# GNAT Box®

# SYSTEM SOFTWARE

## version 3.5

# User's Guide

Global
Technology
Associates, Inc.

### Copyright

**GNAT Box System Software version 3.5 User's Guide 24 March 2004**

### Technical Support

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's website for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized channel partner.

**Tel: +1.407.482.6925 Email: support@gta.com**

### 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 & Copyrights

**Global Technology Associates, Inc.**

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA
Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: http://www.gta.com • Email: info@gta.com
**Lead Development Team:** Larry Baird, Richard Briley, Jim Silas, Brad Plank.
**Technical Consulting:** David Brooks. **Documentation:** Mary Swanson.

# Contents

# 1 Introduction

## GNAT Box Basics

Since 1994, Global Technology Associates, Inc., has been designing and building 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 enterprise-level firewalls, firewalls for remote and branch offices, and a software firewall for user-provided hardware.

### Standard Features

GTA's NAT (Network Address Translation) and Stateful Packet Inspection engine are at the heart of all GNAT Box Systems. These facilities, tightly integrated with the network layer, guarantee maximum data throughput, reliable NAT and unparalleled security. IP Pass Through filters allow the use of the firewall without NAT. GNAT Box version 3.5 features also include:

- Transparent network access for standard TCP and UDP applications.
- Safe access to external networks using the PSN, GTA's DMZ network.
- IPSec VPN (Virtual Private Networking) and Mobile VPN Client.*
- DHCP and DNS services via built-in DHCP and DNS servers.*
- Bridging for user-identified Ethernet protocols.
- User authentication for any platform via the GBAuth utility.
- Encryption methods including DES, 3DES, AES and Blowfish.
- Secure remote logging using the GTAsyslog or a third-party syslog.
- Secure email proxy and spam prevention tools.
- Support for most current application and communication protocols, including FTP, PASV FTP, CU-SeeMe, RealAudio/Video, ICQ, AIM, online gaming, Net2Phone, PPP, PPPoE and PPTP.
- Default stealth mode.

In addition, GNAT Box administrators have a choice of three user interfaces.

- Web interface: Cross-platform, encrypted remote management interface via a graphics or text-based browser, which provides comprehensive access to configuration options.
- GBAdmin: Secure, Windows-based protected network access.
- Console interface: On-site Serial or Video fail-safe and firewall recovery access.

## Options

- Secure mobile remote network access with Mobile VPN Client.
- Internet content filtering with a Surf Sentinel subscription.
- Fault resilience with $H_2A$ High Availability.*
- VPN acceleration.*
- A variety of support offerings for firmware upgrades.

*Available on select GTA Firewalls.

## The GNAT Box System

The GNAT Box system is dedicated to network security. No other applications run on it; there is no user shell, you can’t telnet to it; and you can’t use it as a mail or web server. An authorized user can log on only to configure and administer the firewall.

GNAT Box systems are based on the implicit rule, “That which is not explicitly allowed is denied.” If all filters were deleted, there would be no inbound or outbound packet flow.

A GNAT Box system is:

- A **Firewall** that prevents unauthorized access to internal networks, while allowing authorized connections to operate transparently.
- A **Network Address Translation** engine that allows unregistered IP addresses to be used on the Protected and PSN networks so that IP addresses are hidden from external networks and translated to the primary External Network interface IP address.
- A **DNS Server** that maintains a database of domain names (host names) and their corresponding IP addresses.
- A **DHCP Server** that automates the assignment of IP addresses to host systems on locally attached networks.
- A **Network Gateway** that links network topographies (e.g., 10Mbps to Gigabit) and replaces a router in a PPP configuration.
- A **Bridging Firewall** that links Ethernet networks together transparently like a bridge, while filtering IP packets as a firewall.
- A **Virtual Private Network** between two networks using the IPSec VPN standards and supporting many third-party VPN products.

## Support & Registration

Make sure to register your GTA Firewall product. You can do this at GTA's online support center, at www.gta.com/support/logon.php. If you already have an account, enter your user ID and password to log in; to create a new account, enter your profile information, including product serial number and activation code. See your product guide for more information.

### Activation Codes

GNAT Box System Software is not directly copy-protected, so it may be duplicated for backup purposes. Activation (unlock) codes are required to use the software. For firewall appliances, the required code is pre-installed. Additional features require feature activation codes. Your activation codes can be found under **VIEW PRODUCTS** on the GTA Support site.

### Installation Support

Installation ("up and running") support is available to registered users. If you need installation assistance during the first 30 days after purchase, register your product and then contact the GTA Support team by email at support@gta.com. Include your product name and serial number. Installation support covers only the aspects of configuration related to installation and default setup. See GTA's website for more information.

### Support Options

If you need additional support for GTA products, a variety of contracts are available. Contact the GTA Sales staff for more information. Contracts range from support by the incident to full coverage for a year. Assistance may also be available through an authorized GTA Channel Partner.

#### Mailing List

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

# Documentation

User’s guides, product guides and feature guides are delivered with new GTA products. These manuals and other documentation for registered products can also be found at www.gta.com.

Look in your firewall’s product guide for instructions on installation, registration and setup in default configuration. Look in feature guides for instructions on setting up GTA’s optional features.

## Documentation Map

| | |
|---|---|
| **Products and Options** | |
| GNAT Box System Software | GNAT Box System Software User‘s Guide |
| GTA Firewall Installation | Product Guides |
| Firewall Management | GB-Commander Product Guide |
| Reporting | GTA Reporting Suite Product Guide |
| Content Filtering | Surf Sentinel Content Filtering Feature Guide |
| High Availability | $H_2$A High Availability Feature Guide |
| Virtual Private Networking | GNAT Box VPN Feature Guide |
| VPN Examples | GNAT Box VPN to VPN Tech Docs |
| **Utilities & Information** | |
| Logging Utilities | GNAT Box System Software User’s Guide |
| Troubleshooting | Product and Feature Guides |
| Ports & Services | Product CDs |
| Drivers & NICs | www.gta.com |
| Frequently Asked Questions | FAQs on www.gta.com |
| Web Interface, GBAdmin | GNAT Box System Software User’s Guide |
| Console interface | Console Interface User’s Guide |

Documents available on GTA’s website are either in plain text (*.txt) or Portable Document Format (PDF) which requires Adobe Acrobat Reader version 5.0 or better. A free copy of the reader can be obtained at www.adobe.com. Documents sent by GTA Support may also be in Microsoft Word format (*.doc).

### *Note*

Only initial product purchases are eligible for free printed manuals. Upgrade products include PDF documentation. Check GTA’s website for the latest documentation.

## Inside This Guide

For GNAT Box System Software version 3.5, the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** adds information on new and changed options, such as logging, dynamic DNS, authentication and bridging features. The guide includes advanced configuration options, descriptions of fields, administrative tools and troubleshooting, plus relevant appendices.

### Documentation Conventions

| | |
|---|---|
| SMALL CAPS | FIELD NAMES IN BODY TEXT. |
| **BOLD SMALL CAPS** | **NAMES OF PUBLICATIONS.** |
| **Bold** | **Chapters.** |
| ***Bold Italics*** | ***Emphasis.*** |
| `Courier` | `Screen text.` |
| **ALL CAPS** | **ON SCREEN BUTTONS.** |
| **<BRACKETS>** | **WITH ALL CAPS, KEYBOARD BUTTONS.** |
| **Condensed Bold** | **Menus, menu items, menu selections.** |
| **Slash "/"** | **In menu items, indicates menu structure.** |

### Chapters and Appendices

The configuration and administration chapters, Chapter 2 through Chapter 13, describe functions in the order that they appear on the Web interface. After an explanation of the function and notes on using it, there will be a table of field descriptions and an illustration from the Web interface. Differences in GBAdmin will be noted.

Reports, Administration and System Activity sections are found in the Web interface menu and in the GBAdmin menu items.

The Utilities chapter provides information on GNAT Box utility applications: GBAuth, DBmanager, LogView and GTAsyslog. These utilities are used by GNAT Box System Software, GB-Commander and GTA Reporting Suite.

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

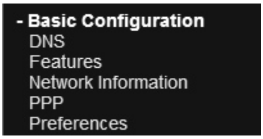
The Appendices are Ports & Services, Log Messages, User Interfaces, GNAT Box Terms and Default Settings.

### User Interface Instructions

For instructions on how to use the Web interface and GBAdmin, see **Appendix C – User Interfaces**. For information on the Console interface, see the **CONSOLE INTERFACE USER'S GUIDE**, available online at www.gta.com or on the GNAT Box product installation CD.

# 2 Basic Configuration

Basic Configuration contains functions for firewall setup and configuration, organized in order of the function's appearance on the menu in the Web interface; DNS, Features, Network Information, PPP and Preferences.



*Basic Configuration Menu*

## DNS

The DNS (Domain Name System) section is used to select the DNS servers for resolving host names and to enable DNS Proxy so that selected networks behind the firewall will use it to resolve domain names. DNS services are optional on certain GTA firewalls.

Use an internal network DNS server if one is available; see **DNS Server** in the Services chapter to configure the firewall as a DNS server. Use a DNS server from outside your network, e.g., a name server accessed through your ISP, as your external network DNS server.

### DNS Proxy

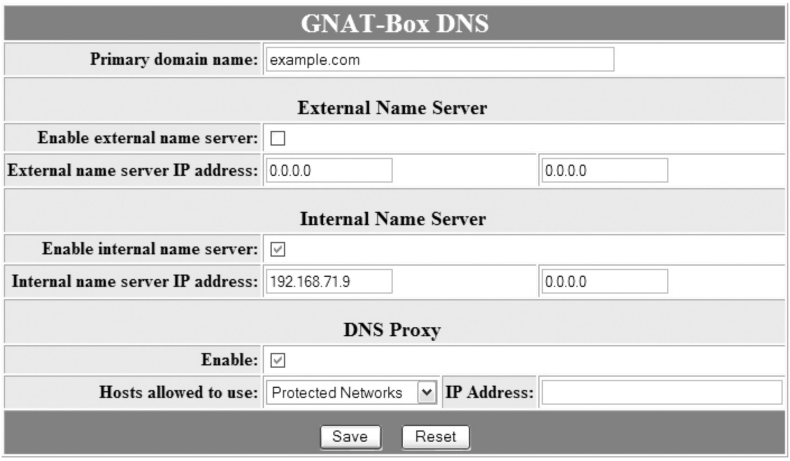
DNS Proxy establishes the firewall as a proxy for translating host names into IP addresses and specifies which hosts use it. DNS Proxy requires a Remote Access Filter to allow DNS proxy replies. The hosts will be represented either by an IP address or an Address Object. The DNS proxy sends a request to all available DNS resolvers (those listed and those acquired dynamically) to resolve a host name. The first reply will be sent to the requestor. DNS Proxy is unnecessary with a local DNS server configured, so enabling DNS Server overrides DNS Proxy.

## DNS Fields

| | |
|---|---|
| Primary Domain Name | Primary domain name used for the network, e.g., gta.com. |
| External name server | Use the name servers listed in this section. Disabled by default. |
| IP address | IP address of an external DNS server. |
| Internal name server | Use the name servers listed in this section. Disabled by default. |
| IP address | IP address of an internal DNS server. |
| DNS Proxy | Enable DNS Proxy. Disabled by default. |
| Hosts allowed | Object 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 **Services/DNS Server** overrides DNS Proxy.



GNAT-Box DNS

| | | | |
|---|---|---|---|
| **Primary domain name:** | example.com | | |
| | **External Name Server** | | |
| **Enable external name server:** | □ | | |
| **External name server IP address:** | 0.0.0.0 | | 0.0.0.0 |
| | **Internal Name Server** | | |
| **Enable internal name server:** | ☑ | | |
| **Internal name server IP address:** | 192.168.71.9 | | 0.0.0.0 |
| | **DNS Proxy** | | |
| **Enable:** | ☑ | | |
| **Hosts allowed to use:** | Protected Networks | **IP Address:** | |

*DNS*

# Features

Enter the system serial number and GTA Firewall activation codes in Features. The **RESET** button reverts to previously saved information if you have not yet saved the section.

## Serial Number

The GTA Firewall serial number can be found on the card shipped with the firewall (along with the activation code), and on GTA Firewall appliances.

## Activation Codes

Enter GTA Firewall activation codes (hexadecimal characters only – 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) in the Activation Code fields and select **SAVE**. The system will 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. Activation codes are available on the card shipped with your product or, for downloaded products, in the GTA Support Center after purchase.

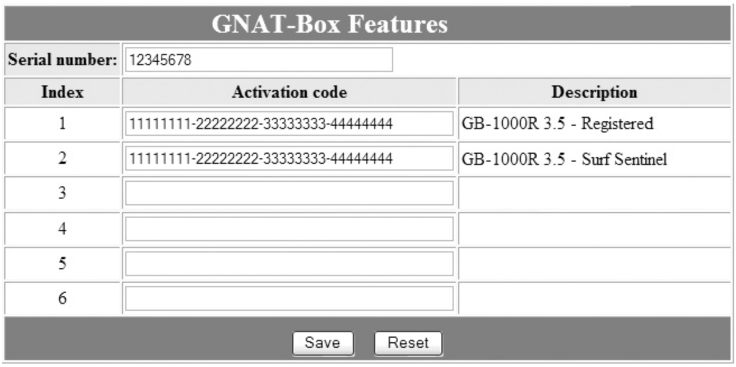
Additional entry spaces will be added as codes are entered and saved. Up to twenty (20) activation codes may be entered in the Features screen.

It is ***not*** necessary to delete old activation codes. If you would like to delete an entry, remove all of the code characters and select **SAVE**.

To add entries in GBAdmin, click the **ADD +** button and then select **SAVE**. To delete saved codes, click **DELETE** (**×**), then select **SAVE**. The **RELOAD** button reverts to previously saved information if you have not yet saved the section.

### *Note*

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



GNAT-Box Features

Serial number: 12345678

| Index | Activation code | Description |
|---|---|---|
| 1 | 11111111-22222222-33333333-44444444 | GB-1000R 3.5 - Registered |
| 2 | 11111111-22222222-33333333-44444444 | GB-1000R 3.5 - Surf Sentinel |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

*Features*

# Network Information

Much of the Network Information data will have been entered during installation, including the required Protected and External Networks. For information on initial configuration during installation, see your firewall product guide.

## Logical Interfaces

The GTA Firewall requires two logical networks, a Protected and an External network, except when in bridging mode. (See more about bridging mode on page 13.) Additional external and protected logical networks can be added, as well as one or more Private Service Networks (PSN).

A logical interface assigns a network (represented by an IP address and netmask) to a physical network interface; designates a method to access it; and identifies it as a gateway (default route).

The logical interface name serves as an Interface Object, allowing the administrator to reference the interface quickly when configuring the firewall.

Logical network interfaces that do not use PPP 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.

### Interface Object Names

Interface Object names may not use a number as the first character.

Use caution when changing the logical names of interfaces; if a logical name is changed, but an Allow filter that references it is not, you will lose the connection maintained by the filter.

To change any 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. After saving the new object, you may delete the original. Alternatively, to change interface 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.

### 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 CIDR-based notation 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: 11111111.111 11111.11111111.11110000. The notation would be “/28”.

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

Dotted decimal may still be used by entering the dotted decimal netmask after the forward slash.

## Host Name

The host name is the system name assigned to the GTA Firewall and used to tag log messages. GTA recommends using a fully qualified domain name as the host name for your GTA Firewall. A fully qualified domain name is the complete domain name for a specific computer (host) on the Internet, consisting of a host, domain, and top-level domain; e.g., gtafirewall.example.com, or www.gta.com. Host names must be unique. If your network DHCP servers make IP address assignments based on the system name, enter the host name, often assigned by your ISP.

## Default Gateway

On a static interface, enter the IP address of the selected default route in the DEFAULT GATEWAY field. This value is usually the IP address of the router connecting the network to the Internet and must be on the same logical network as the associated External interface, except when using PPP.

The gateway value will be set automatically on a dynamically negotiated interface (DHCP or PPP). On the Web interface, select the Default Gateway checkbox for the DHCP or PPP network in the Logical Interfaces section to make the network the default gateway (default route) to the Internet.

In GBAdmin, select the interface object of the DHCP or PPP connection from the Default Gateway dropdown list.

***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.

## Network Information – Logical Interfaces, Host Name, Gateway

Logical Name Interface Object name for this logical network interface.

Type Interface type: Protected, External or PSN.

IP address IP address/netmask assigned to this logical interface. PPP or DHCP connections do not require an IP address.

NIC (& PPP) Network interface device (see Physical Interface/NIC, below) to associate with the network. The dropdown box lists all physical devices on the firewall, including PPP connections. For PPP, configure a PPP/PPPoE/PPTP connection (PPP0, 1, 2, 3 or 4), then select it here.

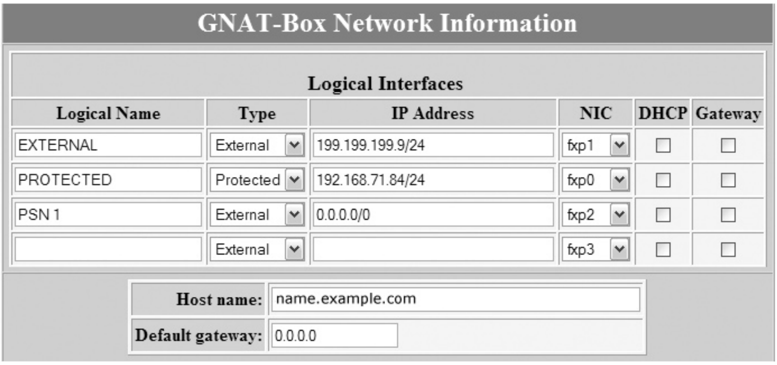
DHCP Dynamic Host Configuration Protocol. When selected, DHCP is used to obtain an IP address for the specified interface. DHCP is typically required for cable modem connections, but may be used on any network interface.

Gateway (Web only). Make the interface the Internet gateway (default route) on a dynamic interface (PPP or DHCP).

**Host Name** Identifying system name for the firewall. GTA recommends using a fully qualified domain name

**Default Gateway** Selected default route on a static interface.

**GBAdmin**: when the gateway is dynamic, select the gateway's logical interface/object.



GNAT-Box Network Information

Logical Interfaces

| Logical Name | Type | IP Address | NIC | DHCP | Gateway |
|---|---|---|---|---|---|
| EXTERNAL | External | 199.199.199.9/24 | fxp1 | □ | □ |
| PROTECTED | Protected | 192.168.71.84/24 | fxp0 | □ | □ |
| PSN 1 | External | 0.0.0.0/0 | fxp2 | □ | □ |
|  | External |  | fxp3 | □ | □ |

Host name: name.example.com

Default gateway: 0.0.0.0

*Network Information – Logical Interfaces, Host Name and Default Gateway*

## Bridged Interfaces

In Bridged Interfaces, additional interfaces can be configured to share the IP address of one of the primary logical interfaces. TCP/IP packets pass between these bridged interfaces according to normal firewall rules on specified ports if allowed by a Pass Through filter. Packets with non-TCP/IP Ethernet protocols that have been allowed in Bridged Protocols can bypass all filtering between the bridged interfaces.

### Bridging Mode

In default mode, a GTA Firewall acts as a firewall router, so that systems on the internal network see it as a gateway to the external network, and systems on the external network see it as the gateway to the internal network.

Using bridging mode, a GTA Firewall connects networks transparently like a bridge for specified Ethernet protocol types, while continuing to filter other IP packets as a firewall.

***Caution***

There is no firewall filtering of the protocol types that have been allowed in Bridged Protocols.

A GTA Firewall in bridging mode can be inserted behind a router to the Internet between the router and the internal networks without changing IP addresses, gateways or any other network addresses.

A GTA Firewall in bridging mode can also be inserted in an internal network to separate networks that are at a peer level, or to further segregate Private Service Networks. This configuration allows two internal networks to communicate as one, while filtering non-bridged IP traffic between them and preventing the passage of non-IP data (except ARP, which operates at both data link layer 2, and network layer 3).

In bridging mode, a GTA Firewall can be connected directly to a host, a switch, a router or a non-bridged GTA Firewall.

***Note***

Bridging can only be configured in GBAdmin or the Web interface.

#### Gateway Selector

In order for gateway selection (see **Routing/Gateway Selector**) to function correctly in bridging mode, the host must use the IP address of a logical interface on the firewall as its gateway.

### Services

The $H_2A$ High Availability service is not supported in bridging mode.

PPP, PPPoE and PPTP are not supported in a bridged interface.

If a host points to a router or gateway on a bridged interface as its default route to the Internet, the firewall will still route the packet through its logical External Network interface.

Also, in bridging mode (as in unbridged firewall operation) any packet that goes through the firewall will use the firewall's routing tables. This means that even though a host has indicated a particular route, the firewall will use the routes set up in Static Routing and RIP to route the traffic.

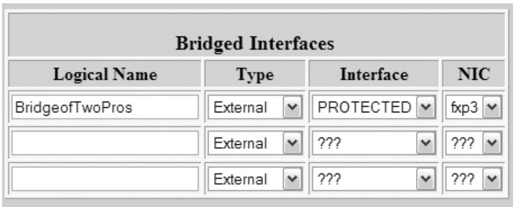
## Network Information – Bridged Interfaces

Logical Name Interface Object name for this bridged logical interface.

Type Interface type: Protected, External or PSN.

Interface Logical Interface to which to bridge the network interface card/physical interface in the NIC field.

NIC Network interface device (see NICs or Physical Interfaces, below) to associate with the bridged network. The dropdown box lists all physical devices on the firewall.



Bridged Interfaces

| Logical Name | Type | Interface | NIC |
|---|---|---|---|
| BridgeofTwoPros | External | PROTECTED | fxp3 |
| | External | ??? | ??? |
| | External | ??? | ??? |

*Network Information – Bridged Interfaces*

## Network Interface Cards (NICs) or Physical Interfaces

Physical interfaces are supported and configured network interface devices detected by the system, including configured PPP connections.

### Network Information – NICs or Physical Interfaces

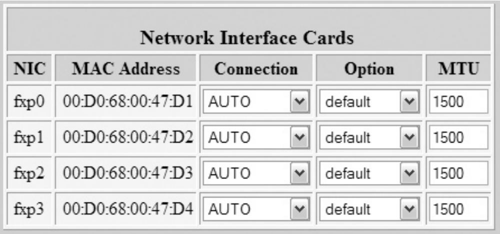
NIC (& PPP) Network interface devices detected, including configured PPP connections.

MAC Address If the physical interface device is an Ethernet card, the card's MAC address will be displayed. Record MAC addresses before installing system software.

Connection AUTO is generally recommended. Selections are:
AUTO: Auto-select the active network connection.
UTP_10: Unshielded twisted pair interface at 10Mbps.
TX_100: Unshielded twisted pair interface at 100Mbps.

Option Default (full- ***or*** half-duplex) or Full Duplex.

MTU Maximum Transmission Unit. Default is 1500.
Incorrect MTUs can cause poor performance, but it may be beneficial to increase MTU for a Gigabit Ethernet interface when jumbo packets are to be used.



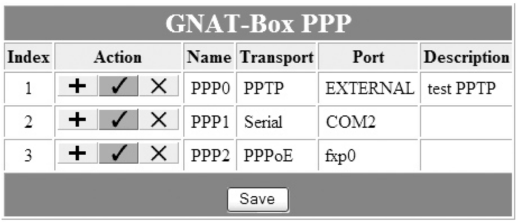
**Network Interface Cards**

| NIC | MAC Address | Connection | Option | MTU |
|---|---|---|---|---|
| fxp0 | 00:D0:68:00:47:D1 | AUTO | default | 1500 |
| fxp1 | 00:D0:68:00:47:D2 | AUTO | default | 1500 |
| fxp2 | 00:D0:68:00:47:D3 | AUTO | default | 1500 |
| fxp3 | 00:D0:68:00:47:D4 | AUTO | default | 1500 |

*Network Information - NICs*

# PPP

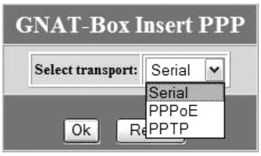
The PPP section is the location to configure a PPP (Point-to-Point Protocol), PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Transport Protocol) connection for the firewall. ***After*** creating the configuration in the PPP section, enable the connection in the Network Information section by associating the configuration with the chosen logical interface.



GNAT-Box PPP

| Index | Action | Name | Transport | Port | Description |
|---|---|---|---|---|---|
| 1 | + ✓ × | PPP0 | PPTP | EXTERNAL | test PPTP |
| 2 | + ✓ × | PPP1 | Serial | COM2 | |
| 3 | + ✓ × | PPP2 | PPPoE | fxp0 | |

*PPP list*



GNAT-Box Insert PPP

Select transport: Serial

*Insert PPP/Select Transport Protocol*

In GBAdmin, create a new PPP configuration by selecting the **ADD +** (plus) button from the toolbar, creating a blank PPP tab with three sub-tabs. Create a PPPoE configuration by selecting the PPPoE or PPTP checkbox, which changes the selections on each sub-tab.

## PPPoE

PPPoE has become widely deployed as a method of assigning IP addresses for DSL service providers.

### *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/PPPoE 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.

***Caution***

PPP connections are automatically named PPP0, 1, 2, 3 or 4, in order of creation. When an entry in the PPP section is deleted, the remaining entries will be renamed according to the new order. Interfaces which use PPP connections must be changed to the revised designations.

## PPTP

PPTP (Point-to-Point Tunneling Protocol) is a specialized PPP (point-to-point) transport protocol for some Microsoft products. A PPTP connection allows a link from a non-routable internal IP address to an external IP address through the use of an internal PPTP server with a routable IP address. To configure a PPTP connection, select PPTP in the **Insert PPP** dialog box.

### Select PPTP in Network Information

After configuring PPTP, go to Network Information to set up an External interface using the PPTP connection. In the Name field, enter an interface object name for the connection. In the Type field, select External, then enter the IP address assigned to the PPTP connection. Select PPTP from the NIC dropdown box. Finally, select the **GATEWAY** checkbox and save the section.

#### Enable the PPTP Connection

Open PPTP again. Select the Interface Object created in Network Information and save the section.

### Create a Remote Access Filter

A Remote Access Filter must be defined and enabled to allow GRE (Generic Routing Encapsulation) access to the PPTP server. Once you have completed the PPTP connection, auto-configure the Remote Access Filter set using the **DEFAULT** button, or manually add a filter similar to the one below in which the Source is the IP address for the ISP and Destination is the PPTP server IP address. Auto-configured filters are broad in scope and may require modification to meet your security policy. Once the settings have been saved, the PPTP connection will dynamically negotiate the gateway IP address.

**PPTP Remote Access Filter**

| | |
|---:|---|
| Description: | Allow GRE from PPTP server. |
| Type: | Accept |
| Interface: | ANY |
| Authentication required: | Select |
| Protocol: | GRE (Protocol 47) |
| Source: | **<Use IP address>** e.g., 192.168.71.220 |
| Destination: | **<Use IP address>** e.g., 10.0.0.81 |

Fields not illustrated above can use the defaults or custom settings.

## PPP, PPPoE, PPTP – Standard Fields

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.

Connection Type ***Dedicated***
Establishes a link when the firewall boots up and remains up until the interface is manually disabled, or the system is halted. Select for PPTP. The logical choice for PPPoE, as DSL is an “always on” connection. Select to test a configuration.

***On-demand***
Initiates and establishes a 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 timeout has expired.

***On-enabled***
Requires manually enabling the External interface to initiate a session and establish a link with the remote site. The link will stay established until disabled. Interfaces may easily be enabled/disabled in **Administration/Interfaces**.

Transport Select in the Insert PPP dialog box.
GBAdmin: enable by selecting the checkbox.

NIC** Network interface on which PPPoE will run.

Interface*** Select the interface defined in Network Information.

PPTP server*** Enter IP address of the internal PPTP server.

