port	The default port for RMC access is 77. Follow the procedure described above for port change.
Allow Updates	By default, updates are allowed.
Encryption	The encryption level is high.

---

[ REMOTE ADMINISTRATION ]

[ WWW ]

Enabled:

Server port: 443

Updates allowed:

Encryption: all

[ RMC ]

Enabled:

Server port: 77

Updates allowed:

[ SAVE ]
[ CANCEL ]
[ DEFAULT ]

*Remote Administration*

# VPNs

The VPNs section provides access for the creation and management of GTA Firewall VPNs using VPN Objects. It contains only the VPN Authorization material. The definition fields that were previously found in the VPN screen are now in the VPN Object screen under Objects. User fields are now found under Users on the Web interface and GBAdmin.

The supported VPN features vary depending on which platform the GTA Firewall is running. All of the flash-based products (GB-Flash, RoBoX, GB-100 and GB-1000) support automated key exchange (IKE), manual key exchange and mobile client. The floppy disk-based GB-Pro supports only manual key exchange.

## VPN Add/Edit Screen Fields

Disable	Check to disable all access for the selected VPN.
IPSec key mode	The key mode.
Description	Enter a brief description of VPN.
VPN Object	Select a VPN Object to define this VPN.
Identity	Enter user email address for user authentication. This field is used to associate the remote user with a pre-shared secret key. Use the mobile user's email address to uniquely identify the user. This value must be unique for all mobile VPN users. (Only needed when "Force Mobile Protocol" is selected.)
Remote Gateway (Destination)	Default is 0.0.0.0. Enter the IP address of the route through which the VPN will pass, the remote network gateway. If the remote network is behind a GTA Firewall, then this IP address would be one assigned to the External Network interface. This IP address will also help determine the routing of the encapsulated packet.

## Remote Network

Object	Select a previously defined Address object.
IP address (Destination)	If you selected "Use IP" to define the remote network, enter the IP address of the remote network that resides behind the remote firewall. (If it is a GTA Firewall, then typically this will be the Protected Network, PSN or a subnet of either.) Use a mask to define the type of network (e.g., 255.255.255.0 or /24 for a Class C). The destination network need not be the entire network, just the part that is to be accessible.

---

### IKE (Automated Key Exchange) Field (Phase I)

---

Preshared secret	Select ASCII or HEX* format value. Enter preshared as defined in VPN. This same key needs to be entered in the GNAT Box VPN Client Policy Editor when configuring the security policy. This field is case sensitive.
------------------	--

---

### Manual Key Exchange Fields

---

Encryption Key*	Select ASCII or HEX* format value. Enter encryption key as defined in VPN.
Hash Key	Select ASCII or HEX* format value. Enter the hash algorithm for the authentication transformation in ASCII or HEX format.

---

### Security Parameter Index (SPI)

---

Inbound/Outbound Default is 256.

---

\* Valid hexadecimal characters: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

### How to Activate a VPN

---

1. Define a VPN Security Association.
  2. Create Remote Access Filters to accept VPN packets from the remote gateway (ESP and/or AH). This can be done using the default button on the Remote Access Filter list or created by hand. Make sure you specify the correct protocol in the Remote Access Filter for the type of VPN connection that will be created. If you have not updated your protocol definition list, you should do so prior to defining any VPN filters, as the ESP and AH protocols may not be included in the list. Go to the protocol list and press the “Default” button to create a list that includes the ESP and AH protocols. Do not use the Default button if you have added protocols by hand. You can add the ESP (protocol 50) and AH (protocol 51) by hand.
  3. Create IP Pass Through Filters that allow inbound and outbound access on the defined VPN. Generally you will need two filters for each VPN definition (one for inbound access and one for outbound). If you have one or more VPN definitions, go to the IP Pass Through filter screen and press the Default button. A set of filters will be created for your VPN definitions. Please note that the Inbound filters will be disabled and set to Deny. Make modifications to these filters as required and enable them as per your local security policy. IP Pass Through Filters for VPN definitions do **not** require that entries be created on the IP Pass Through Host/Network data section.
- 

See the **GNAT BOX VPN USER’S GUIDE** for more information about VPNs.

