GB-Pro

Firewall SYSTEM

Product Guide

powered by
GNAT Box
System Software

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.
Netscape Navigator is a trademark of Netscape Communications Corporation.
Internet Explorer is a trademark of Microsoft Corporation.
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 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

Tel: +1.407.380.0220
Fax: +1.407.380.6080
Web: http://www.gta.com
Email: info@gta.com

Support: support@gta.com

Document Information

GB-Pro Firewall System Product Guide
with GNAT Box System Software Version 3.3.2 November 2002

Contents

1 INTRODUCTION 1

GNAT Box Basics 1

Requirements 1

Registration & Activation 2

Installation Support 3

Documentation 4

User Interfaces 5

About GB-Pro 6

Features 6

Options 7

Hardware Reque 8

2 INSTALLATION 11

Hardware Key Block 11

Install Utilities & Documentation 12

Windows Installation 12

Unix/Linux Installation 12

Macintosh Installation 13

DOS/Windows 3.x Installation 14

Using GNAT Box Utilities 14

Make a Runtime Disk with gbMake Floppy 14

Merge Configuration Data with gbMakeFloppy 15

Make a Runtime Disk Using GBWrite 15

3 SET UP DEFAULT CONFIGURATION 17

Load the System 17

Using the Setup Wizard 18

PPP/PPPoE Configuration 22

Access the GB-Pro 24

4 TROUBLESHOOTING 25

Guidelines 25

Troubleshooting Q & A 26

INDEX 29

1 Introduction

GNAT Box Basics

Since 1994, Global Technology Associates, Inc., has been designing and building Internet firewalls. In 1996, GTA developed the first truly affordable commercial-grade firewall, the GNAT Box®. Since then, ICSA-certified GNAT Box System Software has become the engine that drives all GTA firewall systems.

GTA's firewall systems, powered by GNAT Box System Software, currently include GB-Pro, GB-Flash, GB-1000 and RoBoX™. GTA's optional features include GNAT Box VPN, Surf Sentinel (content filtering), and H_2A (high availability).

Requirements

To use GNAT Box System Software, you need to know the following:

- An understanding of TCP/IP networking.
- Network IP addresses for all network interfaces used.
- Netmasks for each attached network.
- Default route for External Network.
- Services to allow inbound/outbound (if any).

To initially configure the GB-Pro using the Video Console interface, you must have a video card installed, and a monitor and keyboard connected.

To connect the GB-Pro to your network, you need at least two Ethernet cables, one for each required network: a crossover cable to connect the firewall directly to a host or router; or a straight-through cable to connect the firewall to a hub or switch.

Registration & Activation

Each GTA Firewall requires an activation code, serial number and hardware key block to be fully functional. They will only function when installed on the specific system. The activation code and the serial number are located on:

- Label of the product box.
- Registration card included inside the product box.
- Once registered, on the GTA website under Support.

To register, go to www.gta.com, click on Support, then on the GTA Support Center link. This takes you to the login screen. If you already have an account, enter your User ID and password. If you have not yet created an account, click New Account, enter profile information and choose a User ID and password. Once you have completed the form, click Add to save it.

Return to the login screen and enter the User ID and password you created. In the Make a Selection screen, click Support Center, then click on Product Registration in the next screen, the Account Home screen for your support information. In the form that appears, enter your serial number and activation (unlock) code, then click Submit. Your new product will now appear in the View Registered Products screen, accessible from the Account Home page.

Note

If you cannot retrieve your registration code, or a feature code does not appear under View Registered Products, email support with the product serial number and your Support Center User ID in the message subject.

In addition to qualifying you for installation support, your product registration will allow GTA to inform you about upgrades and special offers.

Copy Protection

Copying of GNAT Box System Software is allowed for backup purposes. However, to activate your system and any special features, you will need a serial number and activation codes. Keep a copy of these codes; the codes will also be available online at the GTA Support Center after completing the product registration.

In addition, the GB-Pro and GB-Flash require a hardware key block. This is provided with your product. See Installation, Chapter 2, for instructions on installing the hardware key block.

Activation Codes

All commercial GTA Firewalls–GB-Pro, GB-Flash, GB-100, GB-1000 and RoBoX–use activation codes to protect software. For firewall appliances, the required registration code is pre-installed. Codes are printed on packaging and available at www.gta.com in the GTA Support Center.

Feature Activation Codes

If you purchased additional features for your GTA Firewall, you will be provided with a feature activation code for each. The activation codes for new features must be entered in Features under the Basic Configuration menu. Your feature activation codes can be found under View Registered Products on the GTA Support site by selecting the GB-Pro by its serial number.

Installation Support

Installation ("up and running") support is available to registered users. If you have registered your product and need installation assistance during the first 30 days, contact the GTA Support team by email at support@gta.com.

Include in the email your product name, serial number, registration number any feature activation code numbers for your optional products, and a System Software or Hardware Configuration Report, if possible.

Installation support covers only the aspects of configuration related to installation and default setup of the firewall. For further assistance, contact the GTA Sales staff for information about GTA’s support offerings.

Support Options

If you need support after installation and configuration to defaults, contact the GTA sales department to purchase a support contract. Contracts range from support by the incident to full coverage for a year.

Other avenues for assistance are available through the GNAT Box Mailing List and Forum, on the GTA website, found at www.gta.com, or through an authorized GTA Channel Partner.

Upgrades

Once registered, you can view available upgrades by going to View Registered Products in the GTA Support Center. If there is an upgrade available and you are on the latest version of GNAT Box System Software, e.g., 3.3.x, or have a current support contract, the Action column in the View Registered Products section will have a Free Upgrade link. If no update is available, the Action column will display “Up to date.”

If you are not on the current version and do not have a current support contract, an upgrade for the latest patch release, e.g., 3.3.2, will display if one is available. If no patch is available, the Action column will display "Purchase Upgrade/Support."