Primary COM Port* COM Port used for the PPP interface. COM 1-4 are allowed, except GB-1000: COM 2, and RoBoX: COM 1.

Phone Number* Number used to dial the remote site. This field should contain any required access codes, e.g., “9” to dial out. Characters used for pauses and secondary dial tones can be used. Consult your modem or ISDN TA manual for dialing codes.

User Name User ID for remote access; password and user ID are generally issued by the remote site.

Password Password remote access, obscured in the data field.

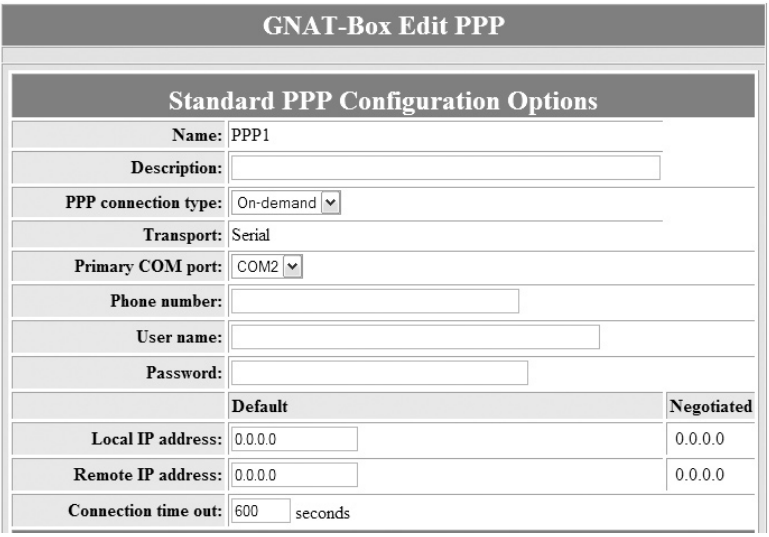
Local IP address A PPP-type link uses a local and remote IP address.

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 — Number of seconds during which a connection will stay connected when inactive. To prevent timing out, enter “0.” Default is 600 (10 minutes).

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

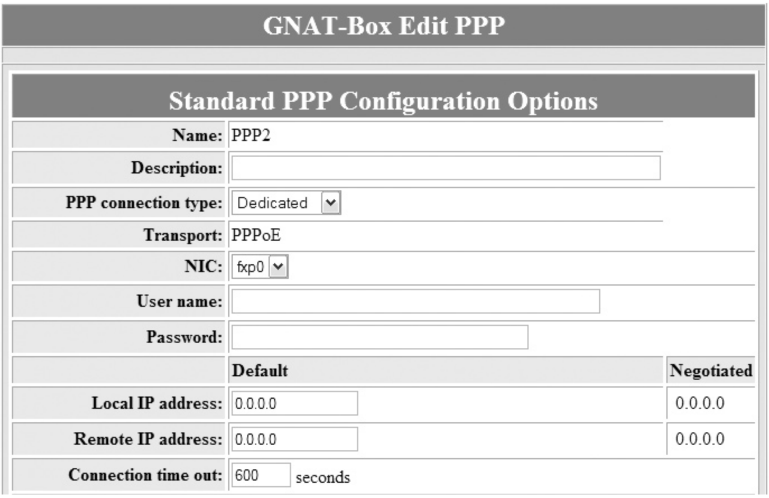


GNAT-Box Edit PPP

Standard PPP Configuration Options

| | | |
|---|---|---|
| Name: | PPP1 | |
| Description: | | |
| PPP connection type: | On-demand | |
| Transport: | Serial | |
| Primary COM port: | COM2 | |
| Phone number: | | |
| User name: | | |
| Password: | | |
| | Default | Negotiated |
| Local IP address: | 0.0.0.0 | 0.0.0.0 |
| Remote IP address: | 0.0.0.0 | 0.0.0.0 |
| Connection time out: | 600 seconds | |

*PPP Serial*

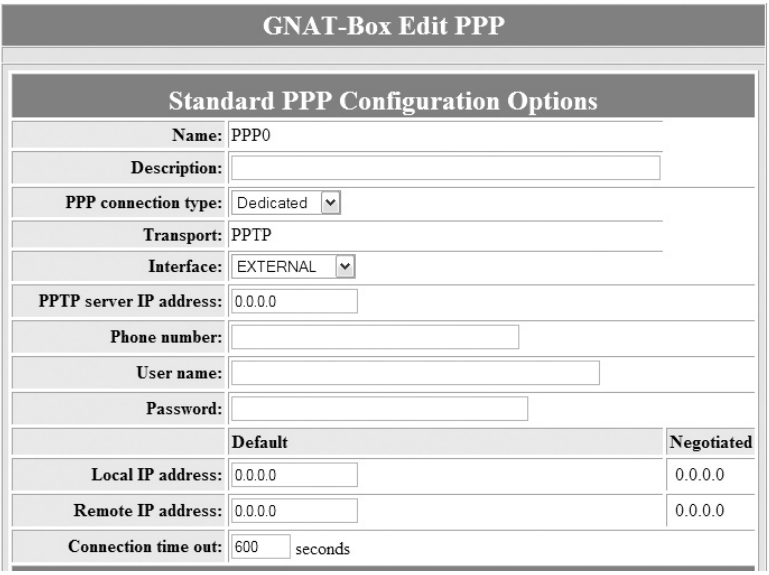


GNAT-Box Edit PPP

Standard PPP Configuration Options

| | | |
|---|---|---|
| Name: | PPP2 | |
| Description: | | |
| PPP connection type: | Dedicated | |
| Transport: | PPPoE | |
| NIC: | fxp0 | |
| User name: | | |
| Password: | | |
| | Default | Negotiated |
| Local IP address: | 0.0.0.0 | 0.0.0.0 |
| Remote IP address: | 0.0.0.0 | 0.0.0.0 |
| Connection time out: | 600 seconds | |

*PPPoE*



GNAT-Box Edit PPP

Standard PPP Configuration Options

| | | |
|---|---|---|
| Name: | PPP0 | |
| Description: | | |
| PPP connection type: | Dedicated | |
| Transport: | PPTP | |
| Interface: | EXTERNAL | |
| PPTP server IP address: | 0.0.0.0 | |
| Phone number: | | |
| User name: | | |
| Password: | | |
| | Default | Negotiated |
| Local IP address: | 0.0.0.0 | 0.0.0.0 |
| Remote IP address: | 0.0.0.0 | 0.0.0.0 |
| Connection time out: | 600 seconds | |

*PPTP*

## PPP, PPPoE, PPTP – Additional Fields

PPPoE Provider** Designation for the PPPoE Provider. Leave 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 setting the field 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 is the speed at which the firewall communicates with the modem. Options: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200, 230400.

Number of retries Number of attempts the system will make to establish a connection. After failure, any new packets arriving for the External Network will restart a new dialing attempt. Dedicated connections do not use retries; they continue to try to connect. Default is 3.

Time before retry This is the amount of time the system waits before re-dialing to establish a connection. Default is 10 seconds.

### Link Control Protocol

Each LCP option has a pair of settings for side of the link: Enable for local and Accept for remote. 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 data in the logs to determine which options have been requested and rejected. Match your LCP settings to the desired requests.

### ISDN*

Use to configure ISDN (Integrated Services Digital Network) 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

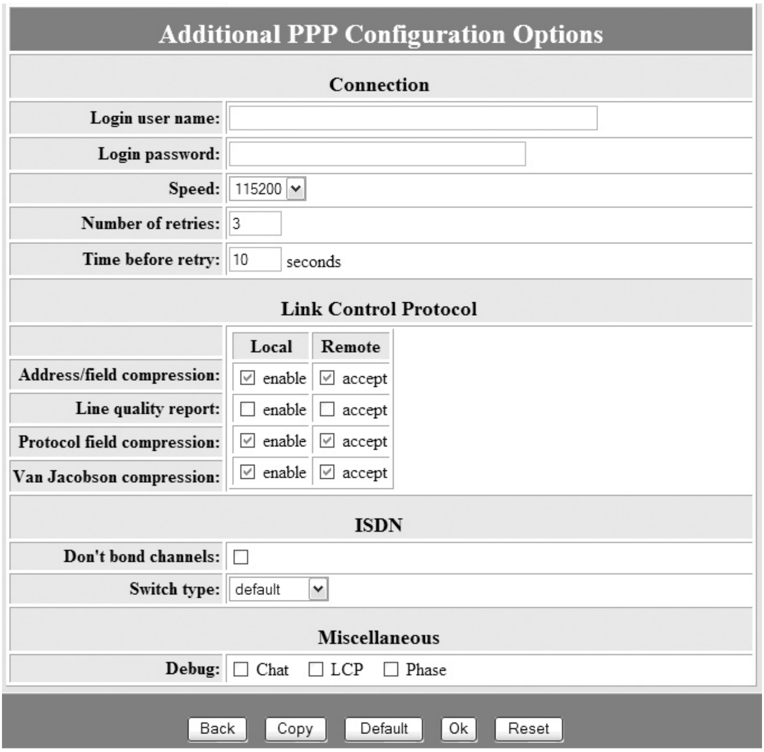
These options provide helpful information when creating a PPP configuration.

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. *** PPTP screens only.**



Additional PPP Configuration Options

Connection

Login user name:

Login password:

Speed: 115200

Number of retries: 3

Time before retry: 10 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

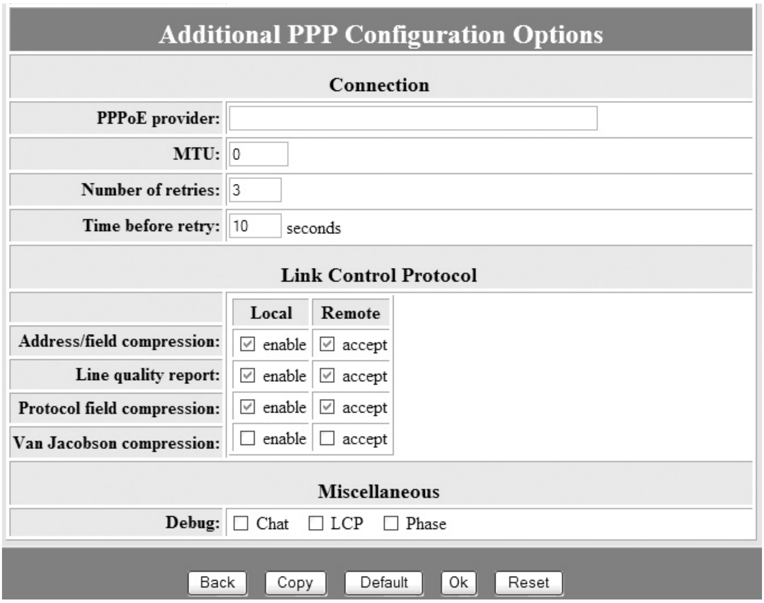
Don't bond channels: □

Switch type: default

Miscellaneous

Debug: □ Chat □ LCP □ Phase

*PPP Serial*



## Additional PPP Configuration Options

### Connection

| | |
|---|---|
| **PPPoE provider:** | |
| **MTU:** | 0 |
| **Number of retries:** | 3 |
| **Time before retry:** | 10 seconds |

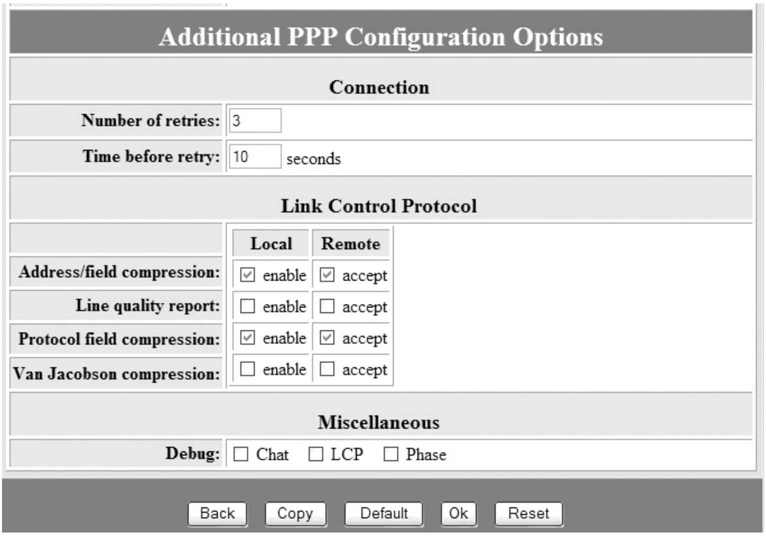
### Link Control Protocol

| | 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*



## Additional PPP Configuration Options

### Connection

| | |
|---|---|
| **Number of retries:** | 3 |
| **Time before retry:** | 10 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

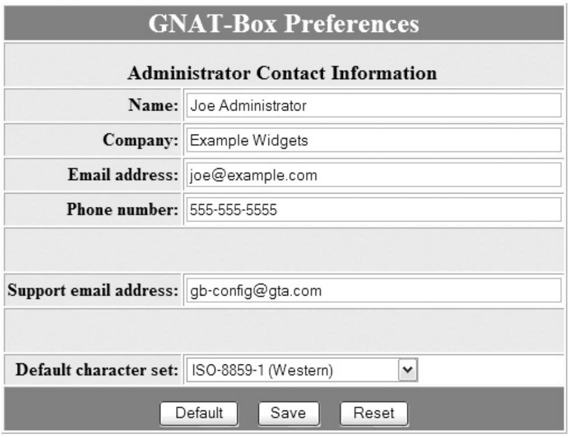
*PPTP*

# Preferences (Contact Information)

The Preferences facility stores contact information used by email, report and list functions.

## Preferences Fields

| | |
|---|---|
| | **Administrator Contact Information** |
| Name | Primary contact name. |
| Company | Company or organization name. |
| Email address | Email address of the contact. |
| Phone number | Phone number of the contact. |
| Support email | Email support address, supplied by GTA or your Authorized GTA Firewall Reseller. |
| Character set | (Web Only) Select the appropriate character set. |



GNAT-Box Preferences

Administrator Contact Information

Name: Joe Administrator

Company: Example Widgets

Email address: joe@example.com

Phone number: 555-555-5555

Support email address: gb-config@gta.com

Default character set: ISO-8859-1 (Western)

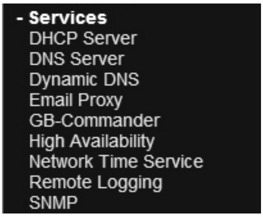
*Preferences (Contact Information)*

# 3 Services

Services contains configuration sections for DHCP Server and DNS Server; Dynamic DNS; the Email Proxy; GB-Commander Server; $H_2A$ High Availability; Network Time Service; Remote Logging; and the SNMP facility. None of these services are required for the GTA Firewall, but many of them can increase network functionality and security. Some services are optional on select GTA firewalls.

***Note***

GTA suggests running Email Proxy to increase network security.



*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 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.

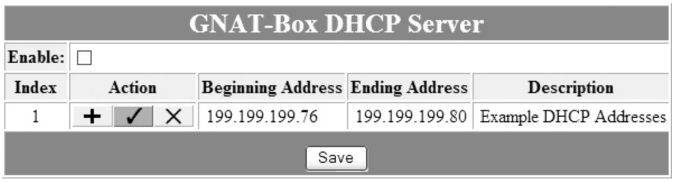
Changes to DHCP will not be applied until the section is saved. If a network connection is established and the section is saved, the DHCP Server changes will be applied immediately to the GTA Firewall.

***Note***

If the DHCP service is for an external network, then the default gateway is most likely the Internet router's IP address.

## DHCP Fields

| | |
|---|---|
| Disable | Disable this DHCP IP address pool. |
| Description | Description of the DHCP IP address pool. |
| Beginning Address | First IP of a block of IPs that will be assigned. |
| Ending Address | Last IP of a block of IPs that will be assigned. |
| Netmask | Netmask to assign to DHCP clients. |
| Lease Duration | 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 address ranges to exclude from each DHCP range. To exclude a single IP address, enter it in both the beginning and ending address fields. |
| Domain Name | DNS domain name, typically, that of the local network. |
| Name Server IP address | IP address of a DNS server that will be issued to the requesting client. This 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 | 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. |

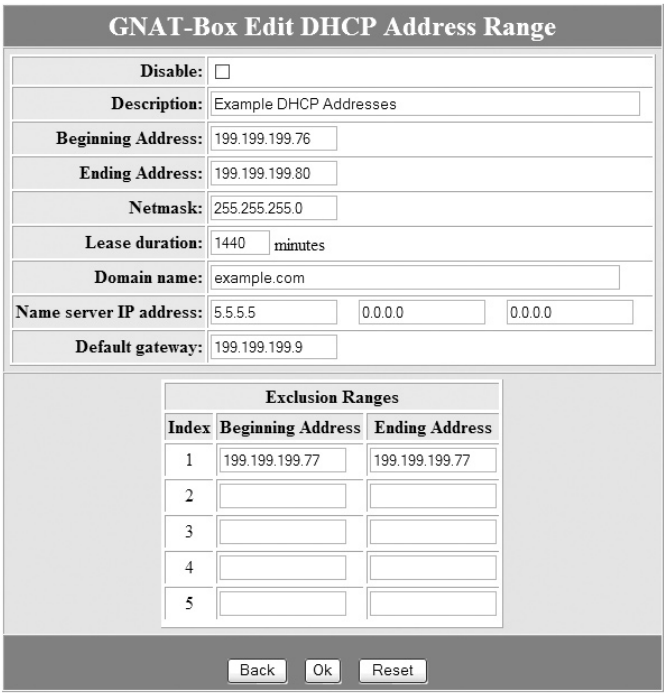


GNAT-Box DHCP Server

Enable: □

| Index | Action | Beginning Address | Ending Address | Description |
|---|---|---|---|---|
| 1 | + ✓ ✕ | 199.199.199.76 | 199.199.199.80 | Example DHCP Addresses |

*DHCP Server List*



GNAT-Box Edit DHCP Address Range

| | |
|---|---|
| Disable: | □ |
| Description: | Example DHCP Addresses |
| Beginning Address: | 199.199.199.76 |
| Ending Address: | 199.199.199.80 |
| Netmask: | 255.255.255.0 |
| Lease duration: | 1440 minutes |
| Domain name: | example.com |
| Name server IP address: | 5.5.5.5 0.0.0.0 0.0.0.0 |
| Default gateway: | 199.199.199.9 |

Exclusion Ranges

| Index | Beginning Address | Ending Address |
|---|---|---|
| 1 | 199.199.199.77 | 199.199.199.77 |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

*DHCP Server Address Range*

### *Note*

The network defined for DHCP must match one of the networks assigned to the firewall interfaces.

In GBAdmin, first click the Enable checkbox to allow DHCP to be edited, then click **ADD +** to insert a DHCP service. Select the inserted line. Once the fields have been 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 DNS (Domain Name System) Server section allows the firewall to be configured to function as a primary Domain Name Server, maintaining a database of domain names (host names) and their corresponding IP addresses. Enabling the DNS Server section overrides the DNS proxy in the **Basic Configuration/DNS** section. On some firewall products, DNS Server is optional and requires an activation code. See your product guide for more information.

GTA recommends a thorough knowledge of the domain name system before configuring any DNS server. One reference is **DNS and Bind, 3rd Edition**, by Paul Albitz & Cricket Liu, published by O'Reilly and Associates.

The built-in DNS server 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

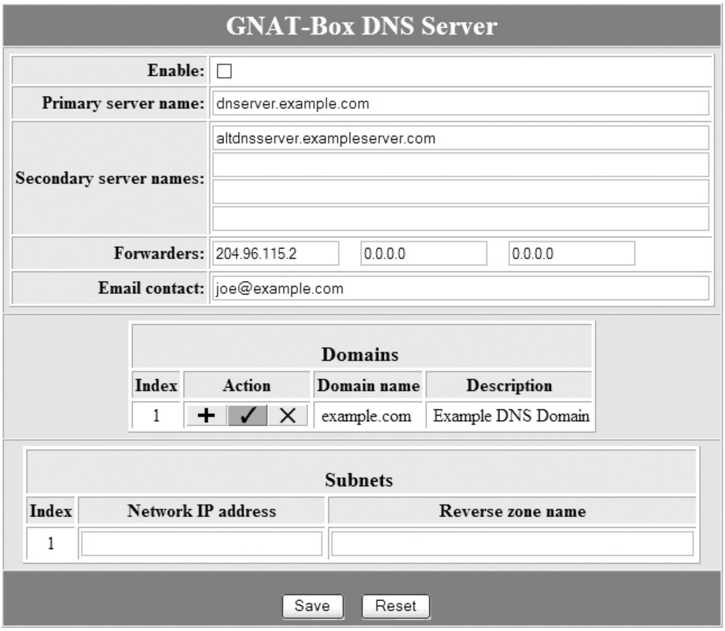
| | |
|---|---|
| Enable | Enable the DNS server. Disabled by default. |
| Primary server | Host name of your DNS server. This will be a host name assigned to your GTA Firewall. When configuring an external DNS server, this will be the host name seen from the Internet side. The host name should be listed as a host in the DNS Domain screen or tab. |
| Secondary server | Host names of DNS servers acting as alternate server for the domain. Up to four alternates may be listed. |
| Forwarders | DNS servers that will be utilized as DNS forwarders. |
| Email contact | Email address of the primary contact for the domain (e.g., administrator@example.com). |
| **Domains*** | See DNS Domain Fields. |

**Subnets***

Subnets make a large network more manageable
by splitting it into a series of contiguous address ranges.

| | |
|---|---|
| Network IP address | 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.<br>Reverse zone names are typically assigned by your ISP. |

* See your product guide for the number of DNS domains and subnets available.



GNAT-Box DNS Server

| | |
|---|---|
| Enable: | □ |
| Primary server name: | dnserver.example.com |
| Secondary server names: | altdnsserver.exampleserver.com |
| Forwarders: | 204.96.115.2 0.0.0.0 0.0.0.0 |
| Email contact: | joe@example.com |

Domains

| Index | Action | Domain name | Description |
|---|---|---|---|
| 1 | + ✓ × | example.com | Example 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 Disable the domain definition so the zone will not be served by the GTA Firewall name server.

Description Description of the domain for reference.

Domain name Domain name for the defined zone, (e.g., gta.com).

Domain IP address 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, meaning that if you have a web server, a visitor can use the zone name rather than the web server's 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, the order of preference is specified 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.

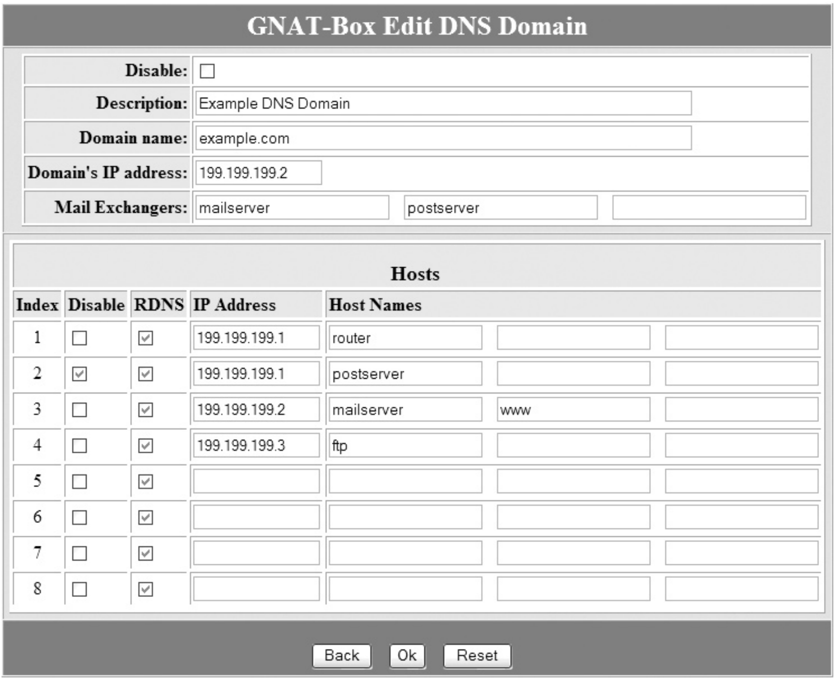
**Hosts**

Disable 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 IP address of the host.

Host Names 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:** | Example DNS Domain | | |
| **Domain name:** | example.com | | |
| **Domain's IP address:** | 199.199.199.2 | | |
| **Mail Exchangers:** | mailserver | postserver | |

**Hosts**

| Index | Disable | RDNS | IP Address | Host Names | | |
|---|---|---|---|---|---|---|
| 1 | □ | ☑ | 199.199.199.1 | router | | |
| 2 | ☑ | ☑ | 199.199.199.1 | postserver | | |
| 3 | □ | ☑ | 199.199.199.2 | mailserver | www | |
| 4 | □ | ☑ | 199.199.199.3 | ftp | | |
| 5 | □ | ☑ | | | | |
| 6 | □ | ☑ | | | | |
| 7 | □ | ☑ | | | | |
| 8 | □ | ☑ | | | | |

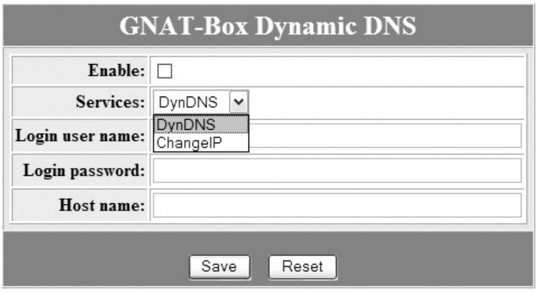
*DNS Domains*

In GBAdmin, to add a secondary name server, forwarder or subnet, click the **ADD +** button next to these fields. To add a DNS Domain, add a tab to the screen below the SUBNET field by clicking the **ADD +** button on the toolbar. To edit a specific DNS Domain, click on the domain name tab. To add a mail exchanger or a host to the DNS Domain, click the **ADD +** button next to these fields. To enter more than one alias, separate aliases with a space.

## Dynamic DNS

Dynamic DNS (DDNS) automates the process of advising DNS servers when the automatically assigned IP address for a network device is changed, ensuring that a specific domain name always points to the correct machine. The domain name tracks the dynamic address so that other users on the Internet can easily reach the domain, allowing you to host a website, FTP server or email server, even when your IP address is dynamic.

GTA's Dynamic DNS service allows you to connect your dynamic IP address from DHCP, PPP, PPPoE or PPTP by selecting one of these services from the dropdown menu: **DynDNS** at **www.dyndns.org** or **ChangeIP** at **www.changeip.com**. The currently used External IP address on the GTA Firewall will update to the selected service each time the IP address changes, or once every month, whichever comes first. To sign up for DDNS services from one of these providers, and for more information about using Dynamic DNS, see the provider's website.



GNAT-Box Dynamic DNS

| | |
|---|---|
| Enable: | □ |
| Services: | DynDNS |
| Login user name: | |
| Login password: | |
| Host name: | |

*Dynamic DNS*

### Dynamic DNS Fields

| | |
|---|---|
| Enable | Enable Dynamic DNS service. Disabled by default. |
| Services | Select Dynamic DNS service from the dropdown list. |
| Login user name | User name for selected service. |
| Login password | Password for selected service. |
| Host name | Host name of the service that will perform Dynamic DNS. |

# Email Proxy

The Email Proxy is used to configure an SMTP (Simple Mail Transfer Protocol) proxy for inbound email on TCP port 25. Email Proxy can be used to shield an internal email server from unauthorized access and reduce or eliminate unsolicited email (spam). The Email Proxy will respond on any IP address assigned to the External Network interface, unless a tunnel is created on TCP port 25.

***Caution***

> The IP address that receives mail for the Email Proxy should not be used in an inbound tunnel on TCP port 25. A tunnel on port 25 using this IP address will bypass the Email Proxy.