[ GNAT Box VPNs ]

Description	
1	Jane User's Home Office
2	Mary Tester's Laptop

[ SAVE ] [ CANCEL ]

*VPN*

[ EDIT VPN ]

Disable:  IPsec key mode: IKE  
 Description: Jane User's Home Office  
 VPN object: IKE  
 Identity: janeuser@gta.com  
 Remote gateway: 25.2.63.2

Remote Network	
Object: <USE IP ADDRESS>	Address: 192.168.24.0/24

Phase 1	
ASCII: <input checked="" type="checkbox"/>	Pre-shared secret:

[ OK ] [ CANCEL ]

*IKE VPN Add/Edit*

# 11 Admin Menu

The Admin Menu contains administrative options available on the Console interface: Archive (for the Video Console), Current Statistics, Flush ARP table, Halt, Interfaces, Ping, Reboot, Set Date/Time and Traceroute.

```
Current Statistics...
Flush ARP table...
Halt...
Interfaces...
Ping...
Reboot...
Set Date/Time...
Trace Route...
```

*Admin Menu (Serial)*

```
Archive...
Current Statistics..
Flush ARP table...
Halt...
Interfaces...
Ping...
Reboot...
Set Date/Time...
Trace Route...
```

*Admin Menu (Video)*

## Archive

Archive is available for GTA Firewalls that use a floppy disk drive: GB-Pro, GB-Flash, GB-100 and the Light and Demo products. Archive functions are used to back up a configuration; to back up and restore a configuration during an upgrade; or when using Reset to Factory Defaults to clear a non-functional configuration and restore a previously stored, working configuration.

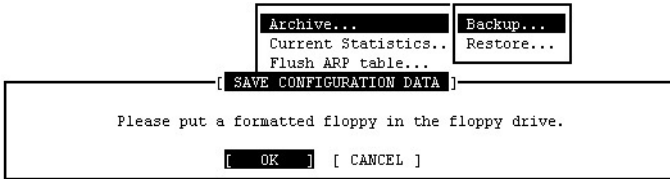
```
Archive...
Current Statistics..
Flush ARP table...
Halt...
Interfaces...
Ping...
Reboot...
Set Date/Time...
Trace Route...

Backup...
Restore...
```

*Archive Menu (Video only)*

## Backup

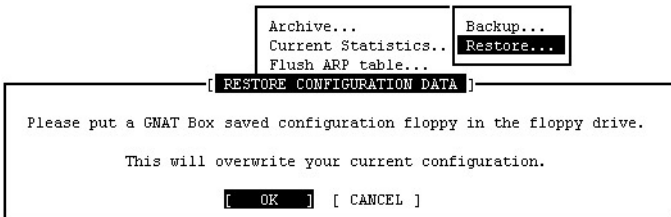
Using Archive > Backup, users of products with a floppy drive may archive a GNAT Box System Software configuration to a floppy disk.



*Backup*

## Restore

Using Archive > Restore, users of products with a floppy drive may retrieve an archived configuration from disk into the currently loaded GTA Firewall.



*Restore*

## Current Statistics

The Current Statistics item provides access to the GTA Firewall statistics display. Statistics are for both connections and packets of the protocols TCP, UDP, and ICMP. The current date, time and uptime are at the top of the form.

On the Video Console, (available on GB-Pro, GB-Flash, GB-100, GNAT Box Light and GNAT Box Demo), press the keys <Alt> <F3> to display the Statistics screen on the third video console.



## Current Statistics List

- Current and average (60 seconds) number of connections by protocol, both inbound and outbound.
- Total number of packets sent and received by protocol for both inbound and outbound traffic.
- Bandwidth utilization by protocol for both inbound and outbound traffic.
- Summary line displays totals for each column in the list.
- Summary line of the total number of packets sent and received since the system was last booted.
- Summary line of the peak bandwidth utilization.
- CPU state, which displays % user process, % system process, % interrupt, and % idle.

		Connections		Total Packets		Bandwidth Utilization	
		Current	Average	Sent	Received	Outgoing	Incoming
fxp0	OUTBOUND:	0	0.0	0	0	0	0
	INBOUND:	0	0.0	0	0	0	0
fxp1	OUTBOUND:	0	0.0	0	0	0	0
	INBOUND:	0	0.0	0	0	0	0
<b>TOTAL</b>	<b>:</b>	0	0.0	0	0	0	0
<b>PEAK</b>	<b>:</b>	0	0.0	0	0	0	0
<b>Total packets sent and received:</b>					0		
<b>Current average bandwidth utilization:</b>					0		
<b>Peak average bandwidth utilization:</b>					0		
<b>CPU states:</b> 1.6% user, 0.0% system, 0.8% interrupt, 97.7% idle							
<b>Date:</b> Thu Sep 26 11:01:37 2002. Up 5 days, 23 hours, 48 minutes.							
Please press <CF> to continue.							

