GNAT Box®

SYSTEM SOFTWARE VERSION 3.3

User's Guide

Global Technology Associates, Inc.

Copyright

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:	http://www.gta.com
Email:	info@gta.com
Support:	+1.407.482.6925
Email :	support@gta.com

Document Information

GNAT Box System Software Version 3.3 September 2002

Contents

1 INTRODUCTION 9

GNAT Box Basics 9

GNAT Box System Software Features 9

Optional Features 9

What is a GNAT Box System? 10

How Does GNAT Box Work? 10

The Implicit Rule 10

Documentation 11

About this Guide 11

User Interfaces 11

Configuration and Administration 12

Troubleshooting 12

Conventions 12

Additional Documentation 13

Activation Codes 13

Support 14

Registration 14

Support Options 14

Mailing Lists 14

2 GNAT BOX TERMS 15

IP Packet 15

Stateful Packet Inspection 15

Tunnels 16

Network Transparency 16

Virtual Cracks 16

IP Aliasing 17

Network Types 18

External Network 18

Protected Network 18

Private Service Network 19

Network Interfaces (NICs) 19

External Network Interface 20

Protected Network Interface 20

Private Service Network Interface 20

Network Address Translation (NAT) 20

Default NAT (Dynamic NAT) 21

Static Address Mapping (Static NAT) 21

IP Pass Through (No NAT) 22

Objects 22

Address Objects 23

Interface Objects 23

VPN Objects 23

Filters 24

Default Filter Sets 24

Filter Types 24

VPN 25

DNS 25

Built-in DNS Server 26

3 USER INTERFACES 27

Web Interface 27

Exclusive Features 27

Web Interface Access 28

Characteristics 28

Navigation and Data Entry 29

Menus 29

Buttons and Fields 30

GBAdmin 34

Exclusive Features 34

GBAdmin Access 34

Characteristics 35

Navigation and Data Entry 35

Keys 36

Scrolling Menu 36

Menubar 38

Toolbar 38

Check Boxes, Lists and Tabs 38

4 BASIC CONFIGURATION 39

DNS 39

DNS Proxy 39

Features 40

Interface Variations 41

Network Information 42

Interface Variations 44

PPP 46

PPPoE 46

Enable PPP in Network Information 46

Interface Variations 51

Preferences (Contact Information) 54

5 SERVICES 55

DHCP Server 55

Interface Variations 57

DNS Server 58

DNS Domains 59

Interface Variations 61

Email Proxy 61
GB-Enterprise Server 63
High Availability 64
Network Time Service 66
NTP Resources 66
Remote Logging 67
WELF (WebTrends Enhanced Log Format) 69
SNMP 70

6 AUTHORIZATION 73
Admin Accounts 73
New SSL Certificate (Web) 74
Host Name 74
Generate Security Certificate 75
Install Security Certificate 76
Remote Admin/Authentication 77
SSL Encryption 77
Encryption Levels 77
Upgrading 78
WWW Administration 78
RMC (GBAdmin) 79
Authorization 79
Users 80
VPNs 81
Selecting the Key Method 81
About Security Parameter Index (SPI) 82
Encryption Key Length 82
Hash Key Length 83

7 CONTENT FILTERING 87
Access Control Lists 87
Surf Sentinel 88
Local Allow and Deny Lists 88
Local Content Lists 90
Adding Sites to LCLs 90
Content Filtering Preferences 91
Traditional Proxy 91
Transparent Proxy 92

8 ROUTING 93
Gateway Selector 93
Using Gateway Selector 93
Using Static and Dynamic Gateways 94
Designating Beacons 94
Interface Variations 96
RIP 96

Static Routes 98

9 OBJECTS 99

Address Objects 99

Creating Address Objects 99

Default Address Objects 100

Interface Variations 101

VPN Objects 102

Default VPN Objects 102

Interface Variations 105

10 FILTERS 107

Outbound Filters 107

Managing Filters 108

Filter Sets 108

Preferences 111

Protocols 115

Remote Access Filters 116

Time Groups 118

11 IP PASS THROUGH 119

Filters 120

Hosts/Networks 122

12 NAT 123

Aliases 123

Inbound Tunnels 124

Creating Inbound Tunnels 125

Set Remote Access Filters 125

Static Address Mapping 127

Allowed Static Address Mapping 127

Timeouts 128

13 ADMINISTRATION 131

Download/Save Configuration 131

Reset Firewall, Default Sections 132

Retain Filters after Default 132

Interface Variations 132

Flush ARP Table 132

Halt 133

Interfaces 133

Ping 134

Reboot 134

Set Date/Time 135

Set Time Zone (Web Only) 135

Interface Variations 135

Trace Route 136

Upload/Open Configuration 136
Interface Variations 137
Upload/Update Runtime 137
Download Floppy Disk Image 137
14 REPORTS 139
Configuration 139
Hardware 140
Verify Configuration 140
Interface Variations 140
Email Configuration 141
15 SYSTEM ACTIVITY 143
Active ARP Table 143
Active Connections 144
Active Filters 144
Active Routes 146
Active VPNs 146
Current Statistics 147
DHCP Leases 148
View Log Messages 149
Locked Out 149
APPENDIX 151
Ports and Services 151
Well-known Ports and Services 151
Registered Port Numbers 152
Log Messages 153
Remote Logging 153
Log Message Configuration 153
Default Log Configuration 154
Filter Logging Configuration 154
Filter Packet Types 154
Received 154
Matched 155
Accepted 155
Rejected 155
Permitted Inbound Request Open 155
Permitted Outbound Request 156
Inbound Outbound Security Policy Violation 157
Unauthorized Firewall Access Attempts 158
Attempts to Compromise Remote Admin Ports 160
Content Filtering URL Proxy Log Messages 161
Network Address Translation Log Messages 162
Close 163
IP Pass Through (No NAT) 163

Default Settings 168
Outbound Security Policies 168
Outbound Filters 168
Remote Access Security Policies 168
Remote Access Filters 168
Troubleshooting 170
Troubleshooting Q & A 171
INDEX 177

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, including GB-Pro, GB-Flash, GB-1000 and RoBoX™.

GNAT Box System Software Features

GNAT Box Systems have the following standard features:

- Secure IP network connectivity to an external network.
- Network Address Translation (NAT) and IP Pass Through (no NAT).
- Remote access to user-designated hosts and services.
- Stateful IP filtering on inbound and outbound packets.
- Transparent network access for standard TCP and UDP applications.
- Full support for application protocols such as FTP (normal and PASV), RealAudio/RealVideo, CU-SeeMe, Microsoft PPTP, Microsoft Netshow, ICQ/AIM, Online Gaming and Net2Phone, with new protocols continually added.
- The PSN, GTA's fully customizable DMZ network that keeps the protected networks secure and separate, while providing safe access to external networks with varying levels of protection.
- DHCP services via built-in DHCP server.*
- Domain name services via built-in DNS server.*
- Virtual Private Networking with GB-VPN.*

Optional Features

- Fault resilient firewall systems (high availability) with H_2A.*
- Secure mobile remote network access with Mobile VPN Client.*
- Integrated Internet content filtering via Surf Sentinel subscription.*

*Available on select GTA Firewalls.

What is a GNAT Box System?

GNAT Box Systems were developed to provide powerful, simple, and affordable IP network security. They are dedicated to network security: there is no user shell, so you can't log on, except for configuration and administration. You can't telnet to one; you can't use it as a mail or web server; and you can't run any other applications on it. So, what ***is*** a GNAT Box System?

A Firewall that prevents unauthorized access to Protected and Private Service Networks (PSN), while allowing authorized outbound connections to operate transparently. It protects against denial of service and spoofing attacks.

A Network Address Translation (NAT) engine that allows unregistered IP addresses to be used on the Protected and the Private Service Networks. All IP addresses are hidden from the External Network and are translated to the primary IP address of the external network interface.

A DNS & DHCP Server in GTA Firewalls GB-1000, GB-Flash, GB-100 and RoBoX.

A Network Bridge that can function as a link between network topographies (e.g., 10Mbps to Gigabit) and replace a router in a PPP configuration.

A VPN providing a Virtual Private Network between two networks using the IPSec VPN standards and supporting many third party VPN products transparently.

A Powerful and Flexible System that runs GNAT Box System Software, supports up to 128,000 concurrent sessions, can be configured for a variety of networks, and supports many popular application protocols.

How Does GNAT Box Work?

At the heart of GNAT Box System Software is GTA's NAT (Network Address Translation) and Stateful Packet Inspection engine. Stateful Packet Inspec tion monitors every IP packet passing through the firewall. These facilities are tightly integrated with the network layer to guarantee maximum data throughput, reliable NAT and unparalleled security.

The Implicit Rule

The GNAT Box System Software is based on the implicit rule, "That which is not explicitly allowed is denied." This means that if all filters were deleted, there would be no inbound or outbound packet flow.

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. 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.

About this Guide

This guide includes GTA-specific terms, user interface instructions, advanced configuration options, description of fields, administrative tools, troubleshooting answers, and some relevant appendices.

User Interfaces

For instructions on how to use the interfaces, see **Chapter 3 – User Interfaces**. GNAT Box System Software has two preferred user interfaces: GBAdmin and the Web interface. Instructions for the Console, an interface used primarily as a fail-safe, are provided on the Installation CD and on the GTA website.

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 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 Interface

The Console interface can be used to reset a misconfigured firewall to defaults. The Console interface is limited on the GB-Pro and GB-100 due to space requirements. A list of these limited functions is in the Console Technical Document provided on the Installation CD and on the GTA website.

Configuration and Administration

The configuration and administration chapters after User Interfaces describe each function on the Web and GBAdmin interface in the order that they appear on the Web interface. Functions within each section are arranged alphabetically in the interfaces, and that arrangement is followed here.

Configuration chapters are organized in order of the function's appearance on the menu in the Web interface. After a brief explanation of the function, there will be a table of field descriptions and a screen illustration from the Web interface. Differences in the function or the interface in GBAdmin will be explained and illustrated.

Menu items for optional features will display in your product only if the feature has been activated. Functions which are optional features or do not appear on a specific interface will be indicated.

The Reports, Administration and System Activity chapters cover the administrative areas on the GNAT Box System Software. These menu items are found in the Menu of the Web interface and in both the scrolling Main Menu and the Menubar in GBAdmin.

Administration chapters are also organized in order of the function's appearance on the menu in the Web interface. After a brief explanation of the function, there will be a screen illustration from the Web interface. Differences in the function or the interface in GBAdmin will be explained and illustrated.

Troubleshooting

The Troubleshooting chapter presents answers to some of the common questions users have when configuring a firewall. For installation and product-specific troubleshooting, see the product and feature guides.

Conventions

Notes are indicated by an indented, italicized headline.

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

Documentation Conventions

Typeface	Convention
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>.

Additional Documentation

Documents are either in plain text (*.txt) or in Adobe® Acrobat® Portable Document Format (PDF; *.pdf) which requires Acrobat Reader for viewing and downloading. A free copy of Acrobat Reader can be obtained at www.adobe.com. Documents received from GTA Support may also be in email or Microsoft Word format (*.doc).

Documentation Map

Topic	Document Name	Location
Installation	Product Guides	Shipped w/product, CD
System Setup	Product Guides	Shipped w/product, CD
Terms	Terms & Concepts	gta.com, CD
Troubleshooting	–	Product Guide, User's Guide
Configuration examples	–	gta.com
Sample reports	–	gta.com
Ports & services	–	gta.com
Drivers & NICs (Pro, Flash)	Product Guides	Shipped w/product, CD
GTA Firewalls	Product Guides	Shipped w/product, CD
Content Filtering	Surf Sentinel Feature Guide	Shipped w/product, CD
High Availability	H_2A Feature Guide	Shipped w/product, CD
VPN	GB-VPN Feature Guide	Shipped w/product, CD
VPN Examples	GB-VPN to VPN Tech Docs	Shipped w/product, CD
GBAdmin interface	User's Guide	Shipped w/GTA Firewalls, CD
GBAdmin	GBAdmin Online Help	Shipped w/GTA Firewalls, CD
Web interface	User's Guide	Shipped w/GTA Firewalls, CD
Console interface	Console Interface Tech Doc	gta.com, CD

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

Activation Codes

GNAT Box System Software is not directly copy-protected, so it may be copied for backup purposes. Activation codes are required to use the software.

All commercial GTA Firewalls–GB-Pro, GB-Flash, GB-100, GB-1000 and RoBoX–use activation (unlock) codes to protect software. For firewall appliances, the required registration code is pre-installed. GB-Pro and GB-Flash also require the use of a hardware key block.

Additional features require that feature activation codes 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.

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 and any feature activation code numbers for your optional products.

Note

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

Registration

To register your new product and qualify for free installation (up and running) support, go to www.gta.com and click on Support, then the GTA Support Center link. Here, enter your User ID and password to log in if you already have an account, or create a new account by entering your profile information, including your product serial number and activation code, and then log in. See your product guide for more information.

Support Options

If you need support after installation and configuration to defaults, contact the sales department to purchase a support contract. Contracts range from support by the incident to full coverage for a year. Other assistance is available on the GTA website at www.gta.com, or through an authorized GTA Channel Partner.

Mailing Lists

To learn more about GNAT Box System Software, join the GNAT Box mailing list at gb-users-subscribe@gta.com, monitored by GTA staff.

2 GNAT Box Terms

This section defines terms used in GNAT Box System Software and documentation and explains how standard term usage differs. These terms, along with a collection of other relevant words, phrases and acronyms, are available in the **GTA Glossary** on the installation CD and GTA's website at www.gta.com.

IP Packet

A basic unit of the TCP/IP protocol is the IP packet. The GTA Firewall system generally operates on the IP packet level, although some facilities of the system perform operations on the application level too. At the IP packet level, the system specifically operates on the IP header, which contains the source and destination IP address, port numbers, IP protocol type, along with various control information. Normally, a GTA Firewall system does not touch the data portion, or packet payload, of an IP packet.

However, some application protocols embed IP addresses and ports in the data portion, and often this information needs to be interpreted in the course of Network Address Translation. It is the ability to support such complex application protocols that makes the GTA Firewall Network Address Translation facility so much more powerful than basic NAT, which is "blind," meaning that it does not look in the application portion of the data packet.

Stateful Packet Inspection

GTA's Stateful Packet Inspection monitors the state of each packet sent through the GTA Firewall so that the GNAT Box System Software can verify that the destination of an inbound packet matches the source of a previous outbound request. These transactions (stateful information) are recorded in the various state tables. (See **Chapter 15 – System Activity.**)

Tunnels

Tunneling is the process of placing an entire packet within another packet and sending it over a network. A GTA Firewall system tunnel allows a host on the External Network or PSN to initiate a TCP, UDP or ICMP session with an otherwise inaccessible host on the PSN or Protected Network for a specific service. This is done by mapping a visible IP address and port (service) to a target IP address and port (service). This map can be performed for all services (host to host tunneling) or more typically for a given service. Tunnels can be created to hosts on both the PSN and the Protected Network.

A host at the source of a tunnel can see only the source side IP address; the IP address on the destination side is always hidden.

Common tunnels include: HTTP (web), FTP, DNS, SQLnet, and telnet.

Network Transparency

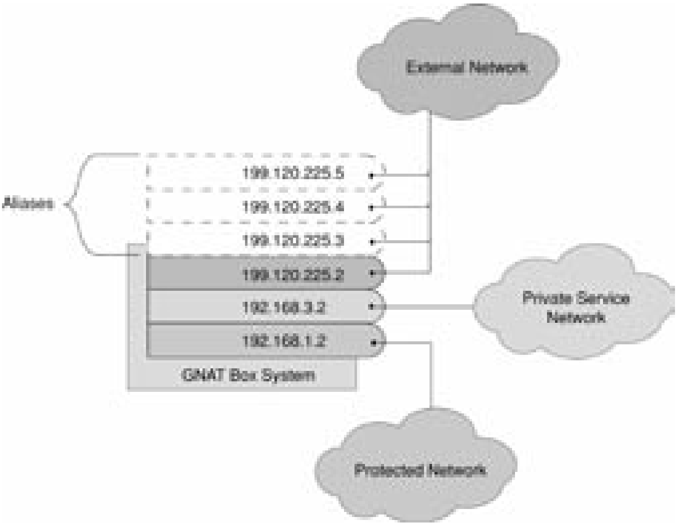
Network Transparency is used to describe the function that allows host systems residing on the PSN and Protected Network to send packets to and receive replies from hosts on external networks in an apparently transparent manner. Network Transparency is implemented as a part of Stateful Packet Inspection. The state of all connections is maintained by the system in a series of tables, along with other connection information that will ensure that only authorized packets are accepted. Network Transparency allows GTA Firewalls to operate without the need for permanent holes in the firewall. Typical IP filtering firewalls require that holes be created in the firewall to allow packets to be accepted for arbitrary inbound connections. Since many application protocols create arbitrary secondary inbound connections, more holes must be created to accommodate a wide range of possibilities.

Virtual Cracks

GTA Firewall systems avoid the security problem of multiple secondary inbound connections through the use of virtual cracks. A virtual crack is part of GTA's Stateful Packet Inspection technology, which allows secondary inbound connections used by some protocols to be accepted without a dedicated hole in the firewall. A virtual crack is automatically configured when the system detects the signature of a nonstandard protocol packet passing outbound through the system, using secondary connections. The virtual crack stays in place until the connection is shut down, timers expire due to inactivity, or when the expected protocol event does not occur. A few application protocols which use secondary connections, and therefore virtual cracks, include: FTP, RealAudio, CU-SeeMe, Net2Phone and many Windows NetBIOS facilities.

IP Aliasing

IP Aliasing is the facility that allows any network interface to have multiple IP addresses assigned. This facility is useful if multiple targets on a PSN or a Protected Network are required for the same service (port) via the State Table Tunnel facility (e.g., multiple web servers). IP aliases can be applied to any interface; see product guide for the number of IP aliases the product supports.

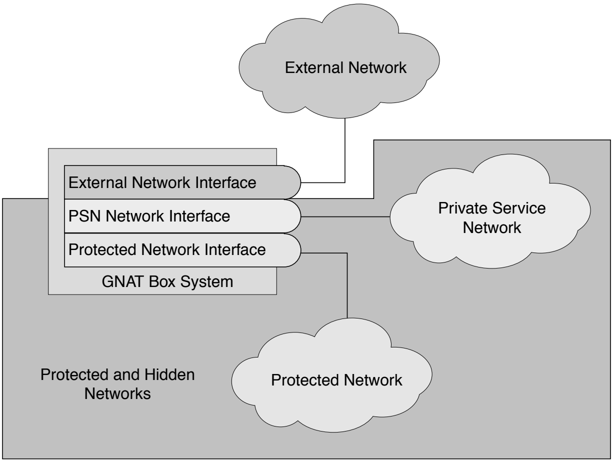


IP aliases assigned to External Network interface

All IP aliases must be registered or legitimate IP addresses if used on an External Network interface connected to the Internet, although they need not be from the same network.

Network Types

The GNAT Box System Software uses three network types: the External Network, the Protected Network and the Private Service Network (PSN). The first two network types do not differ greatly from standard use, but the third is a special and improved variation of the standard DMZ (**De**M**ilitarized **Z**one) network used by other firewalls.



A GTA Firewall System Diagram Example

External Network

An External Network (EXT) is an unprotected network for which no Network Address Translation is performed. An External Network is typically connected to the Internet. However, a GTA Firewall can also be used internally on private networks as an intranet firewall, in which case the External Network is the part of the intranet not hidden behind the Protected Network or the Private Service Network. If connected to the Internet, an external interface must have a registered IP address. A GTA Firewall provides no security for hosts located on an External Network.

Protected Network

A Protected Network (PRO) is a network that is hidden behind a GTA Firewall system. The term is used throughout GTA documentation to refer to a network directly connected to the GTA Firewall. All features and attributes associated with this network also apply to all networks connected to a Protected

Network. All hosts and IP addresses used on this network are hidden from the External and Private Service Networks.

Though hosts on a Protected Network are, by default, not accessible from an External Network or a PSN, the Tunnel facility can be used to allow external access to hosts and services.

Private Service Network

A Private Service Network (PSN) is an optional network located logically between the External Network and the Protected Network, but nearly at a peer level with the Protected Network. The PSN is not trusted by the Protected Network: by default, no unsolicited packets are allowed to pass from the PSN to the Protected Network. All hosts on the PSN are hidden from the External Network but completely accessible from the Protected Network. Since a PSN is hidden, unregistered IP addresses can be utilized.

A PSN is used in conjunction with the Tunnel facility to allow external access to hosts and services, such as web servers, FTP servers and email servers. By tunneling to a server on a PSN, an organization can allow public access to services while maintaining network security for a Protected Network.

A PSN differs from a standard DMZ by being on its own network rather than a subnet and by its ability to provide varying levels of security according to the needs of the organization.

Network Interfaces (NICs)

A network interface (NIC) can be any supported network device operating at any supported speed and utilizing any supported network topography. GB-Pro and GB-Flash, GTA's firewalls on user-provided hardware, can operate with a combination of different network cards, thus performing a bridging function between dissimilar networks. GNAT Box System Software requires at least two network interfaces, one External and one Protected. GTA Firewalls support up to sixteen (16) network interfaces (on GB-Pro and GB-Flash, with the optional multi-interface option enabled). Interfaces beyond the required two may be defined as any of the three types; it is possible to have multiple External, Protected or PSNs.

External Network Interface

An External Network interface is a network device that is attached to an External Network, typically the Internet. An External Network interface requires a registered or legitimate IP address (if attached to the Internet); only one registered IP address is required for the GTA Firewall. Any supported network device can be used as an External Network interface, including those using PPP. More than one External Network interface may be defined, but only one can be designated as the primary Default Gateway or default route.

Protected Network Interface

A Protected Network interface is attached to a Protected Network. Any supported network device may be used with the exception of the PPP device. A Protected Network interface does not require a registered IP address, though RFC 1918 addresses are recommended. More than one Protected Network interface may be defined.

Private Service Network Interface

A Private Service Network (PSN) interface is optional, and may not be required for configurations such as on intranets or for outbound access only; however, if you offer public access to servers, (such as a web server), the installation of a PSN interface is highly recommended. Any supported network device may be used with the exception of the PPP device. A PSN interface does not require a registered IP address, though RFC 1918 addresses are recommended. More than one PSN interface may be defined.

Note

IP Aliasing may be used on any interface. See product guides for the maximum number of IP aliases available on a specific GTA Firewall.

Network Address Translation (NAT)

Network Address Translation, or NAT, is one of the primary features of GNAT Box System Software. NAT is available in two forms: dynamic and static translation, referred to as Default NAT (active by default) and Static Address Mapping. NAT can be bypassed using IP Pass Through. NAT is applied to:

1. Packets outbound from the Protected Network to the External Network.
2. Packets outbound from the Protected Network to the PSN.

3. Packets outbound from the PSN to the External Network.
4. Packets outbound from a Protected Network to a Protected Network.

Default NAT (Dynamic NAT)

GNAT Box System Software Default NAT is a dynamic many-to-one scheme. Packets from all IP addresses located on the source network (PSN or Protected) have their source IP address translated to an IP address assigned to the outbound NIC (External or PSN). This means:

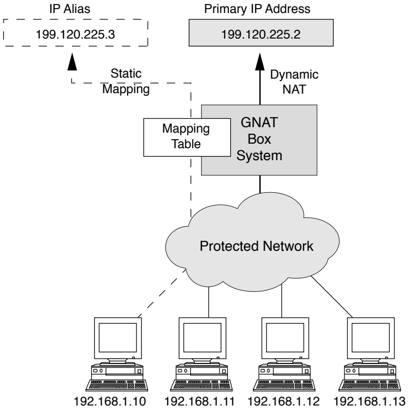
1. Any packet originating from the Protected Network destined for a host that resides external to the External NIC will have its source IP address translated to the IP address of the External NIC.
2. Any packet originating from the Protected Network destined for a host that resides external to the PSN NIC will have its source IP address translated to the IP address of the PSN NIC.
3. Any packet originating from the PSN destined for a host external to the External Network interface (External NIC) will have its source IP address translated to the IP address of the External NIC.

Note

NAT is not applied to packets that originate on one Protected Network destined for another, because they are at a peer level (equally protected).

Static Address Mapping (Static NAT)

Static Address Mapping (also Outbound or Static Mapping) allows an internal IP address or subnet to be statically mapped to an external IP address during the Network Address Translation process. Typically, Static Address Mapping is used with targets on the External Network interface.



Static Address Mapping Illustration

Static Maps are assigned by associating a source IP address to an IP alias assigned to a PSN or External Network interface. A netmask is combined with the specified source IP address to yield an IP number used for comparisons when applying Static Address Mapping.

Mapping is not useful unless IP aliases have been assigned, since by default all IP addresses on the Protected Network are dynamically assigned to the real IP address of the outbound network interface.

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

IP Pass Through (No NAT)

IP Pass Through means, essentially, “no Network Address Translation (NAT).” By default, NAT is applied to all packets passing through the GTA Firewall outbound. The IP Pass Through facility allows the system to transfer certain packets through the firewall without applying NAT. When configured for IP Pass Through, the system creates IP Pass Through tunnels, which are determined by user-designated origination IP addresses. These designated IP addresses can be networks, subnets or individual hosts on either a PSN or a Protected Network. Unlike NAT, which only supports TCP, UDP and ICMP, IP Pass Through will support any defined IP protocol.

IP Pass Through can be applied selectively to packets based on their destination. The IP Pass Through facility allows the user to specify which interfaces will not have NAT applied for a designated IP address. For example, IP Pass Through can be used for specified packets destined for a host external to a PSN interface, while packets for a host external to an External interface still have NAT applied. See Chapter 11 – IP Pass Through for more information.

Objects

Objects are logical groups of IP addresses. They are used to simplify the definition of IP addresses and groups of IP addresses by allowing the administrator to refer to these settings with one name rather than entering them repeatedly, which is time consuming and increases the possibility of error.

Caution

If the name of an address, interface or VPN object is changed, the filters, objects and tunnels that it references ***must be changed***, particularly the names of Logical Interfaces; the associated Remote Access Filters identify the interface by name, allowing Web and GBAdmin connectivity.

Address Objects

Traditionally, an IP address and netmask pair are used to create the Address Object. Address Objects increase speed and consistency in the GNAT Box System Software. Using objects, a user may define an address one time, then select the object in each screen where that definition is required. Once an object is created, the user will only need to change the object to change all the locations where the definition is used.

Interface Objects

The Logical Names in the Network Interface section, the IP Alias Names in the NAT section and the High Availability group names in the Services section are used as Interface Objects. Interface Objects function in the same way as Address Objects, to streamline address selection throughout the GNAT Box System. Interface Objects can be used in:

- Remote Access Filters
- VPN Objects
- Address Objects
- Inbound Tunnels
- Static Address Mapping

VPN Objects

VPN Objects increase the speed and consistency of VPN creation. Using VPN objects, a user may define the VPN once, then select the object in each feature where that definition is required. The user will only need to change the VPN object to change the definition in all the locations where the object is used. The screens where VPN objects are used are: Users and VPNs under Authorization and in VPN Objects itself.

Three VPN objects are created by default: an object for IKE VPNs, one for Manual VPNs and one for Mobile VPNs.

Filters

Filters are a facility that control network access to and through the GTA Firewall. Filter rules are applied to all IP packets that are received by or are seeking to pass through the GTA Firewall system. The GTA Firewall system supports three types of user definable filters: Remote Access Filters, Outbound Filters, and IP Pass Through Filters. A fourth filter type, Automatic Filters, which is not user accessible, are transient filters generated by the system. The built-in implicit rule for the GTA Firewall system is: "That which is not expressly permitted is denied." Therefore, if no filters of any type were defined, packets would not be allowed to flow to or through (inbound and outbound) the GTA Firewall system. See individual product guides for the number of filters available on a specific GTA Firewall.

Default Filter Sets

When the GTA Firewall is initially configured, and whenever you press the Default button on any filter set screen), a set of default filters is generated based on the defined security policy and configured preferences. In the case of a new installation, this is the factory settings policy and preferences. (See the Appendix Default section for a discussion of the default security policy and the default filter sets.) When upgrading the system software, these filter sets are based on the policy and preferences that were set in the existing configuration. When changing the configuration, "defaulting the filters" does not return the filters to the factory settings, but rather to the settings in accordance with the configuration. However, filters created when the Defaulted option is used are Disabled by default. The user must enable them manually.

Filter Types

There are three basic types of filters used by GNAT Box System Software: Remote Access, Outbound and IP Pass Through, which are all generated by the user, either by creating a network configuration and "defaulting" the filters sets by using the Default selection in the filters screens, or by creating custom filters. A fourth type, Automatic Filters, are generated by the system or when applying an Automatic Accept All filter to a tunnel. For more about filter types, see **Chapter 10 – Filters**.

VPN

GNAT Box System Software is provided with a built-in Internet Engineering Task Force (IETF) IP Security (IPSec) standard VPN facility. Since a GTA Firewall is a security gateway, only the tunnel mode of the IPSec standard is implemented. The VPN provides a means to securely connect two or more remote networks together or mobile users to a secure network. The remote gateway can be another GTA Firewall or another compatible security gateway. The GTA Firewall VPN provides support for any IP protocol to be passed through the VPN tunnel to a remote network, if authorized.

Unlike many other VPN implementations, the GNAT Box System applies security policies inside the VPN tunnel. A secure network connection can be established between two sites, however this doesn't mean that "anything goes" in terms of network traffic. The GNAT Box System Software implicit rule also applies to VPN tunnels: "That which is not explicitly allowed is denied." The GNAT Box System requires that access rules for both inbound and outbound access on the VPN tunnel be defined. IP Pass Through filter facility is used to define access control on the VPN.

The GNAT Box VPN Client provides VPN access to mobile or remote users. The GNAT Box VPN Client is compatible with Windows 95, 98, NT4, 2000 and XP. The VPN client operates with a supported GTA Firewall system (GB-1000, RoBoX or GB-Flash) in the ESP tunnel mode. To learn how VPN users and objects are defined, see VPNs in **Chapter 6 – Authorization** and VPN Objects in **Chapter 9 – Objects**. For more information about the GNAT Box VPN and the VPN Client option, see the **GNAT Box VPN Feature Guide**.

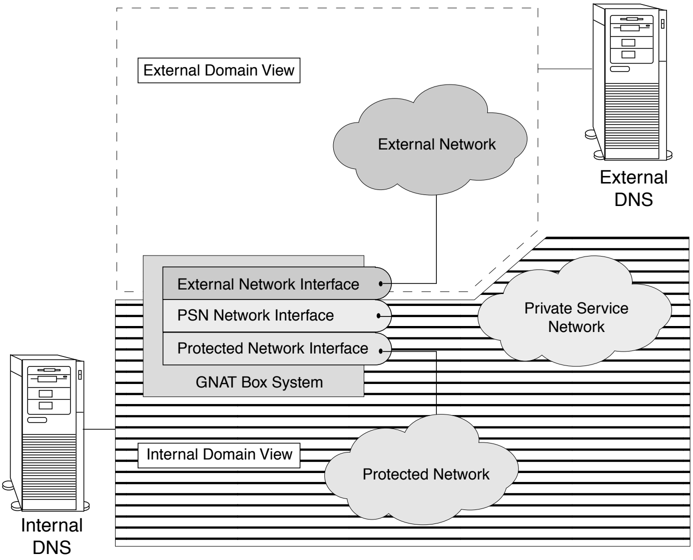
DNS

Since the GTA Firewall system provides network transparency for users on Protected and PSNs, all DNS (Domain Name System) queries (outbound) operate normally. Users on Protected Networks and PSNs may use an external DNS server for address resolution. However, it cannot be used to resolve protected hosts. The GNAT Box System hides all network addresses on both Protected and PSNs. Therefore, providing DNS information about internal hosts to the external network is pointless, as none of the IP addresses on these networks are directly accessible from an External Network.

Built-in DNS Server

A built-in DNS server is available in all GTA Firewall flash-based systems – GB-Flash, RoBoX, GB-100 and GB-1000. This DNS server can be configured as either an internal or external server. It can host multiple domains, however internal and external domains can not be hosted at the same time.

The GNAT Box DNS server functions as a primary (not a secondary) Domain Name System server. Before configuring the DNS server, you should understand how the domain name system functions on the Internet. A good reference book on DNS is: **DNS AND BIND, 3RD EDITION** by Paul Albitz & Cricket Liu, published by O'Reilly and Associates.



Domain Name System (DNS)

3 User Interfaces

GTA Firewalls and GNAT Box System Software include two primary interfaces: the Web interface and GBAdmin. The Web interface is platform independent and can be used on any supported browser. GBAdmin is a Windows-only interface that allows access from a local workstation.