If an upgrade is available for your product, click the upgrade link.

When you return to the View Registered Products list, click the product's serial number and see the Product Details section to obtain the new activation code. The Product Details section will also display your previous activation codes. Upgrades are also available in Support Center Downloads. Only downloads for your version will be shown.

Caution

Back up your configuration before upgrading!

Documentation

This Product Guide describes how to install the GB-Pro on your selection of hardware and set up the GNAT Box System Software in your network's default configuration. The GNAT BOX SYSTEM SOFTWARE USER'S GUIDE includes configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms.

Documentation Conventions

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this in a PDF, color variations are also used to emphasize notes, warnings and new sections.

Documentation Conventions

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

Notes are indicated by an indented, italicized headline.

The note body copy is further indented.

"How to" sections are indicated by an indented, bold headline.

The "How to" body copy is unbolded and closed with a rule line.

Additional Documentation

Documentation is available for GTA Firewall product owners. Product Guides show how to install and set up GTA Firewall products. Feature Guides describe GTA optional features. The GNAT BOX SYSTEM SOFTWARE USER'S GUIDE includes advanced configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms.

Documentation Map

Topic	Document Name	Location
Installation	Product Guides	Shipped w/product*
System Setup	Product Guides	Shipped w/product*
GNAT Box Concepts	Concepts	www.gta.com
Troubleshooting	User’s Guide or Product Guides	Shipped w/product, CD*
Configuration examples	–	www.gta.com
Sample reports	–	www.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_2A Feature Guide	Shipped w/product*
VPN	GNAT Box VPN Feature Guide	Shipped w/product*
VPN Examples	GB-VPN to VPN Tech Docs	www.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	www.gta.com

* All documents for registered products can also be found on the www.gta.com website.

User Interfaces

GNAT Box System Software, GTA's operating system running on the GB-Pro, has three user interfaces: GBAdmin, the Web interface and the Console interface. For more information about the interfaces, see the GNAT BOX SYSTEM SOFTWARE USER'S GUIDE and www.gta.com.

GBAdmin

GBAdmin is a Windows-based interface that can be operated without access to the Internet. The program has on-screen Help and uses standard Windows commands and conventions. It also requires a Windows-based computer or workstation and Internet Explorer, version 5.0 and up.

Web Interface

The Web interface can be used on any compatible browser, including Internet Explorer, Netscape Navigator, Mozilla and Opera, running on platforms such as Windows, Unix and Mac, with any caveats noted in the appropriate product guides and release notes.

Console

After setup, the Console interface is used for limited configuration changes and to reset the firewall to factory defaults. As of the GNAT Box System Software version 3.2.2 release, the Console interface on the GB-Pro and GB-100 is available only as the limited Video Console interface, accessed directly on the target system, due to disk space restrictions. For Console interface instructions, see the CONSOLE INTERFACE USER'S GUIDE at www.gta.com.

Note

The Web interface and GBAdmin offer complete functionality on GB-Pro.

About GB-Pro

GB-Pro is a complete software-based firewall. The GB-Pro contains Global Technology Associates' latest software technology, installable on the user's Intel-based hardware. After installation on the target system, GB-Pro must be configured for local network requirements.

The Product Guide describes and explains how to install, set up and initially configure the GB-Pro. For more instructions on user interfaces and configuration options, see the GNAT BOX® SYSTEM SOFTWARE USER'S GUIDE.

Features

- Stateful Packet Inspection
- Unlimited user license
- Built-in IPSec Manual Key Exchange VPN
- 128,000+ concurrent sessions

- ICSA-certified GNAT Box System Software
- Dynamic & static Network Address Translation (NAT)

* IP aliasing

- RIP support
- Stealth mode
- Remote logging
- Secure encrypted remote management
- Multimedia Application support (Real Audio, QuickTime Streaming)
- Secure Email Proxy (SMTP)
- ISDN TA/Async modem support

Software Specifications

- Max Concurrent Connections: 128,000+
- Remote Access Filters: 400
- Outbound Filters: 400
- Tunnels: 300
- Aliases: 300
- Static Routes: 300
- Static Maps: 300
- Time Groups: 100
- IP Pass Through Filters: 400
- VPN Security Associations (optional): 300
- Objects: 300

CD-ROM Distribution

GB-Pro software is distributed on an ISO 9660-compliant CD-ROM. While a CD-ROM is not a required component of the GB-Pro, the user will need a CD-ROM drive in order to create a GNAT Box runtime floppy disk from the Installation CD-ROM. A DOS, Windows 98, 2000, NT or XP, Macintosh or Unix system may be used to create the runtime disk, as long as the system can read an ISO 9660 CD-ROM.

Options

- Multi-Interface Option
- Support Contract

Hardware

The GB-Pro is designed to operate efficiently on a broad spectrum of hardware, but the hardware you select will impact the GB-Pro's performance. This is especially true when the GB-Pro is used in an Intranet configuration with full network speeds on all interfaces. The best possible performance can be obtained by using a Pentium CPU with PCI based network cards. However, organizations with low speed (56Kb or less) Internet connections will find that 486 ISA based systems perform satisfactorily.

Network performance bottlenecks usually occur at the connection to the Internet when using DSL or T-1 class connectivity. A GB-Pro with 10 Mbps Ethernet cards easily provides enough throughput for network connectivity of up to T-1 speeds (1.5 Mbps). However, when the WAN connectivity is a T-3 or faster, GTA recommends that 100Mbps be used.

If you encounter problems, check your motherboard and IRQ assignments. Make sure any unused devices, such as IDE and SCSI controllers, sound cards and serial ports are disabled. Scan the hardware configuration report for error messages–often the cause of a problem is indicated in this report.