## Email Headers

Email Proxy on the GTA Firewall appends the Received, To and From addresses contained in the initial SMTP (Simple Mail Transfer Protocol) conversation as X-GB-Received, X-GB-To and X-GB-From. The prefix shows that this header was appended by a receiving GNAT Box system firewall, as in the following example:

```
X-GB-Received: from domain.example.com (192.168.71.9) by
gtafirewall.yourcompany.com (3.5.0)
```

```
X-GB-From: sendername@sendexample.com
X-GB-To: recipient@yourcompany.com
```

The “X-GB-Received” line contains the domain name/host where the email originated, followed by the host name and IP address of the receiving firewall. The “X-GB-From” line contains the email address of the sender. (The originating domain and the domain in the sender’s email are not necessarily the same.) The “X-GB-To” line contains the email address of the intended recipient at your company’s domain.

GTA recommends that the host name be a fully qualified domain name (FQDN), as in the example above. The firewall host name is entered in the Host Name field of the **Basic Configuration/Network Information** section.

## RDNS

Selecting the option “Reject if RDNS fails” performs a Reverse DNS lookup on the IP address of the remote host trying to make an SMTP connection, and then compares it to a DNS lookup of the returned host name. If the lookup fails or doesn’t match, the connection is refused. RDNS requires a defined DNS Server to function correctly.

***Note***

> If “Reject if RDNS failed” is selected, legitimate hosts with misconfigured DNS entries will not be able to deliver to your domain.

## Unsolicited Email

The Email Proxy compares the source IP address of incoming messages to the IP addresses of known spammers listed in the enabled Mail Abuse Prevention RBLs (Realtime Blackhole Lists). If a source matches one of these, the IP address is logged, and the message is permanently rejected (the firewall returns a “do not send again” packet to the source IP address) and dropped.

### Mail Abuse Prevention Lists

Providers listed in Mail Abuse Prevention maintain lists of hosts and domains known to transmit or generate spam. These are only a sample of the many lists available; you may enter other providers in lieu of the default providers listed. Some lists require a subscription; for more information, go to the provider’s website.

### Email Proxy Fields

| | |
|---|---|
| Enable | Enable the Email Proxy. Disabled by default. |
| | **Connections** |
| Primary email server | 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 for the Email Proxy to operate. |
| Alternate | Host name (if using an internal DNS server) or IP address of any alternative email server. |
| Timeout | Time to wait between each SMTP command exchange. Default is 120 seconds. |
| Maximum | Number of simultaneous SMTP connections to run. Others are deferred until a connection is available. Each connection invokes a copy of the SMTP proxy facility. |
| | **Domains to Accept** |
| Domain List | Domains from which to accept email; 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. Separate domains with a white space (blank or tab) or a comma. |

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**

Reject if RDNS fails  Performs a Reverse DNS lookup on the remote host and refuses the connection if the lookup fails to match.

Maximum size  Maximum size (in kilobytes) of email message to be accepted. Prevents “email bombs” (large attachments that cause problems for email clients). Enter “0” (zero) not to restrict the size of email messages.

**Mail Abuse Prevention**

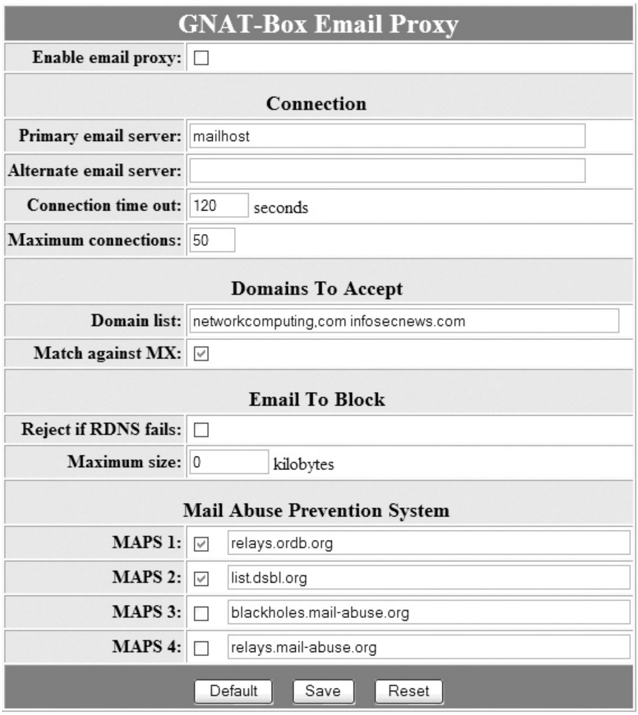
MAPS 1  relays.orbd.org. Open Relay DataBase `www.orbd.org`

MAPS 2  list.dsbl.org. Distributed Server Boycott List `www.dsbl.org`

MAPS 3  blackholes.mail-abuse.org* `www.mailabuse.org`

MAPS 4  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: mailhost

Alternate email server:

Connection time out: 120 seconds

Maximum connections: 50

Domains To Accept

Domain list: networkcomputing,com infosecnews.com

Match against MX: ☑

Email To Block

Reject if RDNS fails: □

Maximum size: 0 kilobytes

Mail Abuse Prevention System

MAPS 1: ☑ relays.ordb.org

MAPS 2: ☑ list.dsbl.org

MAPS 3: □ blackholes.mail-abuse.org

MAPS 4: □ relays.mail-abuse.org

*Email Proxy*

## GB-Commander

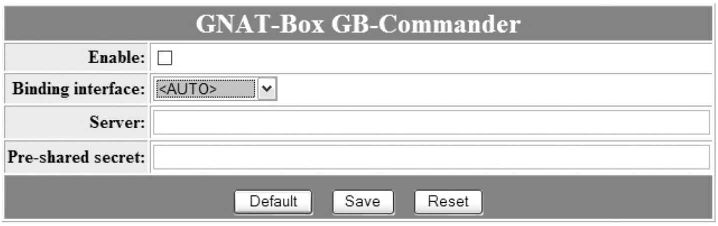
GB-Commander, GTA's Windows-based product option for firewall management, allows an administrator to monitor multiple firewalls from a central location, increasing efficiency and reducing monitoring costs. GTA Reporting Suite, included with GB-Commander, provides summary charts and reports for quick analysis of network usage and trends to identify potential connectivity or security issues. GB-Commander features include:

- Monitor multiple GTA Firewalls using one user-friendly interface.
- Define hierarchies for monitoring and configuration.
- Display status, statistics and alarms for each monitored firewall.
- Process alarm events and send notifications.
- Launch remote administration client to configure individual firewalls.
- Launch GTA Reporting Suite to chart collected data.
- Available for all GTA firewall products.

GB-Commander must be purchased and activated before these features will function. See the **GB-Commander Product Guide** and **GTA Reporting Suite Product Guide** for more information.

To initially configure a firewall to communicate with the GB-Commander Server, leave the Binding Interface field set to **Auto**. The interface is used by the firewall to communicate with the GB-Commander Server when using High Availability or accessing the GB-Commander Server through a VPN. For most configurations, leave the field undefined so that the firewall will detect the correct IP address. Enter the IP address of the GB-Commander Server and modify the default port number, if desired.

For information on the firewall's time zone and GB-Commander, see **Chapter 11 – Administration, Set Date/Time**.



GNAT-Box GB-Commander

| | |
|---|---|
| Enable: | □ |
| Binding interface: | <AUTO> |
| Server: | |
| Pre-shared secret: | |

*GB-Commander Server*

### Note

Once GB-Commander is activated and GB-Commander Server is configured, logs are sent to GB-Commander Server with bandwidth and alarm data.

### GB-Commander Server

| | |
|---|---|
| Enable | Enable communication from the firewall to GB-Commander Server. GB-Commander must be activated to use this option.* |
| Binding interface | Address from which GB-Commander server is sourced. Selecting Auto will indicate the firewall's usual source IP address to the server location. To force the data packets to have a specific source IP address, choose the Interface object from the dropdown list. Auto by default. |
| Server | IP address or host name of a system that will accept the GB-Commander server data. To enter a different port number, use the standard format, e.g., `192.168.71.2:76` or `example.gta.com:76`. Port 76 by default. |
| Preshared secret | ASCII or HEX value. Preshared secret as defined in the GB-Commander service. This field is case-sensitive. |

* GB-Commander is activated separately, and does not require a feature activation code on the firewall.

## High Availability

$H_2A$ High Availability allows two systems to operate as a single virtual firewall, ensuring that network access and security are maintained with minimum downtime. The section allows the firewall to be configured as one of an high availablity pair or group. The service requires no obvious changes to your existing network, making it transparent to end-users. $H_2A$ High Availability is an option available on some GTA firewalls and requires a feature activation code. The **$H_2A$ High Availability Feature Guide** details how to configure and utilize the option.

***Note***

$H_2A$ High Availability is not supported in bridging mode.

### High Availability Fields

| | |
|---|---|
| Enable | Enable $H_2A$. A feature code is required to use this option. |
| Status | $H_2A$ mode: Init, Slave or Master will display. Not editable. |
| VRID | Value between ***0 and 15*** for the VRID (Virtual Router ID), used to uniquely identify the $H_2A$ group. All systems in the group must have the same VRID. |
| Priority | Number between ***1 and 255.*** The system with the highest priority and confirmed communications with beacons will operate in Master mode. This system will process network traffic as the virtual (operational) firewall. If the priority numbers are not set, the pair will select the Master by automatically giving one system higher priority. |

Email Notification
Receive an email when $H_2A$ status changes.

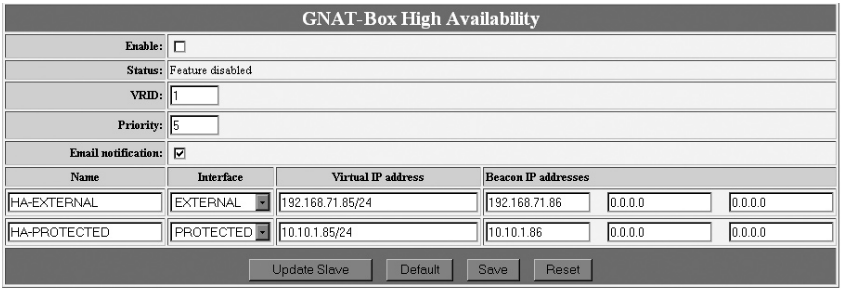
Name
Name to identify this member of the $H_2A$ group.

Interface*
Interface on which this high availability member resides. 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 again.

Virtual IP address
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 referenced by the INTERFACE field.

Beacon
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 the only beacon. This can lead to improper functioning of the $H_2A$ group.

* $H_2A$ systems cannot use dynamically assigned interfaces.

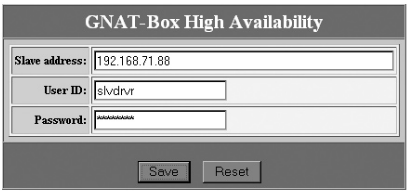


GNAT-Box High Availability

| | |
|---|---|
| Enable: | □ |
| Status: | Feature disabled |
| VRID: | 1 |
| Priority: | 5 |
| Email notification: | ☑ |

| Name | Interface | Virtual IP address | Beacon IP addresses | | |
|---|---|---|---|---|---|
| HA-EXTERNAL | EXTERNAL | 192.168.71.85/24 | 192.168.71.86 | 0.0.0.0 | 0.0.0.0 |
| HA-PROTECTED | PROTECTED | 10.10.1.85/24 | 10.10.1.86 | 0.0.0.0 | 0.0.0.0 |

*$H_2A$ High Availability*



GNAT-Box High Availability

| | |
|---|---|
| Slave address: | 192.168.71.88 |
| User ID: | slvdrvr |
| 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 David L. Mills.

The Network Time Service is highly accurate, with a resolution of under 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).

Enter up to six NTP servers, either by host name or IP address. These servers can be 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.

### NTP Resources

Locate a site that serves your time zone and contact the administrator, as required. Before referencing any NTP server, make sure you adhere to the server’s policies. There are many freely accessible NTP servers, but it is customary to make a formal request before utilizing the server. The following are a sample of the NTP and time server resources available.

- 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***

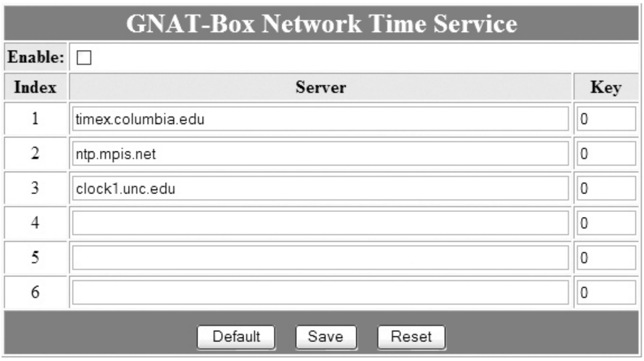
Many Network Time Server sites require contacting the site administrator before using the time server.

### Designate the Firewall as an NTP Server

The firewall can be configured as an NTP server for other hosts on the network. To designate the firewall as an NTP server, enable the Network Time Service and create a Remote Access Filter that accepts connections on UDP port 123. Configure your hosts to indicate the firewall as their NTP server.

**Network Time Service Fields**

| | |
|---|---|
| Enable | Enable the Network Time Service. Disabled by default. |
| Server | Host name or IP address of the time server. |
| Key | Key for the specified server, if required. Some servers require a key value; most do not. |



GNAT-Box Network Time Service

Enable: □

| Index | Server | Key |
|---|---|---|
| 1 | timex.columbia.edu | 0 |
| 2 | ntp.mpis.net | 0 |
| 3 | clock1.unc.edu | 0 |
| 4 |  | 0 |
| 5 |  | 0 |
| 6 |  | 0 |

*Network Time Service*

## Remote Logging

All GTA Firewalls provide remote logging of events. The Remote Logging facility provides a means to configure how and where log information is sent. GNAT Box System Software's GTAsyslog uses the syslog TCP/IP protocol for recording logs remotely. Recent events are kept locally in a buffer on the firewall system and can be accessed using the function **System Activity/View Log Messages** (see **Chapter 13 – System Activity**). Log messages can also be viewed from the LogView utility (see **Chapter 14 – Utilities**), as a log file in a text utility such as Notepad or TextEdit, or using the GTA Reporting Suite application (available separately).

### *Note*

The Remote Logging service is not used by GB-Commander.

Enable Remote Logging, then select the source IP address object from the BINDING INTERFACE dropdown box, and enter the server IP address and port number in the SYSLOG SERVER field . See **Appendix B – Log Messages** for more information about logs and default logging.

### GTAsyslog

GTAsyslog is GTA's syslog server. The configuration screen within the DBmanager utility allows the user to select logging options–how the GTAsyslog and LogView utilities operate, and how the optional standalone program GTA Reporting Suite accesses recorded data. GTAsyslog does not have a user interface separate from DBmanager.

The GTAsyslog automatically writes log data to a circular file. With additional licensing, GTAsyslog sends the log information to a server for GTA Reporting Suite. For more about configuring GTAsyslog, see **Chapter 14 – Utilities**.

## WELF (WebTrends Enhanced Log Format)

The remote logging facility uses the WebTrends Enhanced Logging Format (WELF) to record log messages. The following table shows the fields used.

**WELF Fields**

| | |
|---:|---|
| id | Type of record. |
| time | ***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 number of the item that triggered the entry. |
| proto | Protocol or service used by the event. |
| duration | Time required for 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 | Port number 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 | Port number where the event was generated. |
| interface | 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 | Specific VPN object–shows the most used connections. |
| cat_type | Local or Surf Sentinel category: e.g., Local Accept or Deny List item; Drug Culture or Pornography. |
| cat_action | Action performed by the filter: Block or Pass. |
| fil_type | Filter description: Default, Outbound (OF), IP Pass Through (PTF) or Remote Access (RAF.) |
| fil_action | Filter action: Block or Accept. See WELF log term “attribute” for GNAT Box Filter Action. |

| | |
|---|---|
| msg | Details events such as a VPN starting, the configuration changing, or a port scan being detected; also captures the index/rule number of the generating filter or facility. |
| attribute | Action (as defined in GNAT Box System Software) taken when the filter was triggered, e.g., Alarm, Email, Stop. |

See **Appendix B – Log Messages** for examples of log messages formatted in WELF. For more information about WELF, see `www.netiq.com/partners/technology/welf.asp`.

## Unix Facilities

A syslog service (daemon) that can accept and record the log data is a standard feature on all Unix/Linux based systems. GNAT Box System Software logging provides the unix syslog facilities: auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, news, ntp, security, user, uucp and local0 - local7.

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. The priority (set on each filter definition) is used by the remote log host to determine if and where the information in the log stream should be displayed/stored.

### Filter

Filter log messages are generated due to a filter rule, either explicit or automatic. Filter messages are logged by default to the “local1” facility.

### NAT (Network Address Translation)

Network Address Translation log messages 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. By default, NAT session closes are logged at priority Notice, and NAT session opens are not logged.

### WWW

WWW log messages 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.”

## Remote Logging Fields

Enable
Enable remote logging. Disabled by default.

Binding interface
Address from which logging is sourced, Auto by default. Selecting Auto will indicate the firewall’s usual source IP address to the Syslog server location. To force the logging packets to have a specific source IP address, choose the Interface object from the dropdown list.

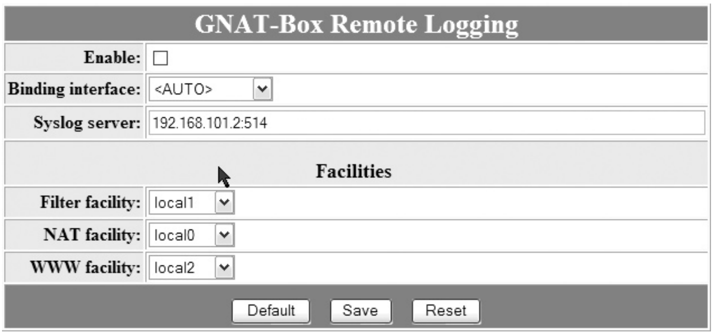
Syslog server
IP address or host name of a system that will accept the remote logging data. Data can be accepted by the supplied GTAsyslog facility or any program that accepts the syslog protocol. The port is 514 by default. To enter a different port number, use the standard format, e.g., `192.168.71.2:514` or `example.gta.com:514`.

**Facilities**

Filter Facility
Logs information associated with any filter that has logging enabled. Any attempts at unauthorized access will be logged to the Filter Facility log stream.

NAT Facility
Logs information associated with Network Address Translation: essentially, outbound packets.

WWW Facility
Logs all URLs accessed through the GTA Firewall.



GNAT-Box Remote Logging

Enable: □

Binding interface: <AUTO>

Syslog server: 192.168.101.2:514

Facilities

Filter facility: local1

NAT facility: local0

WWW facility: local2

*Remote Logging*

# 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 the MIB (Management Information Base) and organized in report form, helps the administrator ensure optimal performance in the managed devices.

SNMP on GNAT Box systems does not utilize a custom MIB. MIBs supplied with your third-party SNMP toolkit will function with the GTA Firewall.

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. Auto-configure the filter set or create appropriate filters, then customize and enable the desired filters.

### *Caution*

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

## SNMP Fields

| | |
|---|---|
| Enable | Enable the SNMP facility. Disabled by default. |
| Contact information | 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 the password, those with access can see SNMP information and/or receive trap notifications. In the full SNMP implementation, there are three community levels: read access, read-write access, and trap notification. Members of a community can access information at the level allowed in the community. |

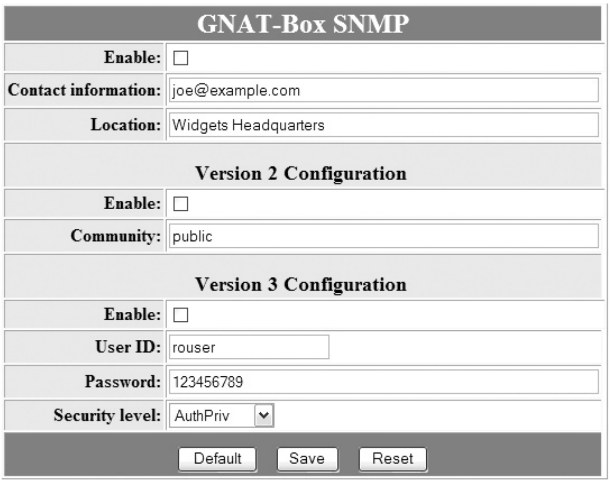
### Version 3 Configuration

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: **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: joe@example.com

Location: Widgets Headquarters

**Version 2 Configuration**

Enable: □

Community: public

**Version 3 Configuration**

Enable: □

User ID: rouser

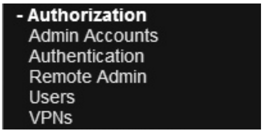
Password: 123456789

Security level: AuthPriv

*SNMP*

# 4 Authorization

The Authorization section consists of Administrative Accounts, Authentication, Remote Administration, GTA Firewall user definitions and VPN definitions using previously defined VPN objects.



*Authorization Menu*

## Admin Accounts

Admin Accounts provides a means to manage the administrative accounts used to access the GTA Firewall. The primary account is used to initially log on to the firewall and is the only one that can log on using the Console interface. The default user ID and password are “gnatbox.” (The Console interface cannot be disabled.)

***Note***

GTA recommends changing the default user ID and password.

Up to five (5) additional accounts can be defined. Each account is assigned a unique user ID and password with selected access privileges.

Accounts that have not been given Admin privileges (the Admin permission field is not selected) are ***read-only***, so they cannot make changes to the firewall or view preshared secrets. These fields, otherwise entered in clear text, will be obscured when Admin permissions are disabled.

## Admin Account Fields

**Enable lockout** Lock out a user’s IP address if the user name or password is entered incorrectly. Enabled by default.

**Lockout threshold** Number of tries a user can make from an IP address before that IP address is locked out.

**Lockout duration** Number of seconds an IP address is locked out.

**Email notification** Send email to administrator if IP address is locked out.

**User ID** Administration account name used to log on to the firewall, up to 39 characters long. Any character that can be generated from the keyboard is valid, except leading and trailing spaces.

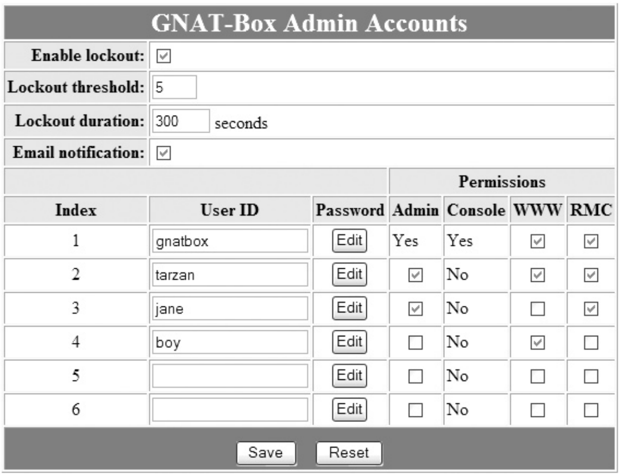
**Password** Password used to log on to the GTA Firewall, up to 39 characters long. Any character generated from the keyboard is valid, except leading and trailing spaces.

**Admin** Enable to give this account user update authority.

**Console** Only the primary account user can log on to the Console.

**WWW** Enable to allow this user to log on via the Web interface.

**RMC** Enable to allow this user to log in via GBAdmin, the Windows remote management interface.

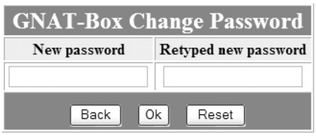


GNAT-Box Admin Accounts

| | |
|---|---|
| Enable lockout: | ☑ |
| Lockout threshold: | 5 |
| Lockout duration: | 300 seconds |
| Email notification: | ☑ |

| | | | Permissions | | | |
|---|---|---|---|---|---|---|
| Index | User ID | Password | Admin | Console | WWW | RMC |
| 1 | gnatbox | Edit | Yes | Yes | ☑ | ☑ |
| 2 | tarzan | Edit | ☑ | No | ☑ | ☑ |
| 3 | jane | Edit | ☑ | No | □ | ☑ |
| 4 | boy | Edit | □ | No | ☑ | □ |
| 5 | | Edit | □ | No | □ | □ |
| 6 | | Edit | □ | No | □ | □ |

*Administration Accounts*



GNAT-Box Change Password

| New password | Retyped new password |
|---|---|
| | |

*Change Password*

# Authentication

The Authentication service allows the administrator to require users to authenticate using GBAuth before initiating a connection to or through the firewall. To use this feature, Authentication must be enabled and a user authentication Remote Access Filter must be configured.

***Note***

All data is sent from GBAuth to the firewall via SSL.

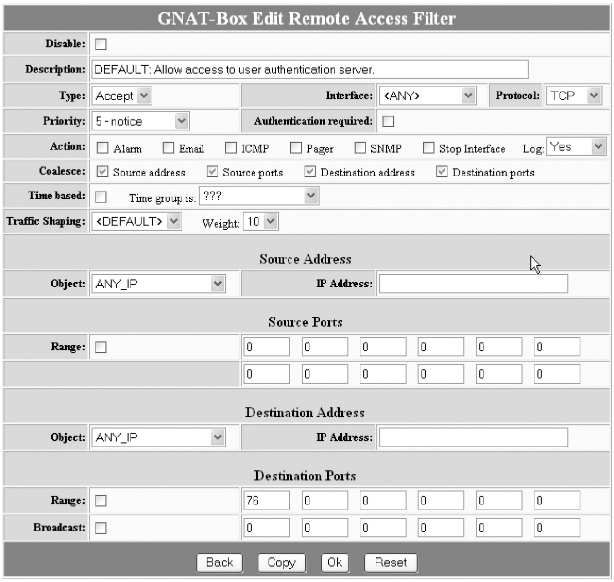
There are three authentication methods on the GTA firewall: GTA authentication, LDAP and RADIUS. See **Chapter 14 – Utilities** for more about configuring and using GBAuth, GTA's authentication client.

## User Authentication Remote Access Filter

A user authentication Remote Access Filter must be configured for any of the three methods of authentication. To use the default filter below, auto-configure the Remote Access filters after enabling and saving the Authentication section.

***Note***

Filters that have never been saved are auto-configured to system parameters every time the system is restarted. If filters have been saved, use **DEFAULT** to auto-configure filters to match the system.



GNAT-Box Edit Remote Access Filter

Disable: □

Description: DEFAULT: Allow access to user authentication server.

Type: Accept  Interface: <ANY>  Protocol: TCP

Priority: 5 - notice  Authentication required: □

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

Coalesce: ☑ Source address ☑ Source ports ☑ Destination address ☑ Destination ports

Time based: □  Time group is: ???

Traffic Shaping: <DEFAULT>  Weight: 10

Source Address

Object: ANY_IP  IP Address:

Source Ports

Range: □  0 0 0 0 0 0
0 0 0 0 0 0

Destination Address

Object: ANY_IP  IP Address:

Destination Ports

Range: □  76 0 0 0 0 0

Broadcast: □  0 0 0 0 0 0

*User Authentication Remote Access Filter*

## GTA Authentication

To use GTA Authentication, enable Authentication and the desired port (TCP port 76, by default). Create a user authentication Remote Access Filter if one has not already been created. If Authentication is enabled, but neither LDAP nor RADIUS are enabled and configured, the firewall uses GTA Authentication.

GTA Authentication requires a user to be set up on the firewall; configure users with the instructions in the Users section in this chapter. GTA Authentication can be selected in VPN objects, Inbound Tunnels, Remote Access Filters and IP Pass Through Filters. Users enter the values in the IDENTITY and PASSWORD fields from Users Authorization to log in using GBAuth.