A third interface, the Console, is used to default filters in case of a configuration error; to recover a GTA Firewall; and for basic configuration. The Console has limited functions for GB-Pro due to the increasing number of features offered in GNAT Box System Software and the space limitations on floppy disks. See the GTA website, www.gta.com, for more about the Console interface.

In this chapter, the Web interface and GBAdmin are illustrated and described, including navigation, common keystrokes, toolbars, menu items and buttons. Features exclusive to each interface are explained.

For initial configuration, use the product guide that came with your GTA Firewall. Use the configuration and administration chapters of this guide to perform basic and advanced configuration.

Web Interface

The GTA Firewall can be remotely administered using the Web interface on a frames-capable web browser, e.g., Microsoft Internet Explorer, Netscape Navigator or the text-based Lynx browser, allowing administration of the GTA Firewall from Windows, Unix, X-Windows and Macintosh platforms.

Exclusive Features

- SSL encryption option.
- Secure administrative access from any location with an Internet connection.
- Intuitive browser interface.
- Platform-independent.
- Compatible with most browser/platform combinations.

Web Interface Access

By default, any host on the Protected Network interface is allowed access to the GTA Firewall Web interface. The Web interface can be disabled or set to a read-only mode in which no updates are allowed.

Note

If the Web interface is disabled, the GTA Firewall will be blocked to web access ***immediately***. If both the Web interface and GBAdmin (RMC) have been disabled, you must use the Console to re-enable them.

By default, the GTA Firewall web server operates at the standard port of 443 using SSL encryption or port 80 with no SSL. If you want to change the port, create a Remote Access Filter to allow the new port before changing the port number, then assign the port number on the Remote Administration screen. This change occurs immediately upon saving.

How to Access the Web Interface

1. Start a frames-capable web browser.
2. Enter the IP address or host name of the GTA Firewall’s Protected Network interface as a URL in the Location: entry field (e.g., http://192.168.71.254/). If your workstation does not have an IP address on the same logical network as the GTA Firewall Protected Network interface, you will need to adjust the Remote Access Filter that controls access.

Characteristics

- The Web interface is dynamic, so changes take place immediately.
- Caching is disabled since the configuration data is dynamic.
- Re-sizing the browser will change the size of the main screen.
- Password authorization is persistent for a session.
- Blanking out data entry fields in a list-oriented form will delete the row when the Submit button is clicked.
- The system contains a built-in web server that only serves the GTA Firewall web pages; it cannot be used for other purposes.
- The factory settings User ID and password are “gnatbox.”

Caution

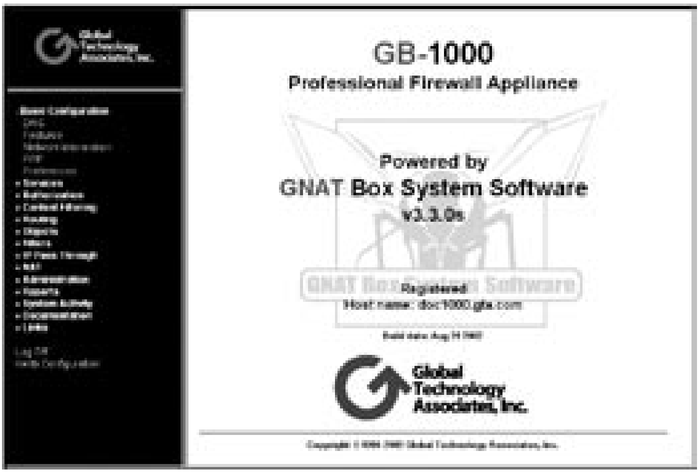
If a browser is left running or is shut down without logging off the firewall, an unauthorized user could access the firewall by returning to that screen in the browser. To prevent unauthorized access, remember to log off.

Navigation and Data Entry

The Web interface uses HTML frames to subdivide the browser's display. The main parts of the Web interface navigation screen are:

GTA Logo:	Link to Global Technology Associates's website.
Menu:	Provides access to all command functions.
Main Window:	Work area where data is entered and displayed.

The navigation of the Web interface screen is easy to use. It employs fields with extensive labeling, check/uncheck boxes, dropdown boxes, dynamic menus, mouse/cursor clicks, keyboard <Tab> and <Return> keys, and verification messages to supply information to the user.



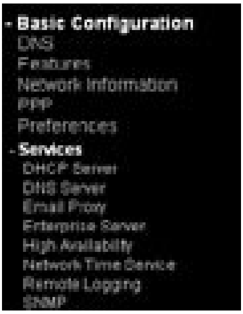
GB-1000
Professional Firewall Appliance
Powered by
GNAT Box System Software
v3.3.0s
Registered
Host name: doc1000.gta.com

Web Interface Main Window

Menus

The Menu that is displayed on the left side of the web browser window is the main navigation tool for the Web interface. The chapters of this guide follow the order of the Web interface menu layout. Certain optional features within sections will not appear on your GTA Firewall until they have been activated using a feature activation code.

The menu consists of 14 main functional areas: Basic Configuration, Services, Authorization, Content Filtering, Routing, Objects, Filters, IP Pass Through, NAT, Administration, Reports, System Activity, Documentation and Links.



Web Menu Example

When selected, each menu title will expand to reveal items in a functional area. Click on the title again to collapse the revealed menu. An open menu has a “-” sign to the left of the menu, and a closed menu has a “+” sign. Click on functions within the sections to display its configuration screen.

Two special functions are listed at the bottom of the menu. Log Off allows the administrator to disconnect from the currently loaded GTA Firewall. Verify Configuration is used to run verification tests on the current system configuration and produce a report using the results.

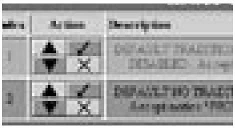
Buttons and Fields

Screen buttons and fields allow the user to navigate, enter data and display information. The Navigation Buttons are the most common.

Navigation Buttons

Reset	Reset	Return screen to previous state.
Submit	Submit	Submit entries made in the current function.
Copy	Copy	Copy filters or other items.
Paste	Paste	Paste copied items into a new screen.
Default	Default	Make the configuration screen items conform to the default security policy for the current configuration.
Back	Back	Go back to the previous screen without saving.
Save	Save	Save this screen or item.
Ok	OK	Keep the current screen – this will allow the material to be saved on the previous screen.

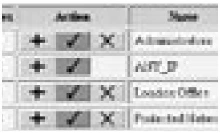
The Icon Buttons appear wherever there are line items to add, delete or edit; see any of the filter set screens for an example of these icons.



Filter Icon Buttons

Filter Icon Buttons

▲▼	Up/Down Arrows	Add a line (e.g., filter) above/below the selected item. Used where order ***is*** important.
✕	X/Delete Sign	Delete the selected line item.
✓	√/Check Mark	Edit the selected line item.



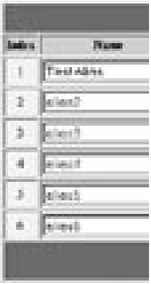
Object Icon Buttons

Object Icon Buttons

+	+/Add Sign	Add a line item. Used where order ***is not*** important.
✕	X/Delete Sign	Delete the selected line item.
	Blank Space	If there is a blank space in place of the X, the item cannot be deleted.
✓	√/Check Mark	Edit the selected line item.

Specialized buttons such as Set Timezone and Update Now serve a specific purpose in the screen in which they are used. These buttons are explained in each section where they are used.

Index Fields are non-editable fields containing index numbers (also called rule numbers) that indicate the number of a line item.

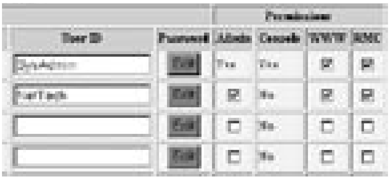


Index	Name
1	[illegible]
2	[illegible]
3	[illegible]
4	[illegible]
5	[illegible]
6	[illegible]

Index Fields

Check Boxes are used to select/deselect items and functions. Read the field label carefully to learn whether the selected the check box will enable/turn on or disable/turn off the function. Some items cannot be changed; these are represented by a field with a Yes/No in place of the check box.

In the example screen below, the WWW column is checked for the two users, indicating that the item is enabled for these users, and they can access the firewall through the Web interface. The Console column is marked with a "Yes" for the Administrator, meaning that the administrator can make changes using the Console, and that this cannot be disabled. The NetTech user cannot access the firewall using the Console, as indicated by a "No" in the field; this access cannot be enabled.



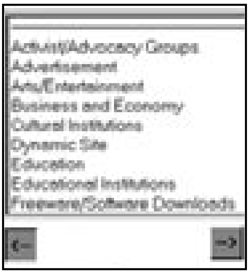
		Permissions			
User ID	Password	Admin	Console	WWW	RMC
SysAdmin	Edit	Yes	Yes	☑	☑
NetTech	Edit	☑	No	☑	☑
	Edit	☐	No	☐	☐
	Edit	☐	No	☐	☐

Check Boxes

Content Filtering has list selection screens which can be scrolled through using standard Windows up and down sliders. Arrow buttons move items from one list to another.

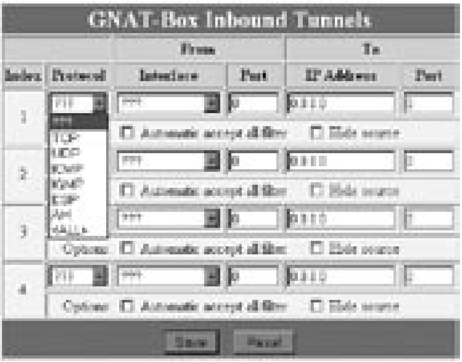
“<–” A left-pointing arrow moves the selected item from the list on the right to the list on the left.

“–>” A right-pointing arrow moves the selected item from the list on the left to the list on the right.



Content Filtering Buttons and Lists

Miscellaneous boxes and fields allow the user to enter data by typing or selecting an item from a dropdown menu. In the example screen below, the Protocol column is displaying a dropdown box. Click on the arrow to open the dropdown menu. The spaces under the Port and IP address columns are examples of data entry fields.



Dropdown Boxes; Data Entry Fields

A field with three question marks “???” indicates an unknown value; the field requires information in order to be used in the configuration being attempted. A field that is greyed out cannot be edited. It is either unavailable in this configuration or is set by the system.

GBAdmin

GBAdmin is the Windows-based GNAT Box System Software configuration tool for administrators who prefer to configure the GTA Firewall from a workstation on the Protected Network. GBAdmin has several unique features. A configuration can be changed and saved to a configuration file. This allows the administrator to use verification notes and configuration reports to adjust settings before committing a new configuration to the running firewall.

Exclusive Features

- Verification checks are performed as configuration changes are made, without saving to the loaded configuration.
- Configurations can be saved to a file and opened in GBAdmin, without saving the data to the running firewall.
- Dropdown menus are customized according to the configuration information already saved to the configuration.
- Familiar Windows-based interface.
- Compact screens.
- Built-in copy and paste function using common keystrokes.

GBAdmin Access

By default, any host on the Protected Network interface is allowed access to the GTA Firewall GBAdmin interface. If you wish to restrict access, modify the default Remote Access Filter that allows access to GBAdmin.

How to Access GBAdmin

1. Click the GBAdmin icon on the desktop if one was created during installation; optionally, open the Windows program menu > GTA GNAT Box folder > GBAdmin Folder and click the program icon.
2. Select File>Open under the File menu, click the Network radio button and enter the IP address or host name of the GTA Firewall's Protected Network interface in the SERVER field, (e.g., 192.168.71.254). If your workstation does not have an IP address on the same logical network as the GTA Firewall Protected Network interface, you will need to adjust the Remote Access Filter which controls access.

Caution

If GBAdmin is left running with a loaded configuration of the running GTA Firewall, an unauthorized user could gain access. To prevent unauthorized users from making changes, remember to log off.

Characteristics

GBAdmin data are not saved to the currently loaded configuration file, remote GTA Firewall or floppy disk, until: a configuration File > Save, a Save All Sections, or a Save Current Section has been performed.

Save Current Section saves only the data in the current function and is available when online (connected to a running firewall.)

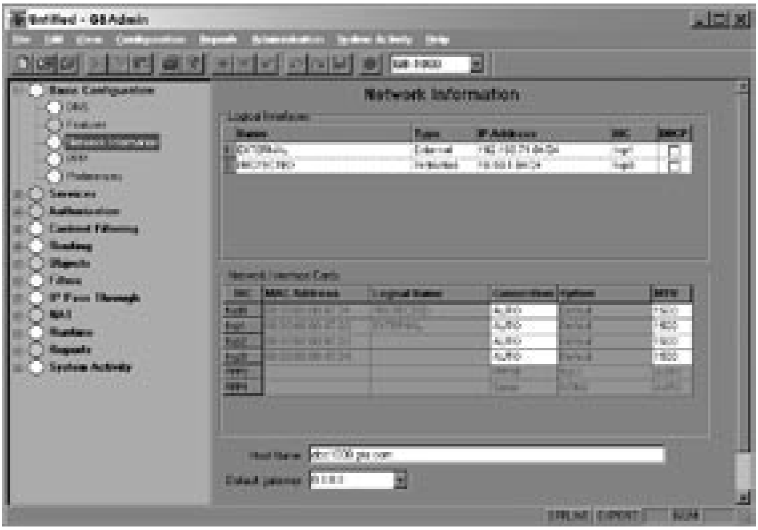
- Re-sizing GBAdmin's display will change the display of the main screen.
- Password authorization is persistent for a session.
- The default User ID and password are "gnatbox."

Navigation and Data Entry

GBAdmin uses a Windows-based browser to subdivide the display. The main parts of the GBAdmin navigation screen are:

Menubar:	Provides access to all command functions, including a standard Windows File Menu, a View Menu and Administration Menu, as well as the Expert Mode selection under the Edit Menu.
Toolbar:	Tools which provide quick access to GBAdmin's most used features.
Scrolling Menu:	Provides access to configuration functions.
Main Window:	Data entry and display area.
Lists:	Provide a compact view of all entered data for the function in one screen.

The GBAdmin interface consists of four basic parts within the standard window: the Menubar provides access to all sections and primary functions; the Toolbar gives the user access to commonly used functions; the Scrolling Menu generally mirrors the Web interface menu; and the Work Area, displays the functions. The screen illustrated appears when GBAdmin is first accessed after login. It always opens displaying the Network Information screen.



GBAdmin Opening Screen

The menus contain 12 functional areas: Basic Configuration, Services, Authorization, Content Filtering, Routing, Objects, Filters, IP Pass Through, NAT, Runtime, Reports and System Activity. The Runtime Menu is unique to GBAdmin, and the Administration Menu is accessed from the Menubar.

Selecting the “+” (plus) next to a Scrolling Menu title will expand the menu to reveal items in a functional area. Clicking the “-” (minus) sign collapses the revealed menu.

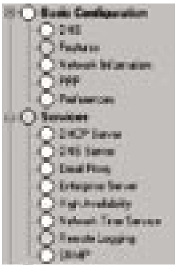
In GBAdmin, clicking on the Scrolling Menu title will display an HTML version of the material available in this guide for each menu title.

Keys

Familiar keyboard keys used in Windows are also used in GBAdmin: arrow keys: < **<--** > and < **-->** > can be used navigate menus; the <Tab> key can be used to navigate the fields in screens; <ctrl>+<S>, <ctrl>+<O>, <ctrl>+<X>, <ctrl>+<C>, etc., all perform the usual Windows functions. Available keyboard alternates for menu items are listed in the Menubar menus.

Scrolling Menu

The Scrolling Menu is similar to the Menu in the Web interface. However, it does not contain the Administrative menu; it reports the runtime version in its own menu section; as well as several other minor variations mentioned in individual sections.



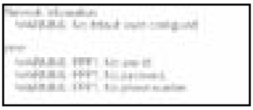
Scrolling Menu Example

To access the functions within the Scrolling Menu, click the "+" (plus) sign to the left of the section labels. To close the menu section, click the "-" (minus) sign that appears to the left of the label when the menu section is open.

To use a function, click the function label or indicator dot.

Pop-up Verification Notes and Indicator Dots

A feature of GBAdmin is the instant verification provided for a configuration. A change made, even if it is not saved, creates a Pop-up Verification Note if the function has not been configured correctly or completely. The notes appear in front of the section when the user "hovers" the mouse by resting the cursor over the section label. There are two kinds of note: Warning, which report a possible problem and Error, which reports a configuration problem that will prevent the operation of the firewall.



Network information
  WARNING: No default route configured

PPP
  WARNING: PPP1: No user id
  WARNING: PPP1: No password
  WARNING: PPP1: No phone number

Pop-up Verification Note

Indicator Dots (also called "lights" or "buttons") give the user an instant impression of whether the section or function is configured correctly.

SCROLLING MENU
VERIFICATION INDICATORS

🔴 ERROR (RED)

🟢 CORRECT (GREEN)

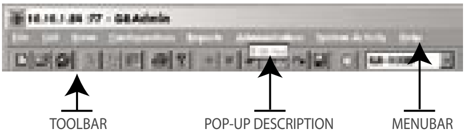
🟡 WARNING (YELLOW)

○ EMPTY (WHITE)

Indicator Dots

Menubar

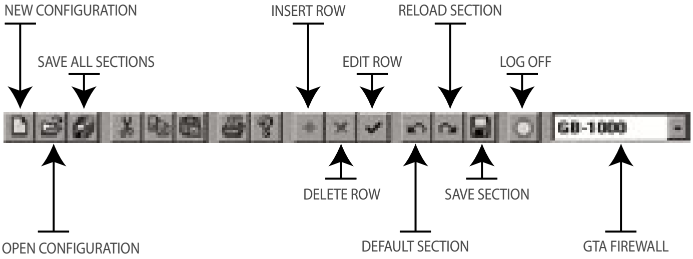
The Menubar contains all the same functions as the Scrolling Menu, plus the Administration menu and many of the familiar Windows functions.



Menubar

Toolbar

The Toolbar contains GBAdmin's most common functions in a graphic icon format. Several of the tools are Windows tools used in the standard way; others are used for a purpose specific to GBAdmin. The illustration below shows the location, name and description of each of these tools.



Toolbar

Pop-up Description Notes

Pop-up Notes are similar to Verification Pop-ups and are a standard Windows feature. Use the mouse to hover the cursor over the object for which you would like a description. (See the Menubar illustration, above.)

Check Boxes, Lists and Tabs

Check boxes and other navigation items in GBAdmin are similar to their Web interface counterparts. A special kind of selection icon is the radio button: this is similar to a check box, but indicates that only one of the items can be selected at one time.

4 Basic Configuration

Basic Configuration contains functions that address basic GTA Firewall setup and configuration. Some GTA Firewall configurations do not require all of these 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 Web interface. After a brief explanation of the function, there will be a table of field descriptions and screen illustrations from the Web interface. After that, if there are any differences in the function or the interface in GBAdmin, these will be explained and illustrated.

Basic Configuration Menu

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

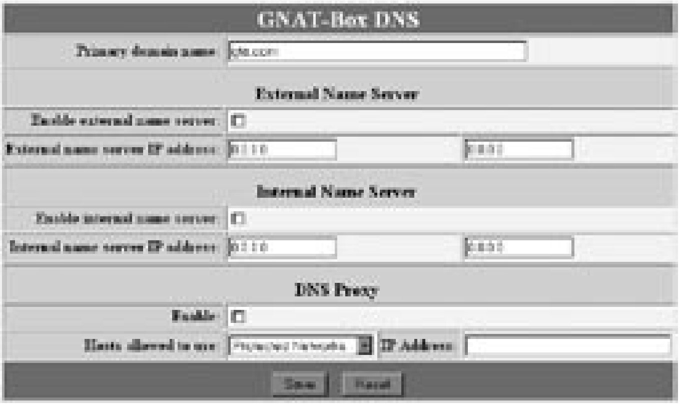
DNS Proxy is enabled by default, except when upgrading. DNS proxy specifies which hosts on a network will use the firewall as a DNS proxy. The hosts will be represented either by an IP address or an Address Object. The DNS proxy sends a request to all available DNS servers (those listed and those acquired dynamically) to resolve a host name. The first reply will be sent to the requestor. A Remote Access Filter to allow DNS proxy replies is also enabled, except when upgrading from a version previous to 3.3.

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.



GNAT-Box DNS

Primary domain name: gta.com

External Name Server

Enable external name server: □

External name server IP address: [illegible] [illegible]

Internal Name Server

Enable internal name server: □

Internal name server IP address: [illegible] [illegible]

DNS Proxy

Enable: □

Hosts allowed to use: Protected Networks   IP Address:

DNS

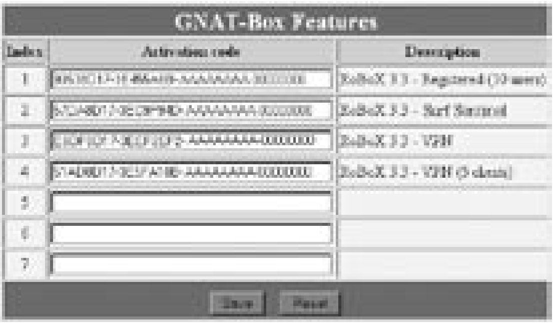
Features

Enter GTA Firewall activation codes (hexadecimal characters only – 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) for options such as H_2A, Surf Sentinel, Multi-Interface and VPN Client in Features. System activation codes entered during installation or pre-installed with hardware appliances will also appear.

Select Save; the system will then display a description of what has been activated. If this description is garbled or does not appear, the code has 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.

Note

Activation codes will not function without the system serial number entered in the Preferences screen. Hardware appliances have this number pre-installed.



GNAT-Box Features

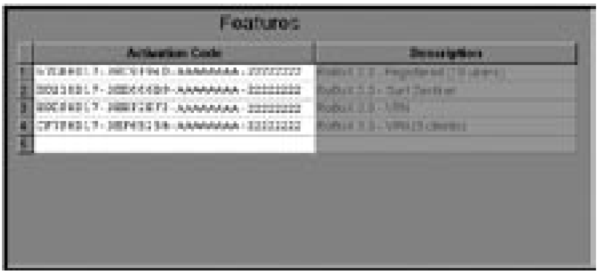
Index	Activation code	Description
1	[illegible]	RoBoX 3.3 - Registered (10 users)
2	[illegible]	RoBoX 3.3 - Surf Sentinel
3	[illegible]	RoBoX 3.3 - VPN
4	[illegible]	RoBoX 3.3 - VPN (5 clients)
5		
6		
7		

Features

Interface Variations

To add entries in the Web interface, enter the codes and select Save. Entry spaces will be added as codes are entered and saved. Delete entries by deleting all of the code characters and then selecting Save. If you have not yet saved the Features information and you would like to reload the saved information, use the Reset button to revert to the saved code information.

To add entries in GBAdmin, click Add (+) and then select Save. To delete saved codes, click Delete (X), then select Save. If you have not yet saved the Features information and you would like to reset the screen to the saved information, use Reload to revert to the saved information.



Features

	Activation Code	Description
1	[illegible]	RoBoX 3.3 - Registered (10 users)
2	[illegible]	RoBoX 3.3 - Surf Sentinel
3	[illegible]	RoBoX 3.3 - VPN
4	[illegible]	RoBoX 3.3 - VPN (5 clients)
5		

Features (GBAdmin)

Network Information

Much of the Network Information data will have been entered during installation, including the required Protected Network and External Network. Most additional information is completed before other configuration tasks. (Exceptions such as PPP setup are noted in each section.)

Warning Note

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

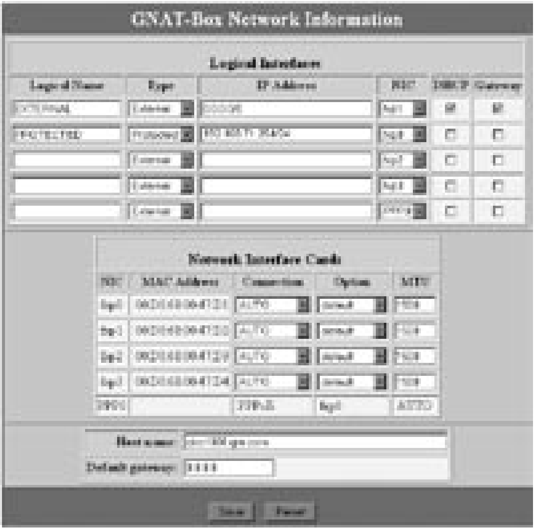
	Logical Interfaces
Logical Name	Assign a logical name to suit company convention. Interface Object names may not use a number as the first character. See Warning Note, above.
Type	Select the interface type: Protected, External and PSN.
IP address	All active network interfaces that do not use PPP/PPPoE 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.
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.
Gateway (Web only)	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. See Interface Variations, below, for more about selecting a gateway.

Network Interface Cards/Physical Interfaces/NICs

NIC (& PPP/PPPoE)	The name of a supported and configured network interface device detected by the system. Configured PPP/PPPoE connections will appear here.
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.
Connections	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- ***or*** 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.
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	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 PPP/PPPoE. The gateway value will be set automatically if it is set on a dynamically negotiated interface. See Interface Variations.

How to Change an Object Name

To change an object name without losing connectivity: copy the object, change the name in the copy, enable it, then change the parts of the configuration that reference it. You may then delete the original object. Alternatively, to change logical names, first create filters using the new interface names. Next, change the Logical Names in Network Information, and then remove the filters referring to the old logical names.



GNAT-Box Network Information

Logical Interfaces

Logical Name	Type	IP Address	NIC	DHCP	Gateway
EXTERNAL	External	[illegible]	[illegible]	☑	☑
PROTECTED	Protected	[illegible]	[illegible]	☐	☐
	External		[illegible]	☐	☐
	External		[illegible]	☐	☐
	External		[illegible]	☐	☐

Network Interface Cards

NIC	MAC Address	Connection	Option	MTU
[illegible]	[illegible]	AUTO	default	1500
[illegible]	[illegible]	AUTO	default	1500
[illegible]	[illegible]	AUTO	default	1500
[illegible]	[illegible]	AUTO	default	1500
[illegible]		[illegible]	[illegible]	AUTO

Host name: [illegible]

Default gateway: 1.1.1.1

Network Information

Interface Variations

The Web interface is different from GBAdmin in that there is a Gateway checkbox in the Web's Network Information screen. In the Web, when the interface is dynamic, the Default Gateway can be selected from the GATEWAY checkbox field. However, when the gateway is dynamic in GBAdmin, select the gateway's interface object/logical interface by using the Default Gateway dropdown box at the bottom of the screen.

When the interface is static, the IP address must be entered in the DEFAULT GATEWAY field in either GBAdmin or the Web.

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

CIDR (Classless Inter-Domain Routing) aggregates routes so that one IP address represents thousands served by a backbone provider. GNAT Box System Software uses notation based on CIDR as the default for subnet masks.

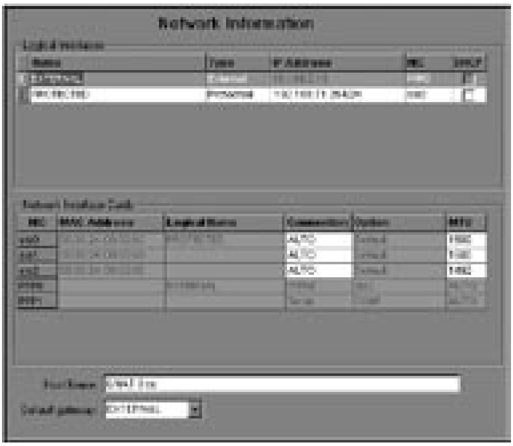
Instead of the fixed 8, 16 and 24 bits used in the Class A-B-C network IDs, CIDR-based notation can further divide the network into subnets by using network IDs (in a Class C network) from 24-31, (/32 representing one IP address).

For example, the CIDR address 204.12.01.42/24 indicates that the first 24 bits are used for the network ID. The "/24" mask will include all 254 hosts on the network, and is equivalent to “255.255.255.000” in dotted-decimal 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

The user may still use dotted decimal by entering a forward slash and then the dotted decimal netmask.



Network Information

Logical Interfaces

Name	Type	IP Address	NIC	DHCP
EXTERNAL	External	[illegible]	[illegible]	□
PROTECTED	Protected	[illegible]	[illegible]	□

Network Interface Cards

NIC	MAC Address	Logical Name	Connection	Option	MTU
[illegible]	[illegible]	[illegible]	AUTO	[illegible]	[illegible]
[illegible]	[illegible]		AUTO	[illegible]	[illegible]
[illegible]	[illegible]		AUTO	[illegible]	[illegible]
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]
[illegible]			[illegible]	[illegible]	[illegible]

Host Name: [illegible]

Default gateway: EXTERNAL

Network Information (GBAdmin)

PPP

The PPP section is the location to configure a PPP (Point-to-Point Protocol) or PPPoE (PPP over Ethernet) connection for the firewall. ***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 on each tab (GBAdmin) or screen section (Web) 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 from the configuration screen when PPP is selected. PPP has fields not found in PPPoE; these fields are indicated in the fields table by "*" (one asterisk).

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).

Note

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.

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.

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.

PPP/PPPoE Fields

	General Tab
Name	PPP0, 1,2,3 or 4. The name is automatically assigned, and will be the same for a PPPoE connection. The name will appear as a tab in GBAdmin.
Description	A user-defined name for the connection.
PPPoE	Enable using the dialog box on the Web interface. In GBAdmin, enable by selecting the checkbox.
NIC**	Network interface on which PPPoE will run.
Connection Type	***Dedicated*** Establishes a PPP/PPPoE link when the firewall boots up. The link will remain up until the interface is manually disabled, or the system is halted. For PPPoE, this is the logical choice, as DSL is an “always on” connection. Select “Dedicated” to test a configuration. ***On-demand*** Initiates and establishes a PPP/PPPoE link with the remote site whenever a packet arrives on a Protected or PSN interface, destined for the External Network. The link will stay up as long as packets continue to be received before the time-out period has expired. ***On-enabled*** Requires manually enabling the External Network interface. When the interface is enabled, this connection type initiates a PPP/PPPoE session and establishes a link with the remote site. The PPP link will stay established until disabled. Interfaces may easily be enabled/disabled in Administration > Interfaces.
Primary COM Port*	Select the COM Port used for the PPP interface. COM 1-4 are allowed, except on the GB-1000, which is set to COM 2, and the RoBoX, which is set 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 Password	User ID and password for remote PPP/PPPoE access, generally issued by the remote site. The password is obscured in the data entry field.

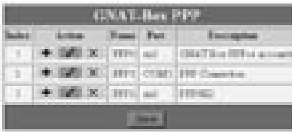
Local IP address Remote IP address	A PPP/PPPoE link uses a local and remote IP address. If the remote site supports ***dynamic*** address assignment (as for most ISPs and remote sites), leave the local address set to the default, 0.0.0.0. Set the remote address to an IP address on the remote network, such as the router IP or the DNS server address. PPP will use that address to dynamically negotiate the actual value. If the Remote IP address is ***static (dedicated)***, enter the address and leave the Local IP address set to 0.0.0.0. If ***both addresses are static***, set both fields to the appropriate IP address.
Connection time out	The number of seconds during which a connection using PPP/PPPoE will stay connected when inactive. The default is 600 (10 minutes). To prevent timing out, enter "0."
PPPoE Provider**	Designation for the PPPoE Provider. Leave this field blank if you do not know the ***exact*** designation; the value is not required for the connection, and an incorrect setting can prevent the connection.
MTU**	Maximum Transmission Unit. GTA recommends leaving the field set at "0", which allows the system to negotiate the MTU value for each PPPoE connection. Incorrect values can cause the system to perform poorly, or not at all.
Login user name* Login password*	For cases in which CHAP or PAP is negotiated, and a separate name and password are required to log in.
Speed*	DTE (Data Terminating Equipment) speed. 1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200, 230400. This is the speed at which the firewall communicates with the modem.
Number of retries	Default is 3. This is the number of attempts the system will make before stopping the attempt to establish a connection. After failure, any new packets arriving for the External Network will restart a new dialing attempt. (Retries are not used on dedicated connections; these connections will continue to try to connect.)
Time before retry	Default is 10 seconds. This is the amount of time the system waits before re-dialing to establish a connection.

Link Control Protocol

Each LCP option has a pair of settings: Enable for the local and Accept for the remote side. If Local is enabled, the firewall will request that the remote side use that LCP. If Local is disabled, the firewall will not send a request for that LCP. If Remote is set to Accept (enabled), and the remote side of the connection offers to use the protocol, the firewall will accept it. If it is set to Deny (disabled), then the firewall will not accept the LCP if the remote side offers it.