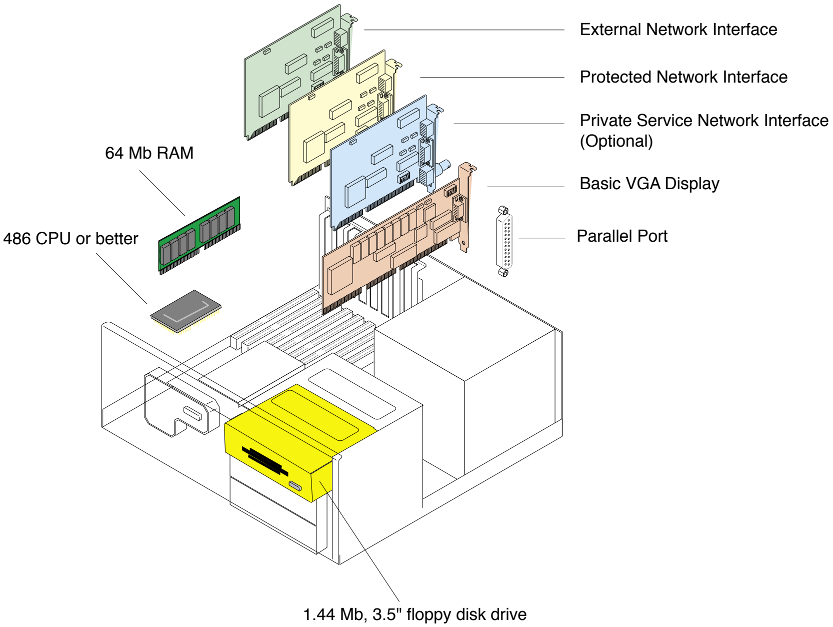
Note

Check www.gta.com for an up-to-date list of compatible NICs and drivers.

Hardware Requirements for GB-Pro

Qty	Description
1	Intel or compatible, 486 or better
1	64 MB RAM
1	1.44 Mbyte 3.5" disk drive
2	Supported network interface cards (minimum)
1	Basic VGA display adapter
1	Parallel printer port
1	Monitor (installation only)
1	Keyboard (installation only)
18	Additional NICs supported with Multi-interface option
1	Serial Port - COM 1-4 (1645x/1655x UARTs only)
1	Async modem for PPP connections or pager
1	ISDN TA with RS-232 interface for PPP connections

* Multi-interface option supports up to 20 total NICs.


External Network Interface
Protected Network Interface
Private Service Network Interface (Optional)
Basic VGA Display
Parallel Port
64 Mb RAM
486 CPU or better
1.44 Mb, 3.5" floppy disk drive

Hardware Diagram

Note

GTA recommends only installing the required components in the system. Devices such as SCSI controllers, sound cards and hard disks remain unused and may complicate installation and compromise performance.

PPP Hardware

The GNAT Box System Software supports the use of a PPP network connection in place of a network interface card for the External Network interface. The PPP interface supports only a dial-up connection and a single remote system configuration.

- An external asynchronous modem. COM ports 1-4 are supported; only COM ports based on the 1645x/1655x UARTs are supported.
- An internal asynchronous modem. Only modems that use 1645x/1655x compliant UARTs are supported.
- An ISDN external modem/terminal adapter. COM ports 1-4 are supported; only COM ports based on the 1645x/1655x compliant UARTs are supported.
- NIC card for use with PPPoE (ADSL).

Serial Ports

Most serial ports will easily support any asynchronous modem or a single BRI 64KB ISDN connection. If both channels of a BRI line are used to achieve 128KB, throughput may be limited to 115KB, due to serial port limitations.

Modem/ISDN TA Configuration

GTA recommends configuring the modem or ISDN TA on another system before installing it on the GTA Firewall system. Most modems allow the storage of a user configuration and the recall of this configuration using a specific command (e.g., ATZ). It is usually easiest to recall a configuration and set the modem to a known state with a few commands.

Note

The default configuration for most modems will generally work.

It’s recommended to configure the modem to use a fixed DTE speed (the speed at which the computer talks to the modem). If the modem supports DTE speeds of 38,400 or 57,600, use one of these values to ensure the highest throughput. Configure your serial port to the highest possible speed when using an ISDN TA. Unless you wish to connect at a specific speed, set DCE (the speed at which the modem talks to a remote modem) to auto-negotiate.

Cable Modems and xDSL Configurations

Cable modems and xDSL configurations utilize a passive inter-connection device (cable modem, xDSL box) that is typically connected to an Ethernet card via a special network patch cable (crossover cable).

Memory Requirements

The GNAT Box System Software can operate with a memory size as small as 32 megabytes. However, you should consider certain factors when selecting a memory configuration for your GB-Pro. The table below lists the maximum concurrent sessions possible for a given memory configuration.

Memory and Concurrent Connections

RAM	Connections
32	24,576
40	24,576
64	32,765
128	128,000

* Generally, the more services that are being utilized (e.g., local Access Control Lists, Email Proxy), the more RAM is recommended for optimum performance.

2 Installation

Hardware Key Block

After setting up the hardware and before creating the runtime disk, install the hardware key block (sometimes called a dongle).

GTA's system is different from other key blocks because it is attached only to the GTA Firewall and not to any client workstations. The key block also provides freedom to upgrade or change system hardware: simply attach the hardware key block to the new equipment and boot the runtime disk.

The hardware key block must be installed in the parallel (printer) port. The side to be attached to the port is labeled COMPUTER, with arrows pointing in the direction of the computer. Screws are provided to connect the key block securely to the port. If the computer is close to a wall or other obstacle, you can attach an extension cable to the port, then attach the hardware key block to the cable. Use a straight-through, 25-pin, male-to-female cable.

If the Hardware Key Block is not recognized by your system, and you have checked that your serial number and activation code are both entered correctly, make sure that your system's parallel port is set to the values below.