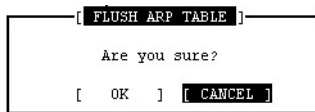
*Current Statistics Example*

## Flush ARP Table

Flush ARP Table clears the cache of addresses resolved by the Address Resolution Protocol and recorded in the ARP table.

ARP is used to dynamically map host addresses to Ethernet addresses and then cache the maps. When an interface requests a map for an IP address not in the cache, ARP queues the message and broadcasts a request for the map on the associated network. If a response is provided, the new map is cached, and any pending message is transmitted. ARP will queue one packet while waiting for a response to a map request; only the most recent packet is kept. If the target host does not respond after several requests, the host is considered to be down for 20 seconds, allowing an error to be returned for transmission attempts during this interval. The error “host is down” indicates a non-responding destination host, and “host unreachable” indicates a non-responding router.

The ARP cache is stored in the system routing table as dynamically-created host routes. These routes time out 20 minutes after being validated; entries are not validated when not in use.

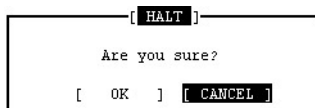


*Flush ARP Table*

---

## Halt

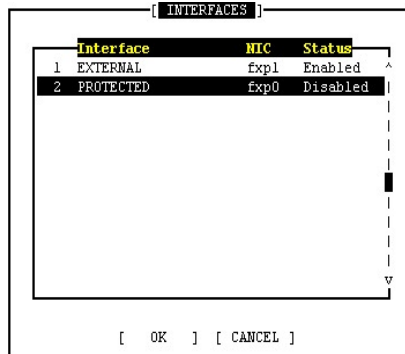
Halt stops the remote GTA Firewall. Since this will terminate your network connection to the web server, your web browser will never receive a reply. It should eventually time out or you can just press the stop button on your browser. Once halted, the GTA Firewall must be restarted either from the Console interface or by performing a power cycle or hardware reset.



*Halt Firewall*

# Interfaces

The Interfaces dialog allows a network interface on the remote firewall to be enabled, meaning up and ready to send/receive packets, or Disabled, meaning down and not accepting or sending packets. If you are using PPP/PPPoE for your External Network device, please review the PPP section of this guide.



*Interfaces*

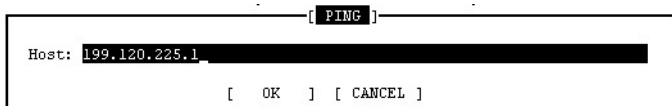
# Ping

The Ping facility provides a dialog which will execute the network connectivity test by using the Ping ICMP protocol. Since the target IP address can be on any network, the Ping facility is useful in validating your network connectivity for all network interfaces.

## How to use Ping

Enter the IP ADDRESS in dotted decimal notation or fully-qualified HOST NAME of the IP address (if DNS has been enabled).

Select OK to start the ping. The process will attempt to send five ping ICMP packets to the target IP address.



*Ping*

```
Ping host 199.120.225.1 five times.

--- PING STATISTICS ---
  5 packets transmitted.
  0 packets received, 100% packet loss.

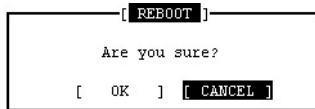
Please press <CR> to continue.
```

*Ping Results Example*

---

## Reboot

Reboot restarts the remote GTA Firewall. Since this action will terminate the Web interface's network connection to the web server, your web browser will never receive a reply. The connection will eventually time out unless you click the stop button on your web browser.



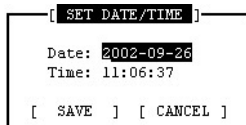
A dialog box titled "REBOOT" with the text "Are you sure?" and two buttons: "OK" and "CANCEL".

*Reboot*

---

## Set Date/Time

The Set Date/Time form provides a means to set and adjust the date and time values used on the remote GTA Firewall. The current, local time should be used when setting the time. The date should be entered in the form century, year, month and day (ccyy-mm-dd).



A form titled "SET DATE/TIME" with the following fields and buttons:

Date:	2002-09-26
Time:	11:06:37
[ SAVE ] [ CANCEL ]	

*Date/Time*

It is not possible to change the time zone facility using Console. This change must be made on the Web interface.