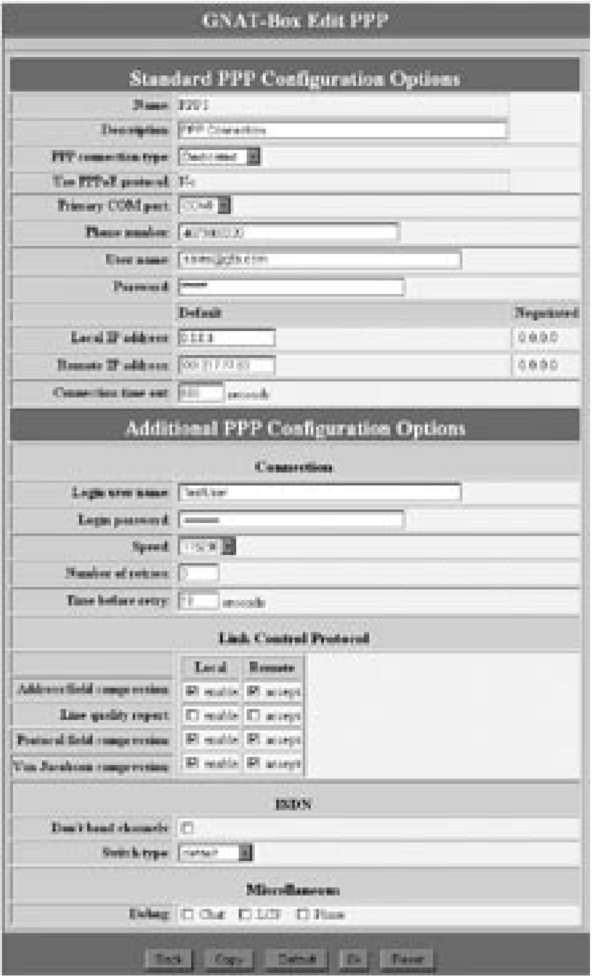
Address/field compression	Enable	Accept
Line quality report	Enable	Accept
Protocol field compression	Enable	Accept
Van Jacobson compression	Enable	Accept
Default LCP settings are correct for most cases. If you are unsure which options to select, use the default setting and enable the LCP debug option (see below). Then, when a session is attempted, use the debug output in the syslog to determine which options have been requested and rejected. Match your LCP settings to the desired requests.		
ISDN* Use to configure ISDN connections. Check with your provider for required settings.		
Don’t bond channels	Bond Channels is enabled by default. Select this option to disable bonding channels.	
Switch type	Options: Default; NI-1; DMS-100; 5ESS P2P; 5ESS MP.	
Debug These options provide helpful information when creating a PPP configuration.		
Chat	Records dialing and login chat script conversations.	
LCP	Records LCP conversations. Use to set non-default Link Control Protocol options.	
Phase	Records network phase conversations. Use to determine the Local and Remote IP address specifications.	

*** PPP screens only.** **** PPPoE screens only.**



PPP list

New PPP/PPPoE dialog



Standard PPP Configuration Options

Name	[illegible]	
Description	PPP Connection	
PPP connection type	[illegible]	
Use PPPoE protocol	No	
Primary COM port	[illegible]	
Phone number	[illegible]	
User name	[illegible]	
Password	*****	
	Default	Negotiated
Local IP address	[illegible]	0.0.0.0
Remote IP address	[illegible]	0.0.0.0
Connection time out	[illegible] seconds	

Additional PPP Configuration Options

Connection

Login user name	[illegible]
Login password	******
Speed	[illegible]
Number of retries	[illegible]
Time before retry	[illegible] seconds

Link Control Protocol

	Local	Remote
Address field compression	☒ enable	☒ accept
Line quality report	☐ enable	☐ accept
Protocol field compression	☒ enable	☒ accept
Van Jacobson compression	☒ enable	☒ accept

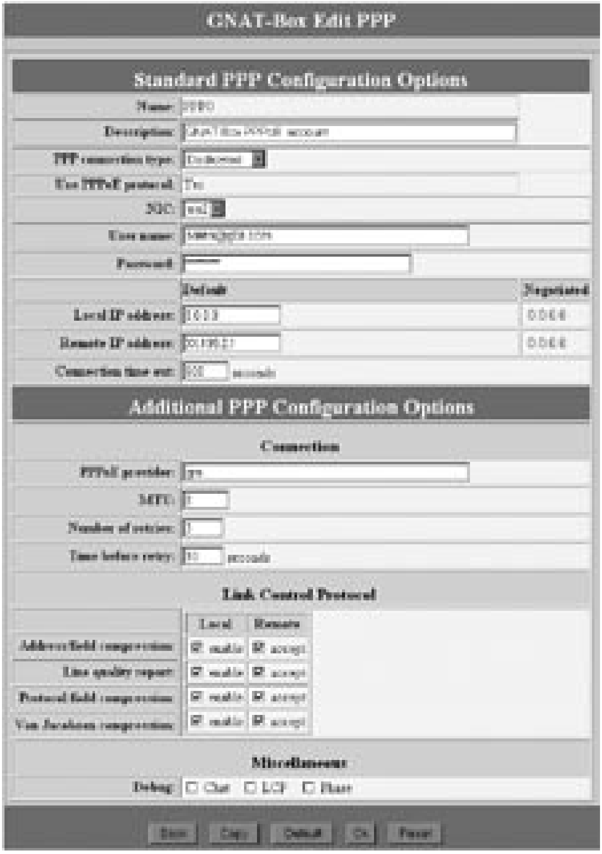
ISDN

Don't bond channels	☐
Switch type	[illegible]

Miscellaneous

Debug	☐ Chat ☐ LCP ☐ Phase

PPP screen



CNAT-Box Edit PPP

Standard PPP Configuration Options

Name: [illegible]

Description: [illegible]

PPP connection type: [illegible]

Use PPPoE protocol: Yes

NIC: [illegible]

User name: [illegible]

Password: [illegible]

	Default	Negotiated
Local IP address:	[illegible]	0.0.0.0
Remote IP address:	[illegible]	0.0.0.0

Connection time out: [illegible] seconds

Additional PPP Configuration Options

Connection

PPPoE provider: [illegible]

MTU: [illegible]

Number of retries: [illegible]

Time before retry: [illegible] seconds

Link Control Protocol

	Local	Remote
Address field compression:	☑ enable	☑ accept
Line quality report:	☑ enable	☑ accept
Protocol field compression:	☑ enable	☑ accept
Van Jacobson compression:	☑ enable	☑ accept

Miscellaneous

Debug: □ Chat □ LCP □ Phase

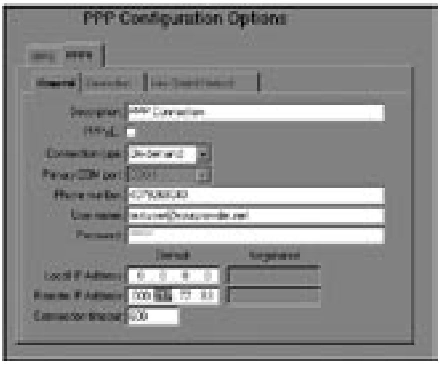
PPPoE

Interface Variations

The Web interface and GBAdmin have the same options, but the fields and selections are arranged differently.

In the Web interface, the user selects the Add (+) button to add a PPP/PPPoE configuration. In the Insert PPP dialog, the user chooses either PPPoE (the default), or PPP (by selecting No from the dropdown box), then clicking OK.

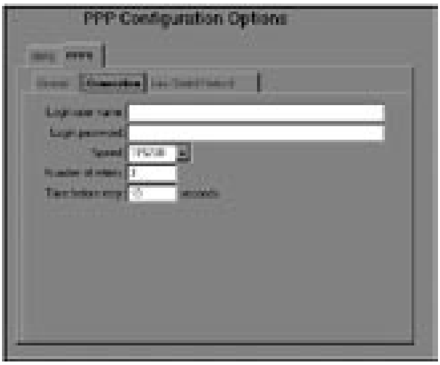
In GBAdmin, the user creates a new PPP or PPPoE configuration by selecting the Add + (plus) from the toolbar, which creates a default, blank PPP tab with three sub-tabs, General, Connection and Link Control Protocol. To create a PPPoE configuration, the user selects the PPPoE checkbox, which changes the selections on each sub-tab.



PPP Configuration Options

Description: PPP Connection
PPPoE: □
Connection type: On-Demand
Primary COM port: COM1
Phone number: [illegible]
User name: [illegible]
Password: [illegible]
Default Negotiated
Local IP Address: 0 . 0 . 0 . 0
Remote IP Address: [illegible]
Connection timeout: [illegible]

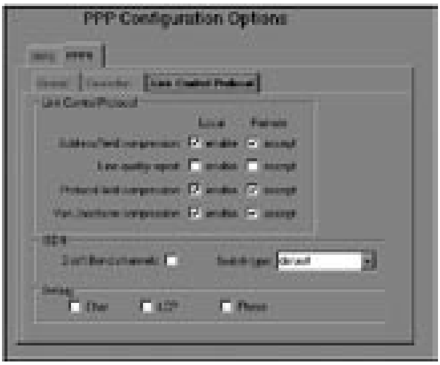
PPP – General Tab (GBAdmin)



PPP Configuration Options

Login user name:
Login password:
Speed: [illegible]
Number of retries: [illegible]
Time between retry: [illegible] seconds

PPP – Connection Tab (GBAdmin)



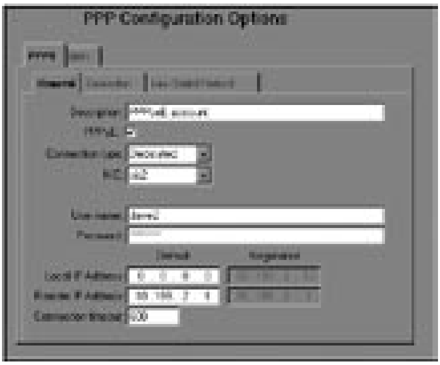
PPP Configuration Options

Link Control Protocol
Local Remote
Address/field compression: ☑ enable ☑ accept
Line quality report: □ enable □ accept
Protocol field compression: ☑ enable ☑ accept
Van Jacobson compression: ☑ enable ☑ accept

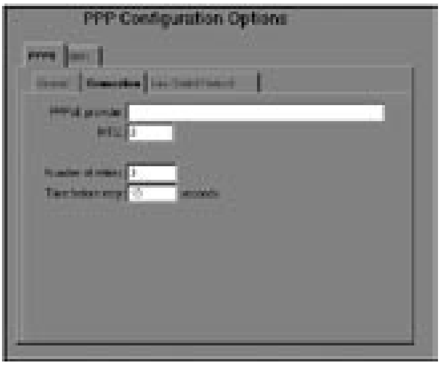
ISDN
Don't Bond channels: □ Switch type: default

Debug
□ Chat □ LCP □ Phase

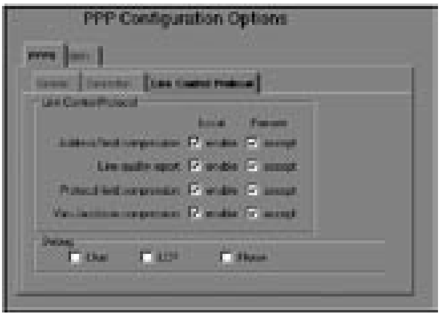
PPP – Link Control Protocol Tab (GBAdmin)



PPPoE – General Tab (GBAdmin)



PPPoE – Connection Tab (GBAdmin)



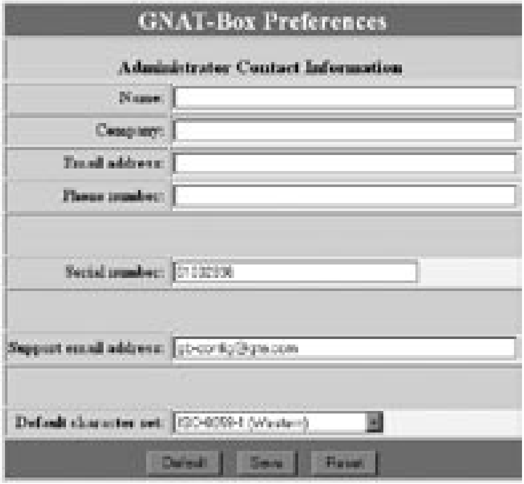
PPPoE – Link Control Protocol Tab (GBAdmin)

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.



GNAT-Box Preferences

Administrator Contact Information

Name:	
Company:	
Email address:	
Phone number:	
Serial number:	[illegible]
Support email address:	[illegible]
Default character set:	ISO-8859-1 (Western)

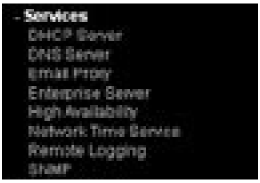
Preferences (Contact Information)

5 Services

The Services section consists of DHCP Server and DNS Server; the Email Proxy; GB-Enterprise Server; the H_2A High Availability service; the Network Time Service; Remote Logging; and the SNMP facility. None of these services are required for the GTA Firewall.

Note

GTA highly recommends running Email Proxy. This, as well as the other services, can increase the security of your firewall.



Services Menu

DHCP Server

The DHCP (Dynamic Host Configuration Protocol) Server automates the process of assigning IP addresses to host systems on locally attached networks. Additionally, a DNS server and default gateway can be provided by the DHCP server. The DHCP server manages a range of IP addresses (e.g., 10.10.10.4–10.10.10.254) which can be assigned to clients. Non-contiguous ranges of addresses can be defined using exclusion ranges. Exclusion ranges indicate which IP addresses within the previously defined address range are not to be assigned to host systems by the DHCP server.

When the DHCP Server receives an initial request from a client host, it assigns an available IP address from its pool. Upon subsequent requests by the same client, the DHCP server will attempt to reassign the same IP address. The only case in which it will not reassign the same IP address is when the number of clients exceeds the number of addresses in the pool, and the IP address was assigned to a different host.

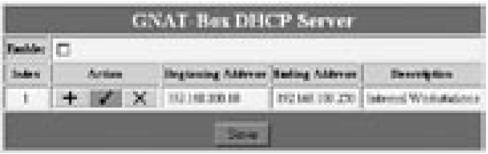
Note

If the DHCP service is for an External Network then the default gateway is most likely the Internet router’s IP address.

Changes to DHCP will not be applied until the section is saved. If a network connection is established and the section is saved, the DHCP Server changes will be applied immediately to the GTA Firewall.

DHCP Fields

Enable	Select this checkbox to enable the currently displayed DHCP IP address pool.
Description	Enter a description of the currently displayed DHCP IP address pool.
Beginning Address	This is the first IP of a block of IPs that will be assigned.
Ending Address	This is the last IP of a block of IPs that will be assigned.
Netmask	This is the netmask to assign to DHCP clients.
Lease Duration	Enter the maximum time the DHCP address is valid for use by a requesting client. A client must negotiate to reuse the assigned address before the end of the lease time or quit using the address.
Exclusion Ranges	Define up to five ranges of addresses to exclude from being assigned within each DHCP address range. To exclude a single IP, enter the IP address to be excluded in both the beginning and ending address fields.
Domain Name	The DNS domain name, typically, that of the local network.
Name Server IP address	Enter the IP address of a DNS server that will be issued to the requesting client. This IP can be any valid server: a local server, such as the built-in GNAT Box DNS server, or a remote server, such as one located at an ISP. Up to three name servers can be defined.
Default Gateway	The IP address that the requesting clients will use for their default gateway (default route). For hosts located behind a GTA Firewall (on Protected or PSNs) this value will be the IP address of the GTA Firewall NIC where the network is attached (e.g., if the client is located on the Protected Network, then the default gateway will be the Protected Network's' IP address).

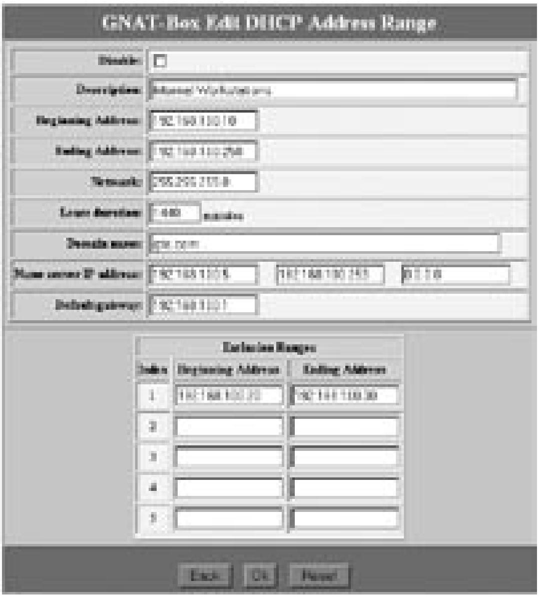


GNAT Box DHCP Server

Enable: □

Index	Action	Beginning Address	Ending Address	Description
1	+ ✎ ✕	[illegible]	[illegible]	[illegible]

DHCP Server List



GNAT-Box Edit DHCP Address Range

Disable:	□
Description:	Internal Workstations
Beginning Address:	192.168.110.10
Ending Address:	192.168.110.250
Netmask:	255.255.255.0
Lease duration:	1440 minutes
Domain name:	[illegible]
Name server IP address:	192.168.110.5 [illegible] [illegible]
Default gateway:	192.168.110.1

Exclusion Ranges

Index	Beginning Address	Ending Address
1	192.168.110.20	192.168.110.30
2		
3		
4		
5		

DHCP Server Address Range

Interface Variations

In GBAdmin, first enable the service to allow it to be edited, then click Add (+) to insert a DHCP service. Select the line to open the editing fields. Once the fields have been edited and saved, the basic information will appear in the DHCP service line below.

To add an exclusion range, click Add (+) next to the EXCLUSION fields. This will create a blank IP address for both the beginning and ending of the range. Double-click within the field to edit the BEGINNING IP address. Delete any extra characters, then edit the ENDING field.

DNS Server

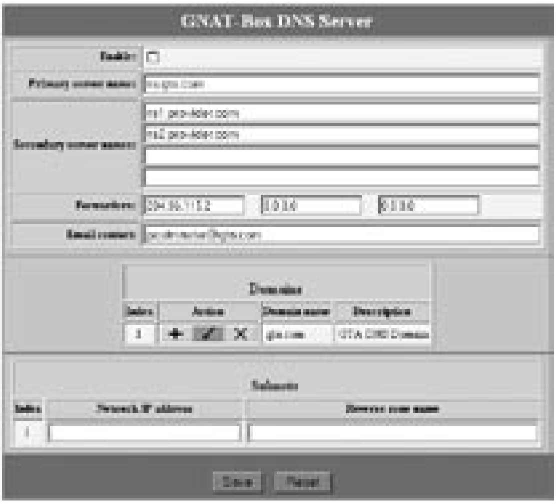
The GNAT Box DNS (Domain Name System) Server allows the firewall to function as a primary Domain Name Server. Before configuring any DNS server, you should thoroughly understand the domain name system. A good reference is **DNS and Bind, 3rd Edition**, by Paul Albitz & Cricket Liu, published by O’Reilly and Associates.

The built-in DNS server in the GTA Firewall is functional and flexible enough for most GTA Firewall users, but cannot be configured to support all possible DNS options. If your site requires a more complex configuration, or hosts secondary name services, GTA suggests using an outside DNS host.

DNS Server Fields

Enable	Enable the DNS server.
Primary Server Name	The host name of your DNS server. This will be a host name assigned to your GTA Firewall. When configuring an external DNS server, this will be the host name seen from the Internet side. The host name should be listed as a host in the DNS Domain screen or tab.
Secondary Server Name	Host names of DNS servers acting as alternate servers for the domain. Up to four alternates may be listed.
Forwarders	The DNS servers that will be utilized as DNS forwarders.
Email Contact	This field should contain the email address of the primary contact for the domain (e.g., administrator@gta.com).
Domains* Use the Add, Edit and Delete buttons to manage DNS domains. See DNS Domain Fields	
Subnets* DNS subnets make a larger network more manageable by splitting it into a series of contiguous address ranges.	
Network IP address	Enter the network address/netmask of the desired subnet. Class C: /24 (255.255.255.0) and Class B: /16 (255.255.0.0) are commonly used networks.
Reverse Zone Name	Optional name used by reverse DNS, which looks up an IP address to obtain a domain name. The GTA Firewall can determine the zone name automatically if the subnet uses a Class A, B or C netmask. Reverse zone names, if needed, are typically assigned by your ISP.

* See product guides for the number of DNS Server domains and subnets available.



Enable: □

Primary server name: ns.gta.com

Secondary server names: ns1.provider.com
ns2.provider.com

Forwarders: [illegible] [illegible] [illegible]

Email contact: [illegible]

Domains

Index	Action	Domain name	Description
1	+ ✎ X	gta.com	GTA DNS Domain

Subnets

Index	Network IP address	Reverse zone name
1		

DNS Server

DNS Domains

The DNS Domain screen allows the user to define host names and associated IP addresses (A records), aliases (CNAME records) and mail exchangers (MX records) for the selected domain. To create DNS Domains, click the Add (+) button and continue configuration of the DNS Server on the DNS Domain screen using the fields below.

DNS Domain Fields

Disable	Select to disable the domain definition so the zone will not be served by the GTA Firewall name server.
Description	Enter a brief description of the domain for your reference.
Domain name	Enter the DNS domain name for the current zone definition, (e.g., gta.com).
Domain's IP address	Enter the IP address of a host to respond to the zone name. A host can have the same name as the zone, e.g. gta.com. This means that if you have a web server, a visitor can use the zone name rather than the web server's fully-qualified host name.

Mail Exchangers
When a remote system sends mail to a domain, it will query a DNS server to determine which IP addresses are designated to accept email for the zone. The Mail Exchanger fields define the mail servers for the domain. When there is more than one Mail Exchanger, they are specified in order of preference by entering the preferred server in the first field, followed by a second and third entry. The first mail exchanger will be priority 5, the second – priority 10, and the third – 15.

Hosts

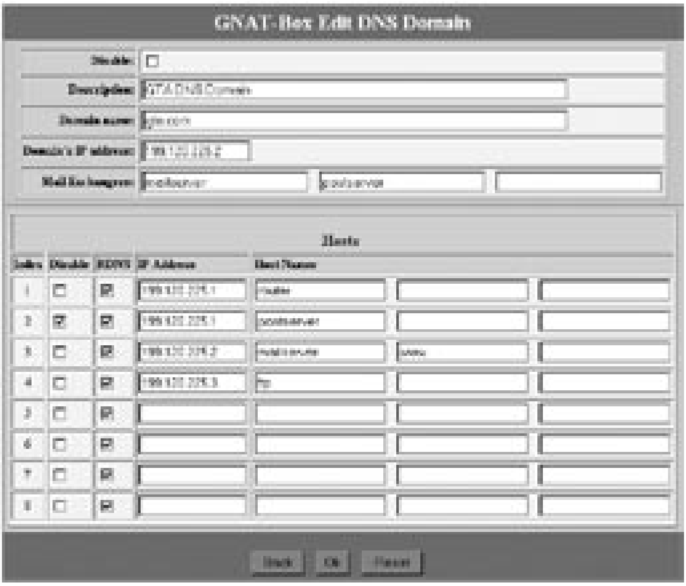
Define host name and IP address associations.

Disable
Select to disable this host entry.

RDNS
Reverse Domain Name System. Select to have a reverse database entry created for the host. Enabled by default.

IP address
The IP address of the host.

Host Names
Enter the primary host name in the first field and aliases in succeeding fields. The domain portion of the host name should not be entered. To define more than two aliases on the Web interface, repeat the IP address in the next row. These names will also be used as aliases.



GNAT-Box Edit DNS Domain

Disable: □
Description: GTA DNS Domain
Domain name: gta.com
Domain's IP address: 199.120.225.2
Mail Exchangers: mailserver | [illegible] |

Hosts

Index	Disable	RDNS	IP Address	Host Names		
1	□	☑	199.120.225.1	router		
2	☑	☑	199.120.225.1	[illegible]		
3	□	☑	199.120.225.2	[illegible]	www	
4	□	☑	199.120.225.3	ftp		
5	□	☑				
6	□	☑				
7	□	☑				
8	□	☑				

DNS Domains

Interface Variations

In GBAdmin, the functions are the same, but the appearance of the screens is different. To add a secondary name server, forwarder or subnet, click the Add (+) button next to these fields.

To add a DNS Domain, click the Add (+) tool on the toolbar. This will add a tab to the screen below the SUBNET field. To edit a specific DNS Domain, click on the tab with the domain's name.

To add a mail exchanger or a host in the DNS Domain tab, click on the Add (+) button next to these fields.

To enter more than one alias in the ALIAS field, separate aliases with a space.

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.
	Connection
Primary email 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.
Alternate email server	Enter the host name (if an internal DNS server has been configured) or IP address of any alternative email server.
Timeout	Default is 120 seconds. Timeout is the time to wait between each SMTP command exchange.
Maximum	Enter the largest number of simultaneous SMTP connections to run. Additional connections are deferred until a connection becomes available. Each connection invokes a copy of the SMTP proxy facility.

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.

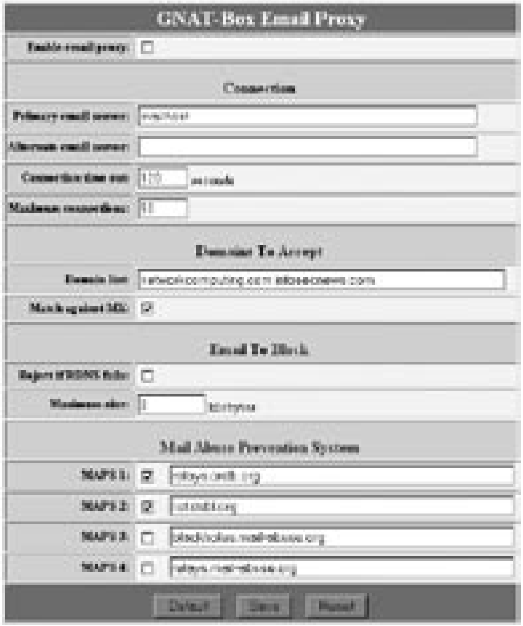
Reject if RDNS fails	Performs a Reverse DNS lookup on the IP address of the remote host trying to make an SMTP (Simple Mail Transfer Protocol) connection, and then compares it to a DNS lookup of the returned host name. If the lookups fail or don’t match, the connection is refused.
Maximum size	Enter 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: `www.orbd.org`
MAP2	list.dsbl.org. Distributed Server Boycott List: `www.dsbl.org`
MAP3	blackholes.mail-abuse.org** `www.mailabuse.org`
MAP4	relays.mail-abuse.org** `www.mailabuse.org`

* Mail Abuse Prevention System LLC lists require a subscription.



GNAT-Box Email Proxy

Enable email proxy: □

Connection

Primary email server: localhost

Alternate email server:

Connection time out: 120 seconds

Maximum connections: 10

Domains To Accept

Domain list: networkcomputing.com [illegible].com

Match against MX: ☑

Email To Block

Reject if RDNS fails: □

Maximum size: 1 kilobytes

Mail Abuse Prevention System

MAPS 1: ☑ relays.ordb.org

MAPS 2: ☑ [illegible].org

MAPS 3: □ blackholes.mail-abuse.org

MAPS 4: □ relays.mail-abuse.org

Email Proxy

GB-Enterprise Server

The GB-Enterprise Server feature allows the configuration of a GTA Firewall so that it can be managed from GB-Enterprise. GB-Enterprise runs on a Windows platform and consists of a service and a client program. A GB-Enterprise feature code must be entered to use GB-Enterprise Server. The **GB-Enterprise User's Guide** will provide more information on this feature. Please check with GTA Sales regarding the availability of GB-Enterprise.

GB-Enterprise is designed to:

- Monitor multiple GTA Firewalls.
- Facilitate management by creating a logical hierarchy.
- Display status, statistics and alarm information for each firewall.
- Process alarm events and send alarm notifications.
- Configure individual GTA Firewalls from within GB-Enterprise.

High Availability

The High Availability option allows two or more GB-1000 systems to operate as a single virtual GB-1000. The **H_2A High Availability Feature Guide** details how to configure and utilize the high availability option.

The High Availability feature for the GB-1000 ensures that network access and security are maintained with minimum downtime. High Availability functionality requires no obvious changes to your existing network configuration, making it totally transparent to end-users.

High Availability Fields

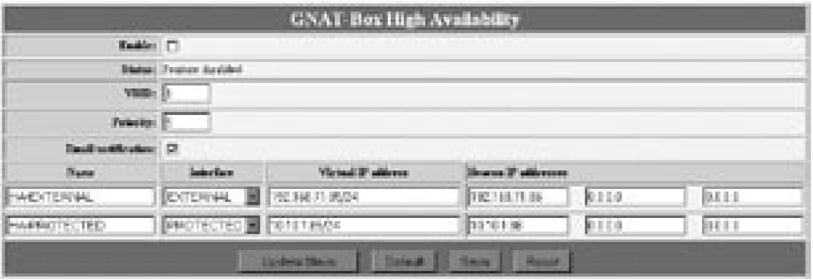
Enable	Enable the H_2A feature. You must have the H_2A Feature code entered in the Features screen to use this option.
Status	This field is not editable. When the system is running in the H_2A mode, the Status field will display the current H_2A mode of the system: Init, Slave or Master.
VRID*	Enter a value between ***0 and 15*** for the VRID (Virtual Router ID), used to uniquely identify the H_2A group. All systems must have the same VRID.
Priority**	Enter a priority number between ***1 and 255*** for the H_2A system. The system with the highest Priority and confirmed communications with its beacons will operate in the Master mode. The system operating in Master mode will be the operational firewall and process network traffic as the virtual firewall. If the priority number for the systems are not set, the system will select the Master by automatically giving one system a higher priority.
Email Notification	Select to receive an email when H_2A changes.
Name	Enter a name for the H_2A member. See How to Change an Object Name, below.
Interface*	Select the interface on which this H_2A member resides using the appropriate Interface Object. Any change to the IP address assigned to the specified network interface on the Network Information screen will change its interface object in the H_2A configuration. Interfaces may only be used once in the H_2A screen. In GBAdmin, an H_2A member that has already been selected for one interface will not appear in the other H_2A dropdown lists.

Virtual IP address	Enter the Virtual IP address that will be used for a given network interface. (This IP address is for the firewall users.) By default, the Virtual IP address is one address higher than the network interface address referenced by the INTERFACE field.
Beacon IP addresses	Enter up to three Beacon IP addresses. Normally, one beacon address is the Interface (configuration) IP address on the other H_2A system, but do not make it your only beacon IP address. This can lead to improper functioning of the H_2A group.

* H_2A systems cannot use dynamically assigned interfaces.

How to Change an Object Name

To change an object name without losing connectivity: copy the object, change the name in the copy, enable it, then change the parts of the configuration that reference it. You may then delete the original object.

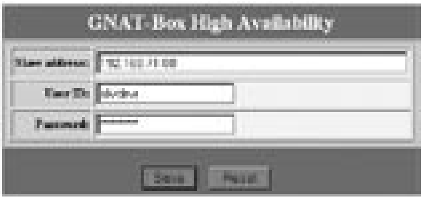


GNAT-Box High Availability

Enable: □
Status: Feature disabled
VHID: 1
Priority: 1
Email notification: ☑

Name	Interface	Virtual IP address	Beacon IP addresses		
HAEXTERNAL	EXTERNAL	192.168.71.85/24	192.168.71.86	0.0.0.0	0.0.0.0
HAPROTECTED	PROTECTED	[illegible]	[illegible]	0.0.0.0	0.0.0.0

H_2A High Availability



GNAT-Box High Availability

Slave address: [illegible]
User ID: [illegible]
Password: ********

H_2A High Availability Update Slave function

Network Time Service

The Network Time Service facility synchronizes your GTA Firewall and computers behind the firewall with an NTP server located on the Internet. Network Time Service uses the Network Time Protocol (NTP), an Internet protocol originally developed by Professor David L. Mills at the University of Delaware.

The Network Time Service facility is highly accurate, with a resolution of less than a nanosecond (one billionth of a second) and the ability to combine the output of the available time servers to reduce error. It also uses past measurements to estimate the current time when the network is down. The Network Time Service facility uses UTC (Universal Time Coordinated), which evolved from GMT (Greenwich Mean Time).

NTP Resources

The following are a sample of the NTP and time server resources available. Locate a site that serves your time zone and contact the administrator, as required.