Hardware Key Block Settings

Address (Hex Value)	IRQ
0x378	7
0x278	5
Mode	ERP, SPP or Both

Note

If you have received a demo disk or downloaded demo GB-Pro software from GTA's website, you will not have the required hardware key block. Without the key block the software will be operational for a limited time. (180 minutes, decreasing by 30 minutes at each reboot.)

Install Utilities & Documentation

Prior to setting up the GB-Pro, install the utility software and documentation on your workstation. If the workstation is running Windows 95, 98, NT, Me, XP or 2000, there is an automated installer on the CD-ROM that will install these files. If the workstation is running a non-Windows based OS (e.g., Macintosh or Unix) or an older version of Windows, follow the instructions for your workstation platform. These instructions are also available in the ReadMe in the directory on the CD-ROM for your OS.

Note

If you obtained the GB-Pro system via the Internet, skip the references to the CD-ROM and begin following the procedure after the software has been extracted from the CD-ROM.

Windows Installation

1. Insert the CD-ROM into a CD-ROM drive; the installer should auto-start.
2. If the installer doesn't start automatically, open the "My Computer" icon on your desktop by double-clicking it. Find the GNAT Box CD icon and double-click to open it. Double-click the "Install" icon, launching the installer application.
3. Options range from a complete install of all software, to copying just the GNAT Box System Software runtime image to your hard disk. A complete installation includes GNAT Box System Software, GBAdmin, the remote logging client, the database client, Acrobat PDF manuals and useful text files. At a minimum, select the GNAT Box System Software runtime image and GBAdmin program.
4. Next, you have the option to create a GNAT Box System Software runtime disk. Choosing this option ensures that you will have a bootable runtime system disk. You may instead choose to create a runtime disk after the installation process by using the utility applications gbMakeFloppy or GBAdmin.

Unix/Linux Installation

Unix systems vary, but most systems that support 3.5" 1.44Mb floppy disk drives should be able to create the GNAT Box System Software runtime disk. On most systems you will need to execute these commands as "root." The file names on the CD-ROM may appear in upper or lower case depending on how your operating system mounts the CD-ROM. Use the following procedure:

1. Create a directory where you want to install the GNAT Box software.
2. Format a 3.5” 1.44Mb disk.
3. Mount the GNAT Box CD-ROM as a ISO 9660 file system.

   (e.g. SunOS mount -r -t hsfs /dev/sr0 /cdrom).
4. Change directory to the Unix directory on the CD-ROM (e.g. cd /cdrom/unix).
5. Copy the contents of the Unix directory to the directory you created on your Unix system.
6. Insert the formatted floppy disk into your Unix system.
7. Use the Unix “dd” command to copy the GNAT Box System Software runtime image to the floppy disk.

Examples:

Write a GNAT Box disk:

```
dd if=gbp300.flp of=/dev/rfd0c bs=18k
```

Read a GNAT Box disk:

```
dd of=/tmp/myGNATBox.flp if=/dev/rfd0c bs=18k
```

Read only the configuration data from a disk:

```
dd if=/dev/rfd0c of=/tmp/config.flp seek=78 bs=18k
```

Write only the configuration data from to disk:

```
dd of=/dev/rfd0c if=/tmp/config.flp skip=78 bs=18k
```

Note

These examples are for Free BSD; your raw floppy disk device may have a different name.

Macintosh Installation

The GNAT Box System Software CD-ROM is a hybrid ISO 9660/Mac CD-ROM. Macintosh users should have no problem mounting the disc. A GNAT Box System Software boot/runtime disk image has been provided in the runtime folder.

Macintosh OS9

The runtime image has been stored in a Stuffit archive, in the DiskDup+ format. Unstuff the archive by double-clicking the .sit file. Launch DiskDup+ to create the runtime image. This program can be used to write the GNAT Box System Software runtime disk image to a DOS-formatted disk.

Macintosh OSX

The runtime image has been stored in a WinZip archive. Unstuff the archive by double-clicking the Mac OSX .tar file; this will create folder on the desktop. Double-click the folder to show the GNAT Box .flp files.

DOS/Windows 3.x Installation

Use the command line utility GBWrite.exe to create the disks. Use the following command:

```
GBWRITE A gbp-3xx.flp
```

or

```
GBWRITE A gbp-3xx-ppp.flp
```

Command line syntax is:

```
GBWRITE floppy_disk_drive_letter runtime_image_filename
```

Using GNAT Box Utilities

As an alternative to the automatic Install and Setup Wizards, use these GNAT Box utilities to perform installation and configuration tasks.

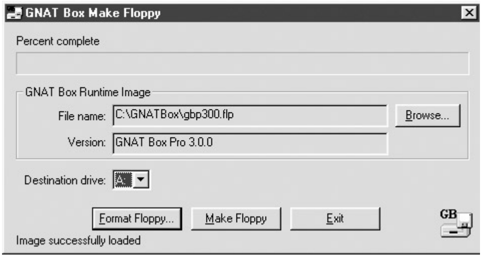
Make a Runtime Disk with gbMake Floppy

The utility gbMakeFloppy provides a convenient method for making clean unconfigured runtime disk images for either GB-Pro or GB-Pro for PPP. Use the Installation CD-ROM on a workstation; the disk cannot be created using your runtime system.

The program is accessible under the GTA Firewall group in the Start menu as “Make GB-Pro Floppy” and “Make GB-Pro PPP Floppy.”

1. Click the gbMakeFloppy menu item or icon. Launching the program from the Start menu will load the specified runtime image (Pro, Demo or Light) automatically into gbMakeFloppy. The runtime image version information is displayed in the Version field.
2. Insert a 3.5” 1.44Mb disk into the floppy drive.
3. Select the destination drive letter of the floppy drive (usually, “A”) from the “Destination Drive” pull down menu.
4. If the disk is not formatted, use the “Format Floppy...” button to format the disk.