## LDAP

GTA supports the LDAPv3 protocol for user authentication. LDAP (Lightweight Directory Access Protocol) is a specification for accessing directories on the Internet to obtain information such as email addresses and public keys. LDAP is based on the X.500 directory access protocol, DAP, but is less comprehensive. It also supports TCP/IP for Internet access. Like the Internet protocols HTTP and FTP, LDAP is used in the protocol prefix of a URL, i.e., **ldap://example.com**. LDAP version 3, completed in 1997, is the latest implementation at the time of this release.

### Using LDAP on a GTA Firewall

To use LDAP, enable Authentication and the LDAPv3 feature. Enter the IP address and desired port (TCP port 389 by default) of the LDAP server and the Base DN used by your company, as in the LDAP section of the Authentication illustration. Create a user authentication Remote Access Filter if one has not already been created.

LDAP requires users, organizational units and domains to be set up on and LDAP server. LDAP authentication can be selected in Inbound Tunnels, Remote Access Filters and IP Pass Through Filters.

When LDAP is used, authentication cannot be selected in a VPN object. To use LDAP with VPNs, select authentication on the appropriate filter. Using this method, the VPN can be initiated, but cannot not be used until the user has authenticated with GBAuth. However, a user is authenticated for all firewall services until the authentication times out or is closed by the user.

### LDAP Authentication Components

cn common name

Case-sensitive name specified on the LDAP server and entered in the IDENTITY field of GBAuth, e.g., `Joe Tech`.

rdn relative distinguished name

The common name plus “cn=” identifier; `cn=Joe Tech`.

ou organizational unit

Group to which the user has been assigned. There can be a hierarchy of ou’s defined; enter each in the order of its specificity: if Joe Tech belongs to the FreeBSD group within the support group, ou would be entered into the IDENTITY field of GBAuth, after the cn, as: `ou=FreeBSD,ou=support`.

dn distinguished name

Entries in an LDAP server are located by way of the distinguished name, a globally unique identifier designed to be readable by any LDAP-compliant client. This is the entire string sent to the LDAP server by GBAuth. `cn=Joe Tech,ou=supported, dc=qa,dc=com,dc=gta`.

dc domain component

Single domain component of an FQDN (fully-qualified domain name) such as `qa.gta.com`, e.g., `dc=qa,dc=com,dc=gta`.

The IDENTITY field value in GBAuth (cn and the ou together) can be up to 127 characters.

See the GBAuth section in **Chapter 14 – Utilities** for more information about how a user authenticates to the LDAP server using GBAuth.

In the example illustrated in the Authentication graphic on page 51, the structure for the Base DN is: `dc=qa, dc=gta, dc=com`; the organization unit is: `ou=support`; the user is `cn= Joe Tech`. The identifier `cn=` is prepended to the IDENTITY field of GBAuth, and the Authentication BASE DN field values are appended to the data, creating the dn string that is sent by GBAuth to the LDAP server.

## RADIUS

GTA supports RADIUS (Remote Authentication Dial-In User Service) for authentication. RADIUS is an authentication and management system used by many ISPs, requiring the customer to enter a username and password to access the service. A RADIUS server verifies the information, and then authorizes access. The RADIUS specification is not an official IETF standard.

### Using RADIUS on a GTA Firewall

To use RADIUS, enable Authentication and the RADIUS feature. Enter the IP address, desired port (TCP port 1812 by default) and preshared secret of the RADIUS server, as in the Authentication illustration example. If a user authentication Remote Access Filter has not already been created, configure and enable the filter.

## Authentication Fields

Enable — Select this checkbox to enable the use of any of the three methods of authentication. If only this checkbox is selected, GTA Authentication can be used. Selecting the services below allows LDAPv3 and/or RADIUS authentication to be used as well.

**GTA Authentication**

Service port — Default port for GTA authentication is 76.

**LDAPv3**

Enable — Enable the use of an LDAP service.

Binding interface — Address from which authentication information is sourced, Auto by default. Selecting Auto will indicate the firewall's usual source IP address to the server location. To force packets to have a specific source IP address, choose the Interface object from the dropdown list.

Server — Server IP address or host name and port number of the LDAP server that will perform the authorization. The service port number defaults to 389. To enter a specific port number, use the format `ldap.example.com:389`.

Base DN — Root distinguished name on the LDAP server, comparable to the domain name in an internet address. Maximum, 127 characters.

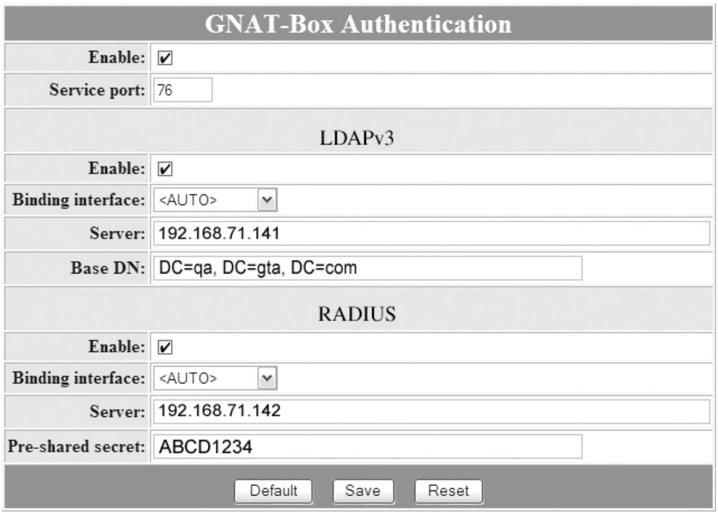
**RADIUS**

Enable — Enable the use of the RADIUS service.

Binding interface — Address from which authentication information is sourced, Auto by default. Selecting Auto will indicate the firewall's usual source IP address to the server location. To force packets to have a specific source IP address, choose the Interface object from the dropdown list.

Server — Server IP address or host name and port number of the RADIUS server that will perform the authorization. The port number defaults to 1812. To enter a specific port number, use the format `radius.example.com:1812`.

Preshared secret — Alphanumeric value. Preshared secret as defined in the RADIUS service. This field is case-sensitive.



GNAT-Box Authentication

| | |
|---|---|
| Enable: | ☑ |
| Service port: | 76 |
| **LDAPv3** | |
| Enable: | ☑ |
| Binding interface: | <AUTO> |
| Server: | 192.168.71.141 |
| Base DN: | DC=qa, DC=gta, DC=com |
| **RADIUS** | |
| Enable: | ☑ |
| Binding interface: | <AUTO> |
| Server: | 192.168.71.142 |
| Pre-shared secret: | ABCD1234 |

*GTA, LDAP and RADIUS Authentication*

## Remote Admin

Remote Admin provides a means to regulate administration via the Web interface or GBAdmin (Remote Management Console or RMC). The factory settings enable remote administration and the ability to apply updates. By default, the Web interface is served on standard TCP port 443 for SSL encryption, port 80 for non-SSL encryption and GBAdmin on TCP port 77.

The firewall can also be accessed using the Console interface using the primary account. The Console interface cannot be disabled.

### WWW

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

When using SSL encryption for Web administration, the address will begin “https:”, e.g., `https://192.168.71.254`. When SSL encryption is set to “None,” the address will begin “http:”, e.g., `http://192.168.71.254`.

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.

### Change the Server Port

To maintain access when changing the port number used for remote administration, a remote access filter for the new port must be in place before changing the port number. Implement a port number change in this order:

1. In Remote Access Filters, find the filter that controls remote administration access and add the new port number value. Save the section.
2 In Remote Administration, change the port to the new value and save the section.
3. In Remote Access Filters, return to the remote administration access filter and delete the old port. Save the section.

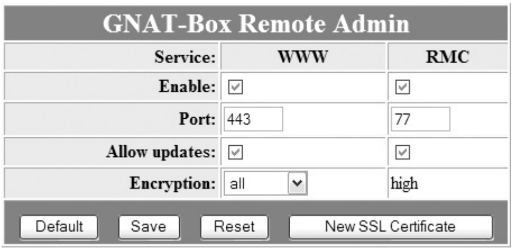
Your firewall will now use the new port value for access.

## RMC (GBAdmin)

The RMC (Remote Management Console) establishes an encrypted network connection to the GTA Firewall on TCP port 77. 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.

### Remote Administration Fields

| | |
|---|---|
| | **WWW** |
| Enable | Enable remote administration via the Web interface. Enabled by default. |
| Server Port | SSL encryption default is 443; non-SSL default is 80. |
| 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** |
| Enable | Enable access via GBAdmin (RMC). Enabled by default. |
| Server Port | Default port for RMC access is 77. |
| Allow Updates | By default, updates are allowed. |
| Encryption | Encryption level is high. |



GNAT-Box Remote Admin

| Service: | WWW | RMC |
|---|---|---|
| Enable: | ☑ | ☑ |
| Port: | 443 | 77 |
| Allow updates: | ☑ | ☑ |
| Encryption: | all | high |

*Remote Administration*

## 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. SSL encryption, developed by Netscape, is the standard in Internet security for HTTP, supporting server/client authentication, and maintaining security and integrity in transmission. Used for the Web and GBAdmin access, SSL may be configured from any user interface.

SSL encryption is selected by default in GNAT Box System Software installations after 3.3.2. SSL encryption requires a Remote Access Filter with a port that matches the Remote Administration port (443, by default).

***Note***

SSL Encryption is known to be incompatible with Internet Explorer 5 for Macintosh. One option is to use another browser such as Opera (www.opera.com) or Netscape (www.netscape.com); another is to use GBAdmin or a compatible browser to install the firewall, then disable SSL encryption in GNAT Box System Software.

**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. |

***Note***

GNAT Box System Software supports SSL version 3.0. Due to potential security flaws, support for SSL version 2.0 has been removed.

## SSL Certificate Automatic Renewal

Each time you upgrade GNAT Box System Software, the SSL certificate is renewed for a year from the release build date.

## New SSL Certificate

The New SSL Certificate feature, available on all user interfaces, allows the user to create a new SSL certificate for the currently loaded GTA Firewall. An SSL certificate is valid for one year from the date it is created.

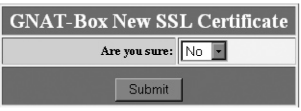
The SSL certificate will include three levels of validity: the issuer, or self-issued certificate authority; the date, which will be the date of certificate generation; and the name, which will be the firewall's host name.

### Host Name

After the firewall has been installed, enter the host name in the HOST NAME field in **Basic Configuration/Network Information**. To create a certificate in which the name on the security certificate matches the name on the site, the host name entered in Network Information must match 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 to generate a certificate for the GTA Firewall.

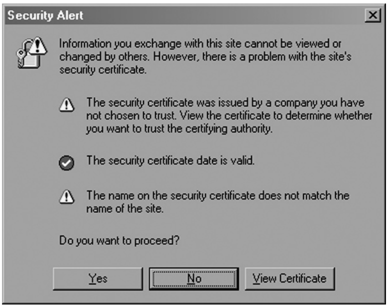


GNAT-Box New SSL Certificate

Are you sure: No

*SSL Certificate*

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.



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.

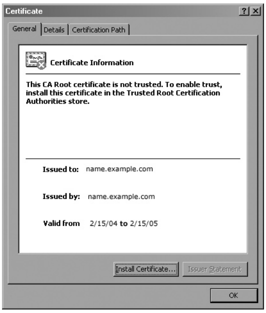
Do you want to proceed?

*SSL Certificate Security Alert*

The dialog indicates that the listed Certificate Authority is not one you have chosen to trust; the certificate date is valid; and the name on the certificate does not match the name of the site. Select **YES**. Your security will not be compromised.

### Install Security Certificate

To install the SSL security certificate, click **VIEW CERTIFICATE**. In the Certificate screen that appears, click **INSTALL CERTIFICATE**.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: name.example.com

Issued by: name.example.com

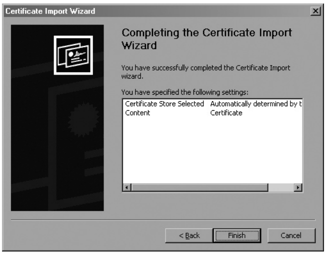
Valid from 2/15/04 to 2/15/05

*Internet Explorer 5 for Windows Install Certificate*

In Internet Explorer 5 for Windows, a Certificate Import Wizard will appear. Click **NEXT** and choose whether to automatically select the Certificate Store (recommended), or select a location manually. Click **FINISH**.

Verify that you want to install to the Root Certificate Store. If a dialog reports that the import was successful, you have completed the certificate installation.

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, a new certificate can be created at any time.



Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by t |
| Content | Certificate |

*Certificate Import Wizard Complete*

## Users

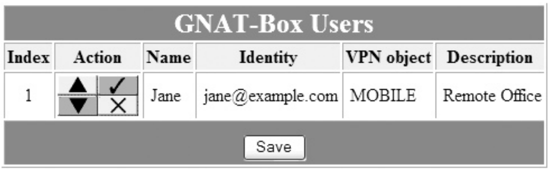
The Users section allows the administrator to create a user and enable the user for general access, VPNs, or other restricted access points, and to create and authorize GTA Firewall mobile VPNs using IP addresses or objects. One or more mobile VPNs are defined by linking a VPN object (such as the VPN object **MOBILE**) to a remote network address or address object. See the next section, VPNs, for more about GTA Firewall VPN authorizations.

Users can be selected in filters to regulate access from outside the Protected Network and in Inbound Tunnels to restrict access from a specified network interface to an IP address/port. See **Chapter 8 – Filters** and **Chapter 9 – Pass Through**, for more about filters. See **Chapter 14 – Utilities** and the **GNAT Box VPN Feature Guide** for more about authentication.

### User Add/Edit Screen Fields (Web & GBAdmin)

| | |
|---|---|
| Disable | Disable all access for the selected user. |
| Name | Full name of the user. |
| Description | Description of user. |
| Identity | User email address for user authentication. |
| | **Authentication** |
| Method | Password method. |
| Password | Password for user authentication. |
| | **Mobile VPN** |
| Disable | Disable VPN access for the selected user. |
| VPN Object | Previously defined VPN object. |
| Remote Network | IP address or address object of the remote network. |
| Preshared secret | ASCII or HEX* value preshared secret. |

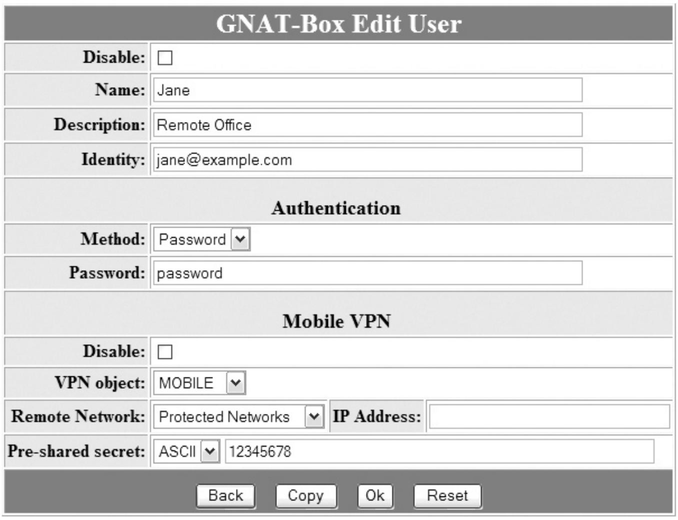
* Valid hexadecimal characters: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.



GNAT-Box Users

| Index | Action | Name | Identity | VPN object | Description |
|---|---|---|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | Jane | jane@example.com | MOBILE | Remote Office |

*Users List*



GNAT-Box Edit User

| | |
|---|---|
| Disable: | □ |
| Name: | Jane |
| Description: | Remote Office |
| Identity: | jane@example.com |

**Authentication**

| | |
|---|---|
| Method: | Password |
| Password: | password |

**Mobile VPN**

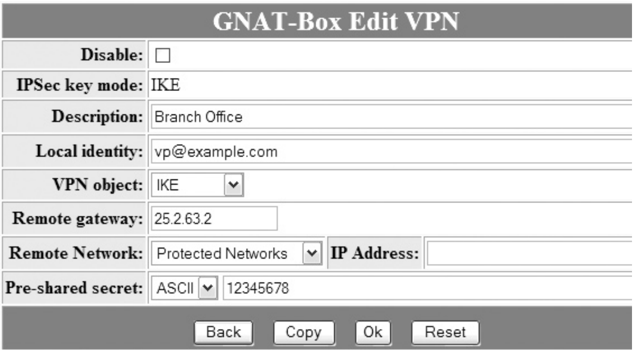
| | | | |
|---|---|---|---|
| Disable: | □ | | |
| VPN object: | MOBILE | | |
| Remote Network: | Protected Networks | IP Address: | |
| Pre-shared secret: | ASCII | 12345678 | |

*User Authorization*

## VPNs

The VPNs section allows the creation and authorization of GTA Firewall VPNs using addresses or objects. One or more VPNs are defined by linking a VPN object to a remote network address or address object.

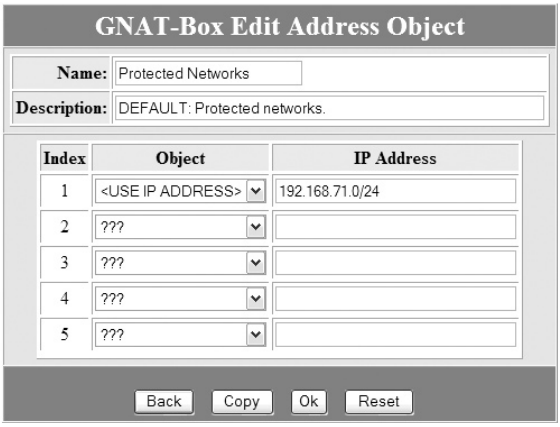
The authorization of a VPN connection between two single networks defines one VPN. For example, in the VPN authorization illustrated below, the local network VPN object **IKE** contains the address object **Protected Networks**, which in turn represents all the protected networks in the home office. The remote network is single network address. Any subnets have been combined to create one network using a /24 netmask.



GNAT-Box Edit VPN

| | | | |
|---|---|---|---|
| Disable: | □ | | |
| IPSec key mode: | IKE | | |
| Description: | Branch Office | | |
| Local identity: | vp@example.com | | |
| VPN object: | IKE | | |
| Remote gateway: | 25.2.63.2 | | |
| Remote Network: | Protected Networks | IP Address: | |
| Pre-shared secret: | ASCII | 12345678 | |

*VPN Authorization*

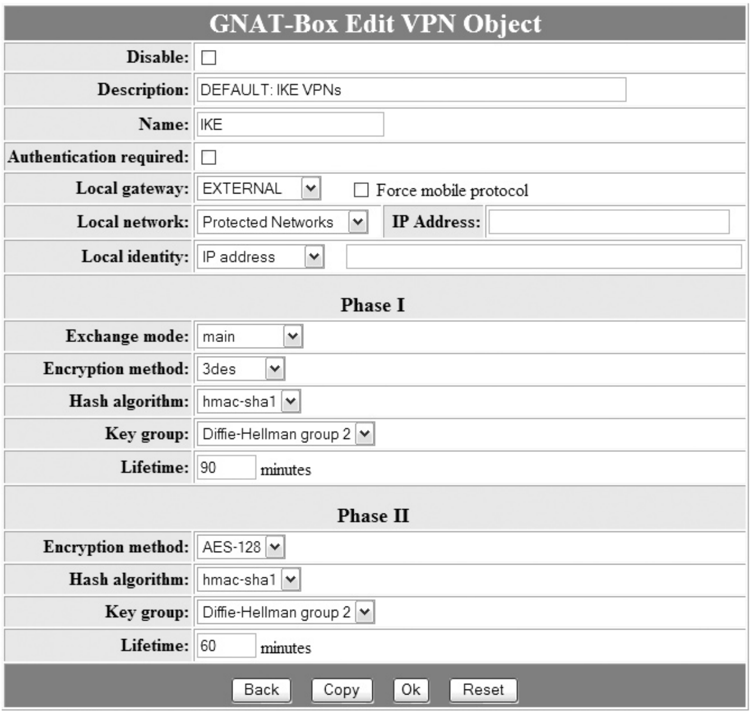


GNAT-Box Edit Address Object

| | |
|---|---|
| Name: | Protected Networks |
| Description: | DEFAULT: Protected networks. |

| Index | Object | IP Address |
|---|---|---|
| 1 | <USE IP ADDRESS> | 192.168.71.0/24 |
| 2 | ??? | |
| 3 | ??? | |
| 4 | ??? | |
| 5 | ??? | |

*Address Object*



GNAT-Box Edit VPN Object

| | |
|---|---|
| Disable: | □ |
| Description: | DEFAULT: IKE VPNs |
| Name: | IKE |
| Authentication required: | □ |
| Local gateway: | EXTERNAL □ Force mobile protocol |
| Local network: | Protected Networks IP Address: |
| Local identity: | IP address |
| Phase I | |
| Exchange mode: | main |
| Encryption method: | 3des |
| Hash algorithm: | hmac-sha1 |
| Key group: | Diffie-Hellman group 2 |
| Lifetime: | 90 minutes |
| Phase II | |
| Encryption method: | AES-128 |
| Hash algorithm: | hmac-sha1 |
| Key group: | Diffie-Hellman group 2 |
| Lifetime: | 60 minutes |

*VPN Object*

# VPN Concepts

## Security Associations

A Security Association (SA) specifies the parameters connecting two hosts. Each two-way connection uses a minimum of two SAs, one for each direction of communication. Any time a defined VPN is active (in use, or not yet timed out), it will use at least two SAs.

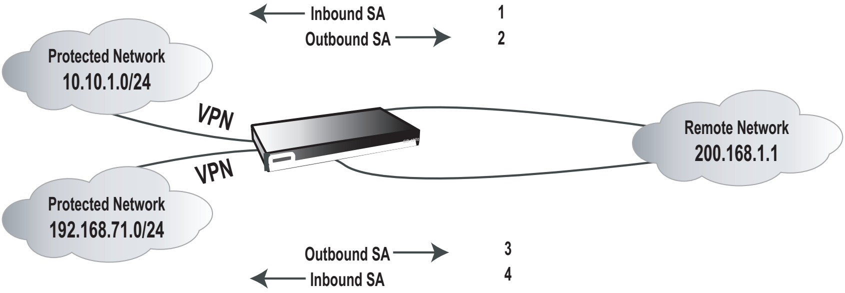
For the total number of potential SAs used by each VPN authorization, see the Authorization section in the system configuration report, found in **Reports/ Configuration**. See individual GTA Firewall product guides for the number of Security Associations supported by a specific firewall. To see the current number of VPN Security Associations, see **System Activity/Active VPNs**. Each active VPN will have two entries, one for each direction of communication.

***Note***

Each authorization in the configuration report will contain one or more VPNs, depending on the number of networks represented by each VPN or address object.

### Multiple Networks

A GTA Firewall VPN authorization can define one VPN or many, depending on the number of networks represented by each object. For example, if a VPN authorization contains an object with two separate local networks and a single remote network, two VPNs are defined, for a total of four SAs.



*Two VPNs, four VPN Security Associations*

### Mobile Protocol

A VPN using mobile protocol – either a mobile VPN created in the **Authorization > Users** section, or gateway to gateway VPN with **Force Mobile Protocol** selected – will use SAs while active. The number of SAs potentially used by mobile and gateway to gateway VPNs can be higher than the number of licensed SAs; however, the number of SAs used by active VPNs, mobile VPNs included, cannot exceed this number. See the previous section for more about changes to Users authorization.

### Encryption Key Length

The Blowfish 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.

### Algorithms

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

### 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 SHA-1 transformations is 160 bits, which is 20 ASCII (40 hexadecimal) characters. It provides 80 bits of security. The key length for the SHA-2 (SHA-256) transformations is 256 bits, which is 32 ASCII (60 hexadecimal) characters. It provides 128 bits of security against collision attacks.

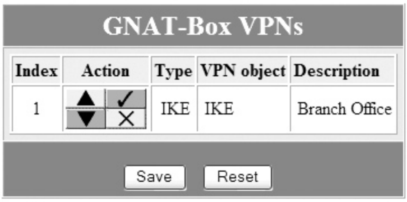
### Security Parameter Index (SPI)

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.

# Create a VPN

## Create an Authorization

Presuming that you use the default VPN objects, create a VPN by selecting the **Authorization/VPNs** menu item. Create a new VPN authorization.



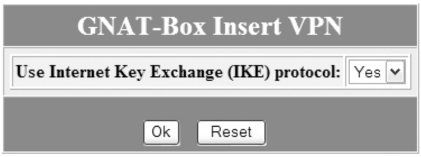
GNAT-Box VPNs

| Index | Action | Type | VPN object | Description |
|---|---|---|---|---|
| 1 | ▲▼ ✓ ✕ | IKE | IKE | Branch Office |

*VPN Authorization List*

### 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.



GNAT-Box Insert VPN

Use Internet Key Exchange (IKE) protocol: Yes

*Select Key Method*

## IKE VPN Fields

Disable — Check to disable all access for the selected VPN.

IPSec key mode — IKE.

Description — Description of VPN.

Identity — User email address for user authentication. This field is used to associate the remote user with a preshared 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.)

VPN Object — VPN Object to define this VPN.

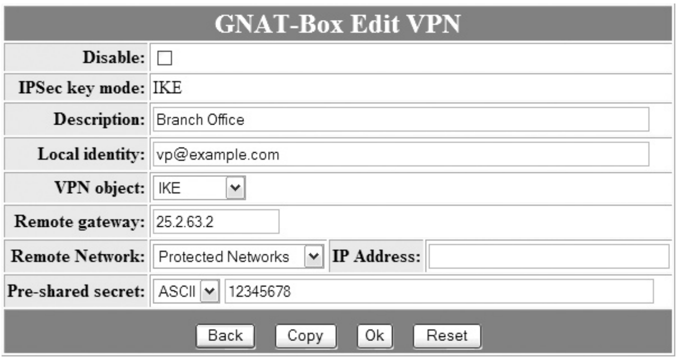
Remote Gateway — (Destination) Default is 0.0.0.0. IP address of the route through which this VPN will pass, the gateway to the remote network. If the remote network is behind a GTA Firewall, then this would be one assigned to the External Network interface. This IP address will also help determine the routing of the encapsulated packet.

Remote Network — Previously defined Address object or Use IP address.

IP address — Destination IP address of the network that resides behind the remote firewall. This can be just the part of the network to which access is desired. (On a GTA Firewall, 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).

Preshared secret — ASCII or HEX* format value preshared secret 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. (Phase I)

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



GNAT-Box Edit VPN

Disable: □

IPSec key mode: IKE

Description: Branch Office

Local identity: vp@example.com

VPN object: IKE

Remote gateway: 25.2.63.2

Remote Network: Protected Networks IP Address:

Pre-shared secret: ASCII 12345678

*VPN Authorization–IKE*

## Manual VPN Fields

Disable — Check to disable all access for the selected VPN.

IPSec key mode — Manual.

Description — Enter a brief description of VPN.

VPN Object — VPN Object to define this VPN.

Remote Gateway — (Destination) Default is 0.0.0.0. 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 would be one assigned to the External Network interface. This IP address will also help determine the routing of the encapsulated packet.

Remote Network — Previously defined Address object or Use IP address.

IP address — Destination IP address of the remote network that resides behind the remote firewall. This need not be the entire network, just the part that is to be accessible. (Typically this will be the Protected Network, PSN or a subnet of either, on a GTA Firewall.) Define the type of network with a mask (e.g., 255.255.255.0 or /24 for a Class C).

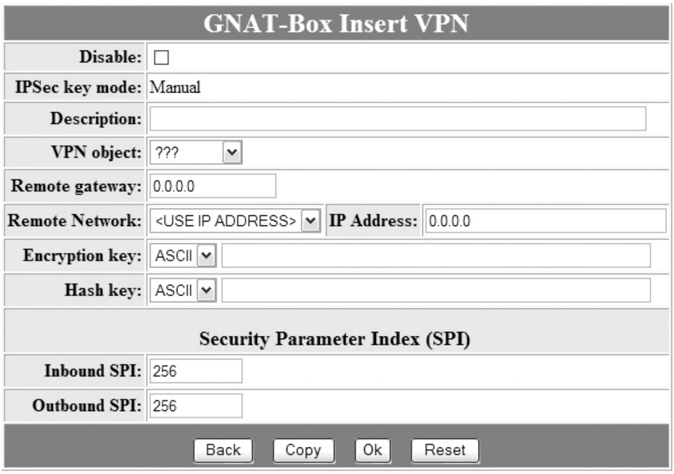
Encryption Key* — ASCII or HEX* format value encryption key as defined in VPN.