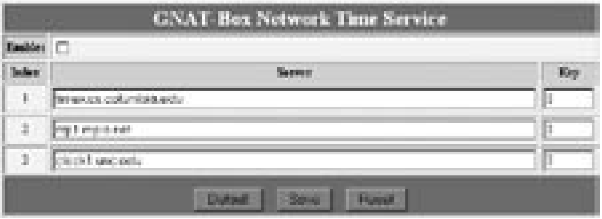
- NIST Network Time Servers. www.boulder.nist.gov/timefreq
- Network Time Protocol organization. www.ntp.org
- Network Time Protocol RFC 1305
- NTP Zeit. www.ntp-zeit.de

Note

Many Network Time Server sites require contacting the site administrator before using the time server.

Network Time Service Fields

Enable	Enable the Network Time Service.
Server	Enter up to three NTP servers, either by name or IP address. These servers can be located on your internal network or external to your system. You must have DNS server defined in the Basic Configuration section if you use host names. Before referencing any NTP server, make sure you adhere to the policies for a given server. There are many freely accessible NTP servers, but it is customary to make a formal request before utilizing the server.
Key	Some servers require a key value; most do not. Enter the appropriate key for the specified server if required.



GNAT Box Network Time Service

Enable: □

Index	Server	Key
1	[illegible]	1
2	[illegible]	1
3	[illegible]	1

Network Time Service

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).

Remote Logging Fields

Use old log format*	Select this to use the log format for GNAT Box System Software version 3.2.x and before.
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.
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.

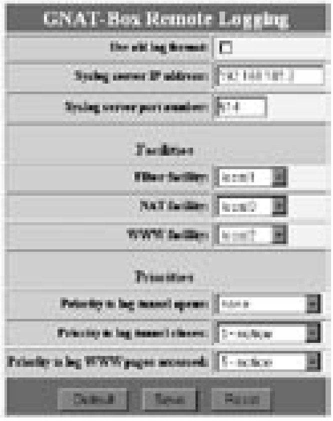
NAT Facility	The NAT facility logs information associated with any Network Address Translation process: essentially, outbound packets. Select None from the list to disable.
WWW Facility	The WWW facility is the syslog stream which logs all URLs accessed through the GTA Firewall. Disable by selecting None 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	This is set to None by default. When a network connection is initiated, an Open record is generated. Select None to disable generation of Open log records.
Priority to log tunnel closes	This is set to 5 (notice) by default. When a network connection is terminated, a Close record is generated. Close records also contain the number of packets and bytes sent and received. Select None to disable generation of Close log records.
Priority to log WWW pages accessed	This is set to 5 (notice) by default. Whenever an Internet web page connection is initiated, a log record will be generated with the URL accessed listed. Disable generation of WWW log records by selecting None

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



GNAT-Box Remote Logging

Use old log format: □

Syslog server IP address: [illegible]

Syslog server port number: 514

Facilities

Filter facility: local1

NAT facility: local2

WWW facility: local7

Priorities

Priority to log tunnel opens: None

Priority to log tunnel closes: 5 - notice

Priority to log WWW pages accessed: 5 - notice

Remote Logging

WELF (WebTrends Enhanced Log Format)

GNAT Box System Software version 3.3 and later supports WELF in log entries. The fields available in the format are listed below. For more information about WELF, see `www.netiq.com/partners/technology/welf.asp`. See the Log Messages section of the Appendix for examples of WELF in GNAT Box System Software. See sample reports in the **GB-Reports Feature Guide** or on the GTA website for examples of WELF in GB-Reports.

WELF Fields

id	Type of record.
time	Shows the ***local*** date and time of the event.
fw	Firewall logging the event.
pri	Event priority: 0=emergency, 1=alert, 2=critical, 3=error, 4=warning, 5=notice, 6=information, 7=debug.
rule	Index (rule) number of the item that triggered the entry.
proto	Protocol or service used by the event.
duration	Time required to perform the event operation, in seconds.
sent	Number of bytes transferred from source to destination.
rcvd	Number of bytes transferred from destination to source.
src	IP address that generated the event.
srcport	Number of the port where the event was generated.
nat	IP address where NAT was performed for the event.
nat_port	Port number where NAT was performed for the event.
dst	IP address that received the event.
dstport	Number of the port where the event was generated.
interface	The network interface where the event occurred.
user	User name.
op	For HTTP and FTP, an operation such as GET or POST.
arg	For HTTP and FTP, this is the URL.
vpn	Identifies a specific VPN (VPN object.) Used to discover the most used connections.
cat_type	Category to which this event belongs: e.g., Local Accept or Deny List IP address/name; or Surf Sentinel or CyberNOT category, e.g., Drug Culture or Pornography.
cat_action	Action performed by the filter: Block or Pass.
fil_type	Description of the filter: Default; Outbound (OF), IP Pass Through (PTF) or Remote Access (RAF.)

fil_action	Action performed by the filter: Block or Accept. See WELF log term “attribute” for GNAT Box Filter Action.
msg	Details specified events such as a VPN starting, the configuration changing, or a port scan being detected. The “msg” field will also capture the index (rule) number of filter (or the facility) that generated the event.
attribute	An action as defined in GNAT Box System Software. Indicates what action was taken by the system when the event triggered the filter, e.g., Alarm, Email, Stop.

SNMP

SNMP (Simple Network Management Protocol) is a standard for managing IP devices, retrieving data from each device on a network and sending it to designated hosts. In its full implementation, SNMP enables both read and write access. In GNAT Box System Software the SNMP facility is ***read-only***. It does not allow the write access needed, for control and configuration. The data, contained in a MIB (Management Information Base) and organized in report form, helps the administrator ensure optimal performance in the managed devices.

SNMP version 2 provides enhancements including security and an RMON (Remote Monitoring) MIB, which provides continuous feedback without being queried by the SNMP facility.

SNMP version 3 introduced a revised nomenclature for SNMP, a new access method using authentication, and the ability to encrypt SNMP data packets.

SNMP requires appropriate Remote Access Filters. Either default the filter set or create appropriate filters; then customize and enable the filters as needed.

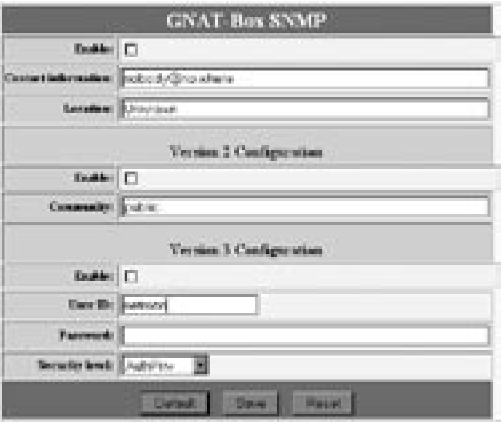
Warning Note

GTA strongly recommends restricting SNMP access to specific hosts in order to reduce dissemination of information about the network. It is important to allow access to the information only from designated, secure hosts because the data is transmitted in clear (non-encrypted) text.

SNMP Fields

Enable	Select to enable the SNMP facility. Disabled by default.
Contact	Email address of the administrator.
Location	User-defined description of the administrator’s location.
	Version 2 Configuration
Enable	Enable SNMP version 2.

Community	Essentially, a password. With this password, those with SNMP access can see SNMP information and/or receive SNMP trap notifications. In the full implementation of SNMP, there are three levels of community: read access, read-write access, and trap notification. Members of a community defined by this password can access SNMP information at the level allowed in that community.
	Version 3 Configuration
Enable	Enable SNMP version 3.
User ID	User name assigned separately from other user authorization names. An extra layer of protection against impolite and undesirable interest in your network.
Password	Password for this extra authorization level. This is an encrypted password.
Security Level	Security levels in the SNMP facility allow: **AuthPriv (Authentication, Privacy**). Access to SNMP information only with ***both*** authentication and data encryption of all SNMP packets (privacy). **AuthNoPriv (Authentication, No Privacy).** Access to SNMP information with ***only*** authentication.



GNAT-Box SNMP

Enable: □

Contact information: nobody@nowhere

Location: Unknown

Version 2 Configuration

Enable: □

Community: public

Version 3 Configuration

Enable: □

User ID: nobody

Password:

Security level: AuthPriv

SNMP

6 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.

Admin Accounts

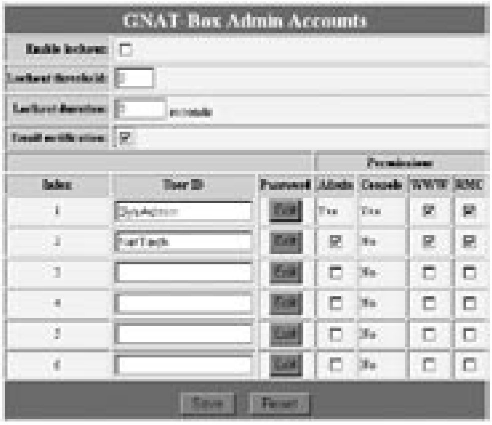
The Admin Accounts section provides a means to manage the administration accounts used to access the GTA Firewall. The primary account is the one initially used to log on to the firewall, with the default user ID and password "gnatbox." Up to five (5) additional accounts can be defined. Each account 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 wrong.
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 used to log on to the GTA Firewall. Any character that can be generated from the keyboard is valid, except leading and trailing spaces. It may be up to 39 characters long.
Password	Password used to log on to the GTA Firewall. Any character that can be generated from the keyboard is valid, except leading and trailing spaces. It 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 this account user authority to log in via GBAdmin, the Windows remote management console.



GNAT Box Admin Accounts

Enable lockout: □

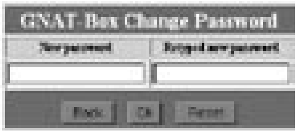
Lockout threshold: [illegible]

Lockout duration: [illegible] minutes

Email notification: ☑

			Permissions			
Index	User ID	Password	Admin	Console	WWW	RMC
1	SysAdmin	Edit	Yes	Yes	☑	☑
2	FairTech	Edit	☑	No	☑	☑
3		Edit	□	No	□	□
4		Edit	□	No	□	□
5		Edit	□	No	□	□
6		Edit	□	No	□	□

Administration Accounts



GNAT Box Change Password

New password	Retyped new password

Change Password

New SSL Certificate (Web)

The New SSL Certificate feature 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 will include three levels of validity: the issuer, or self-issued certificate authority; the date, which will be the date of certificate generation; and the name, which will be the firewall's host name.

Before generating a certificate, you must have installed the firewall and entered the correct host name in Network Information.

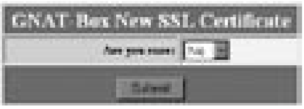
Host Name

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.

Generate Security Certificate

Select “New SSL Certificate,” select “yes” from the dropdown list, and then click the Submit button. This will start the process of generating a new certificate for the currently loaded GTA Firewall.

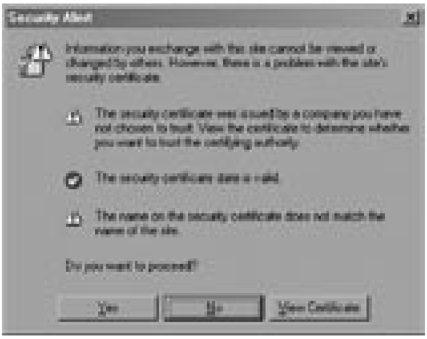


GNAT-Box New SSL Certificate

Are you sure: No

SSL Certificate (Web only)

Since the certificate is self-issued and your browser will not recognize your GTA Firewall as a Certificate Authority (CA), you will be prompted with a Security Alert similar to the one illustrated below. This alert dialog indicates that the listed Certificate Authority is not one you have chosen to trust; the security certificate date is valid; and the name on the security certificate does not match the name of the site. Choose the selection that allows you to proceed. Your security will not be compromised by continuing, and you will establish your certificate once you have signed on to the firewall.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate does not match the name of the site.

Do you want to proceed?

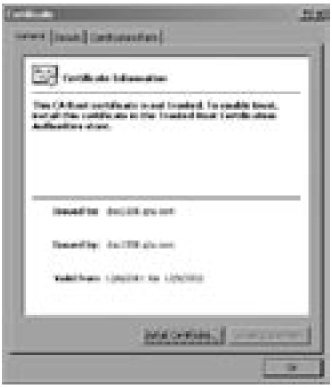
SSL Certificate Security Alert

Note

SSL Encryption is known to be incompatible with Internet Explorer 5 for Macintosh, so in IE 5 for Mac, the option to accept the certificate will not be offered. There are two options: use a compatible browser such as Netscape (www.netscape.com) or Opera (www.opera.com) to administer your firewall; or, after installation using another method, disable SSL, then use Internet Explorer 5 with SSL encryption disabled.

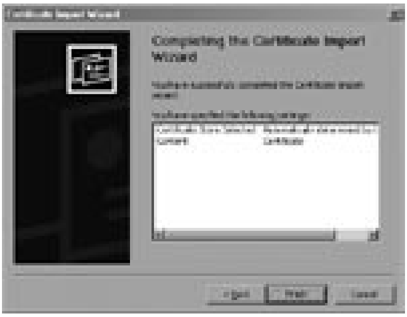
Install Security Certificate

To install the SSL security certificate, click the View Certificate button on the Security Alert screen. (This screen will vary from browser to browser.) In the Certificate screen that appears, click the Install Certificate button.



IE 5 for Windows Install Certificate

In IE 5 for Windows, a Certificate Import Wizard will appear, with information about certificates. Click Next and choose whether to automatically select the Certificate Store (recommended), or to select a location on your computer for the certificate manually. Click Finish.


Completing the Certificate Import Wizard

Certificate Import Wizard Complete

In the next screen, verify that you want to install the certificate to the Root Certificate Store. If you receive a dialog saying the import was successful, you have completed the installation of the certificate.

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 using the Web interface.

Remote Admin/Authentication

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.

SSL Encryption

For additional security and to coordinate with increased security requirements on the Internet, GTA has added the use of SSL (Secure Sockets Layer) encryption to its Web interface for the GB-1000, RoBoX and GB-Flash firewall products. SSL encryption, developed by Netscape, is the current standard in Internet security for HTTP, supporting server/client authentication, and maintains security and integrity in transmission. SSL encryption is the default in new installs of GNAT Box System Software. Though used only for Web access, SSL may be configured from any user interface.

Encryption Levels

Once SSL encryption is activated, make sure that you have the appropriate Remote Access Filter in place and enabled. The Remote Access Filter port must match the port set in Remote Administration, above. The default port for SSL is 443. The default port for no SSL is 80. Setting up your port and then defaulting your filters will correct any port mismatch.

Encryption Levels

Level	Key Strength	Comment
None	N/A	Disables SSL encryption.
All	N/A	Accepts all levels plus SSL with no encryption.
Low	40, 56, 64-bit	Accepts low encryption SSL
Medium	128 bit	Accepts medium encryption SSL
High	168-bit	Accepts only high encryption SSL.

Upgrading

If you are upgrading from GNAT Box System Software version 3.2 or earlier, default your options to turn on SSL encryption. When using SSL encryption, the www address will begin “https:”, e.g., `https://192.168.71.254`. When SSL encryption is set to “None,” the www address begins “http:”, e.g., `http://192.168.71.254`.

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. 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 remote Web interface from unauthorized use 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

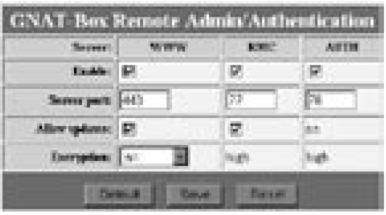
Enable	Enable access via GBAdmin (RMC).
Server Port	The default port for RMC access is 77. Follow the procedure described above for port change.
Allow Updates	By default, updates are allowed.
Encryption	The encryption level is high.

Authorization

The Authorization section allows the user to choose whether to require the use of the user authentication utility **GBAuth** before initiating a VPN connection. The default port for Authorization is 76/TCP. A Remote Access Filter must be in place and enabled to use Authorization. For more about setting up a GTA Firewall for User Authorization/Authentication, see the **GNAT BOX VPN FEATURE GUIDE**.

Authorization Fields

Enable	Select to require the use of the user authentication program GBAuth before initiating a VPN connection.
Server Port	The default port for Authorization is 76. Follow the procedure described above for port change.
Allow Updates	Allow Updates is not available.
Encryption	The encryption level is high.



GNAT-Box Remote Admin/Authentication

Server:	WWW	RMC	AUTH
Enable:	☑	☑	☑
Server port:	443	77	76
Allow updates:	☑	☑	n/a
Encryption:	[illegible]	high	high

Remote Administration/Authentication screen

Users

The Users screen allows the administrator to create a user and indicate whether that user is enabled for general access, and whether the user is enabled for VPN access.

User information from the VPN Authorization section in version 3.2.1 and earlier will be mapped to the 3.3 User Authorization section.

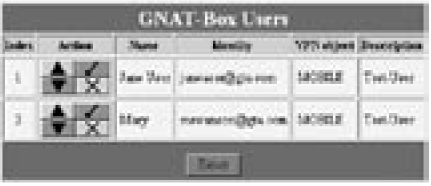
Note

> Currently, this feature affects only Mobile Users, but may be expanded to authorize other types of users.

User Add/Edit Screen Fields (Web & GBAdmin)

Disable	Check to disable all access for the selected user.
Name	Enter full name of the user.
Description	Enter description of user.
Identity	Enter user email address for user authentication.
Authentication	
Method	Password method.
Password	Enter password for user authentication.
Mobile VPN	
Disable	Check to disable VPN access for the selected user.
VPN Object	Select a previously defined VPN object.
Remote Network	Enter IP address of the remote network.
Preshared secret	Select ASCII or HEX value. Enter preshared secret as defined in VPN in ASCII or HEX format.

See VPNs Authorization for HEX values, network selection and preshared secrets.



GNAT-Box Users

Index	Action	Name	Identity	VPN object	Description
1		Jane Doe	[illegible]	MOBILE	Test User
3		Mary	[illegible]	MOBILE	Test User

Users Add/Edit Screen

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. VPNs Authorization retains the information necessary to continue running your VPNs when you upgrade from 3.2 or earlier.

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.

Selecting the Key Method

In the Web interface, a dialog box appears to prompt the administrator to select IKE or Manual mode. In GBAdmin, the IKE or Manual mode is selected on the main VPN screen. See illustrations after the fields tables.

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.)
	Gateways
Remote Gateway (Destination)	Default is 0.0.0.0. Enter the IP address of the route through which this VPN will pass, the gateway to the remote network. 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) Fields	
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.

About Security Parameter Index (SPI)

The Inbound and Outbound Security Parameter Index are used to uniquely identify a Security Association (SA). The Inbound SPI will be the Outbound SPI on the remote side of the VPN. The Outbound SPI will be the Inbound SPI on the remote side of the VPN. The SPI should be unique for each SA, although the inbound and outbound SPI may have the same value. The minimum SPI value is 256.

Encryption Key Length

The Blowfish, CAST128 and Twofish transformations use variable length keys, while AES, DES and 3DES use a fixed length key. If you exceed the maximum key length in these fields, you will generate an error and not be able to save the configuration until it is corrected. You may enter a shorter length key – the system will pad it to the minimum key size, e.g., in CAST128, the key will be padded to 128 bits.

Hash Key Length

The key length for the MD5 transformations is 128 bits, which is 16 ASCII characters or 32 hexadecimal characters. The key length for the SHA1 transformations is 160 bits or 20 ASCII characters or 40 hexadecimal characters.

Algorithms

Algorithm	Key Size	ASCII and HEX Characters
AES	128 bits	16 ASCII chars or 32 Hex chars
Blowfish	40-448 bits	5-56 ASCII chars or 10-112 Hex chars
CAST128	40-128 bits	5-16 ASCII chars or 10-32 Hex chars
DES	64 bits	8 ASCII chars or 16 Hex chars
3DES	192 bits	24 ASCII chars or 48 Hex chars
Twofish	40 - 256 bits	5-32 ASCII chars or 10-64 Hex chars

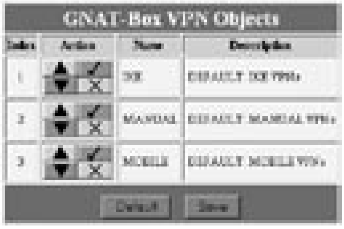
How to Activate a VPN

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.

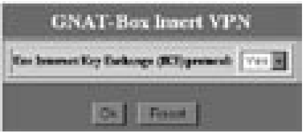
Please see the **GNAT BOX VPN FEATURE GUIDE** for more information about the VPN facility.



GNAT-Box VPN Objects

Index	Action	Name	Description
1		IKE	DEFAULT IKE VPNs
2		MANUAL	DEFAULT MANUAL VPNs
3		MOBILE	DEFAULT MOBILE VPNs

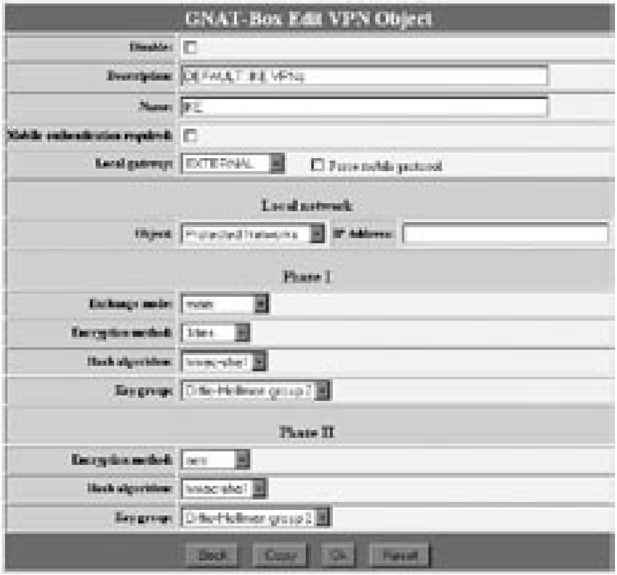
VPNs Screen



GNAT-Box Insert VPN

Use Internet Key Exchange (IKE) protocol: Yes

VPN key mode selection screen



GNAT-Box Edit VPN Object

Disable:	□
Description:	DEFAULT IKE VPNs
Name:	IKE
Mobile authentication required:	□
Local gateway:	EXTERNAL □ Force mobile protocol

Local network

Object:	Protected Networks	IP Address:	

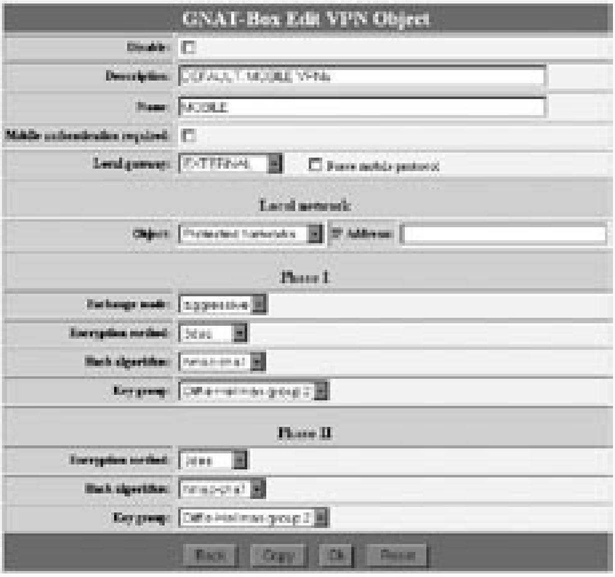
Phase I

Exchange mode:	main
Encryption method:	3des
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2

Phase II

Encryption method:	aes
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2

IKE VPN Add/Edit Screen



GNAT-Box Edit VPN Object

Disable: □

Description: DEFAULT MOBILE VPNs

Name: MOBILE

Mobile authentication required: □

Local gateway: EXTERNAL □ Force mobile protocol

Local network

Object: Protected Networks IP Address:

Phase I

Exchange mode: aggressive

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

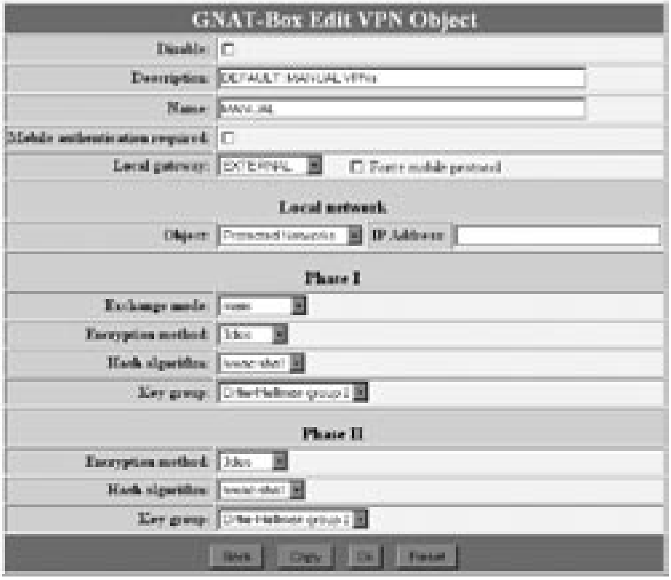
Phase II

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

Mobile VPN Add/Edit Screen



GNAT-Box Edit VPN Object

Disable: □

Description: DEFAULT MANUAL VPNs

Name: MANUAL

Mobile authentication required: □

Local gateway: EXTERNAL □ Force mobile protocol

Local network

Object: Protected Networks IP Address:

Phase I

Exchange mode: main

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 1

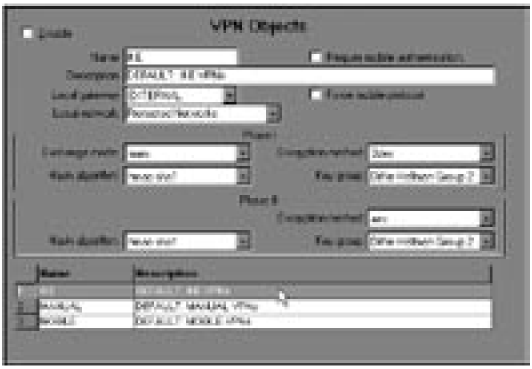
Phase II

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 1

Manual VPN Add/Edit Screen



VPN Objects

□ Enable

Name: IKE

□ Require mobile authentication

Description: DEFAULT IKE VPNs

Local gateway: [illegible]

□ Force mobile protocol

Local network: Protected Networks

Phase I

Exchange mode: main

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie Hellman Group 2

Phase II

Encryption method: aes

Hash algorithm: hmac-sha1

Key group: Diffie Hellman Group 2

Name	Description
IKE	DEFAULT IKE VPNs
MANUAL	DEFAULT MANUAL VPNs
MOBILE	DEFAULT MOBILE VPNs

VPN Screen–IKE (GBAdmin)

7 Content Filtering

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.

These functional areas allow the administrator to select one or more of the three content access facilities: Surf Sentinel, GTA's subscription service; Local Content Lists, which are part of the core functions for GNAT Box System Software, and do not require a subscription; and CyberNOT, a facility supported for current subscribers. For a description of CyberNOT categories, please see www.surfcontrol.com.

Content Filtering menu

Note

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

Access Control Lists

Access Control Lists (ACLs) provide a means to select web access control facilities (Surf Sentinel or CyberNOT and/or Local Allow and Local Deny lists) and specify how they will be applied to web requests. Each Access Control List consists of a description, a source IP address or Interface Object representing a group of IP addresses to be filtered, and how the selected content filtering facility will be applied to them. Access Control Lists are processed sequentially, so order is very important.

Note

Access Control List order is important. A site higher on the list that denies access will be blocked even if a later item allows access.

Surf Sentinel

GTA's Surf Sentinel provides GTA Firewall system administrators with a user-friendly interface and easy access to an exhaustive list of categories.

Surf Sentinel is superior to Local Content Lists alone. Using LCL only, an administrator is only able to enter a limited number of sites. Surf Sentinel is driven by Cerberian Web Filter, a premier content analyzing service with several ***million*** URLs in its database. The administrator can easily allow or deny types of content, as defined in Surf Sentinel 55 categories. By adding GTA's Local Content Lists, Surf Sentinel can be customized even further to suit your organization's unique requirements.

Surf Sentinel is specifically designed for firewall and VPN solutions. It features a small, ultra-light footprint and a proprietary Cerberian Dynamic Real-Time Rating and vectoring facility that reads and rates URLs in real-time. New URLs are immediately put into one of Cerberian's 55 content categories and become available quickly for all Surf Sentinel users.

An annual subscription for Surf Sentinel can be purchased from Global Technology Associates, Inc., or through an authorized GTA Channel Partner. With your subscription, you will receive the **SURF SENTINEL FEATURE GUIDE**, which provides information on using Surf Sentinel categories.

Local Allow and Deny Lists

Local Allow and Local Deny lists allow customization of content filtering. You can choose to execute all content filtering locally, allow access to sites that are blocked by another content filtering facility, or deny access to sites that are otherwise allowed. See the next section, Local Content Lists, to set the Local Allow and Deny Lists.

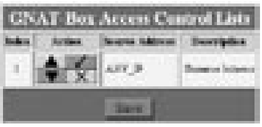
Access Control Lists (ACL) Fields

Disable	Select this checkbox to disable the designated ACL.
Description	Enter a description for the ACL.
Source Address	An Interface Object representing the IP address. If a request matches an element of the specified object, content filtering will be used to process the packet.
	Content Filtering Facility
Local Allow List	Select to process against GTA's Allow list.
Local Deny List	Select to process against GTA's Deny list.
Surf Sentinel	Select to process against the Surf Sentinel list.
CyberNOT	Select to process against the CyberNOT list.

Subscription Allow/Deny Lists

Use these lists to allow/block categories in Surf Sentinel and/or CyberNOT. Categories are moved from one list to the other by selecting the line item of the category and clicking the Arrow button.

Surf Sentinel	Use these lists to allow/block categories in Surf Sentinel.
CyberNOT	Use these lists to allow/block categories in CyberNOT.

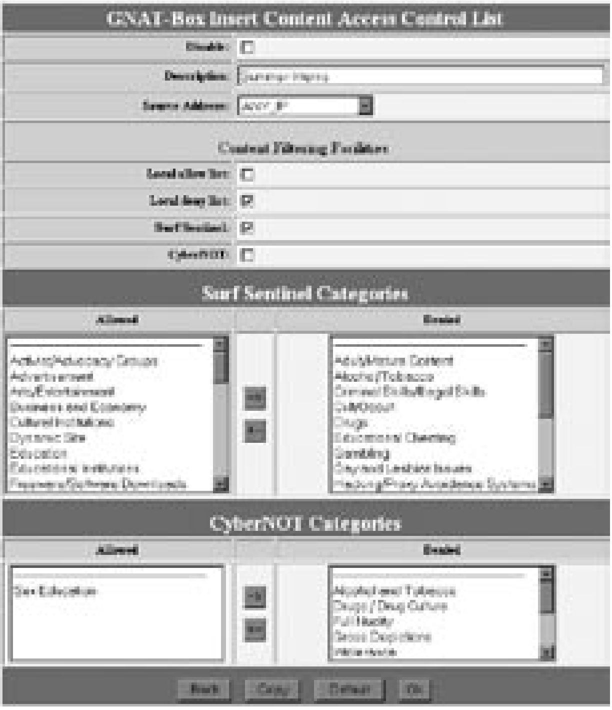


GNAT Box Access Control Lists

Index	Action	Source Address	Description
1		ANY_IP	Summer Interns

Save

Access Control Lists Summary



GNAT-Box Insert Content Access Control List

Disable: □

Description: Summer Interns

Source Address: ANY_IP

Content Filtering Facilities

Local allow list: □

Local deny list: ☑

Surf Sentinel: ☑

CyberNOT: □

Surf Sentinel Categories

Allowed	Denied
Activist/Advocacy Groups	Adult/Mature Content
Advertisement	Alcohol/Tobacco
Arts/Entertainment	Criminal Skills/Illegal Skills
Business and Economy	Cult/Occult
Cultural Institutions	Drugs
Dynamic Site	Educational Cheating
Education	Gambling
Educational Institutions	Gay and Lesbian Issues
Freeware/Software Downloads	Hacking/Proxy Avoidance Systems

CyberNOT Categories

Allowed	Denied
Sex Education	Alcohol and Tobacco
	Drugs / Drug Culture
	Full Nudity
	Gross Depictions
	Militant/Extremist

Access Control Lists Add ACL

Local Content Lists

Local Content Lists (LCLs) allow customization of content filtering. LCLs take precedence over subscription Content Filtering facilities so that you can allow access to sites that have been blocked or deny access to sites that are otherwise allowed. Maximum string length for a URL and comment is 180 characters. You can also choose to do simple content filtering by entering the sites your company wishes to allow/deny.