5. After the disk is formatted, click the “Make Floppy” button to copy the runtime image to your disk. (A progress bar at the top of the application window will display the percentage of data copied.) When the process is complete, you may remove the disk.
6. Insert the disk into your target GTA Firewall system and boot it up. The Setup Wizard will appear. Use this to initially configure your system.



File name: C:\GNATBox\gbp300.flp

Version: GNAT Box Pro 3.0.0

Destination drive: A:

Image successfully loaded

gbMakeFloppy

Merge Configuration Data with gbMakeFloppy

You can also use gbMakeFloppy to merge a previous configuration with a new runtime image, allowing you to save the settings created. (See release notes for which system versions are readable by the current runtime system.)

1. Before creating the runtime disk, click the GNAT Box icon in upper left hand corner of the title bar. This will display a menu.
2. Select the “Merge configuration” menu item.
3. Select the configuration file you wish to merge.

   The file should contain only GNAT Box configuration data, not a complete runtime disk image. Your configuration data will then be merged with the runtime image.
4. Continue with the instructions to make a runtime disk. Your runtime disk will blend the new runtime image with the specified configuration data.

Make a Runtime Disk Using GBWrite

Use the command line program GBWrite.exe to copy the runtime disk image to your formatted floppy disk. The GBWrite.exe program will prompt you for the target disk drive letter and the name of the GNAT Box System Software runtime disk image file.

Example: `GBWRITE A GBP332.FLP`

3 Set Up Default Configuration

Load the System

To load the GB-Pro system, insert the GB-Pro runtime disk into the 3.5” 1.44 MB floppy disk drive of your target system. Make sure the floppy disk is not write-protected, as your configuration parameters need to be stored on this disk. Apply power, and let the GB-Pro system boot from the disk and load into memory. (Your monitor and keyboard must also be attached.)

The Video Console interface will start automatically when the runtime disk is booted up, and the Setup Wizard will appear. A limited Video Console is installed with GB-Pro, GNAT Box Light and GNAT Box Demo.

Three virtual modes operate on the Video Console: log messages, the main interface and statistics. View log messages on the Video Console by pressing <ALT><F1>. Press <ALT><F2> to switch to the main Video Console interface. These keys are always active. After initial setup, see firewall statistics by pressing <ALT><F3>. For more information, see the CONSOLE INTERFACE USER’S GUIDE, available on the installation CD and on the web at www.gta.com.

Video Console Interface Keystroke Guide

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

Once the system kernel is loaded, it will begin to probe for system hardware. To verify that the system has discovered and recognized your network cards, press <Alt><F1> to see the log messages. To scroll through the messages, engage the Scroll Lock key, and use either the <Page Up> <Page Down> keys, or the up/down <Arrow> keys.

Note

> After the system has been loaded and configured, you can also view this information using the Configuration Verification item on the Console interface or View Log Messages under the System Activity Menu using GBAdmin or the Web interface.

If your hardware was configured correctly and the system did not encounter any problems, the Setup Wizard should appear.

Using the Setup Wizard

GTA recommends using the GB-Pro Setup Wizard for easy firewall setup. There are a number of options in the GB-Pro setup: a configuration in which one network interface is PPP or PPPoE; a one in which one or both required network interfaces is DHCP; or a configuration in which both interfaces are static connections, neither PPP or DHCP. After step #4, select the option appropriate to your connection type.

1. GNAT Box Licensing Agreement

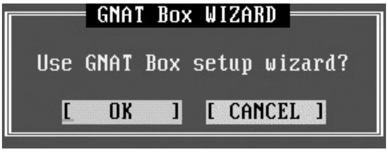
Move the cursor to “View License”; if you agree to the terms, select <Esc> to return to the previous display and select “Accept.” If you don’t accept the terms, select “Do Not Accept” to terminate the software installation.

2. GNAT Box Wizard

The next dialog box will prompt you to use the GNAT Box Wizard. Select “OK.” If you choose not to use the Wizard, select “Cancel.”

Note

> Canceling will call up the “Network Information” screen. After completion, the system will continue the boot process. Please consult the **Console Interface User’s Guide** at www.gta.com for a complete reference.



GNAT Box WIZARD

Use GNAT Box setup wizard?

Setup Wizard

3. Host Name

The next dialog box will prompt you for the Host Name of your GTA Firewall. The host name identifies your GTA Firewall system, but is not a fully-qualified domain name. Once you enter the name, select Next.

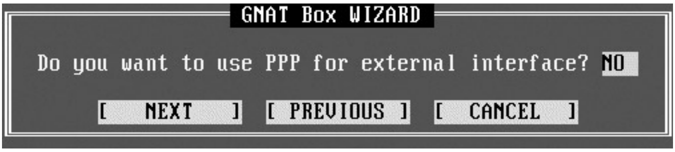
4. Contact Information

In the next dialog box, fill in the contact information and serial number for your GTA Firewall. The activation code and serial number are located on the product box, the registration card, and on the GTA website under Support after registration. Go to 5a if you are loading a PPP/PPPoE runtime image, otherwise, go to step 5b.

5a. PPP/PPPoE Runtime Image

If you have loaded a PPP/PPPoE runtime image, the next dialog box will ask whether or not you wish to use PPP on the External interface. Select “No” if you will not be using PPP/PPPoE, and go to step 5b.

Otherwise, select “Yes” by toggling the field value and selecting Next, and go to page 21, PPP/PPPoE Configuration, step A. You must load the PPP runtime image to use PPP/PPPoE.


GNAT Box WIZARD

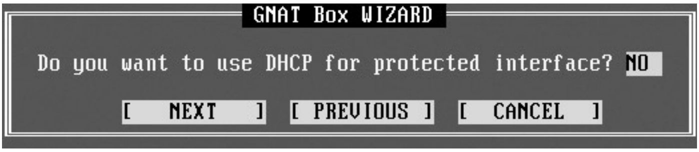
Do you want to use PPP for external interface? NO

Use PPP?