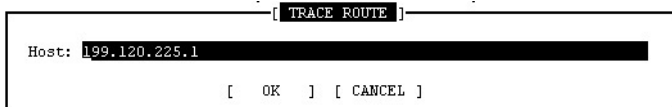
---

# Trace Route

Trace Route executes a network trace to a designated IP address or host name. The trace route is executed from the remote GTA Firewall.

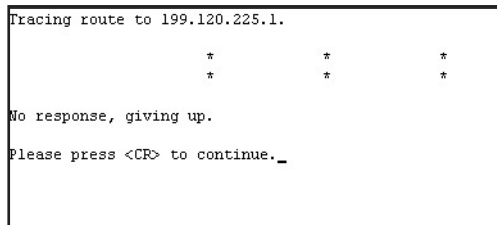
The Trace Route function is another method to test network connectivity. To determine whether a route to an Internet host is viable, Trace Route launches UDP probe packets with a short TTL (Time to Live), and then listens for an ICMP “time exceeded” reply from a gateway.

When the trace is active, three probes are launched for each gateway, with the output showing the TTL, address of the gateway, and round trip time of each probe. The Trace Route form will accept either a fully qualified host name (if DNS has been enabled on the GTA Firewall system), or an IP address in dotted decimal notation.



```
[ TRACE ROUTE ]
Host: 199.120.225.1
[ OK ] [ CANCEL ]
```

*Trace Route*



```
Tracing route to 199.120.225.1.
          *           *           *
          *           *           *
No response, giving up.
Please press <CR> to continue._
```

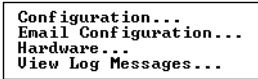
*Trace Route Results Example*



# 12 Reports

The Reports section provides access to functions that help create reports for the system hardware and software configuration: Configuration, Hardware and Email Configuration and View Log Messages.

GNAT Box System Software is delivered with GB-Reports, GTA's reporting utility. GB-Reports includes a MySQL database shell and the ODBC Data Source Names needed for access. The utility provides a standard group of spreadsheets, charts and graphs based on reports from your GTA Firewall WELF logs. GB-Reports builds its reporting menu options based on the contents of an XML (eXtensible Markup Language) file. A standard version of this file (reports.xml) is distributed with the utility. For more information, see the **GB-REPORTS FEATURE GUIDE**.

A screenshot of a menu box with a black border. It contains four lines of text: 'Configuration...', 'Email Configuration...', 'Hardware...', and 'View Log Messages...'.

```
Configuration...
Email Configuration...
Hardware...
View Log Messages...
```

*Reports Menu*

---

## Configuration

The Configuration Report is a diagnostic tool that reports the current configuration state of the GTA Firewall. The report displays information about all configuration parameters. If you need to contact the GTA support staff, they may request that you generate a current configuration report.

### **Note**

---

In non-Flash-based systems, if the configuration was loaded from a previously booted runtime disk, Ethernet MAC address information will display. Otherwise, and unknown value will be signified by ???.

```

Network Information
LOGICAL INTERFACES
Name                Type                IP Address          NIC    D
-----
EXTERNAL           EXTERNAL           192.168.71.84/24   fxp1
PROTECTED         PROTECTED         10.10.1.84/24     fxp0

NETWORK INTERFACE CARDS
NIC    MAC Address          MTU    State  Connection
-----
fxp0   00:D0:68:00:47:D1   1500   up     AUTO
fxp1   00:D0:68:00:47:D2   1500   up     AUTO
fxp2   00:D0:68:00:47:D3   1500   down   AUTO
fxp3   00:D0:68:00:47:D4   1500   down   AUTO
PPP0   0                   0       down   MANUAL
PPP1   0                   0       down   MANUAL

Default gateway: 10.10.1.1
                Hostname: doc1000.gta.com

PPP

```

*Configuration Example*

## Email Configuration

Email Configuration allows the user to email a copy of the system information to a designated support email address. GBAdmin has the Email Configuration function under the Reports Menu on the Menubar.

Email Configuration sends an email with these reports:

- A Configuration Report.
- A Hardware Configuration Report.
- A Verification Report.
- A copy of the current routing table.
- A copy of the current ARP table.
- A binary copy of the system configuration data in MIME encapsulated format.
- Active VPNs.
- Active Filters.
- Current Statistics.