Hash Key — ASCII or HEX* format value hash algorithm for the authentication transformation.

**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.



**GNAT-Box Insert VPN**

Disable: □

IPSec key mode: Manual

Description:

VPN object: ???

Remote gateway: 0.0.0.0

Remote Network: <USE IP ADDRESS> IP Address: 0.0.0.0

Encryption key: ASCII

Hash key: ASCII

**Security Parameter Index (SPI)**

Inbound SPI: 256

Outbound SPI: 256

*VPN Authorization–MANUAL*

### Remote Access Filters

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 auto-configure a list that includes the ESP and AH protocols. If you have created additional protocols, using the **DEFAULT** button will delete them– in this case, add the ESP (protocol 50) and AH (protocol 51) by hand.

### IP Pass Through Filters

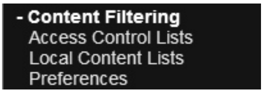
Create IP Pass Through Filters that allow inbound and outbound access on the defined VPN. Generally you will need two filters for each VPN definition (one for inbound access and one for outbound). If you have one or more VPN definitions, go to the Pass Through filter screen and press the **DEFAULT** button. A set of filters will be auto-configured 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. Pass Through Filters for VPN definitions do ***not*** require that entries be created on the Pass Through Host/Network data section.

# 5 Content Filtering

Content Filtering provides the ability to control web site access based on the content of the site. GNAT Box System Software has three primary functions for access control: Access Control Lists (ACLs), Local Content Lists (LCLs) and proxy settings. ACLs allow configuration of Surf Sentinel, GTA's subscription content filtering service (purchased separately).

***Note***

Access to Content Filtering relies on an efficient DNS server. Define a DNS server to access the selected list server.



*Content Filtering menu*

## Access Control Lists

Access Control Lists (ACLs) provide a means to specify how web access control facilities will be applied to web requests. Each ACL 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. ACLs are processed sequentially, so order is important.

***Note***

Access Control List order is important. Each web request is compared to the list, starting at ACL Index #1. The packet is compared sequentially against each ACL until one of two events occurs: ***1.*** An ACL is matched. The web request is either Allowed or Blocked based on the ACL. ***2.*** No ACLs are matched and the list is exhausted. In this case the web request is rejected.

### Local Allow and Deny Lists

Local Allow and 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.

## Mobile Code Blocking

Mobile Code Blocking for Java, Java Script and ActiveX objects is built in. These objects or scripts appear in inbound HTML on TCP port 443, 80, 8000 and 8080. Prior to GNAT Box System Software version 3.5, Mobile Code Blocking was applied as a global option. Effective in version 3.5, it can be applied to individual ACLs.

## Surf Sentinel

GTA's Surf Sentinel 2.0 provides GTA Firewall system administrators with a user-friendly interface and easy access to an exhaustive list of web categories.

Surf Sentinel 2.0 is superior to LCLs alone. Using LCLs, an administrator is able to enter only a limited number of sites. With Surf Sentinel, the administrator can easily allow or deny types of content, as defined in Surf Sentinel's extensive list of categories. LCLs then allow further customization.

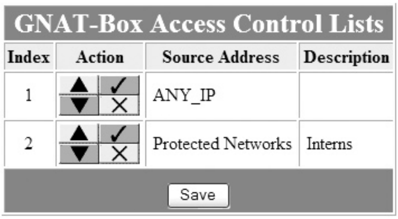
Surf Sentinel 2.0 is specifically designed for firewall and VPN solutions. It features a small, ultra-light footprint. An annual subscription for Surf Sentinel can be purchased from Global Technology Associates, Inc., or through an authorized GTA Channel Partner. With your subscription, you will receive the **Surf Sentinel 2.0 Feature Guide**, which provides more information on using Surf Sentinel categories.

### Access Control Lists (ACL) Fields

| | |
|---|---|
| Disable | Disable this ACL. |
| Description | Description for the ACL. |
| Source Address | If a request matches an element of the specified address object, the packet will be compared to the ACL. |
| | **Content Filtering Facilities** |
| Local Allow List | Process against GTA's Allow list. |
| Local Deny List | Process against GTA's Deny list. |
| Surf Sentinel | Process against the Surf Sentinel list. |
| | **Mobile Code Blocking** |
| Java | Disabled by default. |
| Java Script | Disabled by default. |
| ActiveX Objects | Disabled by default. |
| | **Surf Sentinel Categories*** |

Allow or block URLs in Surf Sentinel categories. Switch a category from one list to the other by selecting the item and clicking the left or right arrow button.

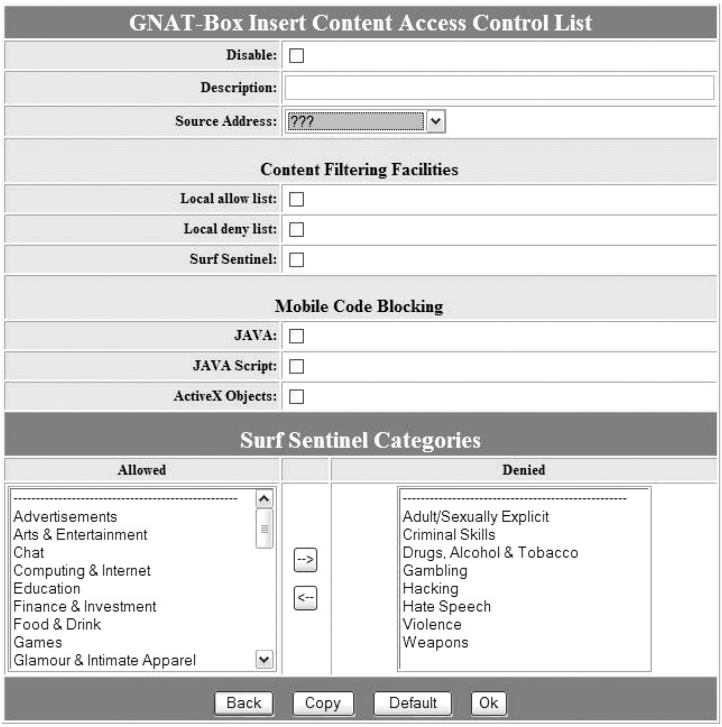
* Requires a feature activation code.



GNAT-Box Access Control Lists

| Index | Action | Source Address | Description |
|---|---|---|---|
| 1 | ▲▼ ✓✕ | ANY_IP | |
| 2 | ▲▼ ✓✕ | Protected Networks | Interns |

*ACLs List*



GNAT-Box Insert Content Access Control List

Disable: □

Description:

Source Address: ???

Content Filtering Facilities

Local allow list: □

Local deny list: □

Surf Sentinel: □

Mobile Code Blocking

JAVA: □

JAVA Script: □

ActiveX Objects: □

Surf Sentinel Categories

| Allowed | | Denied |
|---|---|---|
| ----------------------------------------------<br>Advertisements<br>Arts & Entertainment<br>Chat<br>Computing & Internet<br>Education<br>Finance & Investment<br>Food & Drink<br>Games<br>Glamour & Intimate Apparel | --><br><-- | ----------------------------------------------<br>Adult/Sexually Explicit<br>Criminal Skills<br>Drugs, Alcohol & Tobacco<br>Gambling<br>Hacking<br>Hate Speech<br>Violence<br>Weapons |

*Access Control Lists*

## Local Content Lists

Local Content Lists (LCLs) allow customization of content filtering. LCLs take precedence over Surf Sentinel 2.0 content filtering 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.

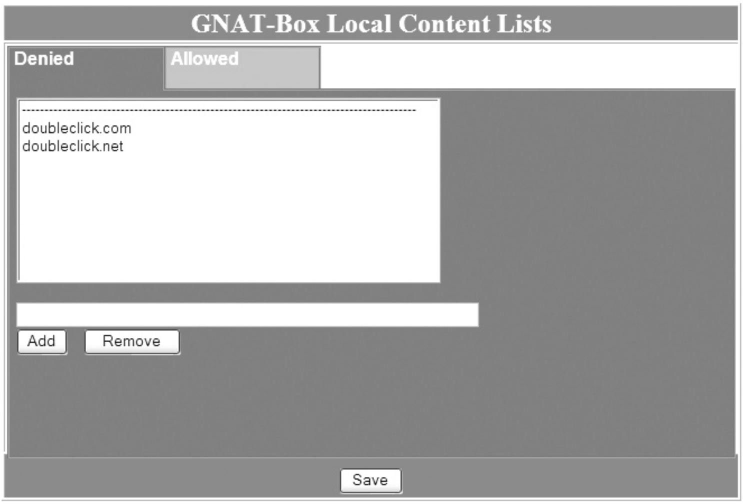
The Allowed list takes precedence over the Denied list; if you have the same URL in both lists, access to the site will be allowed.

### Adding Sites to LCLs

Enter sites in the LCLs 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.



```
--------------------------------------------------------------------------------
doubleclick.com
doubleclick.net
```

*Local Content Lists*

## Content Filtering Preferences

Content filtering requires the use of an HTTP proxy. The Preferences section allows the administrator to specify the use of the Traditional Proxy and associated port, the Transparent Proxy, or both; in addition, a customizable block action (a message or URL) can be selected.

### 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.

#### 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

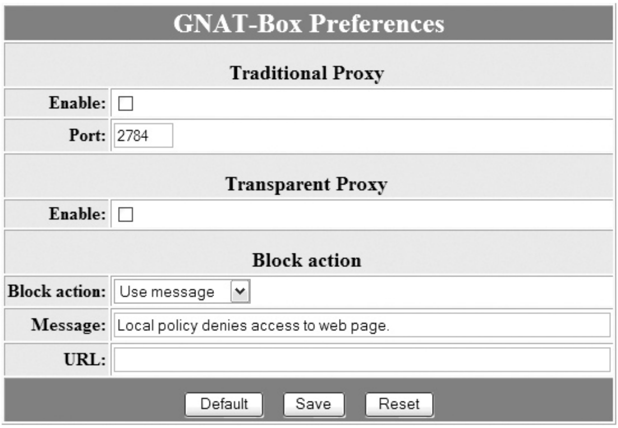
This method is transparent to users located on the Protected Network; no modification to browsers is required, and there is no Proxy port field.

### Block Action

If an ACL blocks a web address (URL), and a user attempts to load a page from that address, the user will see a message, or be redirected to a URL, e.g., an internal website that defines the company’s Internet use policies and the administrative process to get access to a site. The default message, “Local policy denies access to web page,” will appear if a user attempts to reach a blocked address unless a custom message is entered.

## Content Filtering Preferences Fields

| | |
|---|---|
| | **Traditional Proxy** |
| Enable | Enable the traditional proxy. Disabled by default. |
| Proxy Port | Port through which the proxy will run. Default is 2784. |
| | **Transparent Proxy** |
| Enable | Enable the transparent proxy. Disabled by default. |
| | **Block Action** |
| Block Action | Use message or Redirect to URL. |
| Message | If message is selected, enter a custom message or use the default, “Local Policy denies access to web page.” |
| URL | If URL is selected, enter the address of the web page to which blocked users will be redirected. If the web site is encrypted, (port 443) use `https://address`. If the site is unencrypted (port 80 or 8080), use `http://address`. |



**GNAT-Box Preferences**

**Traditional Proxy**

Enable: □

Port: 2784

**Transparent Proxy**

Enable: □

**Block action**

Block action: Use message

Message: Local policy denies access to web page.

URL:

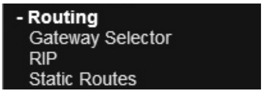
*Content Filtering Preferences*

# 6 Routing

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

### Note

Any packet that goes through the firewall will use the firewall's routing tables. This means that even though a host has indicated a particular route, the firewall will use the routes set up in Static Routing and RIP to route the traffic.



*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.

When the gateway changes, 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 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 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 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 DOWN, if desired. Next, select the External Interface Object that represents the interface you wish to use as the default gateway (route), 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 can be no more than five (5) hops away. (Hops are nodes such as routers or gateways.) A beacon more than five hops away will not be accessible to the route, and the gateway selector will 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.

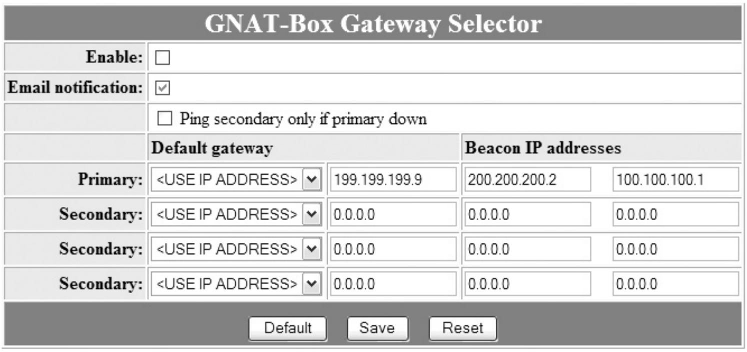
The GNAT Box System pings each beacon IP address every .5 seconds. When a beacon address does not respond for five (5) consecutive pings or 2.5 seconds, the Gateway Selector will consider the route down, and switch to the next accessible route in the list.

### Gateway Selector and Bridging Mode

In order for gateway selection to function correctly in bridging mode, the host must use the IP address of the firewall's logical External Network interface as its gateway.

## Gateway Selector Fields

| | |
|---|---|
| Enable | Enable Gateway Selector. Disabled by default. |
| Email notification | Notify the administrator if the default route changes. |
| Ping secondary only if primary down | Allow the system to probe (ping) the beacons for secondary connections only when the primary gateway is not functional; recommended for a PPP connection, because it prevents the system from maintaining a connection just for the ping activity. |
| | **Default Gateways** |
| Primary | 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 | IP addresses the firewall will use to test connectivity for the Primary Default Gateway. |
| Secondary | Routes the system will use if the Primary 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: | <USE IP ADDRESS> | 199.199.199.9 | 200.200.200.2 | 100.100.100.1 |
| Secondary: | <USE IP ADDRESS> | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| Secondary: | <USE IP ADDRESS> | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| Secondary: | <USE IP ADDRESS> | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |