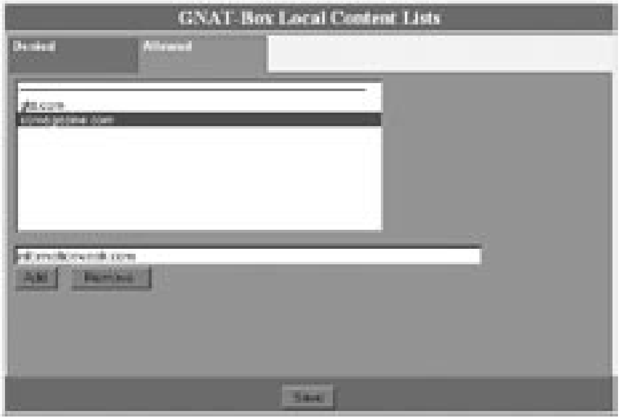
The Allowed list takes precedence over the Denied list; if you have the same URL in both lists, access to the site will be allowed.

Adding Sites to LCLs

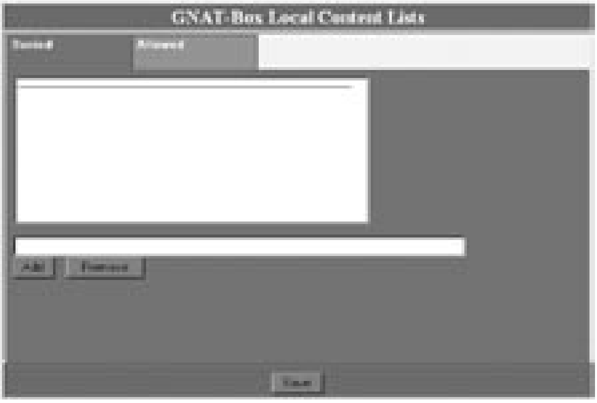
Enter sites in the Local Allow and Deny lists by typing the domain in the ADD/REMOVE field and clicking the Add button. To retain the sites you have added to the list, click Save before leaving the Allow or Deny list screen. The items will appear in alphabetical order after they have been entered.

Add comments at the end of the ADD/REMOVE field on the Web interface and in the COMMENT field in GBAdmin.

Enter items in the following format: `DomainName.com`; `DomainName.edu` or `DomainName.co.uk`, etc. WWW and other such designators (www2, www3) limit the effect of the line item. For example, the value `www.DomainName.com` only denies or accepts access for the specific site, not to sites associated with it such as `www2.DomainName.com`. If you wish to block an entire domain, enter `DomainName.com`. This will block all sites.



LCL Allow List



LCL Deny List

Content Filtering Preferences

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; to specify Mobile Code Blocking preferences; and to allow CyberNOT subscribers to schedule or activate list updates.

Traditional Proxy

When the GTA Firewall is operating without content filtering enabled, it does not use a proxy. When the HTTP proxy is used in conjunction with a content filtering facility, it runs on TCP port 2784 by default. To run the HTTP proxy on a different port, enter the value in the PORT field.

Traditional Proxy requires users located on Protected Networks to have browsers configured with the proxy port number and the proxy IP address.

How to Set Up an RAF for a Traditional Proxy

Traditional Proxy requires a Remote Access Filter. The default filter is:

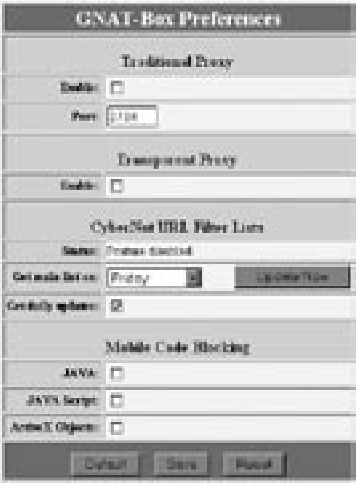
```
#DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy.

Type: Accept Interface: “PROTECTED” Protocol: TCP Priority:
Notice Log: Default

Source IP: Object - “ANY _ IP”

Source Port: 0 (or blank)

Destination: Object - “ANY _ IP”

Port: 2784
```

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.

Content Filtering Preferences Fields

<table>
<tr><th colspan="2">Traditional Proxy</th></tr>
<tr><td>Enable</td><td>Select this checkbox to enable the traditional proxy.</td></tr>
<tr><td>Proxy Port</td><td>Default is 2784. Port through which the proxy will run.</td></tr>
<tr><th colspan="2">Traditional Proxy</th></tr>
<tr><td>Enable</td><td>Select this checkbox to enable the transparent proxy.</td></tr>
<tr><th colspan="2">CyberNOT URL Filter List
This facility only functions if you have an activation code for the CyberNOT subscription.</th></tr>
<tr><td>Schedule updates on</td><td>Valid selections are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday.</td></tr>
<tr><td>Get daily updates</td><td>Enable automatic daily updates.</td></tr>
<tr><td>Update Now</td><td>Manually update the CyberNOT URL Filter List.</td></tr>
<tr><td>Status</td><td>Active (enabled/running), Inactive or Disabled.</td></tr>
<tr><th colspan="2">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.</th></tr>
</table>



GNAT-Box Preferences

Traditional Proxy

Enable: □

Port: 2784

Transparent Proxy

Enable: □

CyberNot URL Filter Lists

Status: [illegible]

Get main list on: Friday

Get daily updates: ☑

Mobile Code Blocking

JAVA: □

JAVA Script: □

ActiveX Objects: □

Content Filtering Preferences

8 Routing

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

Routing Menu

Gateway Selector

The Gateway Selector provides support for alternative default routes (gateways). If your site has multiple routes to the Internet, you can use the Gateway Selector feature to switch automatically to an alternative route if the primary gateway to the Internet is down.

One primary gateway is allowed; this is usually the gateway specified in Network Information. Up to three alternative default routes are allowed.

> ***Note***
>
> To use Gateway Selector, a default gateway must be selected on an External interface in Network Information. Failure to select a default gateway may cause the system to function improperly.

The Gateway Selector gives priority to the primary gateway. If one of the alternative routes is active as the default route, and the primary route comes back up, the primary will take over, becoming the active gateway again.

The GNAT Box System logs a Route Change Notification in the Logging facility and sends a notification by email. In addition, the Active Routes table in the System Activity section will be updated with the new default gateway.

Using Gateway Selector

Gateway Selector uses either static or dynamic interfaces as gateways: Static designates a static (fixed) IP address on an External interface as the gateway; Dynamic uses a dynamic connection, typically a PPP/PPPoE connection.

Using Static and Dynamic Gateways

Select the Default Gateway in Network Information under the Basic Configuration section, either by selecting the Gateway checkbox for a dynamic connection, or entering the IP address in the DEFAULT GATEWAY field for a static connection. If DHCP or PPP/PPPoE has been selected, (dynamic connections), the value will be automatically filled by the system.

Note

Before testing Gateway Selector using a dynamic IP address, you should confirm that the PPP, PPPoE or DHCP client is performing correctly. To set up a dynamic connection, see the PPP section and the Network Information section in Basic Configuration.

Next, enable the Gateway Selector, select Email Notification and PING SECONDARY ONLY IF PRIMARY IS DOWN, if desired. Next, select the External Interface Object that represents the interface you wish to use as the default route (gateway), or select Use IP address. Enter the gateway defined in the DEFAULT GATEWAY field in Network Information, then one or two beacon IP addresses in the primary BEACON IP field to test the primary route.

Select Secondary Default Route alternatives to the Primary Default Gateway. Secondary beacons are optional, but follow the same rules as primary beacons.

Note

When Gateway Selector is enabled, it overrides the Network Information gateway. This means that if you enter one IP address in the PRIMARY DEFAULT GATEWAY field in Gateway Selector, but enter a different IP address in the Network Information DEFAULT GATEWAY field, you can select the Network Information Default Gateway as a Secondary Default Route rather than the Primary Default Route.

If the Primary gateway is down and there is more than one secondary dynamic route, the first route up will usually become the default route. Typically, a PPPoE or DHCP address interface should be active before an on-demand PPP interface. However, order matters if routes are up at the same time.

Designating Beacons

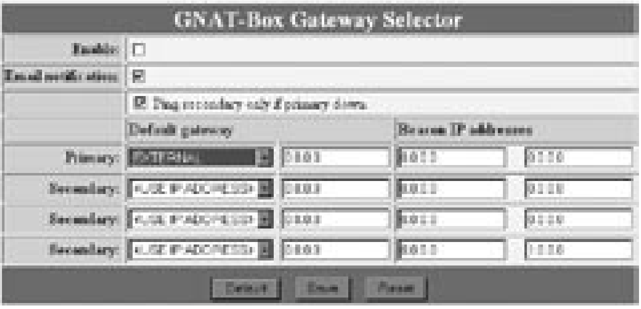
Using beacons helps to determine if a route is accessible by testing the route's connection to the beacons. Beacon IP addresses typically reside on the remote side of a WAN connection or beyond. GTA recommends using two beacons. Each beacon must be unique.

The Gateway Selector TTL (Time To Live) value is five; therefore, beacons should be no more than five (5) hops away. (Hops are nodes such as routers or gateways.) A beacon that is more than five hops away will cause the system to perform improperly. One way to select a beacon is to run a trace route out of each interface. Select the next one or two IP addresses in the trace past the gateway as beacons.

The GNAT Box System pings each beacon IP address every .5 seconds. When a beacon address does not respond for five (5) consecutive pings or 2.5 seconds, the Gateway Selector will consider the route to be down, and will switch to the next accessible route in the list.

Gateway Selector Fields

Enable	Select to enable Gateway Selector.
Email Notification	Select to send an email to the administrator if the default route changes.
Ping Secondary Only if Primary is Down	Select to allow the system to probe (ping) the beacons for secondary connections only when the primary gateway is not functional. This is recommended for a PPP connection, because it prevents the system from maintaining a connection just for the ping activity.
Primary Default Gateway	Usually the same as the Default Gateway selected in Network Information. If using an IP address, make sure that the Default Gateway in Network Information remains current. If the selector is disabled, and the static gateway entered in Network Information is inoperative, Internet connectivity will shut down.
Beacon IPs	The IP addresses the firewall will use to test connectivity for the Primary Default Gateway.
Secondary Default Gateway	These are the routes the system will use if the Primary Default Gateway is down. The system will use whichever route comes up first. If more than one becomes active simultaneously, the route will be selected using list order.
Beacon IPs	Beacons for Secondary Default Gateways. These follow the same rules as primary gateway beacons.



GNAT-Box Gateway Selector

Enable: □

Email notification: ☑

☑ Ping secondary only if primary down

	Default gateway		Beacon IP addresses	
Primary:	[illegible]	[illegible]	[illegible]	[illegible]
Secondary:	<USE IP ADDRESS>	[illegible]	[illegible]	[illegible]
Secondary:	<USE IP ADDRESS>	[illegible]	[illegible]	[illegible]
Secondary:	<USE IP ADDRESS>	[illegible]	[illegible]	[illegible]

Gateway Selector

Log Message Example

```
May 29 12:58:56 selector: No reply from 199.120.225.79.

May 29 12:58:56 selector: No reply from 205.111.80.180.

May 29 12:58:56 selector: No reply from 205.111.110.180.

May 29 12:58:57 selector: Verification of default gateway
199.120.225.79 failed.

May 29 12:58:57 selector: Default gateway set to
200.120.225.79.
```

Email Example

```
NOTIFICATION TYPE: Default gateway change

NAME: firewall.acme.com

DATE: Wed 2002-05-29 12:59:18 EDT

Default gateway changed to 200.120.225.79.
```

Interface Variations

Gateway Selector is essentially the same in the Web interface and GBAdmin, but the Network Information screen varies slightly in each interface. See the Network Information section, Interface Variations, for more information.

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.

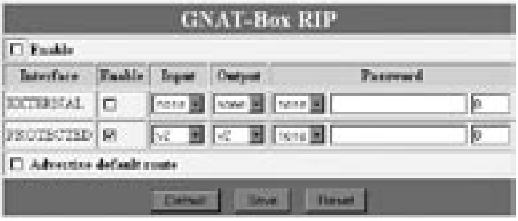
RIP Fields

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.
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.



GNAT-Box RIP

□ Enable

Interface	Enable	Input	Output	Password		
EXTERNAL	□	none	none	none		0
PROTECTED	☑	v2	v2	none		0

□ Advertise default route

RIP

Static Routes

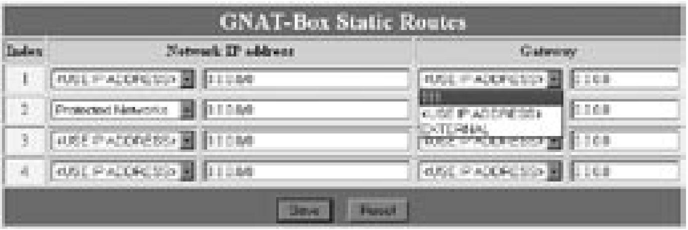
The Static Routes facility allows the administrator to define static (fixed) routes used to create a path between one part of a network and another. By default, a GTA Firewall does not listen to routing protocols such as RIP, so a static route allows information to move in a specific path across the 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).

One situation in which defining a static route would be useful is when there is a router between different parts of an internal network. If the Default Gateway is used, the system will send the packet out through the External Network interface. If the packet is being sent to an IP address on your network, it will not travel the most efficient path. If the destination IP address is internal, the packet will not be able to locate the remote network or IP address after leaving the internal network. Using a static route, the system is able to identify the correct path by which to send packets destined for this location.

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

9 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.

How to Change an Object Name

To change an object name without losing connectivity: copy the object, change the name in the copy, enable it, then change the parts of the configuration that reference it. You may then delete the original object.

Objects Menu

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.

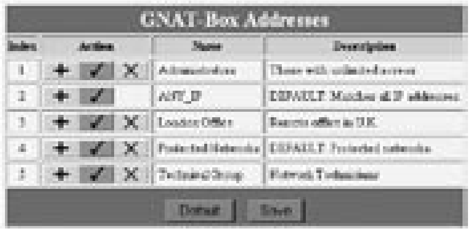
To add members to the object, select a previously defined Interface or Address Object from the OBJECT field dropdown box, select Use IP address and enter the IP address in the IP ADDRESS field, or select ANY_IP. The IP address can be a single IP address or host, a range of addresses, or an IP address/netmask.

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

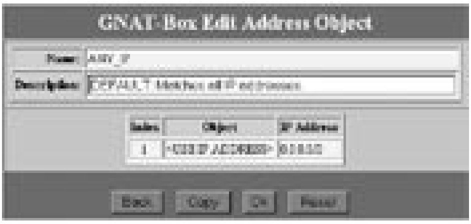
Name	Unique name by which the object will be referenced.
Description	Describe the address object.
Object	Select a previously defined Interface or Address Object as a member of this object.
IP address	Enter an IP address/netmask to be included in this address object. Use this field if Use IP address was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



GNAT-Box Addresses

Index	Action	Name	Description
1	+ ✓ ✕	Administrators	Those with unlimited access
2	+ ✓	ANY_IP	DEFAULT: Matches all IP addresses
3	+ ✓ ✕	London Office	Remote office in UK
4	+ ✓ ✕	Protected Networks	DEFAULT: Protected networks
5	+ ✓ ✕	Technical Group	Network Technicians

Address Object List



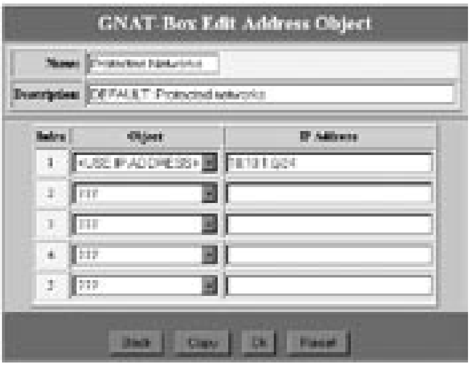
GNAT-Box Edit Address Object

Name: ANY_IP

Description: DEFAULT: Matches all IP addresses

Index	Object	IP Address
1	<USE IP ADDRESS>	0.0.0.0

Default "ANY_IP" Address Object



GNAT-Box Edit Address Object

Name: Protected Networks

Description: DEFAULT: Protected networks

Index	Object	IP Address
1	<USE IP ADDRESS>	[illegible]
2	???	
3	???	
4	???	
5	???	

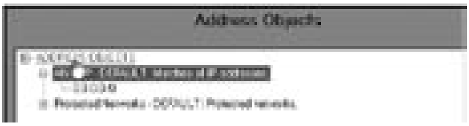
Address Object Add/Edit

Interface Variations

In GBAdmin, select the Address Objects line and click Add (+) to add a new address object. This will create a new object in the address object list and bring up a dialog in which to enter the NAME and DESCRIPTION field values. To edit this dialog at any time, select the object and double- or right-click.

To add a member to the address object, select the address object and click Add (+). This will add a new member for the address object: `0.0.0.0-0.0.0.0`.

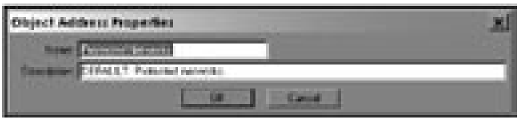
To edit the member, either select an object from the dropdown menu, or enter an IP address/netmask or range. Click OK.



Address Objects

ADDRESS OBJECTS
ANY_IP: DEFAULT: Matches all IP addresses
0.0.0.0/0
ProtectedNetworks: DEFAULT: Protected networks

Address Objects (GBAdmin)

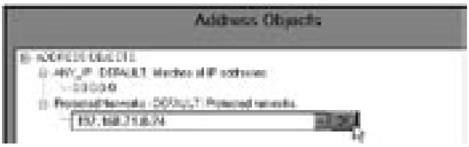


Object Address Properties

Name: ProtectedNetworks

Description: DEFAULT: Protected networks

Address Object Properties (GBAdmin)



Address Objects

ADDRESS OBJECTS
ANY_IP: DEFAULT: Matches all IP addresses
0.0.0.0/0
ProtectedNetworks: DEFAULT: Protected networks
192.168.71.0/24

Address Object Add Member OK (GBAdmin)

VPN Objects

The VPN Objects list displays the name and description of all defined VPN Objects. VPN Objects are defined primarily by 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 often replace the sometimes extensive VPNs built in GNAT Box System Software prior to version 3.2.2

When upgrading from an older software version, the default VPN objects will be created and added to existing objects. Defaulting the VPN Objects set will display only these default objects. 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 one default VPN object.

To use the default objects, click Save at this point. To return to the previously saved VPN Objects, click on another function. When you return to VPN Objects, the saved configuration will display.

Save a Configuration Copy

GTA recommends ***always*** copying the active configuration to a file (*.GBcfg) or printing the Configuration Report before making changes. See **Chapter 13 – Administration**, Download Configuration.

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 **GBAuth** authentication utility. (The User ID and Password for user authentication are set in User Authorization.) A Remote Access Filter must also be defined and enabled using the Default option, or by defining an appropriate filter. See **VPN CLIENT USER'S GUIDE** for more information.

Local Gateway

An IP address, alias or H_2A 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 authorizing and saving a VPN, defaulting the filter set will create appropriate Remote Access Filters.

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 One exchange establishes a security association by negotiating the terms of the VPN, authenticating the validity of the VPN peer, and setting connection parameters. Manual Key Exchange Phase I settings cannot be user-configured. For mobile connections, Phase I will default to Aggressive, 3DES, SHA-1 and Diffie-Hellman Group 2.

Exchange Mode

Main: Static IP to Static IP
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.

Aggressive: Static IP to Dynamic IP
Set to Aggressive when the connection is from a gateway with a dynamic IP address to one with a static IP address, i.e., in all VPN mobile connections, and in most connections using PPP/PPPoE or DHCP.

In either mode, if the vendor's VPN device has a setting or identification method, always set it to the IP address.

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.

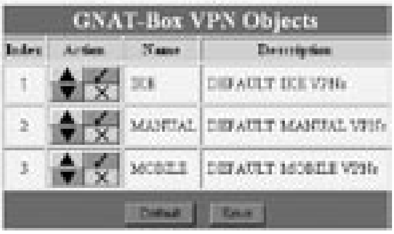
Phase II

In IKE, a Phase Two 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 the method that will be used 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

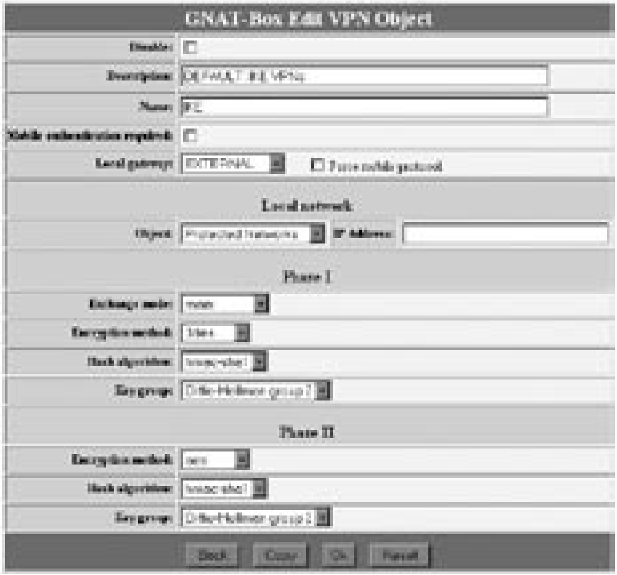
The GNAT Box IPSec VPN always has PFS and Replay Detection enabled. When communicating with another vendor's VPN device, enable PFS and Replay Detection on the other device. The anti-replay protocol prevents the insertion of changed packets into the data stream.



GNAT-Box VPN Objects

Index	Action	Name	Description
1		IKE	DEFAULT IKE VPNs
2		MANUAL	DEFAULT MANUAL VPNs
3		MOBILE	DEFAULT MOBILE VPNs

VPN Object List



GNAT-Box Edit VPN Object

Disable: □

Description: DEFAULT IKE VPNs

Name: IKE

Mobile authentication required: □

Local gateway: EXTERNAL □ Force mobile protocol

Local network

Object: Protected Networks IP Address:

Phase I

Exchange mode: main

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

Phase II

Encryption method: aes

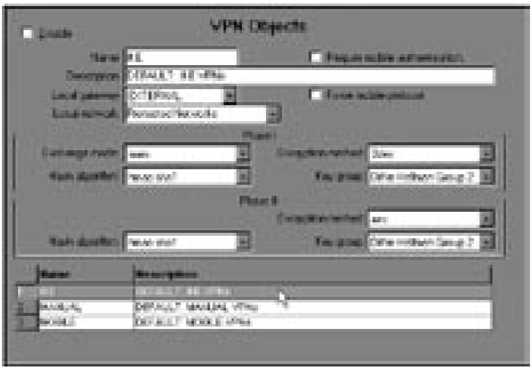
Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

VPN Object Add/Edit, Default IKE

Interface Variations

GBAdmin has the list of VPNs at the bottom of the VPN Object screen. Select one of these list items to change it; add a VPN Object by clicking Add (+).



VPN Objects

□ Enable

Name: IKE □ Require mobile authentication

Description: DEFAULT IKE VPNs

Local gateway: EXTERNAL □ Force mobile protocol

Local network: Protected Networks

Phase I

Exchange mode: main Encryption method: 3des

Hash algorithm: hmac-sha1 Key group: Diffie-Hellman Group 2

Phase II

Encryption method: aes

Hash algorithm: hmac-sha1 Key group: Diffie-Hellman Group 2

Name	Description
IKE	DEFAULT IKE VPNs
MANUAL	DEFAULT MANUAL VPNs
MOBILE	DEFAULT MOBILE VPNs

VPN Object, Default IKE example (GBAdmin)

10 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.

Managing Filters

Outbound, Remote Access and IP Pass Through Filters use the same mechanisms for filter management, so this manual will refer the reader to this section for tips and information about managing filters.

Filter Sets

A filter set is all the filters for a specific filter type. The order of the set is important. Each packet is compared to the appropriate set (Remote Access, Outbound or IP Pass Through) starting at filter one (Index 1) in the set. A comparison is performed sequentially against each filter until one of two events occurs:

1. A filter is matched. The packet is either Accepted or Denied based on the filter definition, and the actions associated with the filter are performed.
2. No filters are matched and the filter list is exhausted. In this case the packet is rejected.

Filters will be color-coded on the Web interface and GBAdmin: for Accept, Green; Deny, Red; Enabled, Black on background color; or Disabled, White or Gray on background color.

Tips for Using Filters

Once you have completed entering Network Information, you can use the **Default** option to create an initial set of filters. This action creates filters according to the defined configuration. Using the Default option, filters will be created, but left disabled or enabled, according to their default mode (the most secure setting). The Default Filters command ***does not*** reset filters to original factory settings, nor does it retain manual changes. If you have customized filters you wish to save, make a copy of your configuration before using the Default option.

The **Copy** function can be used to copy the definition of one filter and apply it to a new blank filter. To copy a filter definition into the copy/paste buffer, click on the Edit button of the filter you wish to copy. Once it is displayed, click the Copy button. Return to the filter list, insert a filter and then click Paste.

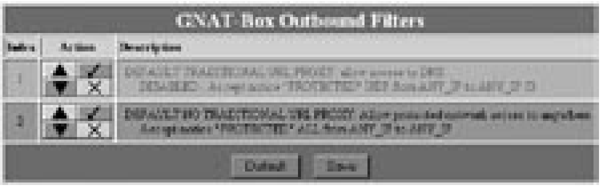
Combining multiple filters can be useful and efficient when they share similar criteria. This most often occurs when all the filter parameters are the same except for the destination port. Filters commonly combined are for SMTP, FTP, and HTTP, since these are all TCP-based protocols, often served from the same system.

The **Disable** selection is useful when testing filter configurations. The GNAT Box System default filter set utilizes this feature. All possible default filters are created, but only those which should be operational, based on configuration parameters, are enabled. If a feature needs to be enabled later, change the configuration and enable the filter.

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.

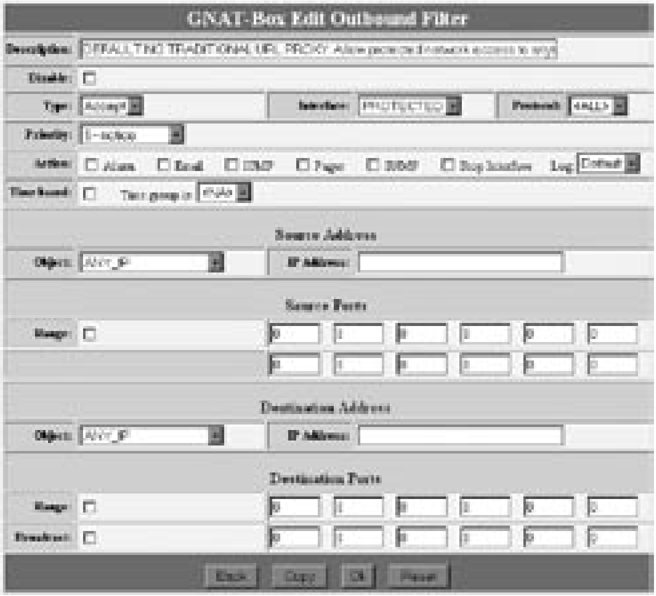
Source Ports	Leave empty for any source port to be accepted. The source port for most client protocols is a random value above 1024. The source port can be a single port, multiple ports or a range of ports. Specified Source Ports are matched against the source port of the IP packet. For Ports, see the Appendix, Ports and Services section. A Source Port Helper, which provides a sorted list of services and port numbers, will appear in GBAdmin. This will not appear if Expert Mode has been enabled. (See **Chapter 3 – User Interfaces** for more information.)
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 Destination.
Destination Ports	Often called services. Well-known service were assigned dedicated port numbers ranging from 1 to 1024, but other services have since been assigned outside this range. See Source Ports, above, for more information.



GNAT Box Outbound Filters

Index	Action	Description
1	▲ ✓ ▼ ✕	DEFAULT TRADITIONAL DNS PROXY: allow access to DNS DISABLED: Accept action "PROTECTED" DEF from ANY_IP to ANY_IP [illegible]
2	▲ ✓ ▼ ✕	DEFAULT NO TRADITIONAL DNS PROXY: Allow protected network access to anywhere Accept action "PROTECTED" ALL from ANY_IP to ANY_IP

Outbound Filter Set



GNAT-Box Edit Outbound Filter

Description: DEFAULT TNG TRADITIONAL URL PROXY: Allow protected network access to any

Disable: □

Type: Accept Interface: PROTECTED Protocol: <ALL>

Priority: 1 - lowest

Action: □ Alarm □ Email □ ICMP □ Pager □ SNMP □ Stop Interface Log: Default

Time based: □ Time group is <NA>

Source Address

Object: ANY_IP IP Address:

Source Ports

Range: □ 0 1 0 1 0 0

0 1 0 1 0 0

Destination Address

Object: ANY_IP IP Address:

Destination Ports

Range: □ 0 1 0 1 0 0

Broadcast: □ 0 1 0 1 0 0

Outbound Filter Add/Edit

Preferences

The Preferences section allows the administrator to define preferences for filters.

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.)

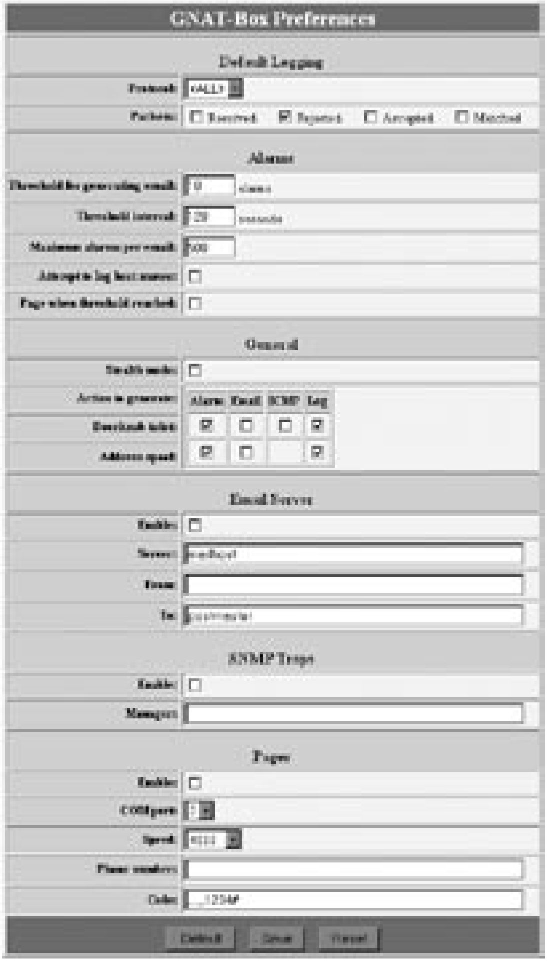
Stealth Mode	In stealth mode, the GTA Firewall will not respond to ICMP ping and traceroute requests, or to UDP traceroute requests, and will not reply with an ICMP message when a packet arrives for a port without a service or tunnel. Selecting Stealth Mode here does ***not*** override the Remote Access Filter default “No Stealth.” After enabling Stealth in this location, the RAF filter must be enabled as well.
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: **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.) **2.** An intrusion attempt is made by altering the source IP address of a packet directed at a network interface.

Email Server The Email Server in this section 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 email notification messages will be sent. Although the email server is typically a host on the Protected Network or PSN, the server can be an external host. The notifications can be sent to 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 host name is an internal host, the DNS server must be internal so that it can resolve the name of the hidden host. 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 `jdoe@gta.com`, or the mailbox name on the specified email server: `jdoe`.
To	Email address where notifications should be sent. The address can be a fully-qualified address, such as `jdoe@gta.com`, or the mailbox name on the specified email server: `jdoe`.
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.

Enable	Enables the Pager alarm facility.
COM Port	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).
Speed	Enter the DTE speed at which the firewall will communicate with the modem.
Phone number	Telephone number for the target numeric pager. You should enter all numbers and dialing codes that are required to make a call.
Code	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.



GNAT-Box Preferences

Default Logging

Protocol: <ALL>

Packets: □ Received ☑ Rejected □ Accepted □ Matched

Alarms

Threshold for generating email: 10 alarms

Threshold interval: 120 seconds

Maximum alarms per email: 500

Attempt to log host names: □

Page when threshold reached: □

General

Stealth mode: □

Actions to generate:	Alarm	Email	ICMP	Log
Default rules:	☑	□	□	☑
Address spoof:	☑	□		☑

Email Server

Enable: □

Server: localhost

From:

To: postmaster

SNMP Traps

Enable: □

Managers:

Pager

Enable: □

COM port: 1

Speed: 9600

Phone number:

Codes: ,,,1234#

Filter Preferences

Protocols

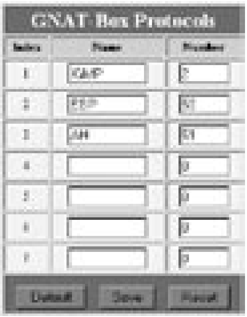
The Protocols function provides a means to define IP protocols to make available in the protocol list used when defining filters. The protocols may only be used with a Deny filter, since the system can only process TCP, UDP and ICMP IP packets. Using the Protocols function, the administrator can explicitly 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. Default the Protocols section will delete customization of protocols. Remove protocols by deleting the fields and saving the section.