Enter any additional information in the COMMENTS field.



[ EMAIL CONFIGURATION SUMMARIES ]	
To:	gb-config@gta.com
Your email address:	
Subject:	GB-1000 3.3.0s configuration, sn=51002936
Your name:	Mary Tester
Your company:	
Your phone number:	
Comment(s):	
[ SEND ] [ CANCEL ]	

### *Email Configuration*

## Hardware

The Hardware Report generates a report of the hardware components detected in your system and is useful in diagnosing hardware problems. If you suspect a hardware problem, generate this report and review the hardware listed. GTA's technical support staff may also request a current hardware report in order to resolve a GTA Firewall issue.

```

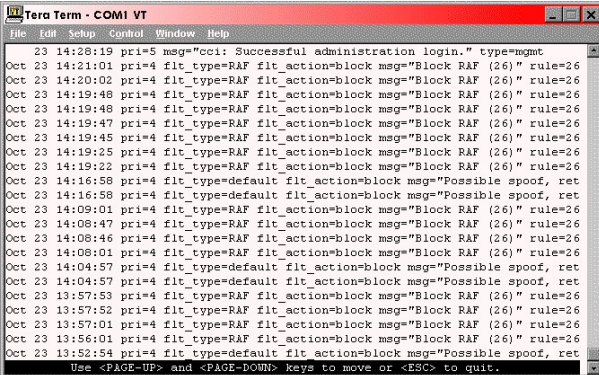
CPU: Pentium III/Pentium III Xeon/Celeron (634.79-MHz 686-class CPU)
  Origin = "GenuineIntel" Id = 0x686 Stepping = 6
  Features=0x383f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,PA
  eal memory = 134152192 (131008K bytes)
  Avail memory = 111042560 (108440K bytes)
  Pentium Pro MTRR support enabled
  hd1: Malloc disk
  Using $PIR table, 7 entries at 0xc00fdcd0
  apx0: <math processor> on motherboard
  apx0: INT 16 interface
  pcib0: <Host to PCI bridge> on motherboard
  pci0: <PCI bus> on pcib0
  pcib2: <VIA 82C598MVP (Apollo MVP3) PCI-PCI (AGP) bridge> at device 1.0 on pci0
  pcil: <PCI bus> on pcib2
  isab0: <VIA 82C596B PCI-ISA bridge> at device 7.0 on pci0
  isa0: <ISA bus> on isab0
  atapci0: <VIA 82C596 ATA66 controller> port 0xd000-0xd00f at device 7.1 on pci0
  ata0: at 0x1f0 irq 14 on atapci0
  atal: at 0x170 irq 15 on atapci0
  uhci0: <VIA 83C572 USB controller> port 0xd400-0xd41f irq 12 at device 7.2 on pc
  usb0: <VIA 83C572 USB controller> on uhci0
  usb0: USB revision 1.0

```

### *Hardware Configuration Example*

# View Log Messages

The data in View Log Messages reflects the most recent activity on the firewall. It is not drawn from the remote logging system and is constantly being updated. By default, data is written in the standard WebTrends Enhanced Log Format (WELF). The locally logged messages are stored in a fixed size circular buffer. When the buffer is filled, it will begin writing over older data. In GB-1000, RoBoX and GB-Flash, up to 1024 record entries are stored in the buffer. On GB-Pro and GB-100, there are 512 record entries in the buffer. Warning messages are displayed in red. See the Appendix in the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more about Log Messages. See Remote Logging in the guide for more about WELF.



```
Tera Term - COM1 VT
File Edit Setup Control Window Help
Oct 23 14:28:19 pri=5 msg="cci: Successful administration login." type=mgmt
Oct 23 14:21:01 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:20:02 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:48 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:48 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:47 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:45 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:25 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:19:22 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:16:58 pri=4 flt_type=default flt_action=block msg="Possible spoof, ret
Oct 23 14:16:58 pri=4 flt_type=default flt_action=block msg="Possible spoof, ret
Oct 23 14:09:01 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:08:47 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:08:46 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:08:01 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 14:04:57 pri=4 flt_type=default flt_action=block msg="Possible spoof, ret
Oct 23 14:04:57 pri=4 flt_type=default flt_action=block msg="Possible spoof, ret
Oct 23 13:57:53 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 13:57:52 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 13:57:01 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 13:56:01 pri=4 flt_type=RAF flt_action=block msg="Block RAF (26)" rule=26
Oct 23 13:52:54 pri=4 flt_type=default flt_action=block msg="Possible spoof, ret
Use <PAGE-UP> and <PAGE-DOWN> keys to move or <ESC> to quit.
```