*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.
```

## 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 2.

## RIP Fields

Enable
Enable the RIP facility on the selected interface. If connected to a remote firewall, the RIP facility will not start until the section is saved. Disabled by default.

Advertise Default Route?
Advertise the default route (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. |

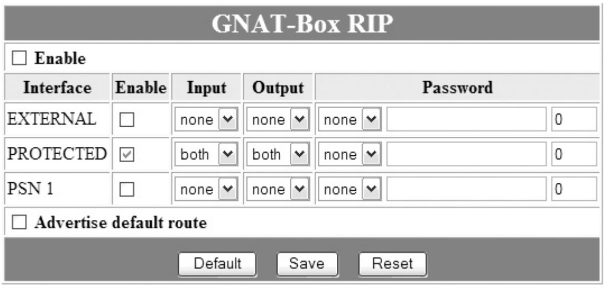
### Password Fields

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

Password Type
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
Password that must be used to collect routing information through RIP.

Key ID
Key ID for the Password.



GNAT-Box RIP

☐ Enable

| Interface | Enable | Input | Output | Password | | |
|---|---|---|---|---|---|---|
| EXTERNAL | ☐ | none | none | none | | 0 |
| PROTECTED | ☑ | both | both | none | | 0 |
| PSN 1 | ☐ | none | none | 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 broadcast 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).

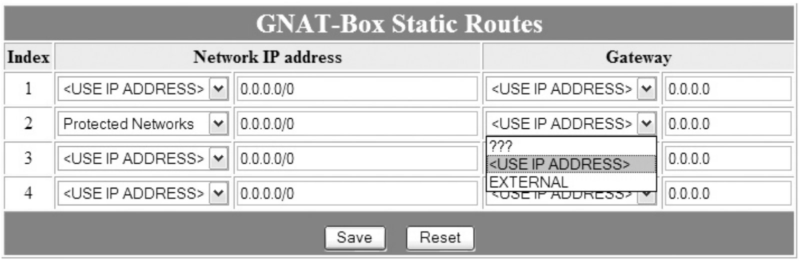
Defining a static route would be useful when there is a router between different parts of an internal network. If the Default Gateway is used, the system will send the packet out through the External Network interface. If the packet is being sent to an IP address on your network, it will not travel the 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 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 IP address of the gateway (default route) to the Destination IP address selected for this static route.



GNAT-Box Static Routes

| Index | Network IP address | | Gateway | |
|---|---|---|---|---|
| 1 | <USE IP ADDRESS> | 0.0.0.0/0 | <USE IP ADDRESS> | 0.0.0.0 |
| 2 | Protected Networks | 0.0.0.0/0 | <USE IP ADDRESS> | 0.0.0.0 |
| 3 | <USE IP ADDRESS> | 0.0.0.0/0 | | 0.0.0.0 |
| 4 | <USE IP ADDRESS> | 0.0.0.0/0 | <USE IP ADDRESS> | 0.0.0.0 |

*Static Routes*

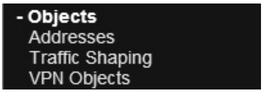
# 7 Objects

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

The Objects section includes Address, Traffic Shaping and VPN objects.

***Note***

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



*Objects Menu*

## 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.

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.

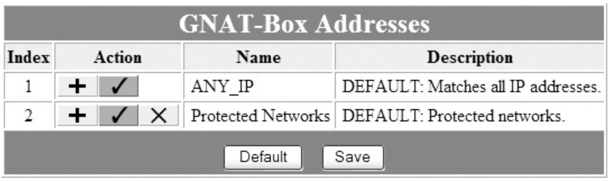
To change an object name without losing connectivity: copy the object, change the name in the copy, enable it, then change the parts of the configuration that reference it. You may then delete the original object.

## Default Address Objects

GNAT Box System Software has two default address objects, ANY_IP and Protected Networks. The ANY_IP address object is essential, so it can be viewed and the description modified, but cannot be deleted. The Protected Networks object contains the IP addresses of each interface with a Protected TYPE field. To return the Address Objects list to this default configuration, click the **DEFAULT** button and save the section.

### Address Object Fields

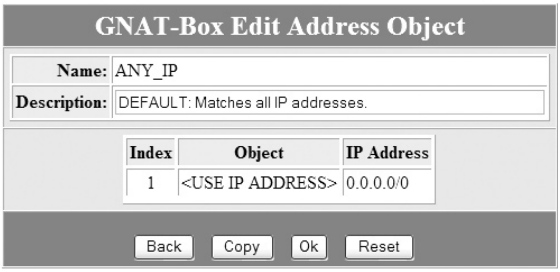
| | |
|---|---|
| Name | Unique name by which the object will be referenced. Name cannot begin with a number. |
| Description | Description of the address object. |
| Object | Previously defined Interface or Address Object as a member of this object. |
| IP address | IP address/netmask to be included in this object. Use this field if Use IP address was selected in the Object field. |



GNAT-Box Addresses

| Index | Action | Name | Description |
|---|---|---|---|
| 1 | + ✓ | ANY_IP | DEFAULT: Matches all IP addresses. |
| 2 | + ✓ × | Protected Networks | DEFAULT: Protected networks. |

*Address Object List*



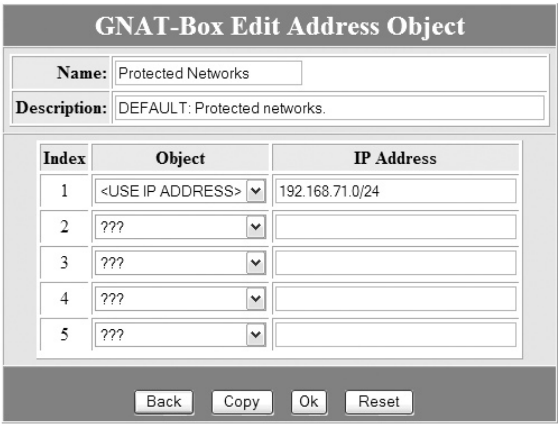
GNAT-Box Edit Address Object

Name: ANY_IP

Description: DEFAULT: Matches all IP addresses.

| Index | Object | IP Address |
|---|---|---|
| 1 | <USE IP ADDRESS> | 0.0.0.0/0 |

*Default "ANY_IP" Address Object*



GNAT-Box Edit Address Object

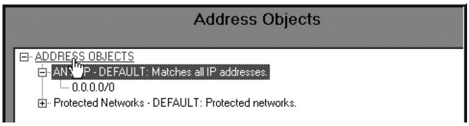
| | |
|---|---|
| **Name:** | Protected Networks |
| **Description:** | DEFAULT: Protected networks. |

| Index | Object | IP Address |
|---|---|---|
| 1 | <USE IP ADDRESS> | 192.168.71.0/24 |
| 2 | ??? | |
| 3 | ??? | |
| 4 | ??? | |
| 5 | ??? | |

*Protected Networks Address Object*

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.

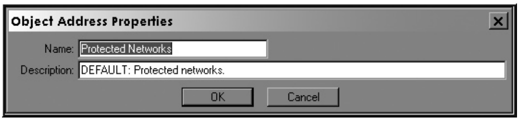
To add a member to the address object, select the address object and click **ADD +**. This will add a new member for the address object: `0.0.0.0-0.0.0.0`. To edit the member, either select an object from the dropdown menu, or enter an IP address/netmask or range. Click **OK**.



Address Objects

ADDRESS OBJECTS
ANY_IP - DEFAULT: Matches all IP addresses.
0.0.0.0/0
Protected Networks - DEFAULT: Protected networks.

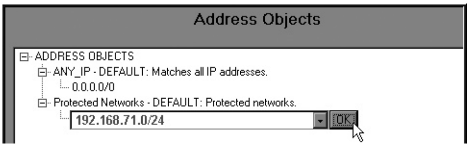
*Address Objects (GBAdmin)*



Object Address Properties

Name: Protected Networks
Description: DEFAULT: Protected networks.

*Address Object Properties (GBAdmin)*



Address Objects

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

*Address Object Add Member* **OK** *(GBAdmin)*

# Traffic Shaping

Traffic Shaping objects allow the administrator to allocate available bandwidth for specific filters and tunnels by defining a bandwidth pipe that can be applied to connections through the use of filters and tunnels. The default object does not restrict traffic, allowing traffic to utilize all available bandwidth, first come, first served. If Traffic Shaping is enabled, the default object cannot be disabled.

Enable Traffic Shaping by selecting the checkbox at the top of the list screen. The default object will be enabled. Other Traffic Shaping objects can be disabled individually.

A filter or tunnel using a Traffic Shaping object restricts users to the amount of bandwidth specified. All users affected will share the allocated bandwidth; filters and tunnels can be defined to command more or less of the allocated or available bandwidth by selecting a weight for each of the filters using the same traffic shaping object. See Chapter 8, Chapter 9 and Chapter 10 for more about weighting traffic shaping objects in filters and tunnels.

## Weight vs. Priority

The weight applied to a filter or tunnel when using a Traffic Shaping object is similar, but not the same as, priority. Two connections with different priorities will use a connection one at a time, the one with the highest priority first. On the other hand, a connection with a higher weight applied to its matching filter or tunnel will use a higher percentage of available bandwidth, still allowing the lower weight connection to use a percentage (though smaller) of the available bandwidth. Weights of 10 have the highest priority, and 1, the lowest.

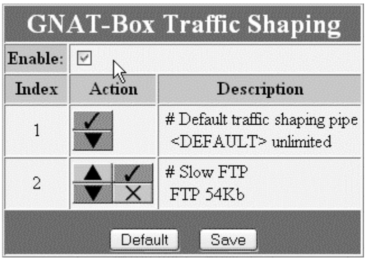
## Using Traffic Shaping or Bandwidth Limiting

Traffic Shaping objects can be used in Remote Access, IP Pass Through or Outbound Filters and in Inbound Tunnels. The following examples show the use of a Traffic Shaping object in an Outbound or IP Pass Through Filter and in an Inbound Tunnel.

### Selecting Traffic Shaping in a Filter

The example Traffic Shaping object is intended to limit the bandwidth that slow FTP connections can use, allowing other, faster traffic more bandwidth. The pipe is 54Kbps and named "FTP," with the description, "Slow FTP."

To utilize this Traffic Shaping object, create an Outbound or IP Pass Through Filter for FTP. This example illustrates using the object in an Outbound Filter.



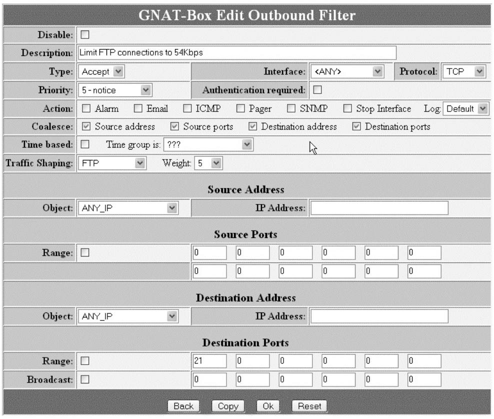
GNAT-Box Traffic Shaping

Enable: ☑

| Index | Action | Description |
|---|---|---|
| 1 | ✓ ▼ | # Default traffic shaping pipe<br><DEFAULT> unlimited |
| 2 | ▲ ✓ ▼ ✕ | # Slow FTP<br>FTP 54Kb |

*Traffic Shaping Example*

In the Outbound filter, select the Traffic Shaping object previously created. Using this "FTP" object, the filter will restrict all inbound and outbound packets, including the virtual crack created for the data, to 54 Kbps, the size of the Traffic Shaping object pipe. Next, select a weight for the connection. The weight selected will prioritize the connections that match the filter.



GNAT-Box Edit Outbound Filter

Disable: □

Description: Limit FTP connections to 54Kbps

Type: Accept Interface: <ANY> Protocol: TCP

Priority: 5 - notice Authentication required: □

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

Coalesce: ☑ Source address ☑ Source ports ☑ Destination address ☑ Destination ports

Time based: □ Time group is: ???

Traffic Shaping: FTP Weight: 5

Source Address

Object: ANY_IP IP Address:

Source Ports

Range: □ 0 0 0 0 0 0

0 0 0 0 0 0

Destination Address

Object: ANY_IP IP Address:

Destination Ports

Range: □ 21 0 0 0 0 0

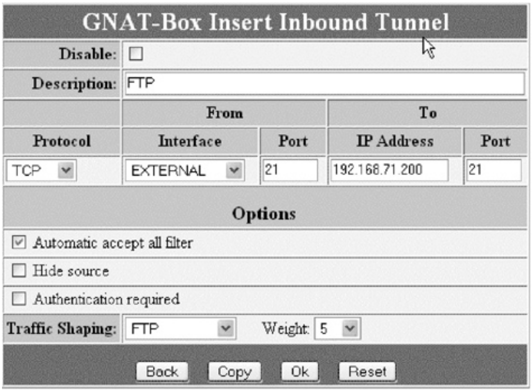
Broadcast: □ 0 0 0 0 0 0

*Outbound Filter with Traffic Shaping*

### Selecting Traffic Shaping on an Inbound Tunnel

Create an inbound tunnel for FTP. (Other protocols can be added to the Inbound Tunnels list by adding the protocol/port number combination in **Filters/IP Protocols**.)

In the Inbound Tunnel, select the Traffic Shaping object previously created. Using this "FTP" object, the tunnel will restrict all inbound and outbound packets, including the virtual crack created for the data, to 54 Kbps, the size of the Traffic Shaping object pipe. Next, select a weight for the connection. The weight selected will prioritize the connections that match the filter.



GNAT-Box Insert Inbound Tunnel

Disable: □

Description: FTP

| | From | | To | |
|---|---|---|---|---|
| Protocol | Interface | Port | IP Address | Port |
| TCP | EXTERNAL | 21 | 192.168.71.200 | 21 |

Options

☑ Automatic accept all filter

□ Hide source

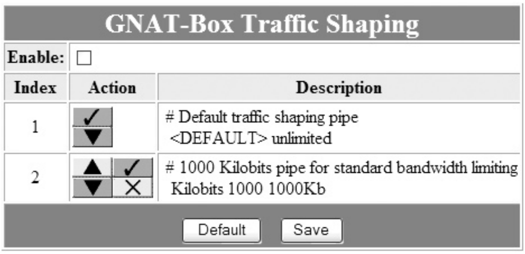
□ Authentication required

Traffic Shaping: FTP Weight: 5

*Inbound Tunnel Using Traffic Shaping*

### Traffic Shaping Objects Fields

| | |
|---|---|
| Disable | Disable defined object. Disabled by default. |
| Description | Description of the traffic shaping pipe. |
| Name | Name by which the objects will be referenced. |
| Bandwidth | Number of kilobits (Kb), kilobytes (KB) or megabytes (MB) to which filters or tunnels using this pipe will be restricted. Bandwidth entered in KB or MB format will be translated to kilobits, e.g., entering `2000 KB` will be translated to `16000` Kb. The largest bandwidth that can be specified is 1,000,000 Kb. A "0" indicates that the object allows unlimited use of the available bandwidth. |

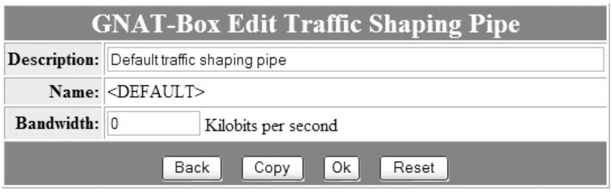


GNAT-Box Traffic Shaping

Enable: □

| Index | Action | Description |
|---|---|---|
| 1 | ✓<br>▼ | # Default traffic shaping pipe<br><DEFAULT> unlimited |
| 2 | ▲ ✓<br>▼ ✕ | # 1000 Kilobits pipe for standard bandwidth limiting<br>Kilobits 1000 1000Kb |

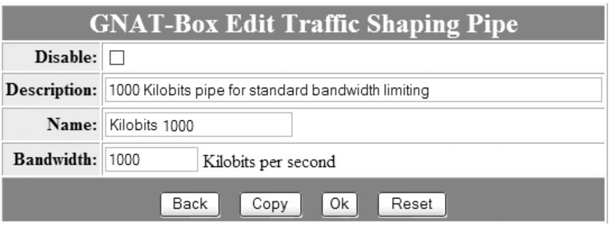
*Traffic Shaping Objects List*



GNAT-Box Edit Traffic Shaping Pipe

| | |
|---|---|
| Description: | Default traffic shaping pipe |
| Name: | <DEFAULT> |
| Bandwidth: | 0 Kilobits per second |

*Default Traffic Shaping Object*



GNAT-Box Edit Traffic Shaping Pipe

| | |
|---|---|
| Disable: | □ |
| Description: | 1000 Kilobits pipe for standard bandwidth limiting |
| Name: | Kilobits 1000 |
| Bandwidth: | 1000 Kilobits per second |

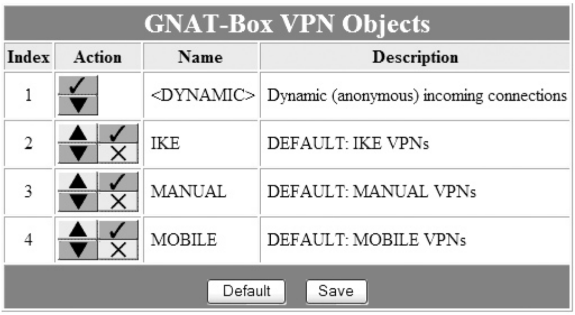
*Traffic Shaping Object*

# 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

Four VPN objects are created by default: an IKE, Manual, Mobile and Dynamic VPN Object. Defaulting VPN Objects resets the firewall to factory settings, reverting to these default objects.



GNAT-Box VPN Objects

| Index | Action | Name | Description |
|---|---|---|---|
| 1 | ✓ ▼ | <DYNAMIC> | Dynamic (anonymous) incoming connections |
| 2 | ▲ ▼ ✓ ✕ | IKE | DEFAULT: IKE VPNs |
| 3 | ▲ ▼ ✓ ✕ | MANUAL | DEFAULT: MANUAL VPNs |
| 4 | ▲ ▼ ✓ ✕ | MOBILE | DEFAULT: MOBILE VPNs |

*VPN Object List*

### Dynamic VPN Object

The Dynamic VPN Object functionality is inherent in the GNAT Box VPN's dynamic to static connection, allowing users to access the firewall from a dynamic IP address. It is used automatically during authentication (Phase I) of the connection. The Dynamic VPN Object settings can be customized in version 3.5 and higher, but GTA recommends using the factory default settings.

### Default Dynamic VPN Object Fields

Description Description of the object.

Name Name by which the objects will be referenced.

Local identity (type) IP address (default), Domain name or Email address. Identifies the VPN by the firewall's external IP address, host name (Fully-Qualified Domain Name/FQDN) or address in the email format: name@hostname.domain (User FQDN). The User FQDN represents a fully-qualified username string and is used when the user will not have a fixed IP address.

Selecting IP address or Domain (host) name without entering the Local identity value, below, uses the IP address or host name from Network Information.

Local identity (value) If something other than the firewall’s identity in Network Information is required, enter an IP address or Domain (host) name. If Email address was selected in the Local identity (type) field, enter the email address that matches the other end of the VPN connection.

**Phase I**

For mobile connections, Phase I will default to Aggressive, 3DES, HA-1, Diffie-Hellman Group 2 and Lifetime 90 minutes.

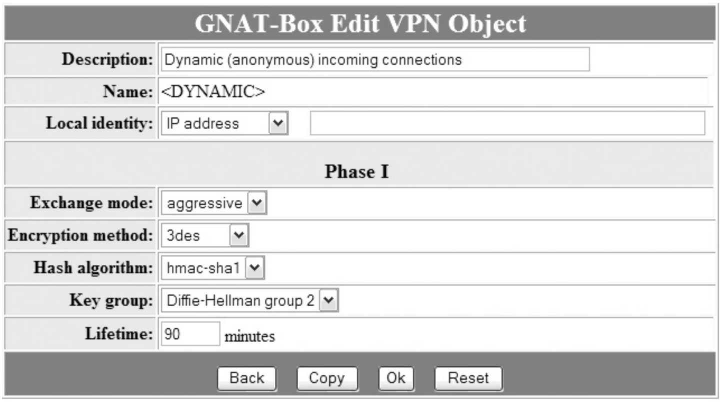
Exchange Mode Aggressive: Static IP to Dynamic IP (fixed value).

Encryption Method Encryption method that the GTA Firewall will accept from a connection initiator during Phase I. 3DES (default for Dynamic Object), AES (128, 192 and 256), Blowfish, DES, and Strong (Any). GTA Firewall initiates connections using Blowfish.

Hash Algorithm Hash method used for the Phase I authentication transformation. All, HMAC-MD5, HMAC-SHA-1 (default for Dynamic Object); HMAC-SHA-2. “All” allows the GTA Firewall to accept any of the hash 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. GNAT Box System Software uses Group 2 by default.

Lifetime TTL (Time to Live) for this connection. 90 minutes by default.



GNAT-Box Edit VPN Object

Description: Dynamic (anonymous) incoming connections

Name: <DYNAMIC>

Local identity: IP address

Phase I

Exchange mode: aggressive

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

Lifetime: 90 minutes

*VPN Object Default Dynamic*

## VPN Objects Fields

Disable
Disable all access for the selected object.

Description
Description of the object.

Name
Name by which the objects will be referenced.

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
Select the address object that has been defined for the local network that is to be accessible via the VPN, or enter the IP address and mask of the local network, typically a Protected Network, PSN or a subnet of either.

Local identity (type)
IP address (default), Domain name or Email address. Identifies the VPN by the firewall’s external IP address, host name (Fully-Qualified Domain Name/FQDN) or address in the email format: name@hostname.domain (User FQDN). The User FQDN represents a fully-qualified username string and is used when the user will not have a fixed IP address.

Selecting IP address or Domain (host) name without entering the Local identity value, below, uses the IP address or host name from Network Information.

Local identity (value)
If something other than the firewall’s identity in Network Information is required, enter an IP address or Domain (host) name. If Email address was selected in the Local identity (type) field, enter the email address that matches the other end of the VPN connection.

### Phase I

In IKE, 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 (see the default Dynamic VPN Object), Phase I will default to Aggressive, 3DES, HA-1, Diffie-Hellman Group 2 and Lifetime 90 minutes.

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 static IP address, 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

Encryption method that the GTA Firewall will accept from a connection initiator during Phase I. 3DES, AES-128, AES-192, AES-256, Blowfish, DES, and Strong (Any). GTA Firewall initiates connections using Blowfish.

Hash Algorithm

Hash method used for the Phase I authentication transformation. All, HMAC-MD5, HMAC-SHA-1; HMAC-SHA-2. "All" allows the GTA Firewall to accept any of the hash 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.

Lifetime

Time to Live for this connection. 90 minutes by default.

### Phase II

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

Encryption Method

Select the method for the Encapsulating Security Payload (ESP) transformation: 3DES, AES (128, 192 and 256), Blowfish, DES, None, Null or Strong. Strong means that any algorithm except None and Null will be accepted from the remote initiator. Null is a special case where there is only IP encapsulation. It has little impact on performance, and is useful when unsupported protocols are used in NAT mode between firewalls. GTA Firewall initiates connections using AES-128.

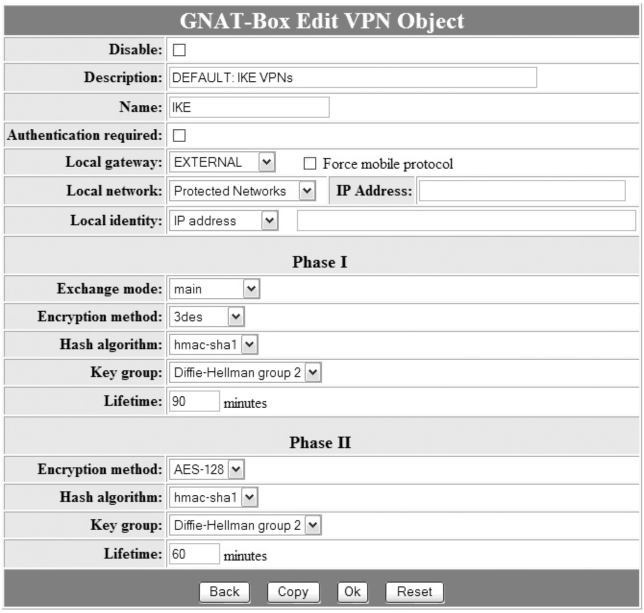
Hash Algorithm — All, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2, None. Select the method that will be used for the Phase II authentication transformation. Selecting None will result in no AH (Authentication Header) transformation being applied to the packet.

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.

Lifetime — Time to Live for this connection. 60 minutes by default for IKE and MANUAL objects, 15 minutes for MOBILE.

***Note***

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 Edit VPN Object**

Disable: □

Description: DEFAULT: IKE VPNs

Name: IKE

Authentication required: □

Local gateway: EXTERNAL □ Force mobile protocol

Local network: Protected Networks IP Address:

Local identity: IP address

**Phase I**

Exchange mode: main

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

Lifetime: 90 minutes

**Phase II**

Encryption method: AES-128

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman group 2

Lifetime: 60 minutes

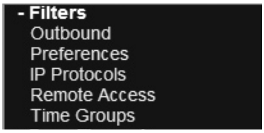
*VPN Object*

# 8 Filters

Filters control access to and through the GTA Firewall. Outbound and Remote Access Filters are created in functions under the Filters section, while IP Pass Through Filters are created in the first IP Pass Through section. Most Automatic Filter options are not directly defined by the user. However, Inbound Tunnels can be configured using an Automatic Accept All filters option, and Stealth mode can be turned on or off in Filter Preferences.

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 at the beginning of this chapter to create Outbound, Remote Access and IP Pass Through Filters.

The Filters configuration section includes Outbound Filters, Filter Preferences, Protocols, Remote Access Filters and Time Groups.



*Filter Menu*

## Managing Filters

Outbound, Remote Access and IP Pass Through Filters use the same mechanisms for filter configuration, so refer to this section to manage filters.

### Filter Sets

A filter set is all filters of a type. The order of the set is important. Each packet is compared to the appropriate set starting at filter one (Index 1). The packet is compared 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; 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 are 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** button to auto-configure an initial set of filters according to the defined configuration. Auto-configured filters will be left disabled or enabled according to their factory default (the most secure setting).
- The Default command ***does not*** reset to original factory filters.
- When a filter set is auto-configured, the filters do not retain manual changes. If you have custom filters you wish to save, either create new filters manually or print a copy of your configuration before auto-configuration to use in restoring custom filters.
- Changes to filters will not be effective until the section is saved. If you leave the filter or filter set without saving, changes will be lost.
- 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 new filter in the desired location and 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, and are often served from the same system.

### Filter Fields

Description
Description of the filter for reference. Any filters generated by the system will have descriptions with a label such as Email Proxy, No RIP or Stealth.

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 IP Protocols 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. Using IP Pass Through, all protocols can be used with either filter.

Priority
Notice sent with the alarm event. Defined by the user.

Authentication required
Authentication allows the administrator to require users to authenticate to the firewall using GBAuth before initiating a connection. By default, GTA’s user authentication is served on TCP port 76.

Actions
Actions 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.

Coalesce
Coalescing blends similar data into a single log event: Source address/ports, Destination address/ports. Enabled by default in new and auto-configured filters.

Interval in Filter Preferences is a global option for all coalescing. Set the interval to zero (0) to turn off ***all*** coalescing. Coalescing selected in Filter Preferences applies only to Automatic Filters.

Time based
Make the filter operate at a specified time.

Time group is
Time parameters for the filter. “???” means no time group has been selected.

Traffic Shaping
Object that defines the pipe to apply to this filter. The **Default** Traffic Shaping object allows unlimited access to the available bandwidth. (Traffic shaping must be enabled under **Objects/Traffic Shaping**.)

Weight
Priority when accessing the pipe’s allocated bandwidth. Weights of 10 have the highest priority, and 1, the lowest.

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
Choose a range of ports to which this filter will apply.

Source Ports
Single or multiple ports, or a range of ports. Leave blank to allow any source port to be accepted. The source port for most client protocols is a random value above 1024. Specified Source Ports are matched against the source port of the IP packet. For Ports, see the Appendix, Ports and Services section.

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
Choose a range of ports.

Broadcast
Select 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.

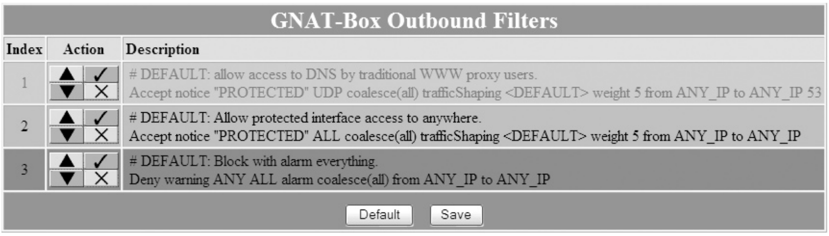
## Outbound Filters

Outbound Filters control access from hosts on Protected networks and PSNs to IP addresses that reside on an external network, and from hosts on a Protected Network to those that reside external to a PSN.

TCP, UDP, ICMP, IGMP, ESP, AH or any other protocol defined in IP Protocols can be matched against the packet.

The implicit rule, “that which is not explicitly allowed is denied,” applies to both outbound packets and inbound packets. The rule is explicitly listed in the Outbound Filters in version 3.5 and higher. See Index #3 in the illustration below.

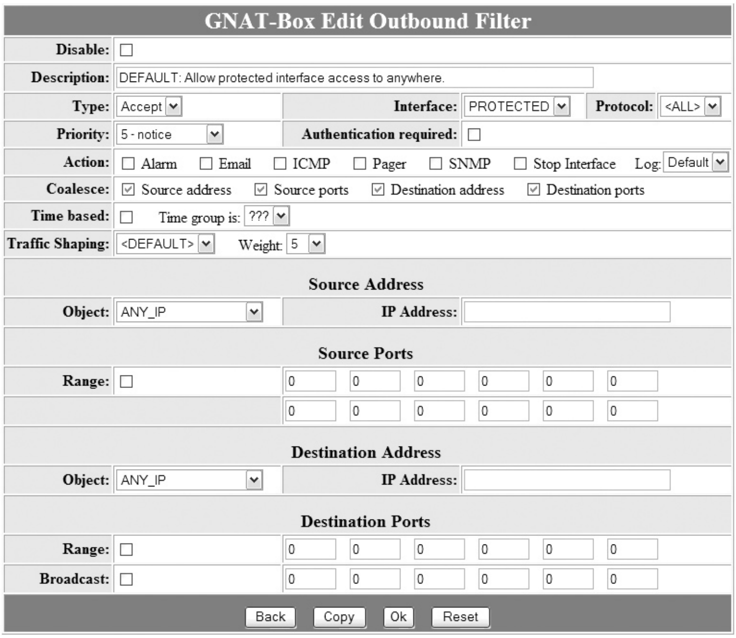
The factory default set of Outbound Filters allows all IP addresses on the Protected Network to access any IP address and service external to the Protected Network. If a PSN interface exists, a similar Outbound Filter will be auto-configured that allows all access to the External Network but not to the Protected Network. These filters can be modified or deleted according to local network security policy.



GNAT-Box Outbound Filters

| Index | Action | Description |
|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | # DEFAULT: allow access to DNS by traditional WWW proxy users.<br>Accept notice "PROTECTED" UDP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 53 |
| 2 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow protected interface access to anywhere.<br>Accept notice "PROTECTED" ALL coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP |
| 3 | ▲ ✓<br>▼ ✕ | # DEFAULT: Block with alarm everything.<br>Deny warning ANY ALL alarm coalesce(all) from ANY_IP to ANY_IP |

*Outbound Filters Set*



GNAT-Box Edit Outbound Filter

Disable: □

Description: DEFAULT: Allow protected interface access to anywhere.

Type: Accept | Interface: PROTECTED | Protocol: <ALL>

Priority: 5 - notice | Authentication required: □

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

Coalesce: ☑ Source address ☑ Source ports ☑ Destination address ☑ Destination ports

Time based: □ Time group is: ???

Traffic Shaping: <DEFAULT> Weight: 5

Source Address

Object: ANY_IP | IP Address:

Source Ports

Range: □ 0 0 0 0 0 0

0 0 0 0 0 0

Destination Address

Object: ANY_IP | IP Address:

Destination Ports

Range: □ 0 0 0 0 0 0

Broadcast: □ 0 0 0 0 0 0

*Outbound Filter*

## Preferences

Filter Preferences allows the administrator to globally define most logging and filter options for user-defined filters in one location, as well as enable or disable Stealth mode. Logging options for automatic filters, tunnel connections (“opens” and “closes”) and filter blocks have been added. ICMP packets dropped by Stealth mode can be logged.

Default logging options are used when the **Default** option is selected in a filter definition Log field, allowing the event selected to be logged whenever the filter is activated. All protocols are logged by default.

Automatic filters are generated by the firewall to allow expected events such as response packets from DNS queries and mail servers. Automatic filters can be logged and disabled. GTA recommends disabling automatic filters only for troubleshooting and configuration testing.

See Appendix B – Log Messages for log examples.

## General

In General Preferences, filter actions basic to the firewall may be adjusted. The administrator can enable or disable filters, generate alarms, send email, send an ICMP “service not available” message, or log a filtered event.

### Address Spoof

A spoof occurs when a packet arrives at one interface and its return path is through a different interface. This may be caused by an intrusion attempt made altering the packet source IP address; or a mis-configured firewall, e.g., when networks or hosts located on, or connected to, the internal side of a firewall have not been defined.

### Doorknob Twist

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.

### Fragmented Packets

By default, fragmented packets are reassembled and forwarded only if the resulting packet does not violate security policy; otherwise, they are dropped.

### Invalid Packets

Invalid packets are those that are not the expected size or have an invalid option bit; e.g., an ICMP port unreachable packet must have at least 28 bytes. Invalid packets are dropped silently by default, but the system now includes the ability to log dropped packets.

### Unexpected Packets

If a packet is valid, but not expected by the state table, the firewall denies it, e.g., a packet can only generate a single ICMP port unreachable response; a second one may indicate an ICMP replay attack; also, an unexpected packet may be a packet that does not have the correct flags during TCP’s three-way handshake. The system now includes the ability to log these packets.

### Stealth Mode

Stealth mode is the factory set default for new GTA Firewall systems. In Stealth mode, the firewall will not respond to ICMP ping requests, ICMP traceroute requests nor UDP traceroute requests. Filters that allow pings, traceroutes, etc., from the External interface are not functional when the firewall is in stealth mode. In addition, the firewall will not respond with an ICMP message when a packet arrives for a port without a tunnel or service set on any External Network interface. Because it is activated at the system kernel level, Stealth mode filtering will not appear in the Active Filters list.

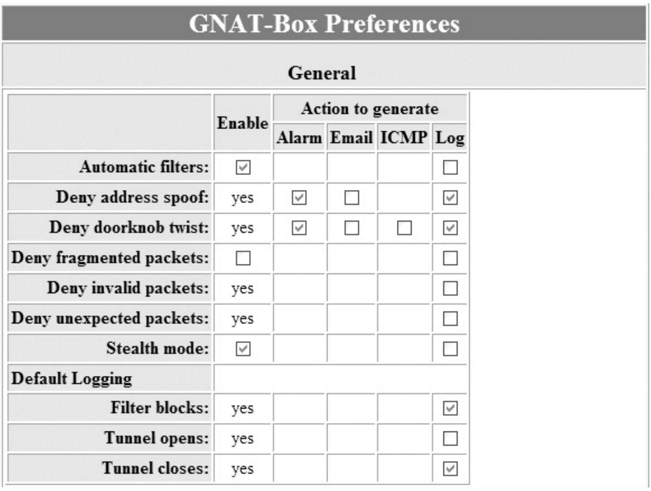
Like all Automatic Filters, Stealth mode has priority over the other filter types.

### Note

Stealth mode does not affect Protected Network or Private Service Network interfaces. If you wish to set Stealth mode for these interfaces, create the appropriate Remote Access Filter.

## Preferences Fields – General

| | |
|---|---|
| Automatic Filters | Options: Enable/Disable; Log. |
| Deny address spoof | Always enabled. Options: Alarm, Email, Log. |
| Deny doorknob twist | Always enabled. Options: Alarm, Email, ICMP, Log. |
| Deny fragmented packets | Options: Enable/Disable, Log. Can be used to block some fragment attacks. |
| Deny invalid packets | Always enabled. Option: Log packets. |
| Deny unexpected packets | Always enabled. Option: Enable/Disable, Log. |
| Stealth Mode | Options: Enable/Disable, Log. Stealth mode has priority over other filters. |
| | **Default Logging** |
| Filter Blocks | Always enabled. Option: Log, enabled by default. |
| Tunnel Opens | Always enabled. Option: Log, disabled by default. |
| Tunnel Closes | Always enabled. Option: Log, enabled by default. Refer to tunnels created by the action of a filter (automatic or user-defined) or an inbound tunnel. |



**GNAT-Box Preferences**

**General**

| | Enable | Action to generate | | | |
|---|---|---|---|---|---|
| | | Alarm | Email | ICMP | Log |
| Automatic filters: | ☑ | | | | □ |
| Deny address spoof: | yes | ☑ | □ | | ☑ |
| Deny doorknob twist: | yes | ☑ | □ | □ | ☑ |
| Deny fragmented packets: | □ | | | | □ |
| Deny invalid packets: | yes | | | | □ |
| Deny unexpected packets: | yes | | | | □ |
| Stealth mode: | ☑ | | | | □ |
| Default Logging | | | | | |
| Filter blocks: | yes | | | | ☑ |
| Tunnel opens: | yes | | | | □ |
| Tunnel closes: | yes | | | | ☑ |

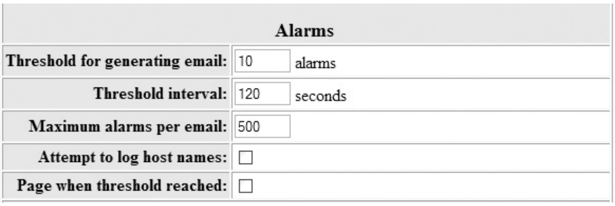
*Filter Preferences – General*

## Alarms

This section allows the default parameters for alarm notifications to be set. When a filter 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. Multiple messages will be sent if the number of events exceeds the maximum count.

**Preferences Fields – Alarms**

| | |
|---|---|
| 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. |



| 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: | □ |

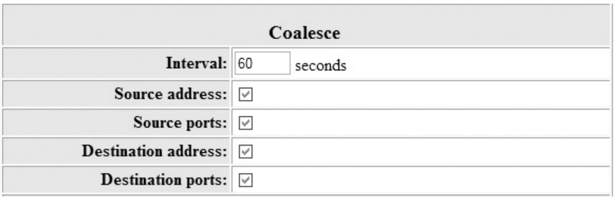
*Filter Preferences – Alarms*

## Coalesce

Data coalescing reduces the amount of individual filter event data that enters the logs, blending similar data into a single log event. Coalescing selected in Filter Preferences applies only to Automatic Filters, such as those created by a tunnel when Automatic accept all is selected on an Inbound Tunnel definition. Coalescing is enabled by default in Filter Preferences. The Interval is a global option for all filter event coalescing. Set the interval to zero (0) to turn off ***all*** coalescing.

**Preferences Fields – Coalesce**

| | |
|---|---|
| Interval | 60 seconds by default. Zero (0) turns off all coalescing. |
| Source address | Enabled by default. |
| Source ports | Enabled by default. |
| Destination address | Enabled by default. |
| Destination ports | Enabled by default. |



| Coalesce | |
|---|---|
| Interval: | 60 seconds |
| Source address: | ☑ |
| Source ports: | ☑ |
| Destination address: | ☑ |
| Destination ports: | ☑ |

*Filter Preferences – Coalesce*

## Email Server

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.

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

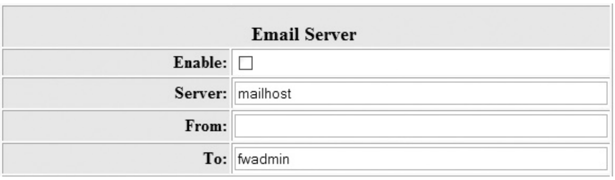
### Preferences Fields – Email Server

Enable Send email and alarm notifications. Disabled by default.

Server DNS host name or IP address of the email server for alarms and email notification messages, `mailhost` by default.