5b. DHCP (No PPP/PPPoE)

The next dialog box offers to run DHCP on the network interface. If your system will not utilize DHCP on the selected interface, select “No,” and go to step 5c.

If your system will use DHCP on the selected interface, go to step 6. (Typically, cable modem and xDSL sites use DHCP.)


GNAT Box WIZARD

Do you want to use DHCP for protected interface? NO

Run DHCP?

5c. IP Address (No DHCP)

If you do not choose to use DHCP on the interface, the dialogs in step 5c will prompt you for the IP address and subnet of the network interface.

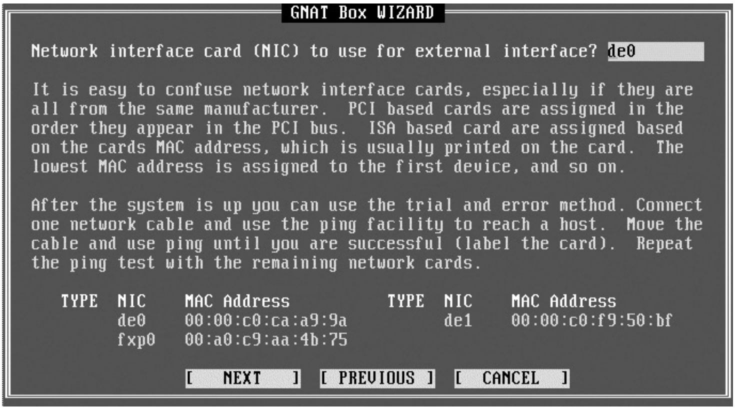
The IP address for the External Network interface should be a valid registered IP address if you will be connecting to the Internet.

6. Network Interface Card for the External, Protected or PSN

Next, select an available NIC (Network Interface Card) to assign to the interface. Use <F2> or the <space bar> to select from the device list. Each NIC detected on your system and its MAC address are listed at the bottom of the screen.

Note

All networks or sub-networks attached to a GTA Firewall interface must be on a logically different network from one another.



```
Network interface card (NIC) to use for external interface? de0

It is easy to confuse network interface cards, especially if they are
all from the same manufacturer.  PCI based cards are assigned in the
order they appear in the PCI bus.  ISA based card are assigned based
on the cards MAC address, which is usually printed on the card.  The
lowest MAC address is assigned to the first device, and so on.

After the system is up you can use the trial and error method. Connect
one network cable and use the ping facility to reach a host.  Move the
cable and use ping until you are successful (label the card).  Repeat
the ping test with the remaining network cards.

   TYPE  NIC    MAC Address          TYPE  NIC    MAC Address
         de0    00:00:c0:ca:a9:9a          de1    00:00:c0:f9:50:bf
         fxp0   00:a0:c9:aa:4b:75
```

Select Network Interface Card

7. Protected Network Interface

The following set of dialogs assist you in selecting DHCP and NIC or assigning an IP address, subnet and NIC device for the Protected Network. (The Protected Network interface is required.) Use steps 5b, 5c, and 6. If you are not setting up a PSN at this time, go to step #9.

Note

Because GTA Firewalls perform NAT (Network Address Translation), the IP address and any network addresses behind the GTA Firewall (i.e., attached to, or on the Protected Network or PSN) can be unregistered.

8. Private Service Network Interface (Optional)

The following set of dialogs assist you in selecting DHCP and NIC or assigning an IP address, subnet and NIC device for the PSN. (The PSN interface is optional.) Use steps 5b, 5c, and 6. Once you have set up the PSN at this time, go to step #9.

Note

If you are setting up a new network, GTA recommends choosing network addresses described in RFC 1918. The Internet Assignment Numbers Authority (IANA) has specified network addresses in RFC 1918 that are designated exclusively for private networks.

IANA Private Networks

Qty	Network Type	Address Range
1	Class A	10.0.0.0 - 10.255.255.255
16	Class B	172.16.0.0 - 172.31.255.255
255	Class C	192.168.0.0 - 192.168.255.255

9. Gateway/Default Route on External Interface (No DHCP or PPP/PPPoE)

If your External Interface is not DHCP, complete this step.

Once the IP address, netmask, and device assignment have been made, you will be prompted for the default route for your GTA Firewall system. The Setup Wizard will have already determined the network portion of the IP address, so only the host portion needs to be entered.

10. Password

Next, assign a password to your GTA Firewall system (required). The dialog will provide data entry fields for password assignment. Initially, the User ID is set to “gnatbox”, however, it can be changed later in Admin Accounts under the Authorization menu.

Note

GTA recommends changing the default user ID and password. See the **GNAT Box System Software User's Guide** for instructions.

The summary screen displays all your configuration settings. If you need to make changes, use the “Previous” button to move back to the desired dialog and make corrections. You cannot make changes directly to the summary.

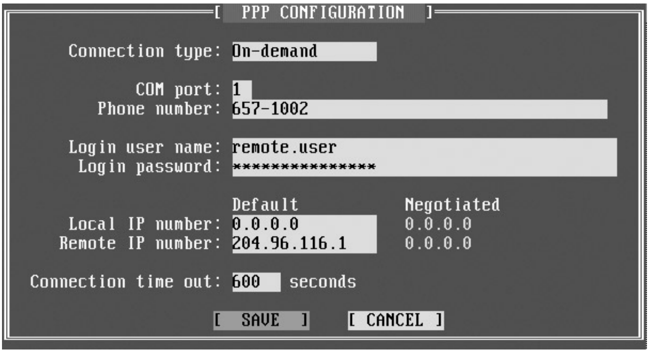
Once you are satisfied with your settings, select Save and allow the GTA Firewall to boot up into its fully operational mode. Initial configuration is complete. Go to the last section in this chapter, “Access the GB-Pro.”