GNAT Box Protocols

Index	Name	Number
1	IGMP	2
2	ESP	50
3	AH	51
4		0
5		0
6		0
7		0

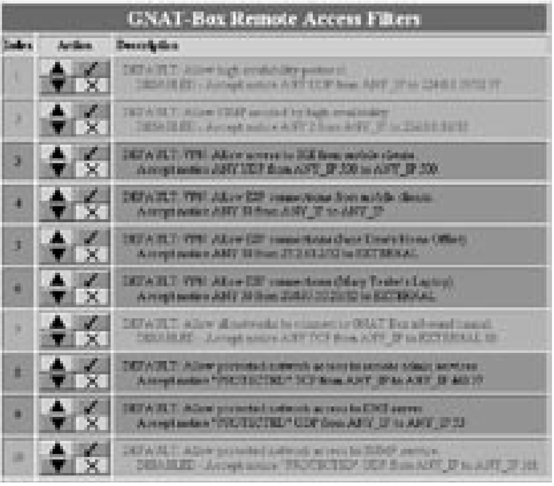
Protocols

Remote Access Filters

Remote Access Filters control inbound access. This control is primarily on Tunnels, but is also on 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.

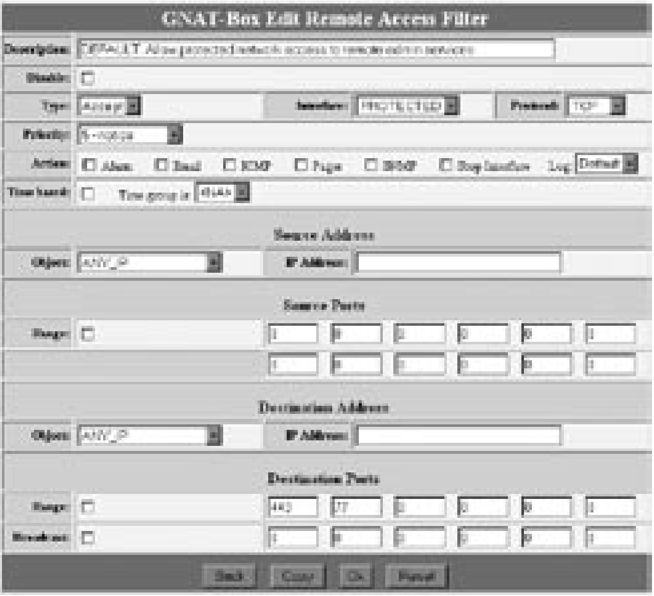
See Outbound Filters in this section for set information, tips and fields for Remote Access Filters.



GNAT-Box Remote Access Filters

Index	Action	Description
1	▲▼ ✓ ✕	DEFAULT: Allow high availability protocol DISABLED - Accept action ANY UDP from ANY_IP to [illegible]
2	▲▼ ✓ ✕	DEFAULT: Allow ICMP needed by high availability DISABLED - Accept action ANY 2 from ANY_IP to [illegible]
3	▲▼ ✓ ✕	DEFAULT: VPN: Allow access to [illegible] from mobile clients Accept action ANY UDP from ANY_IP:500 to ANY_IP:500
4	▲▼ ✓ ✕	DEFAULT: VPN: Allow ESP connections from mobile clients Accept action ANY 50 from ANY_IP to ANY_IP
5	▲▼ ✓ ✕	DEFAULT: VPN: Allow ESP connections [illegible] Accept action ANY 50 from [illegible] to EXTERNAL
6	▲▼ ✓ ✕	DEFAULT: VPN: Allow ESP connections [illegible] Accept action ANY 50 from [illegible] to EXTERNAL
7	▲▼ ✓ ✕	DEFAULT: Allow all networks to connect to GNAT Box [illegible] DISABLED - Accept action ANY TCP from ANY_IP to EXTERNAL:[illegible]
8	▲▼ ✓ ✕	DEFAULT: Allow protected network access to remote admin services Accept action "PROTECTED" TCP from ANY_IP to ANY_IP:443,77
9	▲▼ ✓ ✕	DEFAULT: Allow protected network access to DNS server Accept action "PROTECTED" UDP from ANY_IP to ANY_IP:53
10	▲▼ ✓ ✕	DEFAULT: Allow protected network access to SNMP service DISABLED - Accept action "PROTECTED" UDP from ANY_IP to ANY_IP:161

Remote Access Filter Set sample



GNAT-Box Edit Remote Access Filter

Description: DEFAULT: Allow protected network access to remote admin services

Disable: □

Type: Accept Interface: PROTECTED Protocol: TCP

Priority: 5 - normal

Action: □ Alarm □ Email □ ICMP □ Page □ SNMP □ Stop Interface Log: Default

Time based: □ Time group is: [illegible]

Source Address

Object: ANY_IP IP Address:

Source Ports

Range: □ 1 0 0 0 0 1

1 0 0 0 0 1

Destination Address

Object: ANY_IP IP Address:

Destination Ports

Range: □ 443 77 0 0 0 1

Broadcast: □ 1 0 0 0 0 1

Remote Access Filters Add/Edit

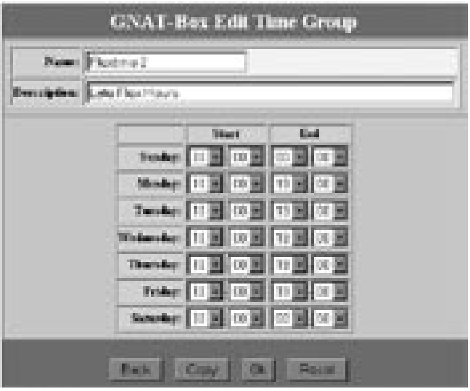
Time Groups

Time Groups are user-defined schedules that can be associated with any type of filter. Time Groups give the administrator the ability to control access (both inbound or outbound) based on time of day and day of the week. A filter with an associated Time Group will be in effect only during the defined period. The time granularity is based on 10 minute increments. Time Groups provide great flexibility, especially when multiple filters are used.

The Time Group list operates similarly to the filter screens. All normal filter functions apply, and a filter may be an Accept or a Deny. Often using the exclusion method may be your best filter solution. If a particular access policy is generally in effect, leave that filter in place and simply insert a Time Group filter earlier in the list. A match will be made on the Time Group filter – if in effect – and no further processing will be performed.

How to Create a Time Group

1. Click on the Add (+) icon in the toolbar to create a new Time Group.
2. In the NAME field, enter a name that will appear in the Time Group selection list when defining filters.
3. Describes the Time Group in the DESCRIPTION field.
4. Click the check arrow to display the Time Add/Edit screen.
5. In Add/Edit, select the desired schedule from the dropdown menus. Use <control> right-click to select non-contiguous sections.
6. Click OK, then click Save.



GNAT-Box Edit Time Group

Name: Flextime2

Description: Late Flex Hours

	Start		End	
Sunday	11	00	00	00
Monday	11	00	19	00
Tuesday	11	00	19	00
Wednesday	11	00	19	00
Thursday	11	00	19	00
Friday	11	00	19	00
Saturday	11	00	00	00

Time Groups

11 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.

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 Hosts/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 in **Chapter 10 – Filters**.

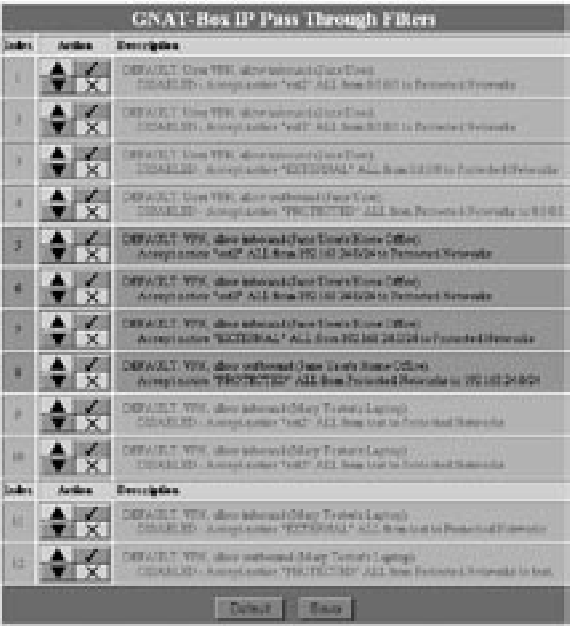
How to Create a Pair of Filters for a Defined IP Pass Through Host

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.

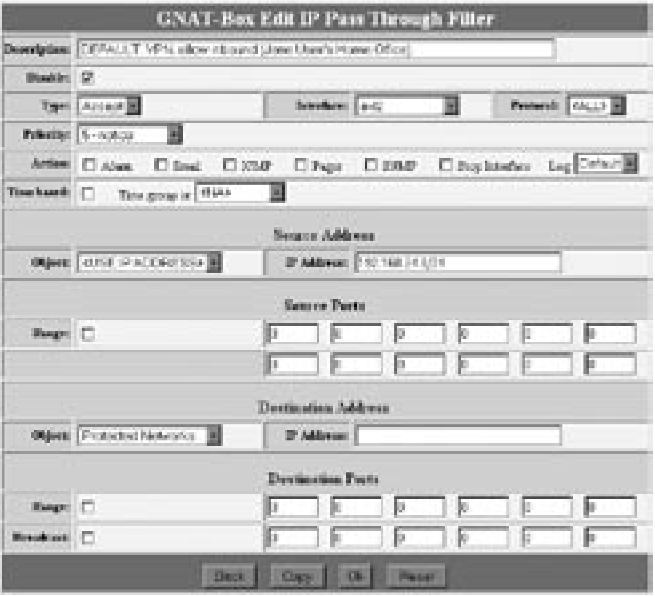
4. Once you have completed all the desired IP Pass Through Filters, click the Save button on the filter set to save the filters and apply them to the system.



GNAT-Box IP Pass Through Filters

Index	Action	Description
1	▲▼ ✓ ✕	DEFAULT: User VPN, allow inbound (Jane User) DISABLED - Accept action "eth0" ALL from 0.0.0.0 to Protected Networks
2	▲▼ ✓ ✕	DEFAULT: User VPN, allow inbound (Jane User) DISABLED - Accept action "eth0" ALL from 0.0.0.0 to Protected Networks
3	▲▼ ✓ ✕	DEFAULT: User VPN, allow inbound (Jane User) DISABLED - Accept action "EXTERNAL" ALL from 0.0.0.0 to Protected Networks
4	▲▼ ✓ ✕	DEFAULT: User VPN, allow outbound (Jane User) DISABLED - Accept action "PROTECTED" ALL from Protected Networks to 0.0.0.0
5	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Jane User's Home Office) Accept action "eth0" ALL from 192.168.243.0/24 to Protected Networks
6	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Jane User's Home Office) Accept action "eth0" ALL from 192.168.243.0/24 to Protected Networks
7	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Jane User's Home Office) Accept action "EXTERNAL" ALL from 192.168.243.0/24 to Protected Networks
8	▲▼ ✓ ✕	DEFAULT: VPN, allow outbound (Jane User's Home Office) Accept action "PROTECTED" ALL from Protected Networks to 192.168.243.0/24
9	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Mary Traveler's Laptop) DISABLED - Accept action "eth0" ALL from host to Protected Networks
10	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Mary Traveler's Laptop) DISABLED - Accept action "eth0" ALL from host to Protected Networks
Index	Action	Description
11	▲▼ ✓ ✕	DEFAULT: VPN, allow inbound (Mary Traveler's Laptop) DISABLED - Accept action "EXTERNAL" ALL from host to Protected Networks
12	▲▼ ✓ ✕	DEFAULT: VPN, allow outbound (Mary Traveler's Laptop) DISABLED - Accept action "PROTECTED" ALL from Protected Networks to host

IP Pass Through Filters List



GNAT-Box Edit IP Pass Through Filter

Description: DEFAULT: VPN, allow inbound (Jane User's Home Office)

Disable: ☑

Type: Accept   Interface: eth0   Protocol: ALL

Priority: 5 - Normal

Action: □ Alarm □ Email □ NTMP □ Pager □ SNMP □ Stop Interface   Log: Default

Time based: □   Time group is: NONE

Source Address

Object: <USE IP ADDRESSES>   IP Address: 192.168.243.0/24

Source Ports

Range: □   0 0 0 0 0 0
0 0 0 0 0 0

Destination Address

Object: Protected Networks   IP Address:

Destination Ports

Range: □   0 0 0 0 0 0

Broadcast: □   0 0 0 0 0 0

IP Pass Through Filters Add/Edit

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.

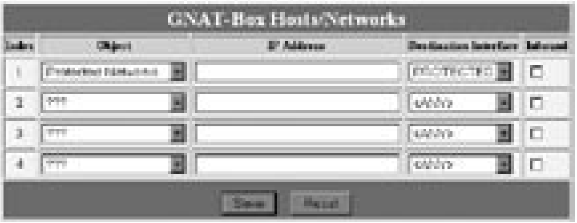
3. Use the Interface dropdown menu to select which network interface will have no NAT applied to the specified IP packets when they pass outbound through the interface.

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.



GNAT-Box Hosts/Networks

Index	Object	IP Address	Destination Interface	Inbound
1	[illegible]		[illegible]	□
2	???		[illegible]	□
3	???		[illegible]	□
4	???		[illegible]	□

Hosts/Networks

12 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

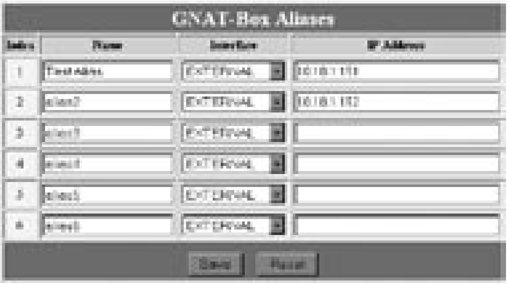
The Alias facility allows a network interface to be represented by multiple IP addresses. An IP alias may be assigned to any network interface. This facility is useful on the External Network interface, or if multiple targets on the PSN or Protected Network are required for the same service (port) via 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.



GNAT-Box Aliases

Index	Name	Interface	IP Address
1	Test Alias	EXTERNAL	10.10.1.111
2	alias2	EXTERNAL	10.10.1.112
3	alias3	EXTERNAL	
4	alias4	EXTERNAL	
5	alias5	EXTERNAL	
6	alias6	EXTERNAL	

NAT IP Aliases screen

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.

Creating Inbound Tunnels

Tunnels are defined by an Interface Object/port and a destination IP address/ port. (See **Chapter 2 – Terms** for more information about using interface objects.) The source and destination port of the tunnel definition need not be the same: it is possible to provide access to multiple hosts for the same service using a single IP address. For example, telnet operates on port 23, but a tunnel could be defined with a source port of 99 and a destination port of 23.

Only the source side of a tunnel is visible. Since GTA Firewall tunnels use Network Address Translation, a user on the source network side will never see the ultimate destination of the tunnel. The tunnel appears to be a service operating on a server with the tunnel's source IP address.

If a tunnel originates from an IP alias address, you may need to map the destination host to the IP alias using Static Address Mapping so that secondary connections appear to originate from the same address as the tunnel.

Caution

> A tunnel with a source and destination port of zero means "tunnel all ports for the specified protocol." It is possible to totally 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.

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.

See the Appendix, Ports and Services section, for some of the common ports and how to use them.

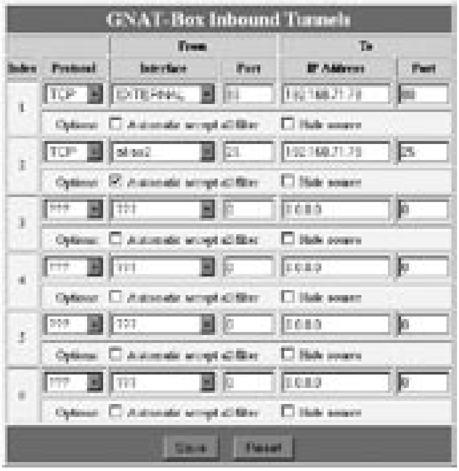
Set Remote Access Filters

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_2A (high availability) group for the source side of the tunnel.
From Port	Enter the port value which users will access. See a list of common services and their port numbers in the Ports & Services section of the Appendix section. For an exhaustive and up-to-date list, see www.iana.org/assignments/port-numbers on the IANA website.
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.

After completing the fields, select the Remote Access Filter menu item and create or modify a filter to allow access to your new tunnel.



GNAT-Box Inbound Tunnels

		From		To	
Index	Protocol	Interface	Port	IP Address	Port
1	TCP	EXTERNAL	80	192.168.71.78	80
	Options: ☐ Automatic accept all filter			☐ Hide source	
2	TCP	alias2	25	192.168.71.75	25
	Options: ☑ Automatic accept all filter			☐ Hide source	
3	???	???	0	0.0.0.0	0
	Options: ☐ Automatic accept all filter			☐ Hide source	
4	???	???	0	0.0.0.0	0
	Options: ☐ Automatic accept all filter			☐ Hide source	
5	???	???	0	0.0.0.0	0
	Options: ☐ Automatic accept all filter			☐ Hide source	
6	???	???	0	0.0.0.0	0
	Options: ☐ Automatic accept all filter			☐ Hide source	

Inbound Tunnel screen

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.

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.

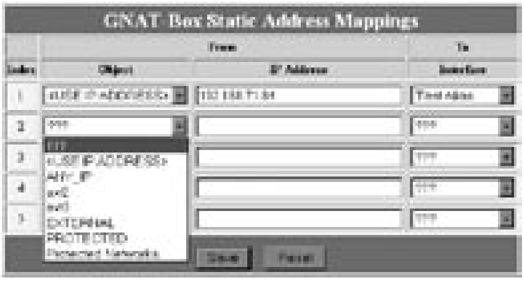
Allowed Static Address Mapping

Static Address Mapping is allowed in these cases:

- 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.

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

Timeouts

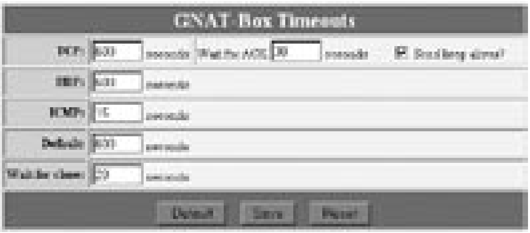
Timeouts define how long a connection should be idle before it is marked ready to close. The result of a connection reaching its timeout value differs for each IP protocol. For example, TCP has enough information embedded for the GNAT Box System to determine when the connection is ready to close, but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

Timeout Fields

Wait for close	Default value is 20 seconds. If your firewall is experiencing spurious “Remote Access Filter” blocks from reply packets, typically from port 80 (the Web), you may want to increase this value, giving 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).
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 as ready to close, the GTA Firewall will wait five seconds before it actually closes the connection. This gives redundant IP packets a chance to clear the GTA Firewall without causing false doorknob twist error messages.

TCP Specific

Wait for ACK	Default is 30 seconds. As part of TCP connection creation, 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, the GTA Firewall keeps a record of seeing this bit. If it is not seen, the remote server is probably down. If the idle time is reached without an ACK from the server, the connection is marked ready for close.
Send keep alives?	Enabled by default. If a successfully created TCP connection remains idle for the timeout period and this field is disabled, the connection is marked ready to close. If this field is enabled, a Keep Alive packet is sent. If the connection is still valid, the GTA 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.



GNAT Box Timeouts

TCP: 600 seconds Wait for ACK: 30 seconds ☑ Send keep alives?

UDP: 600 seconds

ICMP: 15 seconds

Default: 600 seconds

Wait for close: 20 seconds

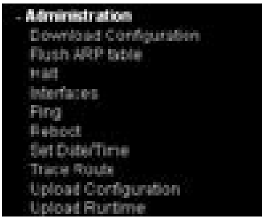
Timeouts

13 Administration

The administrative chapters cover three functional areas of administration in GNAT Box System Software: Administration, Reports and System Activity. These menus are found in the menu of the Web interface and in both the Scrolling Menu and the Menubar in GBAdmin.

Administration chapters are organized in order of the function's appearance on the menu in the Web interface. A brief explanation of the function is followed by an illustration from the Web interface. Differences in the function or the interface in GBAdmin will be explained and illustrated.

Optional features or features that do not apply to a user interface will display in the menu only if they have been activated, or are part of that interface; e.g., the Upload Runtime feature is only for flash-based systems (GB-Flash, GB-1000, RoBoX and GB-100). These functions will be indicated.



Administration Menu

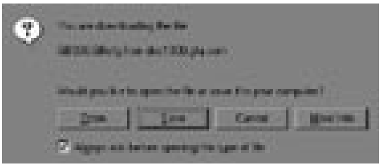
Download/Save Configuration

Download Configuration saves the current configuration to a file that can be opened using GBAdmin. Only the configuration data will be transmitted. When opening a configuration copy, you will need the same password as for the active configuration.

The function will prompt the user to find the desired file download location using the Browse button. The file will be saved with "`.GBcfg`" as the extension. The saved configuration can be used to reload a configuration on a firewall that has been reset to factory defaults or one that was running properly before a network or firewall configuration change.

Reset Firewall, Default Sections

To retain user-customized configurations ***before*** defaulting a section or resetting the firewall to factory settings, use the Download Configuration function under Administration to save a copy of the active configuration.



You are downloading the file:

[illegible]

Would you like to open the file or save it to your computer?

Download Configuration

Retain Filters after Default

After saving a configuration, go back to the desired filter section, click Default, then Save. This will set up generic filters. Use the previously copied configuration as a template to create filters, or use the copy and paste function in GBAdmin to insert the filters into the active configuration.

Interface Variations

GBAdmin's Save Configuration option is located in the File menu: File>Save. GBAdmin can open saved configurations without loading them into the running GTA Firewall.

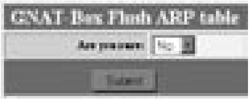
Flush ARP Table

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 which requires the map 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 at most one packet while waiting for a response to a map request and 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 a short period (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.



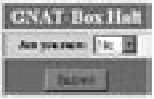
GNAT-Box Flush ARP table

Are you sure: No

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.



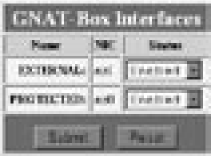
GNAT-Box Halt

Are you sure: No

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.



GNAT-Box Interfaces

Name	NIC	Status
EXTERNAL	[illegible]	Enabled
PROTECTED	[illegible]	Enabled

Interfaces

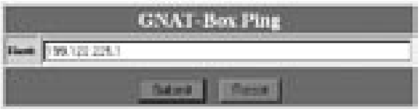
Ping

Provides a dialog which will execute the network ping connectivity test by using the Ping ICMP protocol. The ping is executed from the remote GTA Firewall, not from the local workstation.

Since the target IP address can be on any network, the Ping facility is very useful in validating your network connectivity for all network interfaces.

How to use the Ping Facility

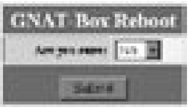
1. Click the Ping menu item to display the ping form.
2. Click in the IP ADDRESS or fully-qualified HOST NAME field (if DNS has been enabled) and enter the IP address to ping. The IP address should be entered in dotted decimal notation.
3. Click the Submit button to start the ping. The process will attempt to send five ping ICMP packets to the target IP address.



Ping

Reboot

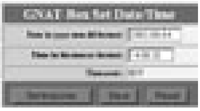
Reboot restarts the remote GTA Firewall. Since this action will terminate the Web interface’s network connection to the web server, your web browser will never receive a reply. The connection will eventually time out unless you click the stop button on your web browser.



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).

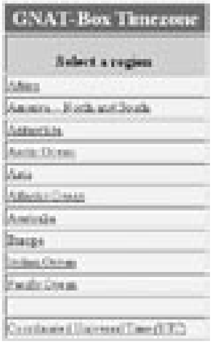


GNAT Box Set Date/Time

Set Date/Time

Set Time Zone (Web Only)

In order to set the time zone, click the Set Timezone button. First a region list will be displayed: select your region. Next, choose a country in the selected region. Finally, select a time zone which observes the same time as your locality. Click OK to apply your selection. Save your changes, then reboot your system.



GNAT-Box Timezone

Select a region

Africa
Americas - North and South
Antarctica
Arctic Ocean
Asia
Atlantic Ocean
Australia
Europe
Indian Ocean
Pacific Ocean

Coordinated Universal Time (UTC)

Set Time Zone

Note

Always reboot your system after changing the time zone.

Interface Variations

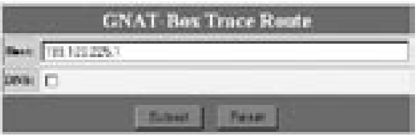
It is not possible to change the time zone facility using GBAdmin. This change must be made on the Web interface.

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.



GNAT-Box Trace Route

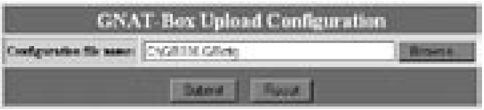
Host: [illegible]

DNS: □

Trace Route

Upload/Open Configuration

This item will allow you to upload a previously saved GNAT Box System Software configuration file. Selecting the item will display a screen that allows you to enter the configuration file name to upload. You can also use the Browse button to find the file on your local workstation.The file will have the extension "`.GBcfg`." Clicking Submit will upload the configuration file to the GTA Firewall. See Download/Save Configuration.



GNAT-Box Upload Configuration

Configuration file name: [illegible]

Upload Configuration

Interface Variations

To open a configuration using GBAdmin, select File>Open from the menubar. GBAdmin can be used to review the saved configuration without loading it into the running system.

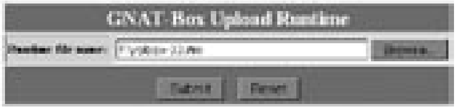
Note

GTA recommends using GBAdmin to open a configuration file on the running GTA Firewall.

Upload/Update Runtime

The Upload Runtime function is available only on flash-based systems (GB-Flash, RoBoX, GB-1000 and GB-100). It is used to upgrade a firewall to a new version or reinstall a previous version.

The GNAT Box System Software has two distinct parts: the runtime operating system and the configuration data. This function allows the administrator to upload and install a GNAT Box System Software runtime system image on a GTA Firewall. When this item is selected, a dialog is displayed which will prompt you to browse for GNAT Box System Software runtime files. These files have a file extension of "`.rtm`". Select Open to upload the runtime file, then confirm that you want to update the runtime on the GTA Firewall. The system will validate the runtime file. If it is valid, the system will install it.



Upload Runtime

Download Floppy Disk Image

Download Floppy Disk Image will only be available if you are connected to a GB-Pro system, since the flash memory-based systems (GB-Flash, RoBoX, GB-1000 and GB-100) do not use floppy disks. This item will initiate a file transfer of the entire GNAT Box System floppy disk image. If the web interface is running on a system with GBAdmin installed, the user can either save the image file or launch GBAdmin with the data.

14 Reports

The Reports section provides access to three functions that help create reports for the system hardware and software configuration: Configuration, Hardware and Email Configuration. In GBAdmin, Reports includes the Verify Configuration item.

These reports are only available when a network connection has been established with a remote GTA Firewall.

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**.

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 technical support about a GTA Firewall issue, the support staff may request that you generate a current configuration report.

Note

In systems that are not Flash-based, if the configuration was loaded from a previously booted runtime disk, Ethernet MAC address information will display. Otherwise, these values will be represented by ???, signifying an unknown value.

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.

Verify Configuration

Verify Configuration is the last item on the Web interface menu. It is under the Reports Menu in GBAdmin. Verify Configuration will run a system configuration verification check of the GTA Firewall. The check will verify the following functional areas: IP addressing, 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 and run the 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.

Interface Variations

GBAdmin locates the Verify Configuration option in the Reports section.

Verification is on-going on the GTA Firewall; in GBAdmin, you will see verification errors appear over the menu when the mouse pointer passes over it (hovers). These verification checks will also be indicated by the color of the Scrolling Menu circle: green for functional, yellow for warning and red for error. These warnings and errors will appear as soon as the administrator clicks on another selection, ***before*** the section or configuration is saved.

Note

Use this feature of GBAdmin to try out a configuration option before saving it to the loaded GTA Firewall.

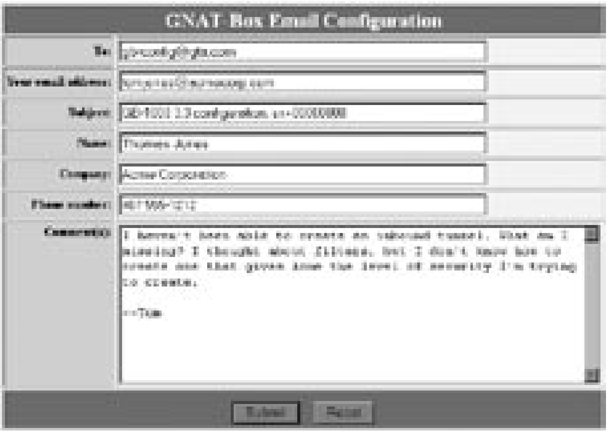
Email Configuration

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.



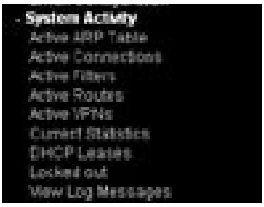
GNAT Box Email Configuration

To:	gbconfig@gta.com
Your email address:	[illegible]
Subject:	GB-1000 3.3 configuration, sn=00000000
Name:	Thomas Jones
Company:	Acme Corporation
Phone number:	407 555-1212
Comment(s):	I haven't been able to create an inbound tunnel. What am I missing? I thought about filters, but I don't know how to create one that gives [illegible] the level of security I'm trying to create. --Tom

Email Configuration Form

15 System Activity

System Activity provides direct access to lists (or reports) about activity on the firewall. It is only active when a network connection is established with a remote GTA Firewall. The Web interface has continuous update ability, so these reports are in real-time. On GBAdmin, the activity lists are only snapshots of the system activity. In GBAdmin, click the desired activity list item to generate a System Activity update. To change the rate at which these tables are updated, click the hotlink Change Refresh Rate at the bottom of the screen.



System Activity Menu

Active ARP Table

The Active ARP Table list will create and display a list of the current ARP (Address Resolution Protocol) addresses. The list displays the IP address to MAC address translations and the TTL (Time to Live) for each entry. ARP table entries are kept for 20 minutes and scanned every five (5) minutes to check for expired entries. Once an entry is expired, the GTA Firewall will not try to re-ARP the address for 20 seconds.

GNAT-Box Active ARP Table

IP Address	MAC Address	Time To Live	Type
[illegible]	[illegible]	expired	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	incomplete		[illegible]

ARP Table

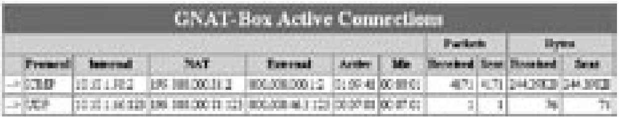
Active Connections

The Active Connections item is used to display a list of currently active connections, both inbound and outbound, on the GTA Firewall. By default, the display is a static snapshot of activity. In order to observe a change in the active connection display, simply click on the Active Connections menu item again to refresh the display. If you wish to have the list automatically updated on a periodic basis, click on the Refresh Rate link on the list display and adjust the interval. To disable updates, enter a value of zero (0). Use your browser’s functions to save, email or print a copy of the displayed Active Connections.