From Email address that will appear in "From" field. 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, `fwadmin` by default. The address can be a fully-qualified address, such as `jdoe@gta.com`, or the mailbox name on the specified email server: `jdoe`.



| Email Server | |
|---|---|
| Enable: | □ |
| Server: | mailhost |
| From: | |
| To: | fwadmin |

*Filter Preferences – Email Server*

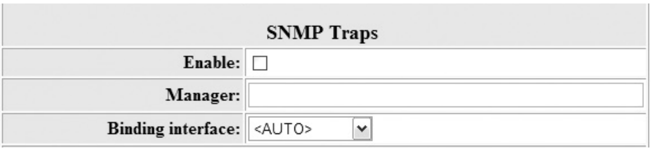
## SNMP Traps

Simple Network Management Protocol (SNMP) is a standard for managing and retrieving data from each network IP device and sending it to designated hosts. If SNMP is not enabled, selecting SNMP filter actions on the filter definition screen has no effect. 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.

Selecting Auto in the BINDING INTERFACE field will select the interface configured in Network Information through which the packet would normally exit based on the routing table.

### Preferences Fields – SNMP Traps

| | |
|---|---|
| Enable SNMP | Enable the SNMP alarm facility. Disabled by default. |
| Manager | Host IP address to receive SNMP trap messages. |
| Binding interface | Address from which SNMP traps are sourced, Auto by default. To force the SNMP traps to have a specific source IP address, choose the Interface object from the dropdown list. |



**SNMP Traps**

| | |
|---|---|
| Enable: | □ |
| Manager: | |
| Binding interface: | <AUTO> |

*Filter Preferences – SNMP Traps*

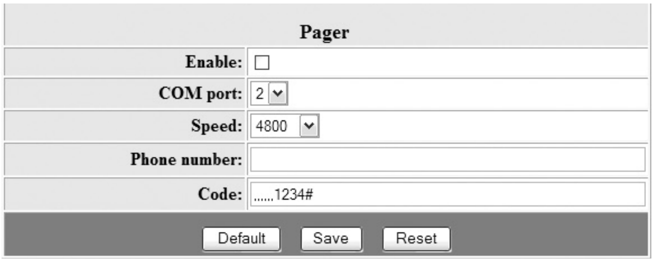
## Pager

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

The CODE field 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.

### Preferences Fields – Pager

| | |
|---|---|
| Enable | Enables the Pager alarm facility. Disabled by default. |
| COM Port | COM port to which the modem used for paging is attached. Choose COM ports 1 through 4. COM 3 by default. |
| Speed | DTE speed at which the firewall will communicate with the modem. 4800 by default. |
| Phone number | Telephone number for the target numeric pager. Enter all numbers and dialing codes required to make a call. |
| Code | Numeric value that will be displayed on the pager. |



**Pager**

| | |
|---|---|
| Enable: | □ |
| COM port: | 2 |
| Speed: | 4800 |
| Phone number: | |
| Code: | ......1234# |

*Filter Preferences – Pager*

## IP Protocols

IP Protocols allows the user to define protocols to make available when creating filters. Using the IP Protocols function, the administrator can explicitly deny a protocol on a certain port in order to generate specific log entries.

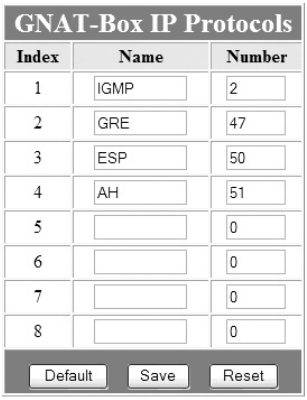
The implicit rule of GNAT Box Systems, "that which is not explicitly allowed is denied," combined with the default in which all rejected packets are logged, can make the "unknown protocol" log events too numerous. Identifying a protocol is useful in reducing these extraneous events.

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, create and enable an appropriate filter to deny the protocol on that port, log it in a specific manner, or explicitly prevent it from being logged.

By default, the Protocols section contains the protocol/port combinations IGMP/2, GRE/47, ESP/50 and AH/51. Defaulting the IP Protocols section will delete customized protocols and restore these defaults. Remove protocols by deleting the field entries and saving the section.

Protocols are saved in the order of the protocol number.



GNAT-Box IP Protocols

| Index | Name | Number |
|---|---|---|
| 1 | IGMP | 2 |
| 2 | GRE | 47 |
| 3 | ESP | 50 |
| 4 | AH | 51 |
| 5 |  | 0 |
| 6 |  | 0 |
| 7 |  | 0 |
| 8 |  | 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. See Managing Filters at the beginning of this chapter for filter set information, tips and fields for filters.

TCP, UDP, ICMP, IGMP, ESP, AH or any other protocol defined in IP Protocols can be matched against the packet.

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 auto-configured filters that reflect the system's configuration. These filters can be used as is, or modified to suit the local network security policy.

## Muffle Benign Protocols

Some events which are implicitly blocked and logged by the firewall are known to be harmless. To suppress the logging of these “benign” protocols, create and enable a Remote Access Filter that will explicitly block the protocol, but not log the event. Use these parameters:

| | |
|---|---|
| Type | Deny (to block the protocol.) |
| Interface | Interface for which block event should not be logged. To “no log” the event on all interfaces, select **<ANY>**. |
| Protocol | Protocol to block. |
| Log | No. |

Select the source address and ports and destination address and ports for which this blocked protocol event should not be logged.

Order is important. Place the No Log filter in the set after any filters that specifically allow and/or log this event in certain cases, and before more restrictive filters.

## Access a Protected Network from a PSN

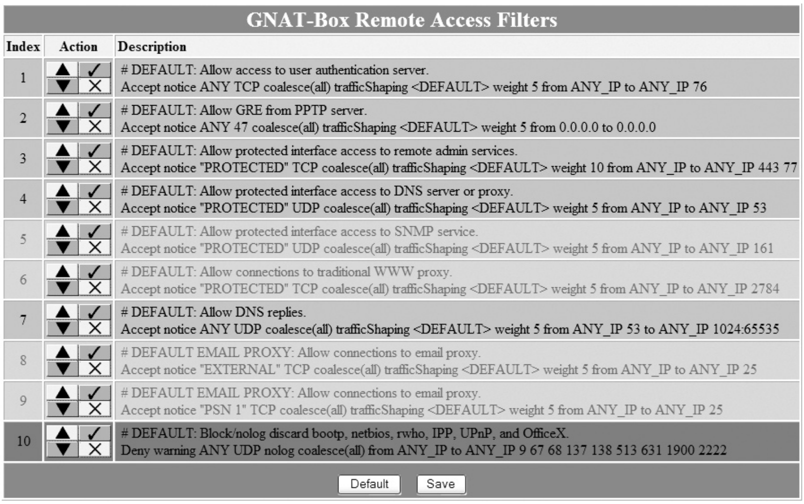
By default, the PSN is untrusted by the Protected Network and may not initiate connections between the two, just as the External Network is untrusted by the networks behind the firewall. However, sometimes it is more efficient to allow the PSN to access a Protected Network for selected services.

Access should be as limited as possible: you can use either an inbound tunnel with an Auto Accept filter or an Allow Remote Access Filter and tunnel on the Protected Network. Using a Remote Access Filter allows the administrator to tightly regulate access and use Network Address Translation to hide the real IP address of the Protected Network from the PSN – and any potential hacker.

The PSN to PRO filter should include these parameters:

| | |
|---|---|
| Type | Accept. |
| Interface | PSN. |
| Protocol | **<ALL>** or select the desired protocol. |

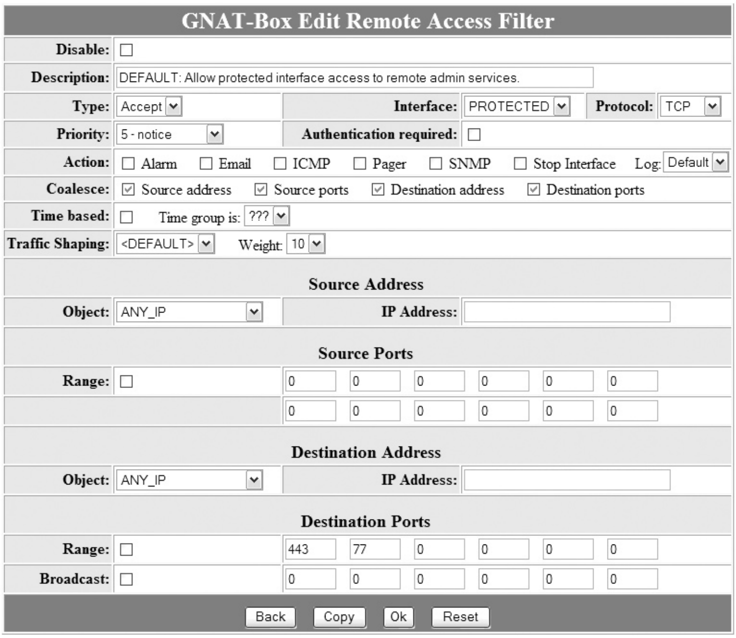
Select the Source IP address and port from which this access will be initiated, then select the connection’s Destination IP address and port on the PSN which should match the beginning of the tunnel.



GNAT-Box Remote Access Filters

| Index | Action | Description |
|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow access to user authentication server.<br>Accept notice ANY TCP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 76 |
| 2 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow GRE from PPTP server.<br>Accept notice ANY 47 coalesce(all) trafficShaping <DEFAULT> weight 5 from 0.0.0.0 to 0.0.0.0 |
| 3 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow protected interface access to remote admin services.<br>Accept notice "PROTECTED" TCP coalesce(all) trafficShaping <DEFAULT> weight 10 from ANY_IP to ANY_IP 443 77 |
| 4 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow protected interface access to DNS server or proxy.<br>Accept notice "PROTECTED" UDP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 53 |
| 5 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow protected interface access to SNMP service.<br>Accept notice "PROTECTED" UDP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 161 |
| 6 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow connections to traditional WWW proxy.<br>Accept notice "PROTECTED" TCP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 2784 |
| 7 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow DNS replies.<br>Accept notice ANY UDP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP 53 to ANY_IP 1024:65535 |
| 8 | ▲ ✓<br>▼ ✕ | # DEFAULT EMAIL PROXY: Allow connections to email proxy.<br>Accept notice "EXTERNAL" TCP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 25 |
| 9 | ▲ ✓<br>▼ ✕ | # DEFAULT EMAIL PROXY: Allow connections to email proxy.<br>Accept notice "PSN 1" TCP coalesce(all) trafficShaping <DEFAULT> weight 5 from ANY_IP to ANY_IP 25 |
| 10 | ▲ ✓<br>▼ ✕ | # DEFAULT: Block/nolog discard bootp, netbios, rwho, IPP, UPnP, and OfficeX.<br>Deny warning ANY UDP nolog coalesce(all) from ANY_IP to ANY_IP 9 67 68 137 138 513 631 1900 2222 |

*Remote Access Filters Set (Partial)*



GNAT-Box Edit Remote Access Filter

Disable: □

Description: DEFAULT: Allow protected interface access to remote admin services.

Type: Accept | Interface: PROTECTED | Protocol: TCP

Priority: 5 - notice | Authentication required: □

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

Coalesce: ☑ Source address ☑ Source ports ☑ Destination address ☑ Destination ports

Time based: □ Time group is: ???

Traffic Shaping: <DEFAULT> Weight: 10

Source Address

Object: ANY_IP | IP Address:

Source Ports

Range: □ 0 0 0 0 0 0

0 0 0 0 0 0

Destination Address

Object: ANY_IP | IP Address:

Destination Ports

Range: □ 443 77 0 0 0 0

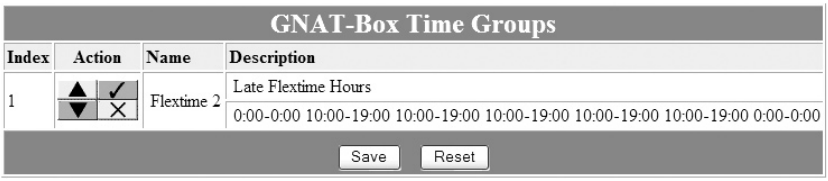
Broadcast: □ 0 0 0 0 0 0

*Remote Access Filter*

# 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.



GNAT-Box Time Groups

| Index | Action | Name | Description |
|---|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | Flextime 2 | Late Flextime Hours<br>0:00-0:00 10:00-19:00 10:00-19:00 10:00-19:00 10:00-19:00 10:00-19:00 0:00-0:00 |

*Time Group List*

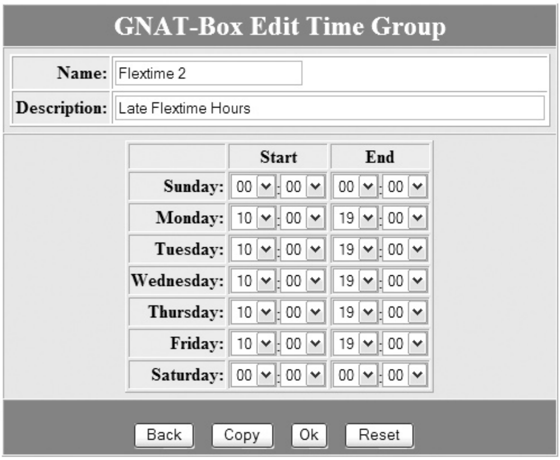
## Time Group Fields

**Name** Name that will appear in the Time Group  selection list when defining the filter.

**Description** Description of the time group.

**Start** Time to begin applying the filter.

**End** Time to stop applying the filter.



GNAT-Box Edit Time Group

Name: Flextime 2

Description: Late Flextime Hours

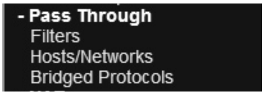
| | Start | End |
|---|---|---|
| Sunday: | 00 : 00 | 00 : 00 |
| Monday: | 10 : 00 | 19 : 00 |
| Tuesday: | 10 : 00 | 19 : 00 |
| Wednesday: | 10 : 00 | 19 : 00 |
| Thursday: | 10 : 00 | 19 : 00 |
| Friday: | 10 : 00 | 19 : 00 |
| Saturday: | 00 : 00 | 00 : 00 |

*Time Group*

# 9 Pass Through

Functions in the Pass Through section allow the user to route protocols through the firewall. IP Pass Through, found in the Filters and Hosts/Networks sections, route protocols through the firewall without Network Address Translation.

The Bridged Protocols section allows the user to route specified Ethernet protocols through the firewall in bridging mode, bypassing all firewall filtering on specified ports.



*Pass Through Menu*

## IP Pass Through (No NAT)

By default, all packets going outbound through the firewall that are destined for the External or PSN interfaces are translated to the IP address of that interface (Network Address Translation or NAT). IP Pass Through is the GTA term for "no NAT," and the Pass Through Filters and Hosts/Networks allow the administrator to define a host, subnet or network and port that will not have NAT applied to packets from specified IP addresses. IP Pass Through filters support all IP protocols.

When you can define IP Pass Through:

- From the Protected Network to the PSN, External or another Protected network.
- From a PSN to the External or another PSN network.

IP Pass Through can be defined for packets from a host on a:

- Protected Network outbound through PSN and External Interface.
- Protected Network outbound through a PSN Interface only.
- Protected Network outbound through an External Interface only.
- PSN outbound through an External Interface only.
- Protected Network to a host on another Protected Network.

IP Pass Through requires a routable address on the internal subnet if the Pass Through tunnel goes to the Internet through the External interface. Otherwise, the address can be a non-routable (RFC 1918) public address. For more information on RFC 1918 addresses, go to `http://www.gnatbox.com/Pages/text/rfc1918.txt`.

NAT is not performed on inbound connections: from the External network to the PSN or Protected Network; and from the PSN to the Protected network.

A Pass Through requires the following to operate correctly:

1. Define the IP address in Hosts/Networks or set up a bridging interface.
2. An IP Pass Through filter must be created to allow packets to flow from and/or to the IP Pass Through IP address.
3. If the IP Pass Through is going to the Internet, a static route must be added to the Internet router pointing to the External Interface of the GTA Firewall as the gateway to the internal network. This is a key point, without this route the pass through will fail. Return packets will not know how to get back to the internal network.

***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, 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

Pass Through Filters control access to and from addresses that have been specified as IP Pass Through. These filters are different from Remote Access and Outbound Filters in that they control both inbound and outbound access. Since Pass Through addresses are not translated, the GTA Firewall functions as a router or gateway for these addresses.

Pass Through Filters utilize IP Pass Through addresses in the definitions, not firewall network interface addresses.

Pass Through Filters are used in three cases:

1. When Pass Through hosts/networks are defined.
2. When setting up VPNs.
3. When the firewall is using bridging mode.

Typically, two filters are required for each hosts/networks IP address, one for outbound and the other for inbound access. If Pass Through hosts/networks are defined, auto-configuring filters will create a set based on the addresses defined on the Hosts/Networks screen. The auto-configured (default) filters will vary according to options selected.

The implicit rule, “that which is not explicitly allowed is denied,” applies to Pass Through filters. The rule is explicitly listed in the Pass Through Filters in version 3.5 and higher. See Index #5 in the illustration below.

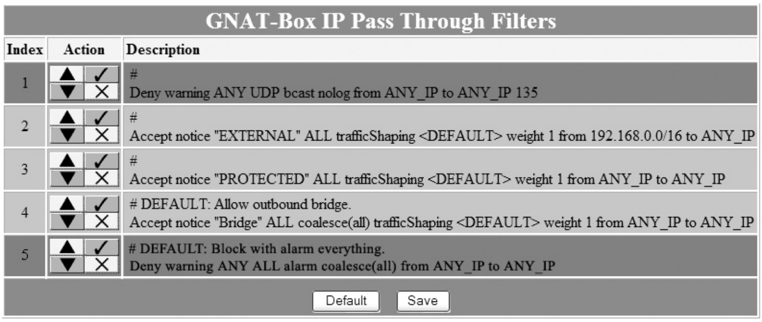
Pass Through filters are defined in the same manner as Remote Access or Outbound filters, and the rules concerning filter order also apply. See Managing Filters in **Chapter 8 – Filters** for filter set information, tips and fields for filters.

### Pair of Filters for a Defined IP Pass Through Host

A Pass Through address must have two filters, inbound and outbound.Create the outbound connection filter by adding an empty filter definition, or editing an existing 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. Click **OK**.

Create the inbound connection filter by adding an empty filter definition, or editing an existing filter. Define the filter as you would a Remote Access Filter except that the destination IP address will be the Pass Through address, not the IP address on the GTA Firewall network interface. Click **OK**.

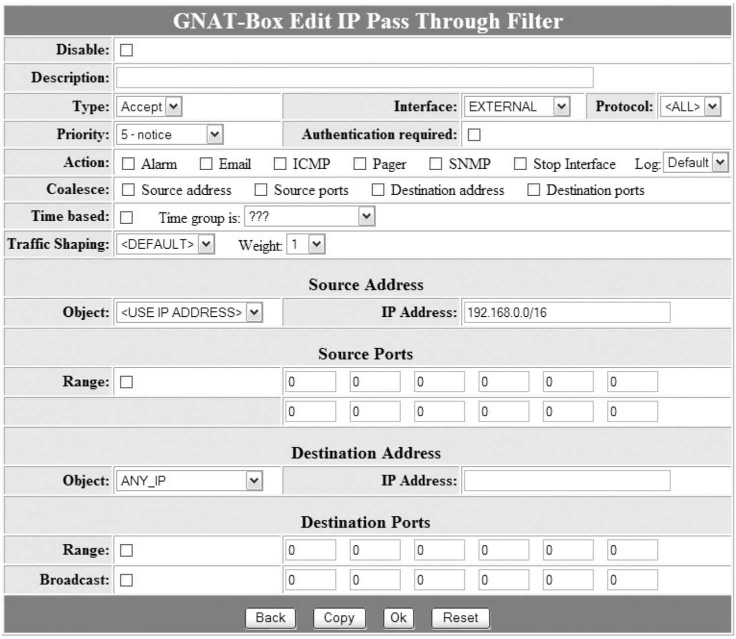
Once you have completed all the desired Pass Through Filters, click the **SAVE** button on the filter set to save the filters and apply them to the system.



GNAT-Box IP Pass Through Filters

| Index | Action | Description |
|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | #<br>Deny warning ANY UDP bcast nolog from ANY_IP to ANY_IP 135 |
| 2 | ▲ ✓<br>▼ ✕ | #<br>Accept notice "EXTERNAL" ALL trafficShaping <DEFAULT> weight 1 from 192.168.0.0/16 to ANY_IP |
| 3 | ▲ ✓<br>▼ ✕ | #<br>Accept notice "PROTECTED" ALL trafficShaping <DEFAULT> weight 1 from ANY_IP to ANY_IP |
| 4 | ▲ ✓<br>▼ ✕ | # DEFAULT: Allow outbound bridge.<br>Accept notice "Bridge" ALL coalesce(all) trafficShaping <DEFAULT> weight 1 from ANY_IP to ANY_IP |
| 5 | ▲ ✓<br>▼ ✕ | # DEFAULT: Block with alarm everything.<br>Deny warning ANY ALL alarm coalesce(all) from ANY_IP to ANY_IP |

*Pass Through Filters List*



GNAT-Box Edit IP Pass Through Filter

Disable: □

Description:

Type: Accept Interface: EXTERNAL Protocol: <ALL>

Priority: 5 - notice Authentication required: □

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

Coalesce: □ Source address □ Source ports □ Destination address □ Destination ports

Time based: □ Time group is: ???

Traffic Shaping: <DEFAULT> Weight: 1

Source Address

Object: <USE IP ADDRESS> IP Address: 192.168.0.0/16

Source Ports

Range: □ 0 0 0 0 0 0

0 0 0 0 0 0

Destination Address

Object: ANY_IP IP Address:

Destination Ports

Range: □ 0 0 0 0 0 0

Broadcast: □ 0 0 0 0 0 0

*Pass Through Filter*

## Hosts/Networks

The Pass Through Hosts/Networks definition form is used to specify an IP address, subnet or network that will not have NAT applied to packets. See individual product guides for the number of IP Pass Through Hosts/Networks available on a specific GTA Firewall.

### *Note*

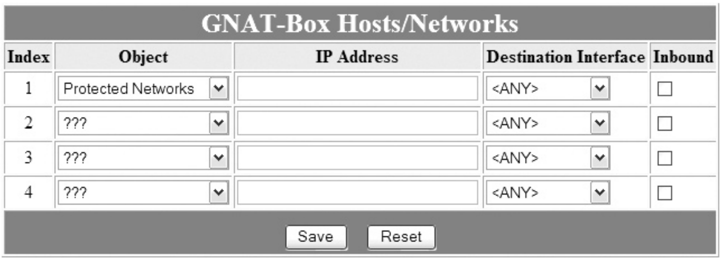
An IP Host/Network is not required for a Pass Through in Bridging mode because no NAT is applied.

### New Host or Network

In the Network/Host table, select an object or **<Use IP address>** and enter an IP address/netmask (single host), subnet, or network (multiple hosts) in the IP ADDRESS field. Single IP addresses use /32 or /255.255.255.255. Select the interface that will have no NAT applied when the IP packets pass outbound through the interface. If unsolicited IP packets should be accepted for the specified address, select the Inbound checkbox. If you wish to allow only IP Pass Through reply packets to return, leave the Inbound option deselected.

### *Note*

The netmask 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 | Protected Networks | | <ANY> | □ |
| 2 | ??? | | <ANY> | □ |
| 3 | ??? | | <ANY> | □ |
| 4 | ??? | | <ANY> | □ |

*Hosts/Networks*

## IP Pass Through Examples

### Protected to External Network

| | |
|---|---|
| Internet Router | 199.100.200.1 |
| External Interface | 199.100.200.2 |
| Protected Network | 199.100.202.0/24 |

**Pass Through Host/Networks**

| | |
|---|---|
| Object/IP address | 199.100.202.0/24 |
| Destination Interface | EXTERNAL |
| Inbound | Checked |

**Pass Through Filters**

**Allow outbound Pass Through**

| | |
|---|---|
| Type | Accept |
| Interface | PROTECTED |
| Protocol | ALL |
| Log | Default |
| Source IP Address | 199.100.202.0/24 |
| Ports | blank or Zero |
| Destination IP Address | Object “ANY_IP” |
| Ports | blank or Zero |

**Deny inbound Pass Through**

| | |
|---|---|
| Type | DENY |
| Interface | PROTECTED |
| Protocol | ALL |
| Log | Default |
| Source IP Address | Object ANY_IP |
| Ports | blank or Zero |
| Destination IP Address | 199.100.202.0/24 |
| Ports | blank or Zero |

**Add Static Route to Internet Router**

| | |
|---|---|
| Network | 199.100.202.0/24 |
| Gateway | 199.100.200.1 |

## Protected to PSN

| | |
|---|---|
| PSN Network | 192.168.1.0/24 |
| Protected Network | 10.1.1.0/24 |

### Pass Through Host/Networks

| | |
|---|---|
| Object/IP address | 10.1.1.0/24 |
| Destination Interface | PSN |
| Inbound | Checked |

### Pass Through Filters

### Allow outbound Pass Through to PSN

| | |
|---|---|
| Type | Accept |
| Interface | PROTECTED |
| Protocol | ALL |
| Log | Default |
| Source IP Address | 10.1.1.0/24 |
| Ports | blank or Zero |
| Destination IP Address | 192.168.1.0/24 |
| Ports | blank or Zero |

### Pass Through Filters

### Deny inbound Pass Through from PSN

| | |
|---|---|
| Type | DENY |
| Interface | PSN |
| Protocol | ALL |
| Log | Default |
| Source IP Address | 192.168.1.0/24 |
| Ports | blank or Zero |
| Destination IP Address | 10.1.1.0/24 |
| Ports | blank or Zero |

### Add Static Route to Internet Router

| | |
|---|---|
| Network | 199.100.200.0/24 |
| Gateway | 199.100.200.1 |

When going to the Internet the key is the Static route on the router. If the static route cannot be configured, the Pass Through will fail.

## Bridged Protocols

The Bridged Protocols section allows the user to specify, allow and log the Ethernet protocols that can be allowed to bypass all firewall filtering between bridged interfaces. TCP/IP packets will still pass between these bridged interfaces according to normal firewall rules on the ports specified in a bridging Pass Through filter.

***Caution***

There is no firewall filtering of the protocol types that have been allowed in Bridged Protocols.

### Protocol Types

Protocol type designations are generally unpublished. To see a collection of known Ethernet protocol types, go to IANA's website at `http://www.iana.org/assignments/ethernet-numbers`.

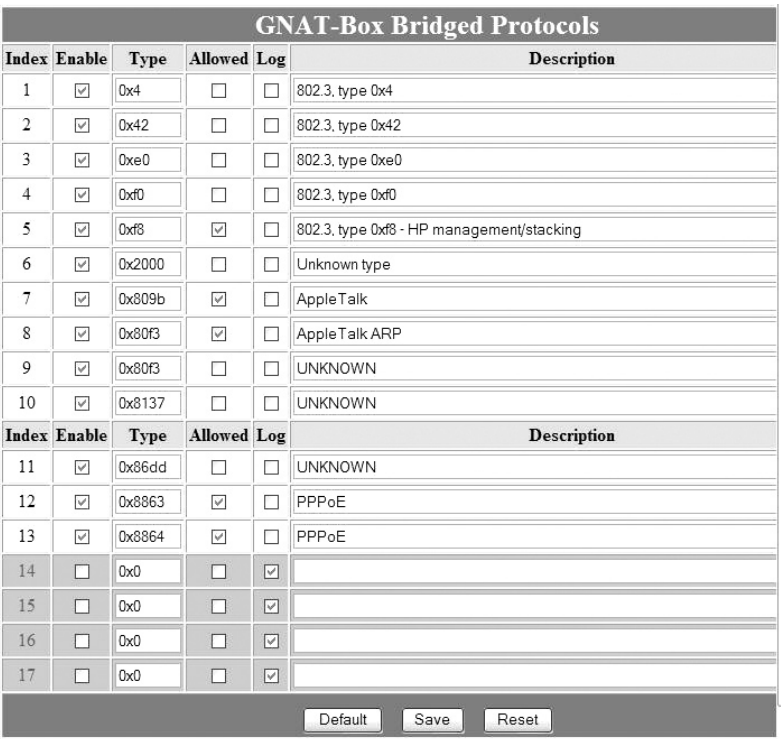
To locate a type designation for a protocol you need to bridge, configure the bridged interface for your operational network. Packets that attempt to pass between the bridged networks are, by default, denied (blocked) but not logged until they have been defined in Bridged Protocols. In order to log non-TCP/IP Ethernet packets, enable logging for DENY UNEXPECTED PACKETS in **Filters/Preferences**. This will generate log messages containing the protocol types of the IP packets. The packet protocol type is logged with a "0x" prefix that identifies the characters as being in hexadecimal format.

Enter the hexadecimal number with its prefix into the TYPE field. Decimal format numbers can also be entered; they will be displayed in hexadecimal.

To continue to deny a specific protocol but not log it, enter the protocol type number and select the **ENABLE** checkbox. To deny a protocol and log the denials, select both the **ENABLE** and **LOG** checkboxes. To allow a protocol and not log it, select the **ENABLE** and **ALLOW** checkboxes.

**Bridged Protocols Fields**

| | |
|---|---|
| Enable | Check to enable the selected bridged protocol. |
| Type | Hexadecimal number of the designated Ethernet protocol. "0x0" is a placeholder for the protocol type. Use the "0x" prefix when entering a number in hex format. |
| Allowed | Allow the designated protocol on the bridged interface. |
| Log | Log events that use the protocol type. |
| Description | Description of the bridged protocol type for reference. |



GNAT-Box Bridged Protocols

| Index | Enable | Type | Allowed | Log | Description |
|---|---|---|---|---|---|
| 1 | ☑ | 0x4 | □ | □ | 802.3, type 0x4 |
| 2 | ☑ | 0x42 | □ | □ | 802.3, type 0x42 |
| 3 | ☑ | 0xe0 | □ | □ | 802.3, type 0xe0 |
| 4 | ☑ | 0xf0 | □ | □ | 802.3, type 0xf0 |
| 5 | ☑ | 0xf8 | ☑ | □ | 802.3, type 0xf8 - HP management/stacking |
| 6 | ☑ | 0x2000 | □ | □ | Unknown type |
| 7 | ☑ | 0x809b | ☑ | □ | AppleTalk |
| 8 | ☑ | 0x80f3 | ☑ | □ | AppleTalk ARP |
| 9 | ☑ | 0x80f3 | □ | □ | UNKNOWN |
| 10 | ☑ | 0x8137 | □ | □ | UNKNOWN |
| Index | Enable | Type | Allowed | Log | Description |
| 11 | ☑ | 0x86dd | □ | □ | UNKNOWN |
| 12 | ☑ | 0x8863 | ☑ | □ | PPPoE |
| 13 | ☑ | 0x8864 | ☑ | □ | PPPoE |
| 14 | □ | 0x0 | □ | ☑ | |
| 15 | □ | 0x0 | □ | ☑ | |
| 16 | □ | 0x0 | □ | ☑ | |
| 17 | □ | 0x0 | □ | ☑ | |

*Bridged Protocols*

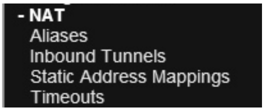
# 10 NAT

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

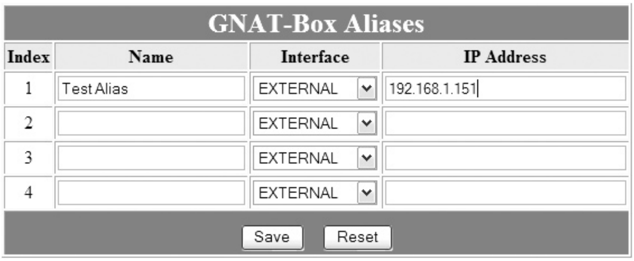
The Alias facility allows a network interface to be represented by multiple IP addresses. An IP alias may be assigned to any network interface. This facility is useful on the External Network interface, or if multiple targets on the PSN or Protected Network are required for the same service (port) via 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 | 192.168.1.151 |
| 2 |  | EXTERNAL |  |
| 3 |  | EXTERNAL |  |
| 4 |  | EXTERNAL |  |

*IP Aliases*

***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 normally used on a Protected Network interface. See product guides for the number of tunnels available on a specific GTA Firewall.

Tunnels can be created 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 **Appendix D – GNAT Box 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.

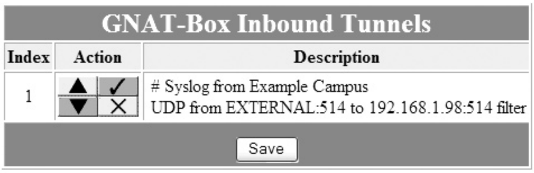
If a tunnel originates from an IP alias address, you may need to map the destination host to the IP alias using Static Address Mapping so that secondary connections appear to originate from the same address as the tunnel.

### *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 **Appendix A – Ports and Services,** for some of the common ports.



GNAT-Box Inbound Tunnels

| Index | Action | Description |
|---|---|---|
| 1 | ▲ ✓<br>▼ ✕ | # Syslog from Example Campus<br>UDP from EXTERNAL:514 to 192.168.1.98:514 filter |

*Tunnel List*

## Allowing Access to an Inbound Tunnel

A tunnel is a mapping from one IP address/port to another IP address/port. The tunnel source will not be usable unless an appropriate filter allows access. There are two methods to allow access to an inbound tunnel: selecting Automatic Accept All Filters on the tunnel or setting Remote Access Filters.

### Automatic Accept All Filters

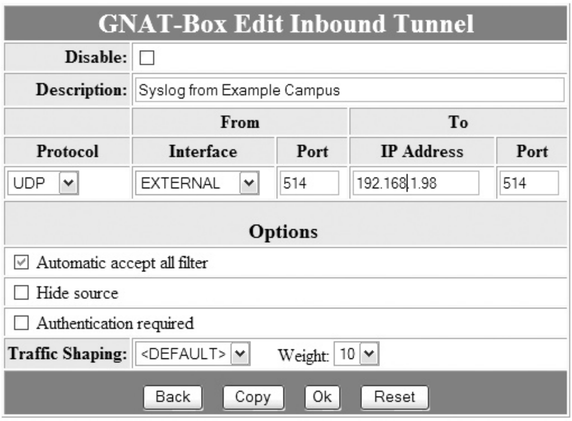
Unless further restriction is desired on a tunnel, selecting Automatic Accept All Filters will allow traffic between the designated interfaces and addresses. If logging for these filters is desired, activate logging for automatic filters in Filter Preferences. When activated, automatic filters will be recorded in the Active Filters table of the System Activity section.

### Remote Access Filters

A Remote Access Filter can also be created to allow traffic between the designated interfaces and addresses. These filters can be activated and logged individually, if close observation of tunnel use it required. The **DEFAULT** button on the Remote Access Filter set screen will auto-configure 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

| | |
|---|---|
| Disable | Disable the defined inbound tunnel. |
| Description | Description of the inbound tunnel. |
| Protocol | Select from the Protocol List: ALL, TCP, UDP, ICMP, IGMP, ESP, AH, etc. |
| From Interface | Interface object representing a network interface, an IP alias or a H2A (high availability) group for the source side of the tunnel. |
| From Port | Port value which users will access. See a list of common services and their port numbers in **Appendix A – Ports & Services**. For an exhaustive and up-to-date list, see IANA's list at www.iana.org/assignments/port-numbers. |
| To IP address | 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 | Port value of the service being offered on the target host, which will be the destination of the tunnel. |
| Automatic Accept All Filter | Make the inbound tunnel connection ignore conflicting filters. When activated, the Automatic filters will appear under **System Activity/Active Filters**. |
| Hide Source | Hide the source of the inbound tunnel connection. Useful when the GTA Firewall is used on an intranet. |
| Authentication required | Authentication allows the administrator to require users to authenticate to the firewall using GBAuth before initiating a connection. By default, GTA's user authentication is served on TCP port 76. |
| Traffic Shaping | Object that defines the pipe to apply to this filter. The **Default** Traffic Shaping object allows unlimited access to the available bandwidth. |
| Weight | Priority when accessing the pipe's allocated bandwidth. Weights of 10 have the highest priority, and 1, the lowest. |



GNAT-Box Edit Inbound Tunnel

Disable: □

Description: Syslog from Example Campus

| | From | | To | |
|---|---|---|---|---|
| Protocol | Interface | Port | IP Address | Port |
| UDP | EXTERNAL | 514 | 192.168.1.98 | 514 |

Options

☑ Automatic accept all filter

□ Hide source

□ Authentication required

Traffic Shaping: <DEFAULT> Weight: 10

*Tunnel Configuration*

## 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:

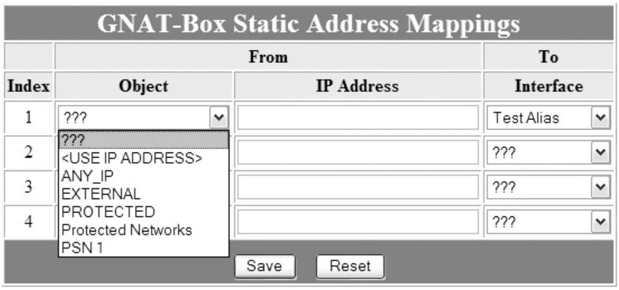
- From a host or subnet on the Protected Network to an IP alias assigned to the PSN interface.
- From a host or subnet on the Protected Network to an IP alias assigned to the External Network interface.
- From a host or subnet on the PSN to an IP alias assigned to the External Network interface.

### 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
Interface Object representing the IP address to which the source will be mapped.



GNAT-Box Static Address Mappings

| | From | | To |
|---|---|---|---|
| Index | Object | IP Address | Interface |
| 1 | ??? | | Test Alias |
| 2 | | | ??? |
| 3 | | | ??? |
| 4 | | | ??? |

*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 timeout value differs for each protocol. For example, TCP has enough information embedded for the firewall to determine when the connection is ready to close, but with ICMP and UDP, it is generally impossible to determine when the connection is ready to close.

## Timeout Fields

### TCP Specific

TCP

Default is 600 (10 minutes).

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 header bit indicating ACK (acknowledgement). As part of Stateful Packet Inspection, the firewall keeps a record of 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 to close.

Send keep alives?

Enabled by default so that if a TCP connection remains idle for the timeout period, a Keep Alive packet is sent. If the connection is still valid, the firewall will set the idle time to zero. If the connection is invalid, the 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 firewall will mark the connection ready to close. If the field is disabled, the connection is marked ready to close.

### Other Protocols

UDP

Default is 600 (10 minutes).

ICMP

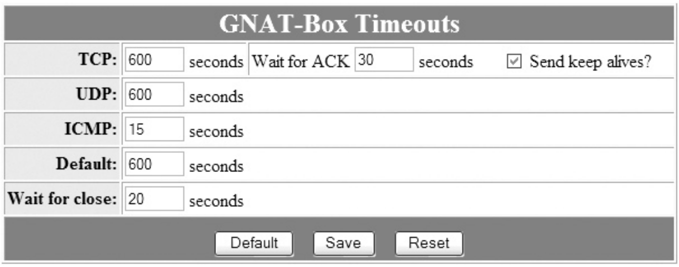
Default is 15.

Default

Default is 600 (10 minutes). Timeout for supported protocols other than TCP, UDP or ICMP. After a connection is marked as ready to close, the firewall waits five seconds before it actually closes the connection, giving redundant IP packets a chance to clear the firewall without causing false doorknob twist error messages.

Wait for close

Default is 20 seconds. If the firewall experiences spurious blocks from reply packets (typically port 80), increasing this value gives packets from slow or distant connections more time to return before the connection is closed.



GNAT-Box Timeouts

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

UDP: 600 seconds

ICMP: 15 seconds

Default: 600 seconds

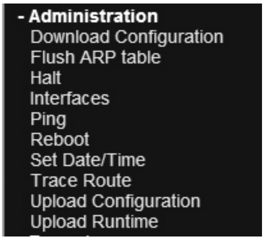
Wait for close: 20 seconds

*Timeouts*

# 11 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. GBAdmin differences will be noted.



*Administration Menu*

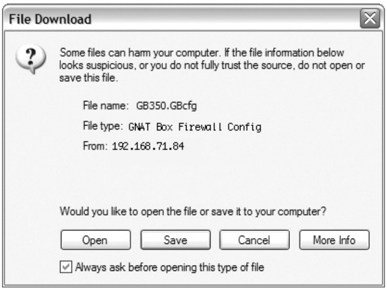
## Download/Save Configuration

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.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: GB350.GBcfg

File type: GNAT Box Firewall Config

From: 192.168.71.84

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

☑ Always ask before opening this type of file

*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.

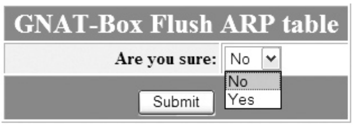
GBAdmin's Save Configuration option is located in the File menu: **File/Save**. GBAdmin can open saved configurations without loading them into the running GTA Firewall.

## 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 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.



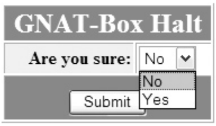
GNAT-Box Flush ARP table

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.



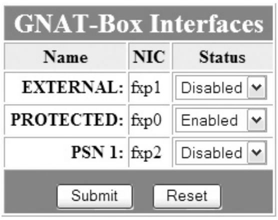
GNAT-Box Halt

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

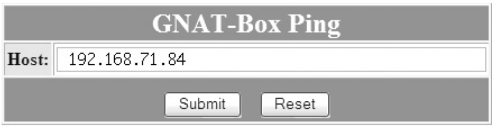
| Name | NIC | Status |
|---|---|---|
| EXTERNAL: | fxp1 | Disabled |
| PROTECTED: | fxp0 | Enabled |
| PSN 1: | fxp2 | Disabled |

*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.

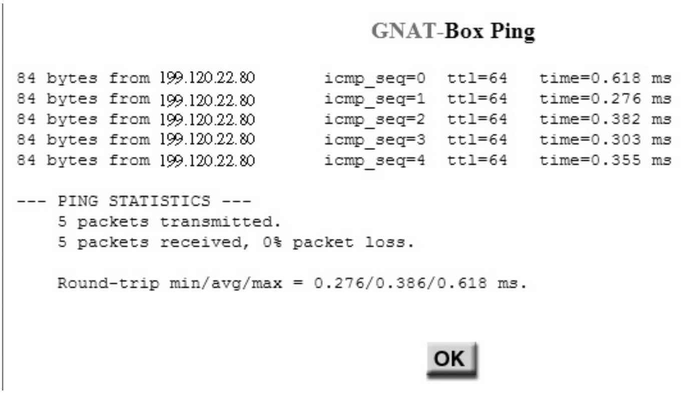

**GNAT-Box Ping**

**Host:** 192.168.71.84

*Ping*

## Using the Ping Facility

1. Click the **Ping** menu item to display the ping form.
2. Click in the Host field and enter the fully-qualified host name or IP address to ping. Enter the IP address 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.

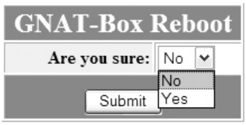

**GNAT-Box Ping**