PPP/PPPoE Configuration

As an alternative to the typical External Network configuration that uses a network interface card (NIC) and stand-alone router, a GTA Firewall can be configured to use serial PPP (Point-to-Point Protocol) or PPPoE (PPP over Ethernet, which uses a NIC connected to a DSL modem) for the External Network interface. The PPP/PPPoE interface can utilize internal and external async modems and external ISDN TAs.

To configure PPP/PPPoE, you must have already set up and installed your communications device according to the GB-Pro hardware installation instructions in Chapter 1–Introduction and the device manufacturer’s guidelines.

The steps in this section, designated A-F, continue from step #5a of the instructions. Note that the selections in step B are different.



```
PPP CONFIGURATION

   Connection type: On-demand

          COM port: 1
      Phone number: 657-1002

   Login user name: remote.user
    Login password: ***************

                    Default            Negotiated
   Local IP number: 0.0.0.0            0.0.0.0
  Remote IP number: 204.96.116.1       0.0.0.0

Connection time out: 600  seconds
```

PPP Configuration

When you have finished the PPP/PPOE portion of the setup, return to the previous section and complete steps #7 through #10.

Note

Using 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. Use the Web interface or GBAdmin to configure additional PPP/PPPoE connections. See the **GNAT Box System Software User’s Guide** for more information.

A. Choose the connection type from the list using the <space bar>.

On-Demand: If the link is down, an on-demand connection will initiate and establish a connection with the remote site whenever a packet arrives on the Protected Network or PSN and is destined for the External Network. The link will stay established unless the time-out period expires.

On-Enabled: An on-enabled connection requires the administrator to manually enable the External Network interface, initiating a session and establishing a link with the remote site. The External Network interface may be enabled either from Admin -> Interfaces menu item on the Console interface or from the Administration -> Interfaces item on the Web interface. The link will stay established until manually disabled.

Dedicated: A dedicated connection establishes a link when the firewall boots up. The link will stay established until manually disabled, or the system is halted.

B.

PPPoE Configuration

i. Select PPPoE if you are creating a connection over Ethernet.

ii. Select NIC to be used for the PPPoE connection.

iii. Leave the PROVIDER field blank unless you know the **exact** designation. An incorrect ISP name will cause the connection to fail.

PPP Configuration

i. Leave PPPoE unchecked (deselected) if you are using PPP.

ii. Select the COM port, internal modem card or serial interface, to be used for the PPP interface. COM ports 1-4 are allowed.

iii. Enter the telephone number of the remote site, The number should contain any special access codes or dialing directives required to call the remote site. Special characters used for pauses and secondary dial tones can be used. Consult your modem or ISDN TA manual for dialing codes.

C. Enter the login user ID and password, then enter the user ID issued by the remote site for PPP access, and the associated password. The password is obscured in the data entry field.

D. Assign IP numbers. A PPP/PPPoE link uses two IP addresses, one local and one remote. GNAT Box System Software is capable of negotiating the addresses dynamically if the remote site supports dynamic address assignment, the default for ISPs and remote sites. Dedicated IP addresses are supported for either, or both, sides of the connection.

How to make dynamic and static IP Address assignments

Both local and remote sites use dynamic address assignment:

- Leave the LOCAL IP ADDRESS field set to 0.0.0.0, the default.
- In the REMOTE IP ADDRESS field, enter an IP address that may be assigned dynamically. It is not important that the IP number is actually the one assigned, since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote

network. A good choice for this number is the remote system's router IP address or DNS server IP address.

Both local and remote sites use static address assignment:

- In the LOCAL IP ADDRESS field, enter the dedicated IP address.
- In the REMOTE IP ADDRESS field, enter the dedicated IP address.

Local site uses static assignment, remote site uses dynamic:

- In the LOCAL IP ADDRESS field, enter the dedicated IP address.
- In the REMOTE IP ADDRESS field, enter an IP address that may be assigned dynamically. It is not important that the IP number is actually the one assigned, since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote network. A good choice for this number is the remote system's router IP address or DNS server IP address.

Local site uses dynamic assignment, remote site uses static:

- Leave the LOCAL IP ADDRESS field set to 0.0.0.0, the default.
- Enter the dedicated (static) Remote IP address.

E. Set the connection time-out value, the number of seconds of inactivity that the PPP link should wait before dropping a connection.

A zero value indicates that no time out should be used.

F. Save your PPP configuration. Select the Next button, and return to step #7 of the configuration instructions on page 20.

Access the GB-Pro

After completing the initial configuration in the Setup Wizard, your GTA Firewall should be active and functioning in default security mode, in which all internal users are allowed outbound, and no unsolicited connections are allowed inbound.

After testing connectivity, you should use the Web interface or GBAdmin to modify the system configuration to your local requirements.

See the GNAT BOX SYSTEM SOFTWARE USER'S GUIDE for more information.

4 Troubleshooting

Guidelines

GTA Support recommends the following guidelines as a starting point when troubleshooting network problems:

- Start with the simplest case of locally attached hosts.
- Use IP numbers, not names. Your real problem could be DNS.
- Work with one network segment at a time.
- Verify your system configuration with the Verification Configuration feature. The verification check is the best method of ensuring that your system is configured correctly. Correct all errors and warnings listed.
- Your first tests should be connectivity tests. Ping and Traceroute are very useful tools for testing connectivity.
- Make sure the network cabling is connected to the correct network interface. It is easy to confuse network interface ports. Some useful guidelines are:
    - In a GB-Pro, the port/NIC numbers, MAC addresses and logical names are listed on the Network Information screen and in the Configuration Report.
    - Use the trial and error method. Connect one network cable and use the ping facility to reach a host on the desired network. Move the cable and use ping until you are successful. Connect the next network cable and perform the test again with the two remaining network interface cards.
    - Generate a hardware report from one of the user interfaces. Check the report to ensure all your network devices have been recognized by the system at boot time.