The list displays the following information for each connection:

Active Connections List

- Connection Direction (“<--” indicates an Inbound connection; “-->” indicates an Outbound connection.
- Protocol
- Internal IP address/port
- NAT/VPN/IP Pass Through IP address/port
- External IP address/port
- Active Time
- Idle Time
- Packets Received/Sent
- Bytes Received/Sent



GNAT-Box Active Connections

							Packets		Bytes	
	Protocol	Internal	NAT	External	Active	Idle	Received	Sent	Received	Sent
-->	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
-->	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	1	[illegible]	[illegible]

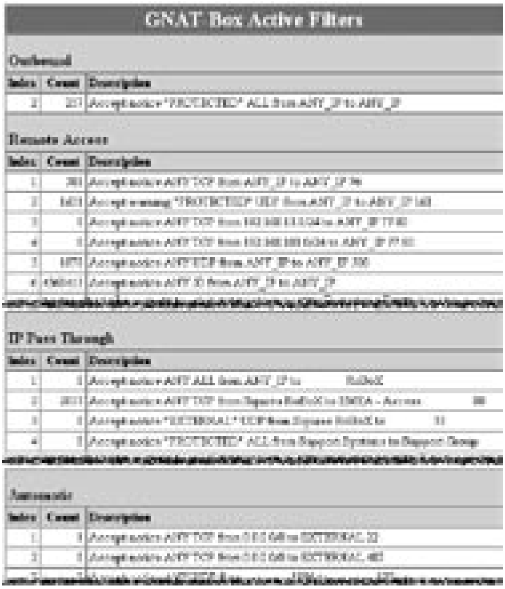
Active Connections

Active Filters

The Active Filters list will create and display a list of all filters for each of the four filter types with the number of hits (times the filter has been activated) on each filter. Inactive Time-based filters are displayed with an asterisk ‘*’ next to the entry. The list is static. However, the frequency of the updates can be adjusted by changing the refresh rate.

Active Filters List Display

- Number (Index, Rule)
- Hits (Counts)
- Description
- Priority
- Filter Actions
- Logical Interface
- Physical Interface
- Protocol
- Source IP address/netmask
- Source Ports
- Destination IP address/netmask
- Destination Ports



GNAT Box Active Filters

Outbound

Index	Count	Description
1	[illegible]	Accept; notice "PROTECTED" ALL from ANY_IP to ANY_IP

Remote Access

Index	Count	Description
1	[illegible]	Accept; notice ANY TCP from ANY_IP to ANY_IP [illegible]
2	[illegible]	Accept; warning "PROTECTED" UDP from ANY_IP to ANY_IP [illegible]
3	0	Accept; notice ANY TCP from [illegible] to ANY_IP [illegible]
4	0	Accept; notice ANY TCP from [illegible] to ANY_IP [illegible]
5	[illegible]	Accept; notice ANY UDP from ANY_IP to ANY_IP [illegible]
6	[illegible]	Accept; notice ANY [illegible] from ANY_IP to ANY_IP

IP Pass Through

Index	Count	Description
1	0	Accept; notice ANY ALL from ANY_IP to [illegible]
2	[illegible]	Accept; notice ANY TCP from [illegible] to [illegible] - Access [illegible]
3	0	Accept; notice "EXTERNAL" UDP from [illegible] to [illegible]
4	0	Accept; notice "PROTECTED" ALL from Support Systems to Support Group

Automatic

Index	Count	Description
1	0	Accept; notice ANY TCP from [illegible] to EXTERNAL 22
2	0	Accept; notice ANY TCP from [illegible] to EXTERNAL [illegible]

Active Filters

Active Routes

The Active Routes list will create and display the active routing table used by the GTA Firewall. This list can be helpful in diagnosing and troubleshooting routing problems. The list displays destination, netmask, gateway and flags.

Active Route Flag Values

B	Recently discarded packets
b	The route represents a broadcast address
C	Generate new routes on use
c	Protocol-specified generate new routes on use
D	Created dynamically
G	Destination requires forwarding by intermediary
H	Host entry
M	Modified dynamically
R	Host or network unreachable
S	Static route, manually added
U	Route is usable
W	Route was generated as a result of cloning

GNAT Box Active Routes

Destination	Netmask	Gateway	Flags
default		[illegible]	[illegible]
[illegible]	255.255.255.0	[illegible]	[illegible]
[illegible]	255.255.255.0	[illegible]	[illegible]
[illegible]	255.255.255.0	[illegible]	[illegible]

Active Routes

Active VPNs

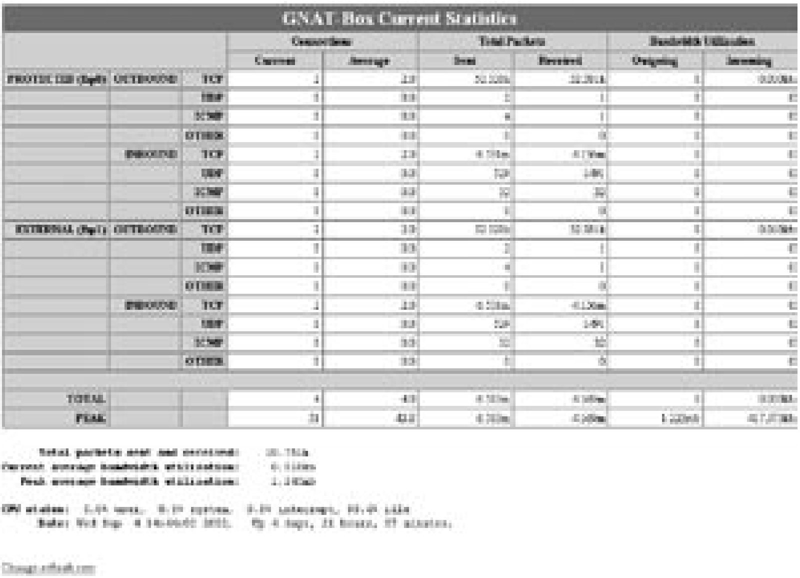
The Active VPNs menu item displays all current active VPN connections. There is an inbound and outbound connection for each VPN. The display shows the following information for each VPN connection:

VPN Information	
Source IP address	Source IP address of the gateway.
Destination IP address	Destination IP address of the gateway.
Type	Type of VPN connection (typically ESP).
Encryption	Encryption algorithm used by the VPN.
Hash	Hash algorithm used by the VPN.
State	Values include: larval, mature, dying and dead. Larval and Dead can happen too quickly to be observed.
Created	Time stamp for when the VPN was created/established.
Idle	Idle time of the VPN.
Bytes	Number of bytes transferred by the connection.
Description	Indentifying name for the VPN.
Leases	GB VPN Client Licenses in use.

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. The list displays the following information:

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 that displays the 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.



GNAT-Box Current Statistics

			Connections		Total Packets		Bandwidth Utilization	
			Current	Average	Sent	Received	Outgoing	Incoming
PROTECTED (fxp0)	OUTBOUND	TCP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		UDP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		ICMP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		OTHER	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	INBOUND	TCP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		UDP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		ICMP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		OTHER	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
EXTERNAL (fxp1)	OUTBOUND	TCP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		UDP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		ICMP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		OTHER	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	INBOUND	TCP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		UDP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		ICMP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		OTHER	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TOTAL			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
PEAK			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

```
       Total packets sent and received:    [illegible]
Current average bandwidth utilization:     [illegible]
   Peak average bandwidth utilization:     [illegible]

CPU states:  [illegible]
      Date:  [illegible]   Up [illegible] days, [illegible] hours, [illegible] minutes.
```

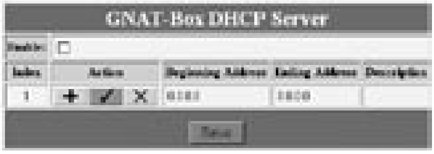
Change refresh rate

Current Statistics

DHCP Leases

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to internal hosts logging onto a TCP/IP network. It eliminates having to manually assign permanent IP addresses. DHCP dynamically updates the DNS servers after making assignments.

The DHCP Leases function provides a list of the IP addresses assigned and the identity of the associated hosts.



GNAT-Box DHCP Server

Enable: □

Index	Action	Beginning Address	Ending Address	Description
1	+ ✎ ✕	[illegible]	[illegible]	

DHCP Leases

View Log Messages

The data in View Log Messages is the latest. 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** for more about Log Messages. See Remote Logging in **Chapter 5 – Services** for more about WELF.

GNAT-Box View Log Messages

```
[illegible]
```

View Log Messages

Locked Out

The table shows the IP address of any user who has entered the wrong password and has been locked out. (See Admin Accounts in **Chapter 6 – Authorization**.) The duration shows how long the user will be locked out and is expressed as a count down. In other words, if the administrator has set five minutes as the lockout duration, the counter will start at 00.05.00 and count down to zero (00.00.00). At that time, the user may again attempt to log in. When the lockout time is up, the user IP address will drop from the table.

GNAT-Box Locked out

IP Address	Duration
[illegible]	[illegible]

Lockouts

Appendix

Ports and Services

Port Numbers are divided into three ranges:

0 – 1023	Well-Known Ports.
1024 – 49151	Registered Ports.
49152 – 65535	Dynamic and/or Private Ports.

Well-known Ports and Services

Well-known ports (also known as common) are assigned by the IANA, and on most systems can only be used by system processes or by programs executed by privileged users. Ports are used in TCP to name the ends of logical connections carrying long-term conversations. To provide services to unknown callers, a contact port is defined. Below is a brief list of these common services and port numbers.

Well-known Port Assignments

Service	Port/Protocol	Description
echo	7TCP/UDP	Echo
ftp	21/TCP/UDP	File Transfer [Control]
ssh	22/TCP/UDP	SSH Remote Login Protocol
telnet	23/TCP	Telnet
smtp	25/TCP	Simple Mail Transfer Protocol
msg-auth	31/TCP/UDP	MSG Authentication
name	42/TCP/UDP	Host Name Server
nicname	43/TCP/UDP	Who Is
domain	53/TCP/UDP	Domain Name Server
gopher	70/TCP/UDP	Gopher
finger	79/TCP/UDP	Finger
http	80/TCP	World Wide Web http
ctf	84/TCP/UDP	Common Trace Facility
pop3	110/TCP	Post Office Protocol - Version 3

auth	113/TCP	Authentication Service
sftp	115/TCP/UDP	Simple File Transfer Protocol
sqlserv	118/TCP/UDP	SQL Services
nntp	119/TCP/UDP	Network News Transfer Protocol
ntp	123/TCP/UDP	Network Time Protocol
netbios-ns	137/TCP/UDP	NETBIOS Name Service
netbios-dgm	138/TCP/UDP	NETBIOS Datagram Service
netbios-ssn	139/TCP/UDP	NETBIOS Session Service
sql-net	150/TCP/UDP	SQL-NET
sqlsrv	156/TCP/UDP	SQL Service
snmp	161/TCP/UDP	Secure Network Management Protocol
snmptrap	162/TCP/UDP	SNMP TRAP
prospero	191/TCP/UDP	Archie Reply
irc	194/TCP/UDP	Internet Relay Chat Protocol
pdap	344/TCP/UDP	Prospero Data Access Protocol
ldap	389/TCP/UDP	Lightweight Directory Access Protocol
https	443/TCP	http over TLS/SSL
syslog	514/UDP	Syslog
printer	515/TCP	Printer spooler
ftps-data	989/TCP/UDP	ftp, data, over TLS/SSL
	1023/TCP/UDP	Reserved IANA <iana@iana.org>

Registered Port Numbers

The Registered Ports are listed by the IANA, and on most systems can be used by ordinary processes or programs executed by ordinary users. The IANA registers uses of these ports as a convenience to the community. The Registered Ports are in the range 1024-49151.

Registered Port Assignments

Service	Port/Protocol	Description
shockwave2	1257/TCP/UDP	Shockwave 2
lotusnote	1352/TCP/UDP	Lotus Notes
shockwave	1626/TCP/UDP	Shockwave
sixnetudr	1658/TCP/UDP	StreamWorks4
WIN Terminal Srv	3389/TCP	

PC Anywhere	5631/TCP/UDP

Log Messages

This section describes and illustrates log messages generated by GNAT Box System Software version 3.3 running on GTA Firewalls using WELF.

Remote Logging

All GTA Firewalls based on the GNAT Box System Software provide remote logging of events. The remote logging facility uses the WebTrends Enhanced Logging Format (WELF) to record these logs. A syslog service (daemon) that can accept and record the log data is a standard feature on all Unix/Linux based systems. GTA also provides a syslog client for Microsoft Windows-based systems on the installation CD-ROM. It can also be downloaded from GTA's website. The log format for these messages is documented in the Remote Logging section of **Chapter 5 – Services** of this guide.

As a convenience, the most recent events are kept locally in a buffer on the firewall system and can be accessed via the Web interface or GBAdmin. The size of the buffer is dependent on the firewall system and memory configuration. Log messages kept in the local buffer are displayed in reverse order, with the most recent message appearing at the top of the display. The display is a static snapshot and must be refreshed in order to display new activity. See View Log Messages in **Chapter 15 – System Activity** for more information about log messages.

Log Message Configuration

In order to use the remote logging facility of the GNAT Box System the remote logging service must be configured. This can be done either in the Web interface or GBAdmin. Configuration is performed on the Remote Logging screen on both the Web interface and GBAdmin. In this screen, the user defines the remote host, log facilities, and the data that will be transmitted.

Since the syslog protocol is used, a facility and priority must be defined for log streams generated by the GNAT Box System. The "facility" is used in the syslog configuration file host to direct a log stream to a log file or other facility such as the Console. "Priority" is used by the remote log host to determine if and where the information in the log stream should be displayed/stored. If the priority is set to None, then log data for that log stream will not be transmitted.

Default Log Configuration

- Filter Messages
  Log messages that are generated due to a filter rule, either explicit or automatic. Filter messages are logged by default to the “local1” facility.
- Network Address Translation Messages
  Log messages that are generated due to a NAT action. These actions can be both outbound traffic and inbound tunnel traffic. All NAT messages are logged by default to the “local0” facility. NAT session closes are logged at priority Notice. NAT session opens are not logged.
- WWW Pages Accessed
  Log messages that are generated when an outbound http access occurs. The complete URL is logged. All http URLs are logged by default to the “local2” facility. Log messages are sent at priority Notice.

Details of configuration setup are described in this guide.

Filter Logging Configuration

The default filter logging configuration is set to log rejected packets for all protocols. If a different filter logging configuration is desired, changes can be made on the Filter Preferences screen under the Filters menu item. Under normal conditions only the Rejected packet type should be selected. All other packet types are provided to assist in debugging network problems; selecting Received, Matched or Accepted will generate excessive log messages.

The protocol options are: All, None, TCP, UDP and ICMP.

Filter Packet Types

Received

If this option is selected all packets that arrive at any of the firewall’s network interfaces that match the Protocol type will be logged. The log message includes the protocol, source IP, source port, destination IP, destination port, network interface, packet length and TCP flags if appropriate.

```
Feb 28 11:00:35 fw.gta.com id=firewall time=″2002-02-28 11:
00:35″ fw=″GNAT-Box″ pri=6 flt _ type=RAF flt _ action=pass
msg=″Received (4)″ rule=4 proto=443/TCP src=192.168.71.12
srcport=1599 dst=192.168.71.254 dstport=443 interface=sis0
flags=0x11
```

Matched

Any packet that matches any Remote Access, Outbound or Pass Through Filter rule will be logged. The rule type (accepted or denied) has no impact, only that a rule was matched. The number of filter matches, filter number and brief filter description are included in the log message.

```
Feb 28 11:04:38 fw.gta.com id=firewall time=”2002-02-28 11:
04:38” fw=”GNAT-Box” pri=6 msg=”FILTER: 130 matches for 4:
Accept notice ‘PROTECTED’ TCP from ANY _ IP to ANY _ IP 443
77 “ type=mgmt
```

Accepted

If a packet matches a filter rule that allows a packet to be accepted by the firewall – regardless of destination: inbound, outbound or directly to the firewall – it will be logged. The message includes the filter type (designated as RAF, NAT or PASS), the filter number, the word “accept”, log priority level, protocol, source IP, source port, destination IP, destination port, network interface, packet length and TCP flags if appropriate.

```
Feb 28 11:06:57 fw.gta.com id=firewall time=”2002-02-28 11:
06:57” fw=”GNAT-Box” pri=5 flt _ type=OBF flt _ action=pass
msg=”Accept OBF (2)” rule=2 proto=500/UDP src=192.168.71.12
srcport=500 dst=199.120.225.8 dstport=500 interface=sis0
```

Rejected

If a packet is denied access either explicitly by a filter or implicitly by the default rule (deny all unless explicitly allowed) it will be logged. The log message includes the filter type (RAF: Remote Access, NAT: NAT or PASS: Pass Through), the filter number, the word “block”, log priority level, protocol, source IP, source port, destination IP, destination port, the word “alarm” if an alarm was generated due to filter settings, network interface, packet length and TCP flags if appropriate.

```
Feb 28 11:13:01 fw.gta.com id=firewall time=”2002-02-28 11:
13:01” fw=”GNAT-Box” pri=4 flt _ type=RAF flt _ action=block
msg=”Block RAF (20)” rule=20 proto=23/TCP src=199.120.225.4
srcport=1601 dst=207.69.99.201 dstport=23 interface=PPP0
attribute=”alarm” flags=0x2
```

Permitted Inbound Request Open

When an authorized inbound connection is made on a tunnel, two possible log messages can be generated. By default, one is created only when the session is closed. To generate a log message when an inbound session is created, set the Priority to log tunnel field to a setting other than None.

The log messages for a permitted inbound request are almost identical for an Open and Close message, except that the Close message contains connection information such as duration, packets sent/received, and bytes transmitted. The IP address/port pairs in the log message detail the route of the packet. The packet example below shows an inbound request to a web server on the Private Service Network.

Note

There is no explicit tag in the log message indicating that the packet was permitted, since the log message indicates this implicitly.

Open

```
Aug 30 09:19:43 pdbtest78.gta.com id=firewall time=”2002-
08-30 09:19:43” fw=”GNAT-Box” pri=5 msg=”Open incoming
NAT tunnel” proto=http src=199.120.225.3 srcport=4175
nat=199.120.225.78 natport=80 dst=192.168.71.98 dstport=80
```

Close

```
Aug 30 09:20:03 pdbtest78.gta.com id=firewall time=”2002-
08-30 09:20:03” fw=”GNAT-Box” pri=5 msg=”Allow incoming
NAT tunnel” proto=http src=199.120.225.3 srcport=4175
nat=199.120.225.78 natport=80 dst=192.168.71.98 dstport=80
duration=22 sent=144 rcvd=120
```

Permitted Outbound Request

When an authorized outbound connection is made on a tunnel, two possible log messages can be generated. By default, one is only created when the session is closed. To generate a log message when an outbound session is created, set the PRIORITY TO LOG TUNNEL field to a setting other than None.

The log messages for a permitted outbound request are almost identical for an Open and Close message, except that the Close message contains connection information such as duration, packets sent/received, and bytes transmitted. An outbound request can be identified by the direction the arrows are pointing in the log file: left for inbound and right for outbound. The IP address/port pairs in the log message detail the route of the packet. The packet below shows an outbound request from the Protected Network to a web server on the Internet

Note

There is no explicit tag in the log message indicating that the packet was permitted, since the log message indicates this implicitly.

```
Feb 28 11:17:48 fw.gta.com id=firewall time=”2002-02-28
11:17:48” fw=”GNAT-Box” pri=5 msg=”Open outbound NAT”
proto=http src=192.168.71.12 srcport=1683 nat=207.69.99.201
natport=1683 dst=160.239.1.10 dstport=80 rule=2
```

```
Feb 28 11:18:50 fw.gta.com id=firewall time="2002-02-28
11:18:50" fw="GNAT-Box" pri=5 msg="Allow outgoing NAT"
cat _ action=pass dstname=www.soliton.co.jp proto=http
src=192.168.71.12 srcport=1684 nat=207.69.99.201 natport=1684
dst=160.239.1.10 dstport=80 rule=2 op=GET arg=/img/
privacy _ txt.gif duration=50 sent=777 rcvd=9657.
```

Inbound Outbound Security Policy Violation

When an unauthorized connection request is attempted, a log message is generated that shows that the attempt was blocked. If the packet source is from the Internet (unprotected side), then a Remote Access Filter will be the cause of the connection refusal. In the log message this is indicated by the FILTER and RAF tag along with the Remote Access Filter number which blocked the connection in parenthesis, followed by the word "block." The log message also includes the priority level, protocol, source IP, source port, destination IP, destination port, network interface, packet length and TCP flags if appropriate.

When an outbound connection (from the protected or Private Service Network) is blocked, then a message is generated indicating that an Outbound Filter was the cause of the connection refusal. This type of log message is identical to the unauthorized inbound message other than the tag "OBF" is used to indicate that an Outbound Filter rule initiated the message.

Blocked Attempt to Connect Inbound on UDP Port 53.

```
Feb 28 11:33:16 fw.gta.com id=firewall time="2002-02-28 11:
33:16" fw="GNAT-Box" pri=4 flt _ type=RAF flt _ action=block
msg="Block RAF (20)" rule=20 proto=53/UDP src=199.120.225.4
srcport=2554 dst=207.69.99.201 dstport=53 interface=PPP0
attribute="alarm"
```

Blocked Attempt to Access a Web Server

The log message below shows a blocked attempt from the Protected Network to access a web server on the Internet. Note that no specific filter rule (indicated by "default") caused the block, but rather the implicit rule (that which is not allow is denied) was applied.

```
Feb 28 11:36:18 fw.gta.com id=firewall time="2002-02-28 11:
36:18" fw="GNAT-Box" pri=4 flt _ type=OBF flt _ action=block
msg="Block OBF" proto=80/TCP src=192.168.71.12 srcport=1728
dst=207.189.82.77 dstport=80 interface=sis0 flags=0x2
```

Unauthorized Firewall Access Attempts

If a GNAT Box System is operating in the default NAT mode, all inbound requests must be directed at the firewall (and to a tunnel) because any hosts on the Protected and Private Service Networks are not visible to the External Network.

An unauthorized remote access attempt described above applies to unauthorized access attempts to access the firewall. This is not to be confused with unauthorized access attempts using Firewall Administrative Interface Access: all administrative access (successful/unsuccessful) from any of the three user interfaces (GBAdmin, Web interface and Console) are logged.

GBAdmin (RMC)

Accepts Connection

```
Feb 28 11:40:54 fw.gta.com id=firewall time=”2002-02-28 11:
40:54” fw=”GNAT-Box” pri=5 msg=”RMC: Accepted connection”
type=mgmt src=192.168.71.12 srcport=1745 dst=192.168.71.254
dstport=77
```

Successful Access

When a successful access attempt is made from GBAdmin, a log entry is created. The entry includes the tag “RMC” indicating the GBAdmin remote management client was the access method. A message indicating a successful login, along with the IP address of the remote management client system, is included.

```
Feb 28 11:41:11 fw.gta.com id=firewall time=”2002-02-28 11:
41:11” fw=”GNAT-Box” pri=5 msg=”RMC: Administration login
successful. “ type=mgmt src=192.168.71.12 srcport=1745
dst=192.168.71.254 dstport=77 duration=17
```

Unsuccessful Access

When an unsuccessful access attempt is made from GBAdmin, a log entry is created. The log entry includes the “RMC” tag, a message indicating a login failure occurred, the user ID and the IP address of the remote management client system.

```
Feb 28 11:41:00 fw.gta.com id=firewall time=”2002-02-28 11:
41:00” fw=”GNAT-Box” pri=4 msg=”RMC: Login failure for
user ‘admin’” type=mgmt src=192.168.71.12 srcport=1745
dst=192.168.71.254 dstport=77 duration=6
```

Web Interface

Successful Access

When a successful access attempt is made from the Web interface, a log entry is created for the first access. Since the http protocol is stateless, each subsequent access from the same authenticated host is not logged (although it is automatically authenticated). Once an hour, however, a successful access entry is added to the log if the same http session is still in existence. A successful log message for a Web interface administrative access includes the tag “WWWadmin,” a message indicating remote administration access, and the IP address of the client’s host system.

```
Aug 30 09:03:44 pdbtest78.gta.com id=firewall time=”2002-
08-30 09:03:44” fw=”GNAT-Box” pri=5 msg=”WWWadmin:
Remote administration access.” type=mgmt src=192.168.71.12
srcport=1107 dst=10.10.1.78 dstport=443
```

Un-Successful Access

When an unsuccessful access attempt is made from the Web interface, a log message is generated. The message includes the tag “WWWadmin” and a message indicating a failed remote administrative access attempt along with the IP address of the client’s host system.

```
Feb 28 11:50:43 fw.gta.com id=firewall time=”2002-02-28 11:
50:43” fw=”GNAT-Box” pri=4 msg=”WWWadmin: Password veri-
fication failure.” type=mgmt src=192.168.71.12 srcport=1812
dst=192.168.71.254 dstport=443 duration=1
```

Console

Successful Access

When a successful access attempt is made from Console, a log message is generated. The message includes the tag “cci” (Console Command Interface) and a message indicating a successful administrative access.

```
Aug 30 15:16:28 pdbtest79.gta.com id=firewall time=”2002-
08-30 15:16:28” fw=”GNAT-Box” pri=5 msg=”cci: Successful
administration login.” type=mgmt
```

Unsuccessful Access

When an unsuccessful access attempt is made from the Console, a log message is generated. The message includes the tag “cci” and a message indicating a failed access attempt.

```
Aug 30 15:15:57 pdbtest79.gta.com id=firewall time=”2002-
08-30 15:15:57” fw=”GNAT-Box” pri=4 msg=”cci: Password
verification failure.” type=mgmt
```

Attempts to Compromise Remote Admin Ports

In order to allow remote management of the firewall over a network, the TCP/UDP ports used for administration need to be able to accept connections. Because these network ports are accessible, they can be susceptible to unauthorized access attempts. The firewall administrator should restrict access to only those networks where remote administration is required.

GBAdmin Compromise

The log message has a “RMC” tag, indicating that this log message is associated with GBAdmin access. In the example below a TCP connection is accepted on the RMC port (default is TCP/77) from a host with an IP address of 192.168.71.12. The second message of the group is generated when the remote host was unable to generate a key, which indicates that the remote management software (GBAdmin) was not running on the remote host. The final message indicates the connection was closed.

```
Aug 30 10:39:40 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:39:40” fw=”GNAT-Box” pri=5 msg=”RMC: Accepted
connection” type=mgmt src=192.168.71.12 srcport=1510
dst=10.10.1.78 dstport=77

Aug 30 10:40:03 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:40:03” fw=”GNAT-Box” pri=3 msg=”RMC: Unable to
negotiate key.” type=mgmt src=192.168.71.12 srcport=1510
dst=10.10.1.78 dstport=77 duration=23

Aug 30 10:40:03 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:40:03” fw=”GNAT-Box” pri=5 msg=”RMC: Close
connection” type=mgmt src=192.168.71.12 srcport=1510
dst=10.10.1.78 dstport=77 duration=23
```

Web Compromise

Remote management using a web browser is normally performed using a SSL connection. Although the web interface can be configured to operate without SSL encryption, this is not recommended. In the example below, the “WWWadmin” tag indicates that the message is associated with Web interface remote administration access. The first example indicates that a remote host (192.168.71.12) connected to the firewall on the Web interface port (by default 443 for SSL or 80 for non-SSL). The next message indicates that the connection was rejected as a key could not be negotiated. This could indicate that SSL was not running, or that an attempt to compromise the firewall was made via the Web interface).

```
Aug 30 10:20:27 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:20:27” fw=”GNAT-Box” pri=5 msg=”WWWadmin: Remote
administration access.” type=mgmt src=10.254.254.205
srcport=1028 dst=10.254.254.1 dstport=443
```

```
Aug 30 10:20:29 pdbtest78.gta.com id=firewall time="2002-
08-30 10:20:29" fw="GNAT-Box" pri=4 msg="WWWadmin: Unable
to establish SSL session" type=mgmt src=10.254.254.205
srcport=1028 dst=10.254.254.1 dstport=443 duration=2
```

Ping Flood/DoS Attack

ICMP Limiting

```
Aug 30 10:51:04 pdbtest78.gta.com id=firewall time="2002-
08-30 10:51:04" fw="GNAT-Box" pri=4 msg="FILTER: Limiting
ICMP ping responses from 149 to 100 packets per second."
type=mgmt
```

Content Filtering URL Proxy Log Messages

On GNAT Box Systems that support content filtering, two different URL proxy mechanisms are used: traditional proxy and transparent proxy. When the traditional proxy is used, each user must configure their browser to use a proxy (the IP address is that of the Protected Network interface of the firewall). The transparent proxy requires no configuration of the user's browser.

Transparent Proxy

Accept

```
Aug 30 10:27:00 pdbtest78.gta.com id=firewall time="2002-
08-30 10:27:00" fw="GNAT-Box" pri=5 msg="Allow outgoing
NAT" cat _ action=pass dstname=www.gta.com cat _
site="Information Technology/Computers" proto=http
src=192.168.71.12 srcport=1439 nat=199.120.225.78 natport=1439
dst=199.120.225.2 dstport=80 rule=2 op=GET arg=/ dura-
tion=43 sent=2701 rcvd=1141
```

Block

```
Aug 30 10:29:59 pdbtest78.gta.com id=firewall time="2002-
08-30 10:29:59" fw="GNAT-Box" pri=4 msg="Block outgoing
NAT" cat _ action=block dstname=www.playboy.com cat _
site="Pornography" proto=http src=192.168.71.12 srcport=1454
nat=199.120.225.78 natport=1454 dst=209.247.228.201 dstport=80
rule=2 op=GET arg=/ duration=25 sent=666 rcvd=44
```

Traditional Proxy

Accept

```
Aug 30 10:35:55 pdbtest78.gta.com id=firewall time="2002-
08-30 10:35:55" fw="GNAT-Box" pri=5 msg="Proxy"
cat _ action=pass proto=http src=192.168.71.12
dst=199.120.225.3 cat _ site="Information Technology/
```

```
Computers” op=GET dstname=www.gnatbox.com arg=/
GeneratedItems/CSScriptLib.js
```

Block

```
Aug 30 10:37:55 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:37:55” fw=”GNAT-Box” pri=4 msg=”Proxy”
cat _ action=block proto=http src=192.168.71.12
dst=209.247.228.201 cat _ site=”Pornography” op=GET
dstname=www.playboy.com arg=/
```

Attempt to Use Proxy without Filter Enabled – default proxy port: TCP 2784

```
Aug 30 10:54:27 pdbtest78.gta.com id=firewall time=”2002-
08-30 10:54:27” fw=”GNAT-Box” pri=4 flt _ type=RAF
flt _ action=block msg=”Block RAF (25)” rule=25 proto=2784/
TCP src=192.168.71.12 srcport=1521 dst=10.10.1.78 dstport=2784
interface=fxp0 attribute=”alarm” flags=0x2
```

Network Address Translation Log Messages

System logging can be configured to record both a session startup (open) and a session termination (close). By default, only the close is enabled, as it contains the most information. A session open log message provides little additional information and increases the log size. However, it is useful for debugging.