*Log Messages Example*

# Index

## Symbols

??? 75

## A

Accept all filters 49

Access

- codes, telephone 18
- Control Lists 58

ACK 52

ACL 58

Acrobat 2

activation code 13, 16

ActiveX 60

Address

- object 32
- spoof 41

Alarms 41

Alias 44, 47

Anti-replay protocol 35

ARP Table 70

Attack

- spoof 41

Authentication Header 35

Authorization 34

Automatic filters 49

## B

Blacklist 24

Broadcast 39

button, define 7

## C

Cable 21

CIDR notation 20

COM Port 18

configuration

- copy 31
- verify. *See* verification

Connection

- type 18

Console

- primary account 57

Contact information 13

Content filtering 16

Current Statistics 68

## D

Dedicated

- address 18
- connection 18

Default

- address objects 32
- character set 14
- enabled by 14, 62
- Gateway 20, 29
- Route. *See* Default Gateway
- route, advertise 27
- VPN objects 33

DHCP 21

Dial access code 18, 45

DNS 14

- Blacklist 24
- proxy 14
- proxy override 15
- server 14

documentation 2

Doorknob twist 41, 52

Dotted decimal  
notation 20

Drivers 2

DTE 45

Dynamic

- address 18
- translation 47

Dynamic Host Configuration Protocol  
21

## E

Email

- abuse 24
- configuration 76
- proxy 23

emulator. *See* TeraTerm

encryption 28, 35, 62, 65

ESP 35, 38, 48, 65

Ethernet

- PPP over 17

Exchange Mode 34

## F

Factory defaults, settings 33.

*See* Reset firewall

Feature

- code 16

field, define 8

Filter 37

- automatic 49
- rule 54

- Fixed routes 29

- Force Mobile Protocol 34

## G

- Gateway 21

  - Default 20

- Gateway Selector 29

- GB-Pro

  - one default object 33

- GBAdmin 2

  - Administration Menu

  - Interfaces* 71

  - Ping* 71

  - Reboot* 72

  - Set Date/Time* 72

  - Trace Route* 73

- GBAuth 34

- gnatbox: user ID, password 3, 4, 5, 57

- GUI, graphical user interface 1, 3

## H

- Halt firewall 70

- Hardware 77

- Hash Algorithm 35

- Hexadecimal 16, 65

- High Availability 2

- Host name 20

  - ssl certificate 61

- How to 2, 17, 20, 22, 31, 54, 59, 62, 65, 71

## I

- ICMP 37, 43, 68, 71

- IGMP 38, 48

- IKE 33, 35, 64, 66

- Inbound Tunnel 40, 47

- Interface

  - disable, enable 71

- IP 43

- IP Pass Through 53

- ISDN 18

## J

- JAVA 60

- Junk mail 24

## K

- Keep Alive 52

- keyboard 16

- Key Group 35

## L

- limited console 6

- Local Content Lists 58

- Lockout 57

- Log

  - old format 25

  - WELF format 25

- Logical name

  - changing 19

## M

- MAC address 21, 75

- Manual Key Exchange 33, 65

- MAPS 24, ii

- Maximum Transmission Value 21

- MD5 28, 35

- mobile authentication. *See* GBAuth

- Mobile Code Blocking 60

- Mobile protocol 34

- Modem 18, 21, 45

- MTU 21

## N

- Name server 14

- NAT 47

- Network

  - Address Translation 47

- Notation

  - / 20

  - CIDR 20

  - dotted decimal 20

  - slash 20

- Note 3, 15, 17, 21, 27, 31, 33, 35, 37, 47, 48, 53, 55, 57, 58, 59, 75

  - Caution 11, 48

  - Warning 19, 21, 78

- Numeric pager 45

## O

- Object 31

- On-demand

  - connection 18

- On-enabled

  - connection 18

- Outbound Filters 37

**P**

Pager 38, 41  
Password. *See also* gnatbox  
  lockout 57  
PDF 2  
Perfect Forward Secrecy 35  
PFS 35  
Phase I 34, 35, 65  
Phase II 35  
Point-to-Point Protocol 17  
Port  
  COM 18  
ports & services. *See* well-known  
  ports, services  
PPP 17  
  over Ethernet 17  
Preferences 13  
  filter 40  
Priority  
  filter 38  
Protocol, anti-replay 35  
protocol, filter by 38  
Proxy  
  DNS 14  
  email 23  
  SMTP 23  
  transparent 60