Troubleshooting Q & A

1. Why can't *all* hosts behind the firewall reach the Internet?

This is usually a routing problem. The Traceroute facility can be very useful in debugging routing problems. Check for these problems:

- Are the hosts that can’t reach the Internet on a different network subnet?
- Have you added a static route to the GTA Firewall to tell it which router is used to reach the problem network? Have you set the router’s default route to be the GTA Firewall? Have you set the default route for hosts on the problem network to be the router?
- Is the wrong IP address assigned? All network interfaces on the GTA Firewall must be on different logical networks.
- Is the default route assigned incorrectly? The default route must always be on the same subnet as the network interface of the host (this is true for all hosts, not just the GTA Firewall). For a GB-Pro, the default route must be an IP address on the network which is attached to the External Network interface.

Exception

When using PPP or PPPoE, the default route is not necessarily on the same subnet. The route is assigned by your PPP provider.

2. Why can't *one* host behind the firewall reach the Internet?

This indicates that the default route is assigned incorrectly (or not at all) to hosts on the Protected or Private Service networks. All hosts protected by the GTA Firewall must use the IP address of the network interface for the respective network. Hosts that reside behind routers or other gateways on these networks generally use the IP address of the gateway or router.

3. Why can't I access the Web interface from the Protected Network?

The default Remote Access filter set is generated from the configuration parameters entered in the Network Information screen. It is possible that the Protected Network interface is on a different subnet from the remote host. Check the Remote Access filter for the Web interface; it may need to be adjusted.

4. Why do I get errors when GBAdmin starts up? Why is online help information not displayed?

GBAdmin requires Microsoft Internet Explorer 5.x or later installed on your workstation. Components from Internet Explorer are used to display the online help information.

For more Troubleshooting suggestions, see the GNAT BOX SYSTEM SOFTWARE USER'S GUIDE and GTA's website at www.gta.com.

5. Why can't I see or ping the Protected Network interface?

You may have the wrong cable for your connection.

- For a direct connection (GTA Firewall to host or router) you need a crossover cable.
- For a connection to a hub or switch you need straight-through cables.

Note

To distinguish between a crossover cable and a straight-through cable, compare the connection ends. On a straight-through cable, the wire order matches; on a crossover cable, the first three of the four cables are in reverse order.

6. Why is my system booting up in demo mode instead of going to the Setup Wizard?

- Check your serial number and activation code.
- If both of these numbers are correct, it may mean that the Hardware Key Block is not being recognized by your system. Set your system’s parallel port to the values below, and try rebooting your system.

Hardware Key Block Settings

Address (hex value)	0x378	0x278
IRQ	7	5
Mode	ERP, SPP or Both	

Index

Symbols
1918 network addresses 21
486 8

A
activation (unlock) code 2
Addresses, MAC 25
automated installer 12, 17
availability, high 1

C
cable modem 19
caution 4
CIDR notation 1
code, activation 2
configuration
    default 4, 10
    Report 3
connections
    concurrent 7
Console interface
    limited Video 6, 17
conventions, documentation 4
Copyright ii
crossover cable 10

D
default
    configuration 4, 10
demo 11
DHCP 19
disk 7, 12, 15, 17
disk image file extension. *See* flp
DNS
    problem 25
documentation 4
dongle 11
drivers and NICs 5, 8
DSL 19

E
Email ii
Exception 26

F
filters
    remote access 7
floppy disk 7
    copy to, with GBWrite 15
    not protected 17
    Unix/Linux 12
flp 13

G
GB-Pro 1
GBAdmin 5
    errors 27

H
hardware key block 11
hex value 11, 27
High Availability 1, 5
How to 4, 23

I
IANA 21
ICSA 1
ID, User 2
installation
    hardware key block 11
    set up on target system 17
    software & utilities 12
Install Wizard 12
Interfaces, User 6
Internet Assignment Number Authority. *See* IANA
Intranet 8
IRQ assignments 8
ISDN 7, 8, 22
ISO 9660 7, 13

K
keyboard 4, 8, 17

L
Login 2

M
Macintosh 12
Memory Requirements 10
modem 10
monitor 8, 17
Multi-interface option 8
Multimedia 7

N

NAT, Network Address Translation 7
Netmask 1
network interface card 8
Note 2, 4, 6, 8, 9, 10, 12, 13, 18, 20, 21, 26, 27
notes & warnings 2, 6, 8, 9, 10, 12, 13, 18, 20, 21, 22
    caution, backup 4
    RFC 1918 numbers 21
    straight-through cable 27
number, serial 2, 19

O

OS 5, 12

P

parallel printer port 11
password 2, 21
Ping 25
PPP/PPPoE 22, 26

Q

QuickTime Streaming 7

R

Real Audio 7
Registration, Product 2, 5
Report, hardware 25
RFC 1918 21
RoBoX 3
runtime disk 14

S

serial number 2, 19
Services 1
Setup Wizard 17
Software, utility 12
Stateful Packet Inspection 6
support options 3
    contract 7
    email ii
    installation 3
Surf Sentinel 1
system 17
    kernel 18
    operating (OS) 5
    target 17
system software
    installing 12

T

T-1, T-3 8
target system 17
TCP/IP 1
telephone number 23
    GTA ii
Terms 4, 5
Traceroute 25
Trademark ii
troubleshooting 5, 25

U

UARTs 9
Unix 12
    “dd” command 13
Unlock 2
unregistered 20
Upgrades 3
User ID 21
Utility software 12

V

Verification 25
Version 6, ii
VGA display. *See* monitor
Video Console interface 6, 17

W

WAN 8
Web 4, 5, 6
Windows 12
    95/98/NT 12
Wizard
    Install 12
    Setup 17