HTML Sessions

Open (Open is usually not logged - debug aid)

```
Aug 30 11:11:17 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:11:17” fw=”GNAT-Box” pri=5 msg=”Open outbound NAT”
proto=http src=192.168.71.12 srcport=1569 nat=199.120.225.78
natport
```

Close

```
Aug 30 11:12:03 pdbtest78.gta.com id=firewall time=”2002-
08-30 11:12:03” fw=”GNAT-Box” pri=5 msg=”Accept outgoing
NAT” cat _ action=pass dstname=www.gta.com proto=http
src=192.168.71.12 srcport=1569 nat=199.120.225.78 natport=1569
dst=199.120.225.2 dstport=80 rule=2 op=GET arg=/Media/GB-
Group.jpg duration=47 sent=547 rcvd=340
```

Outbound ICP

Open

```
Aug 30 11:18:37 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:18:37” fw=”GNAT-Box” pri=5 msg=”Open outbound NAT”
proto=icmp src=192.168.71.12 srcport=3 nat=199.120.225.78
natport=3 dst=199.120.225.1 dstport=3 rule=2
```

Close

```
Aug 30 11:19:46 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:19:46” fw=”GNAT-Box” pri=5 msg=”Close outbound NAT”
proto=icmp src=192.168.71.12 srcport=3 nat=199.120.225.78
natport=3 dst=199.120.225.1 dstport=3 rule=2 duration=70
sent=3240 rcvd=3240
```

Outbound UDP

Open

```
Aug 30 11:37:24 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:37:24” fw=”GNAT-Box” pri=5 msg=”Open outbound NAT”
proto=53/UDP src=192.168.71.98 srcport=1035 nat=199.120.225.78
natport=1035 dst=204.94.136.5 dstport=53 rule=1
```

Close

```
Aug 30 11:32:06 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:32:06” fw=”GNAT-Box” pri=5 msg=”Close outbound NAT”
proto=22/TCP src=192.168.71.98 srcport=1025 nat=199.120.225.78
natport=1025 dst=199.120.225.4 dstport=22 rule=2 dura-
tion=176 sent=847 rcvd=788
```

Outbound TCP

Open

```
Aug 30 11:29:48 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:29:48” fw=”GNAT-Box” pri=5 msg=”Open outbound NAT”
proto=22/TCP src=192.168.71.12 srcport=1026 nat=199.120.225.78
natport=1026 dst=199.120.225.4 dstport=22 rule=2
```

Close

```
Aug 30 11:32:06 pdbtest78.gta.com id=firewall time=”2002-08-
30 11:32:06” fw=”GNAT-Box” pri=5 msg=”Close outbound NAT”
proto=22/TCP src=192.168.71.98 srcport=1025 nat=199.120.225.78
natport=1025 dst=199.120.225.4 dstport=22 rule=2 dura-
tion=176 sent=847 rcvd=788
```

IP Pass Through (No NAT)

Open

```
Aug 30 11:44:37 pdbtest78.gta.com id=firewall time=”2002-
08-30 11:44:37” fw=”GNAT-Box” pri=5 msg=”Open outbound
pass through” proto=23/TCP src=192.168.71.98 srcport=1027
dst=10.254.254.80 dstport=23
```

Close

```
Aug 30 11:46:04 pdbtest78.gta.com id=firewall time=”2002-
08-30 11:46:04” fw=”GNAT-Box” pri=5 msg=”Close outbound
pass through” proto=23/TCP src=192.168.71.98 srcport=1027
dst=10.254.254.80 dstport=23 duration=89 sent=444 rcvd=400
```

Inbound Pass Through Filter Block

Default (No rules in place)

```
Aug 30 11:52:52 pdbtest78.gta.com id=firewall time=”2002-
08-30 11:52:52” fw=”GNAT-Box” pri=4 flt _ type=PTF
flt _ action=block msg=”Block PTF” proto=23/TCP
src=10.254.254.205 srcport=1030 dst=192.168.71.12 dstport=23
interface=fxp2 flags=0x2
```

Match Rule To Block

```
Aug 30 12:22:17 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:22:17” fw=”GNAT-Box” pri=4 flt _ type=PTF
flt _ action=block msg=”Block PTF (1)” rule=1 proto=23/TCP
src=10.254.254.205 srcport=1031 dst=10.10.1.98 dstport=23
interface=fxp2 flags=0x2
```

Outbound Pass Through Filter Block

Default (No rules in place)

```
Aug 30 12:15:54 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:15:54” fw=”GNAT-Box” pri=4 flt _ type=PTF
flt _ action=block msg=”Block PTF” proto=23/TCP
src=10.10.1.98 srcport=1028 dst=10.254.254.80 dstport=23
interface=fxp0 flags=0x2
```

Match Rule To Block

```
Aug 30 12:18:04 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:18:04” fw=”GNAT-Box” pri=4 flt _ type=PTF
flt _ action=block msg=”Block PTF (1)” rule=1 proto=23/TCP
src=10.10.1.98 srcport=1029 dst=10.254.254.80 dstport=23
interface=fxp0 flags=0x2
```

Filter Block Messages – Outbound

Default (No rules in place)

```
Aug 30 12:25:27 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:25:27” fw=”GNAT-Box” pri=4 flt _ type=OBF
flt _ action=block msg=”Block OBF” proto=80/TCP
src=10.254.254.80 srcport=1755 dst=199.120.225.3 dstport=80
interface=fxp2 flags=0x2
```

Match Rule To Block

```
Aug 30 12:27:46 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:27:46” fw=”GNAT-Box” pri=4 flt _ type=OBF
flt _ action=block msg=”Block OBF (2)” rule=2 proto=80/TCP
src=10.254.254.80 srcport=1842 dst=64.58.76.224 dstport=80
interface=fxp2 flags=0x2
```

Filter Block Messages – Remote Access

Default (No rules in place)

```
Aug 30 12:30:03 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:30:03” fw=”GNAT-Box” pri=4 flt _ type=RAF
flt _ action=block msg=”Block RAF” proto=23/TCP
src=192.168.71.12 srcport=1900 dst=10.10.1.78 dstport=23
interface=fxp0 flags=0x2
```

Match Rule To Block

```
Aug 30 12:29:21 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:29:21” fw=”GNAT-Box” pri=4 flt _ type=RAF
flt _ action=block msg=”Block RAF (25)” rule=25 proto=23/
TCP src=192.168.71.12 srcport=1877 dst=10.10.1.78 dstport=23
interface=fxp0 attribute=”alarm” flags=0x2
```

SMTP Proxy

Rejected by MAPS

```
Aug 30 16:48:40 odin.gta.com id=firewall time=”2002-
08-30 16:48:40” fw=”GNAT-Box” pri=4 msg=”Rejected
(MAPS ‘relays.ordb.org’)” proto=smtp src=203.44.213.194
srcport=1025 dst=199.120.225.4 dstport=25
```

SMTP Successful Delivery

```
Aug 30 19:20:18 odin.gta.com id=firewall time=”2002-08-
30 19:20:18” fw=”GNAT-Box” pri=5 msg=”Close” proto=smtp
user=”janeuser@gta.com” srcuser=”janeuser@gta.com”
src=10.254.254.1 srcport=1047 dst=10.254.254.80 dstport=25
duration=29 sent=150 rcvd=98
```

RDNS Failed Connection

```
Aug 30 16:41:08 odin.gta.com id=firewall time=”2002-08-30
16:41:08” fw=”GNAT-Box” pri=4 msg=”smtp: Rejected (RDNS
failure)” proto=smtp src=199.120.220.100 srcport=1033
dst=199.120.225.80 dstport=25
```

Rejected Invalid Domain

```
Aug 30 16:47:09 odin.gta.com id=firewall time=”2002-08-30
16:47:09” fw=”GNAT-Box” pri=4 msg=”smtp: Rejected (invalid
domain ‘open@relay.net’)” proto=smtp srcuser=”hacker@hac
```

```
ker.net” src=199.120.220.100 srcport=1034 dst=199.120.225.80
dstport=25 duration=91
```

Spoof Message

In this example, a packet is arriving on fxp0 (Protected Network Interface) destined for the External Network. The Protected Network consists of only 10.254.254.0/24. Therefore, the packet is considered a spoof, since it should be arriving on the External Interface (fxp1).

```
Aug 30 12:45:46 pdbtest78.gta.com id=firewall time=”2002-
08-30 12:45:46” fw=”GNAT-Box” pri=4 flt _ type=default
flt _ action=block msg=”Possible spoof, return inter-
face fxp1 doesn’t match arrival interface” proto=138/UDP
src=192.168.71.23 srcport=138 dst=192.168.71.255 dstport=138
interface=fxp0 attribute=”bcast”
```

Door Knob Twist Connect to Closed Port

```
Aug 30 13:24:46 pdbtest78.gta.com id=firewall
time=”2002-08-30 13:24:46” fw=”GNAT-Box” pri=3 flt _
type=default msg=”Connect to closed port” proto=23/TCP
src=199.120.220.100 srcport=1036 dst=199.120.225.80
dstport=23 interface=fxp0 flags=0x2
```

VPN Log Messages

Indicates Number Of Allowed Mobile Users

This example shows the log message generated when the IKE server starts up. This occurs when the system boots or after saving VPN sections. The license messages indicate the number of allowed concurrent Mobile Users.

```
Aug 30 14:12:18 ipsec.gta.com id=firewall time=”2002-08-
30 14:12:18” fw=”ipsec” pri=5 msg=”WWWadmin: Starting
IKE server.” type=mgmt src=192.168.71.2 srcport=2206
dst=192.168.71.254 dstport=80 duration=2
```

```
Aug 30 14:12:18 ipsec.gta.com id=firewall time=”2002-08-
30 14:12:18” fw=”ipsec” pri=5 msg=”Licensed for 100 mobile
client connections. type=mgmt,vpn
```

Successful VPN Connection

```
Aug 30 13:39:21 ipsec.gta.com id=firewall time=”2002-08-
30 13:39:21” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

```
Aug 30 13:39:21 ipsec.gta.com id=firewall time=”2002-08-
30 13:39:21” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=24.170.164.183 dst=199.120.225.200
```

Successful Mobile User Connection

```
Aug 30 15:31:24 ipsec.gta.com id=firewall time=”2002-08-
30 15:31:24” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=207.69.100.126 dst=199.120.225.8
```

```
Aug 30 15:31:24 ipsec.gta.com id=firewall time=”2002-08-
30 15:31:24” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=199.120.225.8 dst=207.69.100.126
```

Authentication from a Mobile User

```
Aug 30 13:38:23 ipsec.gta.com id=firewall time=”2002-08-
30 13:38:23” fw=”ipsec” pri=5 msg=”RMCauth: Accepted
connection” type=mgmt src=199.120.225.78 srcport=2170
dst=199.120.225.200 dstport=76
```

```
Aug 30 13:38:27 ipsec.gta.com id=firewall time=”2002-08-30
13:38:27” fw=”ipsec” pri=6 msg=”RMCauth: Authentication
successful for ‘support@gta.com’.” type=mgmt
src=199.120.225.78 srcport=2170 dst=199.120.225.200 dstport=76
duration=4
```

Failed Authentication Attempt

```
Aug 30 14:10:44 ipsec.gta.com id=firewall time=”2002-08-
30 14:10:44” fw=”ipsec” pri=5 msg=”RMCauth: Accepted
connection” type=mgmt src=199.120.225.78 srcport=2197
dst=199.120.225.200 dstport=76
```

```
Aug 30 14:10:48 ipsec.gta.com id=firewall time=”2002-08-30
14:10:48” fw=”ipsec” pri=4 msg=”RMCauth: Authentication
failure for ‘support@gta.com’.” type=mgmt src=199.120.225.78
srcport=2197 dst=199.120.225.200 dstport=76 duration=4
```

Example Of Expiring And Renewing

```
Aug 30 15:00:49 ipsec.gta.com id=firewall time=”2002-08-
30 15:00:49” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

```
Aug 30 15:00:49 ipsec.gta.com id=firewall time=”2002-08-
30 15:00:49” fw=”ipsec” pri=5 msg=”IPsec-SA established
type=mgmt,vpn src=24.170.164.183 dst=199.120.225.200
```

```
Aug 30 15:00:47 ipsec.gta.com id=firewall time=”2002-
08-30 15:00:47” fw=”ipsec” pri=5 msg=”IPsec-SA expired
type=mgmt,vpn src=24.170.164.183 dst=199.120.225.200
```

```
Aug 30 14:48:47 ipsec.gta.com id=firewall time=”2002-
08-30 14:48:47” fw=”ipsec” pri=5 msg=”IPsec-SA expired
type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

Default Settings

The Default Settings section contains the standard default settings for a GTA Firewall that has been configured with an External, Protected, and Private Service Network (GTA’s DMZ), but without further configuration changes.

The implicit rule for GNAT Box Systems is “that which is not expressly permitted is denied.” If all filters were removed, no packets would flow inbound or outbound. A GNAT Box System can generate a default configuration using security policies based on this implicit rule.

Outbound Security Policies

1. All outbound access from the Protected Network is allowed.
2. All outbound access from the Private Service Network is allowed.

Outbound Filters

```
1 #DEFAULT TRADITIONAL URL PROXY: allow access to DNS.
DISABLED - Accept notice “PROTECTED” UDP from ANY _ IP to
ANY _ IP 53
```

```
2 #DEFAULT NO TRADITIONAL URL PROXY: Allow Protected
Network access to anywhere. Accept notice “PROTECTED” ALL
from ANY _ IP to ANY _ IP
```

Remote Access Security Policies

1. All inbound access from the External Network is denied.
2. All access from the External Network to the GTA Firewall is denied.
3. Access to the GTA Firewall using the Web interface is allowed only from IP addresses on the Protected Network.
4. Access from a Private Service Network to the GTA Firewall is denied.
5. Access from a Private Service Network to a Protected Network is denied.
6. Access to the Console interface requires a user ID and password.
7. Access to the Web interface requires a user ID and password.

Remote Access Filters

```
1 #DEFAULT: Allow Protected Network access to remote admin
services. Accept notice “PROTECTED” TCP from ANY _ IP to
ANY _ IP 443 77
```

```
2 #DEFAULT: Allow Protected Network access to DNS server.
Accept notice “PROTECTED” UDP from ANY _ IP to ANY _ IP 53
```

3 #DEFAULT: Allow Protected Network access to SNMP service. DISABLED - Accept notice “PROTECTED” UDP from ANY _ IP to ANY _ IP 161

4 #DEFAULT: DNSproxy - Allow all DNS replies. Accept notice ANY UDP from ANY _ IP 53 to ANY _ IP 53

5 #DEFAULT: DNS server - Allow all DNS replies. DISABLED - Accept notice ANY UDP from ANY _ IP 53 to ANY _ IP 1024:65535

6 #DEFAULT: Allow access to user authentication server. DISABLED - Accept notice ANY TCP from ANY _ IP to ANY _ IP 76

7 #DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy. DISABLED - Accept notice “PROTECTED” TCP from ANY _ IP to 0.0.0.0/0 2784

8 #DEFAULT EMAIL PROXY: Allow connections to email proxy. DISABLED - Accept notice “EXTERNAL” TCP from ANY _ IP to ANY _ IP 25

9 #DEFAULT: Block/nolog discard bootp, netbios, and rwho. Deny warning ANY UDP nolog from ANY _ IP to ANY _ IP 9 67 68 137 138 513

10 #DEFAULT NO RIP: Block/nolog rip. Deny warning ANY UDP nolog from ANY _ IP to ANY _ IP 520

11 #DEFAULT RIP: Accept UDP rip. DISABLED - Accept notice ANY UDP from ANY _ IP to ANY _ IP 520

12 #DEFAULT RIP: Accept IGMP multicast for router addresses. DISABLED - Accept notice ANY 2 from ANY _ IP to 224.0.0.0/24

13 #DEFAULT RIP: Accept router solicitations and advertisements DISABLED - Accept notice ANY ICMP from ANY _ IP to 224.0.0.0/24 9 10

14 #DEFAULT STEALTH: Block with alarm any other access to external interface. DISABLED - Deny warning “EXTERNAL” ALL alarm from ANY _ IP to ANY _ IP

15 #DEFAULT: Accept/nolog authentication (ident). Accept notice ANY TCP nolog from ANY _ IP to ANY _ IP 113

16 #DEFAULT: Allow pings and ICMP traceroutes to GNAT Box. Accept notice ANY ICMP from ANY _ IP 8 to ANY _ IP 8

17 #DEFAULT: Allow UDP traceroutes to GNAT Box. Deny warning ANY UDP nolog genICMP from ANY _ IP to ANY _ IP 32767:65535

18 #DEFAULT: Block/nolog stale WWW accesses. Deny warning ANY TCP nolog from ANY _ IP 80 to ANY _ IP 1024:65535

```
19 #DEFAULT: Block with alarm any other access to all
interfaces. Deny warning ANY ALL alarm from ANY _ IP to
ANY _ IP
```

Troubleshooting

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 in the Reports Menu. The verification check is the best method of ensuring that your system is configured correctly. All errors and warnings listed should be corrected.
- 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 GTA Firewall, the port/network interface 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 are the green LEDs on the back of the GTA Firewall not lighting up? (RoBoX, GB-1000, GB-100)

This indicates that you do not have network connectivity. You may have selected the wrong network connection type. Check the Network Information screen to ensure the appropriate connection type is selected. If you have selected one of the specific settings, reset to AUTO, the factory setting.

2. 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 GTA Firewall, 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.

3. 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 GTA Firewall's 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.

4. 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 GTA Firewall’s 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.

5. 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.

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

You may have the wrong cable for your connection.

- For a direct connection (GB-1000 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.

7. I can’t access a Tunnel that I have created. Why?

A few key points to remember about Tunnels:

- You cannot access a Tunnel from the Protected Network, since you can access the host directly (use the real IP address of the host).
- The source side of the tunnel must have an IP address that is on the External Network for tunnels from the External Network to the PSN or to the Protected Network.

- The source side of the tunnel must have an IP address that is on the Private Service network for tunnels from the PSN to the Protected Network.
- You must have a Remote Access filter that allows access to the Tunnel from the host in question. A Tunnel that has no Remote Access Filter, or an improperly configured filter assigned to it, will generate a “blocked packet” message to the log file. Use the Default option in the filter set to create disabled filters matching your defined tunnels, then customize and enable them.
- Ensure that your Tunnel is active. Check the Configuration Report to verify that both your Tunnel and Remote Access filters are active.
- Check the log messages for filter blocks when a remote host attempts to access the Tunnel. If you see a block message, your Remote Access filter is most likely not configured correctly. If no block message appears, check the host that is specified as the target in the Tunnel definition. The target host should have a default route configured, with the service in question running on the specified port. From the target host try to ping the remote host.

8. My MS Exchange server located on the PSN can’t find the PDC on the Protected Network. Why?

Normally, NetBIOS locates the PDC (and other peer hosts) by using broadcast packets. Since the GNAT Box blocks all broadcast packets, another method of locating the PDC needs to be used. The solution is to use a LMHOSTS file and add an entry for the PDC providing a conduit for NetBIOS traffic to the PDC via a tunnel and allow access via Remote Access filters.

1. Create a LMHOSTS file and insert an entry for the PDC. This entry will use the PDC’s NetBIOS name, the NetBIOS domain name, and the PSN interface IP address where the tunnel will be created.
2. Create three tunnels from the PSN interface to the PDC for NetBIOS services.

   UDP 137 - NetBIOS name resolution
   UDP 138 - NetBIOS datagrams
   TCP 139 - NetBIOS data transfer
3. Create three Remote Access Filters that allow the MS Exchange server on the PSN to access the three tunnels you created in step 2.
4. Reboot the Exchange server.

Example

GNAT Box System

```
EXT 199.120.225.2

PRO 192.168.1.1  PDC 192.168.1.50

PSN 192.168.2.1  Exchange Srv 192.168.2.100
```

LMHOST Entry

```
192.168.2.1  PDCserver  #PRE #DOM:gtanet
```

Tunnels

```
UDP 192.168.2.1 137  192.168.1.50 137

UDP 192.168.2.1 138  192.168.1.50 138

TCP 192.168.2.1 139  192.168.1.50 139
```

Add Remote Access Filters

```
1. Allow Exchange Server to access via NetBIOS UDP

Accept UDP PSN

192.168.2.100/32

192.168.2.1/32 137 138

2. Allow Exchange Server to access via NetBIOS TCP

Accept TCP PSN

192.168.2.100/32

192.168.2.1/32 139
```

Windows NT/2000

Sample: C:\WINNT\System32\drivers\etc\LMHOSTS.SAM

Real File: C:\WINNT\System32\drivers\etc\LMHOSTS

Windows 95/98

Sample: C:\Windows\LMHOSTS.SAM

Real File: C:\Windows\LMHOSTS

9. Why doesn't the feature I enabled (email, RIP, etc.) work?

The correct filters may not be installed/enabled for the selected features.

The initial configuration of the GTA Firewall will create a set of all possible default filters. Depending on which options are enabled, filters will have the Disable selector set or unset. To enable a feature, activate it then supply the required data (if needed) and enable or disable the appropriate Remote Access Filters.

Example: RIP

1. Enable RIP and the options in the RIP section and save.
2. Disable the "DEFAULT RIP" Remote Access filters.
3. Save the Remote Access filter set.

Example: EMAIL Proxy

1. Enable the Email Proxy.
2. Set the IP address of the primary email server.
3. Save the Email Proxy section.
4. Enable the "DEFAULT EMAIL PROXY" Remote Access filter.
5. Save the Remote Access filter set.

10. I get errors when GBAdmin starts up and/or online help information is 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.

Index

Symbols

??? 33, 139

3DES 82

A

Accept all filters 126

Access
- codes, telephone 47
- control for VPN 25
- Control Lists 87
- restrict 34

ACK 129

ACL 87

Acrobat 13

Activation
- code 13, 40

Active
- filters 144
- routes 146
- VPNs 146

ActiveX 92

Address
- MAC 170
- object 23, 100
- spoof 10, 112

Add button 31

AES 82

Alarms 112

Albitz 26

Algorithm 83

Alias 113, 123

Allow list 88

Anti-replay protocol 104

ARP Table 132, 143

Arrow
- connection direction 144
- dropdown menu 33
- up, down 31

ASCII 83

Attack
- denial of service 10
- spoof 10, 112

Authentication Header 103

Authorization 79, 102

Automatic filters 126

A records 59

B

Beacon 95

Blacklist 62

Blocked
- Web interface, GBAdmin 28

Blowfish 82

Broadcast 110

Browser
- Internet Explorer 27
- Lynx 27
- Netscape Navigator 27

C

Cable 42, 170, 172

Can’t access
- Web interface, GBAdmin 28

CAST128 82

Chat 49, 152

Check box 32

Check mark 31

CIDR
- Classless Inter-Domain Routing 44
- notation 44

CNAME records 59

Common ports 151

COM Port 47

Concurrent sessions 10

Configuration
- copy 102

Connection
- direction 144
- type 47

Console 11
- limited 11
- primary account 73

Contact information 54

Contact ports 151

Content filtering 9, 40, 69, 87, 88

Copy protect 13

Current Statistics 147

D

Date 135

Debug 49

Dedicated
- address 48
- connection 47

Default
- address objects 100
- character set 54
- enabled by 39, 49, 78
- filters 24
- Gateway 43, 56
- NAT 21
- route 43

advertise 97
- security

policy 24
- settings 168
- VPN objects 23, 102

Demilitarized Zone 18

Denial of service 10

Deny list 88

DES 82

DHCP 9, 42
- Leases 148
- server 55

Dial access code 47, 114

Direction of connection 144

DMZ 9, 18

DNS 25, 39
- and BIND 26
- Blacklist 62
- domain 59
- problem 170
- proxy 39
- proxy override 40
- server 25, 39

Documentation
- additional 13
- conventions 12
- map 13

Domain Name System. **See** DNS

Dongle 13

Doorknob twist 112, 128

Dotted decimal
- notation 44

Drivers 13

Dropdown 33

DTE 48, 114

Dynamic
- address 48
- NAT 21
- translation 20, 123

Dynamic Host Configuration Protocol 42, 55, 148

E

Email
- abuse 62
- configuration 141
- proxy 61, 175
- server 61

Encryption 82
- level 77

Errors
- GBAdmin 172

Ethernet
- PPP over 46

Exchange Mode 103

Exclusion ranges 56

External
- DNS

server 25
- network 18

F

Factory settings 24, 28, 102, 108, 132

Fault resilient 9

Feature
- code 13, 40
- doesn’t work 175

Field
- greyed out 33
- index 32

Filter 24, 107
- action 25
- active 144
- automatic 126
- packet types 154
- Remote Access 172
- rule 120
- set 108

Fixed routes 98

Force Mobile Protocol 103

Forwarders
- DNS 58

FTP 17

G

Gateway 42
- Default 43
- static and dynamic 94

GB-Pro
- one default object 102

GB-Reports 139

GBAdmin 11, 13
- Administration Menu
  - *Interfaces 133*
  - *Ping 134*
  - *Reboot 134*
  - *Set Date/Time 135*
  - *Trace Route 136*
- errors 172

GBAuth 79, 102

GNAT Box Tunnel 16

Grey field 33

H

Halt firewall 133

Hardware 140
- key block 13

Hexadecimal 40, 82

High Availability 13, 23, 55, 64
- interface object 23

Holes in the firewall 16

Hosts can't reach Internet 171

Host name 43, 60
- ssl certificate 74

I

ICSA 9

IETF 25

IKE 81

Implicit rule 10, 24

Inbound Tunnel 23, 116, 123

Index field 32

Indicator
- dot (light, button) 37

Installation 14

Interface
- Console 11
- disable, enable 133

Interface Object 23

Internal
- DNS server 26

Internet Explorer 27

IP 115

IPSec 25

IP alias 17
- interface object 23

IP packet 15

IP Pass Through 22, 119

ISDN 47, 49

J

JAVA 92

Junk mail 62

K

Keep Alive 129

Key
- length 82
- method 81
- strength 77

Key Block 13

L

LCP 48

Lease Duration
- DHCP 56

LED
- not lit 171

Limited Console 11

Link Control Protocol 48, 51

Liu 26

Local Content Lists 87, 90

Lockout 73, 149
- Web interface, GBAdmin 28

Log
- messages 149, 154
- old format 67
- WELF format 67

Logical name
- changing 42
- interface object 23

Lynx browser 27

M

Macintosh 27

MAC address 43, 139, 143, 170

Mail exchangers 59

Management Information Base 70

Manual Key Method 81
Mapping 21
MAPS 2, 62
Master, HA 65
Maximum Transmission Value 43
MD5 83, 97, 103
Menu
  scrolling 35
MIB 70
Mobile Code Blocking 92
Mobile Key Method 81
Mobile protocol 103
Mobile Users 80, 166
Modem 42, 47, 114
MS Exchange 173
MTU 43
MX records 59

N

Name
  of object 22
Name server 39
NAT 20, 123
  IP Pass Through 22
Net2Phone 17
NetBIOS 173
Netmask 44
Netscape Navigator 27
Network
  Address Translation 10, 20, 123
  bridge 10
  interface 19
  transparency 16
Network Time Service 55, 66
NIC 19
Notation
  / 44
  CIDR 44
  dotted decimal 44
  slash 44
No NAT 22
NTP 66
Numeric pager 114

O

O’Reilly and Associates 26
Object 22, 99
  changing the name 22
On-demand
  connection 47
On-enabled
  connection 47
Outbound Filters 24, 107
Outbound Mapping 21

P

Pager 109, 112
Password
  lockout 73
  persistence 28
PDC 173
PDF 13
Perfect Forward Secrecy 104
PFS 104
Phase 49
PING 134, 170
Platform 27
  Macintosh 27
  Unix 27
  Windows 27
  X-Windows 27
Platform independent 27
Point-to-Point Protocol 46
Port
  COM 47
  no SSL 28
  SSL encryption 28
PPP 46, 171
  over Ethernet 46
Preferences 54
  filter 111
Priority 64
  filter 109
Private Service Networks (PSN) 10
Protected Network 18
Protocol, anti-replay 104
Proxy
  DNS 39
  email 61
  SMTP 61
  traditional 91
  transparent 92
PSN 18

R

Range 45
- exclusion 56

RDNS 60

Read-only 70

RealAudio 17

Reboot 134

Register 14

Remote Access
- filter 24

Replay Detection 104

Report, hardware 170

Restrict access 34

Retry
- PPP/PPPoE 48

Reverse Domain Name System 60

Reverse Zone Name 58

Rijndael 82

RIP 96, 175

RoBoX 13

Route
- active 146
- Default 43
- static 98

Routing Information Protocol 93, 96

Rule
- field 32
- filter 120

Runtime 36, 131, 137

S

Scrolling Menu 35

Secure Sockets Layer 77

Security Association 83

Security Parameter Index 82

Security policy 168

Serial number 14, 41, 54
- email 61

Services 151

SHA1, SHA2 83, 103

Simple Mail Transfer Protocol 61, 151

Simple Network Management Protocol 70

Slash
- notation 44

Slave, HA 65

SMTP 61

SNMP 70

Spam 62

SPI 82

Spoof 10, 112

Spreadsheets 139

SSL encryption
- certificate 73
- port 28

Stateful Packet Inspection 10, 15

Static
- address 48
- NAT 21
- route 98
- translation 20, 123

Static Address Mapping 21, 127

Statistics 147

Stealth Mode 112

Stop firewall 133

StreamWorks 17

Support 14
- contract 14
- up and running 14

Surf Sentinel 9, 40, 69, 87

T

TCP/IP 15

Technical support 2, 14

Telnet 10

Time 135

Timeout 61, 128

Time based
- filter 109

Time Groups 118

Time server 66

Time to Live 143

Time zone 135

Trace route 136, 170

Traditional Proxy 91

Transparent proxy 92

Troubleshooting 170

TTL 94, 136, 143

Tunnel 16
- can’t access 172
- VPN 25

Twofish 82

TX_100 43

Types of filter 24

U

Unauthorized access

- GBAdmin 35
- Web interface 28

Unix 27

- syslog 67

Unlock 13

- code 13

Upgrading

- with SSL 78

Up and running 14

URL 28

User authorization 79, 102

User Interfaces 11

UTP_10 43

V

Verification 30, 34, 139, 140, 170

Virtual crack 16, 119

VPN 25

- access control
- *IP Pass Through 25*
- active 146
- objects 102
- Security Association 83
- tunnel 25
- Virtual Private Network 10

W

Wait for ACK 129

WebTrends Enhanced Log Format 67, 69, 149

Web interface

- block 28

Web server

- built-in 28

WELF 2, 67, 69, 139, 149, 153

Well-known ports 151

Windows

- 98 64, 174
- NT 174

X

X-Windows 27

XML 139

X button 31

TABLE OF ILLUSTRATIONS

Access Control Lists 89
Active Connections 144
Active Filters 145
Active Routes 146
Address Objects 101
Administration Accounts 74
Administration Menu 131
ARP Table 143
A GTA Firewall System Diagram Example 18
Basic Configuration Menu 39
Certificate Import Wizard Complete 76
Change Password 74
Check Boxes 32
Content Filtering Buttons and Lists 33
Content Filtering menu 87
Content Filtering Preferences 92
Current Statistics 148
Default “ANY_IP” Address Object 100
DHCP Leases 148
DHCP Server Address Range 57
DHCP Server List 56
DNS 40
DNS Domains 60
DNS Server 59
Domain Name System (DNS) 26
Download Configuration 132
Dropdown Boxes; Data Entry Fields 33
Email Configuration Form 141
Email Proxy 63
IP aliases assigned to an External Network 17
Features 41
Filter Icon Buttons 31
Filter Menu 107
Filter Preferences 115
Flush ARP Table 133
Gateway Selector 95
GBAdmin Opening Screen 36
H2A High Availability 65
Halt Firewall 133
Hosts/Networks 122
IE 5 for Windows Install Certificate 76
IKE VPN Add/Edit Screen 84
Inbound Tunnel screen 126
Index Fields 32
Indicator Dots 37
Interfaces 133
IP Pass Through Menu 119
IP Pass Through Filters 121
LCL Allow List 90
LCL Deny List 91
Lockouts 149
Manual VPN Add/Edit Screen 85
Menubar 38
Mobile VPN Add/Edit Screen 85
NAT IP Aliases screen 124
NAT Menu 123
Network Information 44
Network Time Service 67
New PPP/PPPoE dialog 49
Objects Menu 99
Object Icon Buttons 31
Outbound Filter 110
Ping 134
Pop-up Verification Note 37
PPPoE 51
PPP 49
Preferences (Contact Information) 54
Protocols 116
Reboot 134
Remote Access Filter 117
Remote Administration/Authentication screen 79
Remote Logging 68
Reports Menu 139
RIP 97
Routing Menu 93
Scrolling Menu Example 37
Services Menu 55
Set Date/Time 135
Set Time Zone 135
SNMP 71
SSL Certificate (Web only) 75
SSL Certificate Security Alert 75
Static Routes 98
Static Address Mapping 128
Static Address Mapping Illustration 21
System Activity Menu 143
Timeouts 129
Time Groups 118
Toolbar 38
Trace Route 136
Upload Configuration 136
Upload Runtime 137
Users Add/Edit Screen 80
View Log Messages 149
VPNs Screen 84
VPN key mode selection screen 84
VPN Object 104
VPN Screen–IKE (GBAdmin) 86
Web Interface Main Window 29
Web Menu Example 30

FIELD TABLES

Access Control Lists (ACL) Fields 88
Active Connections List 144
Active Filters List Display 145
Active Route Flag Values 146
Address Object Fields 100
Admin Account Fields 73
Algorithms 83
Authorization Fields 79
Content Filtering Preferences Fields 92
Current Statistics List 147
DHCP Fields 56
DNS Domain Fields 59
DNS Fields 40
DNS Server Fields 58
Documentation Conventions 12
Documentation Map 13
Email Proxy Fields 61
Encryption Levels 77
Filter Fields 109
Filter Icon Buttons 31
Gateway Selector Fields 95
High Availability Fields 64
Inbound Tunnel Fields 126
Navigation Buttons 30
Network Information Fields 42
Network Time Service Fields 66
Object Icon Buttons 31
PPP/PPPoE Fields 47
Preferences Fields 54
Preferences Fields 111
Registered Port Assignments 152
Remote Logging Fields 67
RIP Fields 97
RMC Fields 79
SNMP Fields 70
Static Routes Fields 98
Static Address Mapping Fields 127
Timeout Fields 128
User Add/Edit Screen Fields 80
VPN Add/Edit Screen Fields 81
VPN Information 147
VPN Objects Fields 102
WELF Fields 69
Well-known Port Assignments 151
WWW Administration Fields 78