**R**

Range 20  
Reboot 72  
Replay Detection 35  
Reset firewall 6, 9, 10, 67  
RIP 27  
Route  
  Default 20  
  static 29  
Routing Information Protocol 27  
Rule  
  filter 54

**S**

Security Association 65  
  serial number 13, 16  
SHA1, SHA2 35  
Simple Mail Transfer Protocol 23  
Slash  
  notation 20  
SMTP 23

Spam 24  
Spoof 41  
Spreadsheets 75  
SSL encryption  
  certificate 57  
Static  
  address 18  
  route 29  
  translation 47  
Static Address Mapping 50  
Statistics 68  
Stealth Mode 41  
Stop firewall 70  
Surf Sentinel 16

**T**

Technical support ii  
TeraTerm 3, 13  
Timeout 23, 51  
Time based  
  filter 38  
Trace route 73  
Transparent proxy 60  
TTL 73  
TX\_100 21

**U**

UDP 37, 48, 68, 73  
Unix 25  
  syslog 26  
User authorization 34  
User ID. *See* gnatbox  
UTP\_10 21

**V**

verification 9  
Virtual crack 53  
VPN  
  objects 33  
  Security Association 65

**W**

Wait for ACK 52  
WebTrends Enhanced Log Format  
  25  
WELF 25, 75, ii  
well-known ports, services 2, 39, 49

**X**

XML 75

## Illustrations

Address Objects, Add/Edit	32, 33
Administration Accounts	58
Admin Menu (Serial)	67
Admin Menu (Video)	67
Archive Menu (Video only)	67
Auth Menu	57
Backup	68
Basic Configuration Menu (Serial)	13
Basic Configuration Menu (Video)	13
Button: Save, Cancel, Send, OK, Default	8
Configuration Example	76
Configuration Verification Example	10
Config Menu	9
Console Interface, TeraTerm	5
Content Filtering Preferences	60
Current Statistics Example	69
Date/Time	72
Default Address Object	33
DNS	15
Email Configuration	77
Email Proxy	25
Filters Services	45
Filter Menu	37
Filter Preferences	42
Flush ARP Table	70
Halt Firewall	70
Hardware Configuration Example	77
Hosts/Networks, Add/Edit	55
IKE VPN Add/Edit	66
Inbound Tunnels, Add/Edit	50
Interfaces	71
IP Pass Through Menu	53
IP Alias, Add/Edit	48
Keyboard Layout (Video only)	16
Log Messages Example	78
NAT Menu	47
Network Information, Add/Edit	20, 22
Objects Menu	31
Outbound Filters, Add/Edit	39
Password Change	58
Ping, Ping Results Example	71, 72
PPPoE	19
Preferences (Contact Information)	14
Protocols, Add	43
Reboot	72
Remote Administration	63
Remote Logging	26

Reports Menu	75
Reset to Factory Defaults	10
Restore	68
RIP, Edit	28
Routing Menu	27
Services Menu	23
SSL Certificate, New	61
Static Routes, Add/Edit	29
Static Address Mapping, Add/Edit	51
Timeouts	52
Trace Route, Results Example	73
VPN	66
VPN Objects, Add/Edit	36

## Fields Tables

Address Object Fields	32
Admin Account Fields	57
Console Buttons	7
Console Menu Items	6
Content Filtering Preferences Fields	60
Current Statistics List	69
DNS Fields	15
Documentation Conventions	2
Documentation Map	2
Email Proxy Fields	23
Filter Fields	38
Filter Services Fields	44
Inbound Tunnel Fields	49
Network Information Add/Edit Fields	21
Network Information Fields	19
PPP/PPPoE Fields	18
Preferences Fields	14
Preferences Fields	40
Remote Logging Fields	25
RIP Edit Fields	28
RIP Fields	27
RMC Fields	63
Serial Console Keystroke Guide	4
Static Routes Fields	29
Static Address Mapping Fields	51
Timeout Fields	51
Video Console Keystroke Guide	5
VPN Add/Edit Screen Fields	64
VPN Objects Fields	34
WWW Administration Fields	62