```
84 bytes from 199.120.22.80       icmp_seq=0  ttl=64   time=0.618 ms
84 bytes from 199.120.22.80       icmp_seq=1  ttl=64   time=0.276 ms
84 bytes from 199.120.22.80       icmp_seq=2  ttl=64   time=0.382 ms
84 bytes from 199.120.22.80       icmp_seq=3  ttl=64   time=0.303 ms
84 bytes from 199.120.22.80       icmp_seq=4  ttl=64   time=0.355 ms

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

    Round-trip min/avg/max = 0.276/0.386/0.618 ms.
```

*Ping Result*

# 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, or you can click the **STOP** button on your web browser.



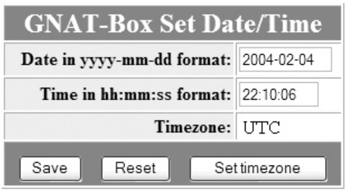
GNAT-Box Reboot

Are you sure: No

*Reboot*

# Set Date/Time

Set Date/Time provides a means to set the date and time values used on the GTA Firewall. The date should be entered in the form of century, year, month and day (ccyy-mm-dd). GTA recommends setting the time zone, either to the local time zone or UTC (Coordinated Universal Time).



GNAT-Box Set Date/Time

| | |
|---|---|
| Date in yyyy-mm-dd format: | 2004-02-04 |
| Time in hh:mm:ss format: | 22:10:06 |
| Timezone: | UTC |

*Set Date/Time*

## UTC and Logging

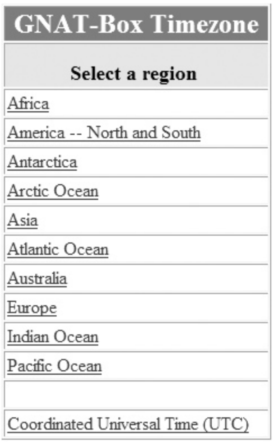
Firewalls report events to the log and to GB-Commander in UTC. When displaying the time, GB-Commander and GTA Reporting Suite convert stored UTC data to the user machine's local time zone. This is relevant when GTA Reporting Suite and GB-Commander reports are compared across time zones.

UTC was formerly known as GMT (Greenwich Mean Time). Other terms used to refer to UTC are Zulu time, universal time and world time. Time is expressed in 24-hour notation in GNAT Box System Software, e.g., 1:00 a.m. is 01:00, and 4:00 p.m. is 16:00.

## Set Time Zone (Web Only)

To set the time zone, click **SET TIMEZONE**. Select a region, country and time zone which observe the same time as your locality. Click **OK** to apply your selection. Save your changes, then reboot the system.

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



*Set Time Zone*

***Note***

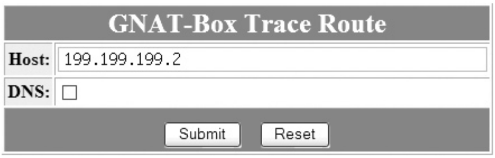
Always reboot your system after changing the time zone.

## Trace Route

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

Trace Route 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.



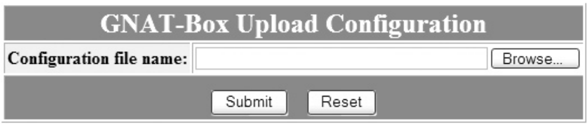
Host: 199.199.199.2

DNS: □

*Trace Route*

## Upload/Open Configuration

This item will allow you to upload a previously saved GNAT Box System Software configuration file. Enter the name of the configuration file to upload, or use the **BROWSE** button to find the file on your local workstation.The file will have the extension "`.GBcfg`." Click **SUBMIT** to upload the configuration file to the GTA Firewall. See Download/Save Configuration.



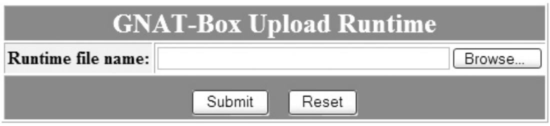
*Upload Configuration*

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

## Upload/Update Runtime

The Upload Runtime function is used to upgrade a firewall to a new version or reinstall a previous version. (Upload/Update Runtime is not available on GB-Light or GB-Pro.)

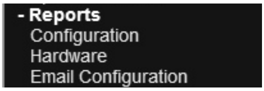
The GNAT Box System Software has two distinct parts: the runtime operating system and the configuration data. The Upload Runtime function allows the administrator to upload and install a GNAT Box System Software runtime system image on a GTA Firewall. When this item is selected, a dialog prompts you 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*

# 12 Reports

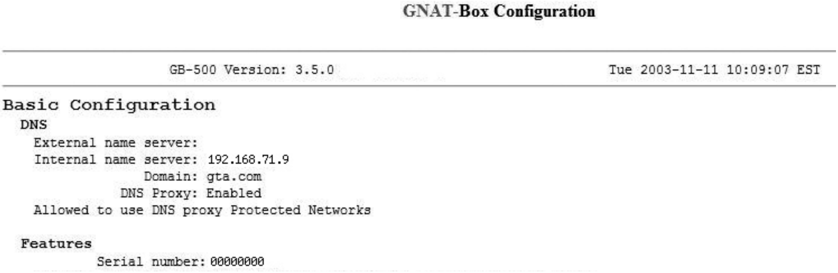
The Reports section provides access to three functions that create reports for the system hardware and software configuration: Configuration, Hardware and Email Configuration. Verify Configuration is the last item on the main menu of the Web interface and is under the Reports section in GBAdmin. Items under the Reports menu in GBAdmin are available only when a network connection is established with a running GTA Firewall.



*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.



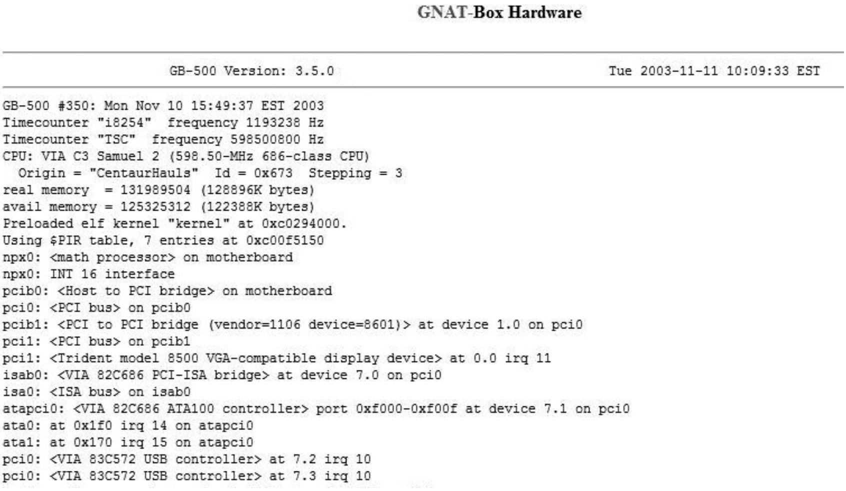
**GNAT-Box Configuration**

```
                 GB-500 Version: 3.5.0                          Tue 2003-11-11 10:09:07 EST

Basic Configuration
  DNS
    External name server:
    Internal name server: 192.168.71.9
                  Domain: gta.com
               DNS Proxy: Enabled
    Allowed to use DNS proxy Protected Networks

  Features
           Serial number: 00000000
```

*Configuration Report Example (Partial)*

## 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.



**GNAT-Box Hardware**

```
                GB-500 Version: 3.5.0                                  Tue 2003-11-11 10:09:33 EST

GB-500 #350: Mon Nov 10 15:49:37 EST 2003
Timecounter "i8254"  frequency 1193238 Hz
Timecounter "TSC"  frequency 598500800 Hz
CPU: VIA C3 Samuel 2 (598.50-MHz 686-class CPU)
  Origin = "CentaurHauls"  Id = 0x673  Stepping = 3
real memory  = 131989504 (128896K bytes)
avail memory = 125325312 (122388K bytes)
Preloaded elf kernel "kernel" at 0xc0294000.
Using $PIR table, 7 entries at 0xc00f5150
npx0: <math processor> on motherboard
npx0: INT 16 interface
pcib0: <Host to PCI bridge> on motherboard
pci0: <PCI bus> on pcib0
pcib1: <PCI to PCI bridge (vendor=1106 device=8601)> at device 1.0 on pci0
pci1: <PCI bus> on pcib1
pci1: <Trident model 8500 VGA-compatible display device> at 0.0 irq 11
isab0: <VIA 82C686 PCI-ISA bridge> at device 7.0 on pci0
isa0: <ISA bus> on isab0
atapci0: <VIA 82C686 ATA100 controller> port 0xf000-0xf00f at device 7.1 on pci0
ata0: at 0x1f0 irq 14 on atapci0
ata1: at 0x170 irq 15 on atapci0
pci0: <VIA 83C572 USB controller> at 7.2 irq 10
pci0: <VIA 83C572 USB controller> at 7.3 irq 10
```

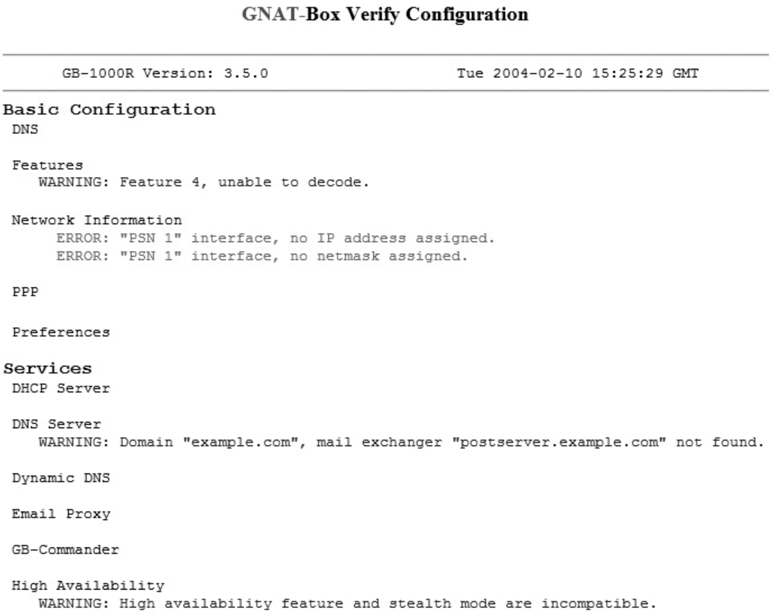
*Hardware Report Example (Partial)*

## Verify Configuration

Verify Configuration is the last item on the main menu of the Web interface and is under the Reports section in GBAdmin.

Verify Configuration will run a system configuration verification check of the GTA Firewall. 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 is on-going on the GTA Firewall, and 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.



**GNAT-Box Verify Configuration**

```
      GB-1000R Version: 3.5.0                     Tue 2004-02-10 15:25:29 GMT

Basic Configuration
 DNS

 Features
    WARNING: Feature 4, unable to decode.

 Network Information
      ERROR: "PSN 1" interface, no IP address assigned.
      ERROR: "PSN 1" interface, no netmask assigned.

 PPP

 Preferences

Services
 DHCP Server

 DNS Server
    WARNING: Domain "example.com", mail exchanger "postserver.example.com" not found.

 Dynamic DNS

 Email Proxy

 GB-Commander

 High Availability
    WARNING: High availability feature and stealth mode are incompatible.
```

*Verify Configuration Example (Partial)*

In GBAdmin, in addition to the Verify Configuration item, verification errors will appear over the menu item when the mouse pointer hovers over it. Verification checks will also be indicated by the color of the Scrolling Menu circle: green for functional, yellow for warning and red for error. In GBAdmin, these warnings and errors will appear as soon as the administrator clicks on another selection, even when the configuration has not yet been saved.

### *Note*

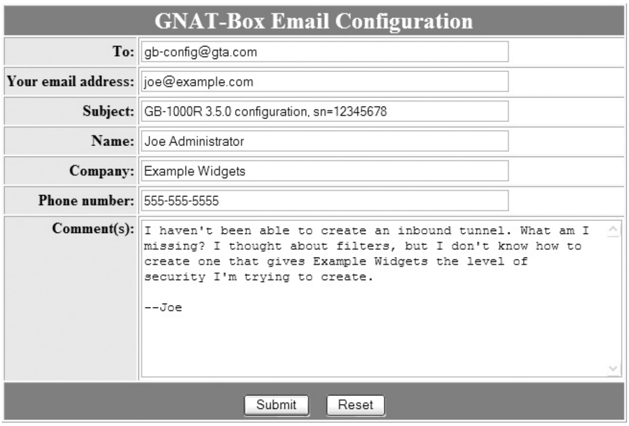
Use this feature of GBAdmin to try out a configuration option before saving it to the loaded GTA Firewall.

# Email Configuration

Email Configuration allows the user to email a copy of the system information to a designated support email address. Email Configuration sends an email with these reports:

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

Enter any additional information in the COMMENTS field.



GNAT-Box Email Configuration

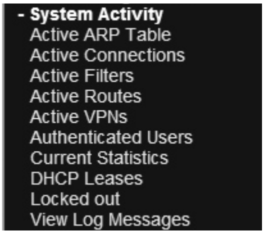
| | |
|---|---|
| To: | gb-config@gta.com |
| Your email address: | joe@example.com |
| Subject: | GB-1000R 3.5.0 configuration, sn=12345678 |
| Name: | Joe Administrator |
| Company: | Example Widgets |
| Phone number: | 555-555-5555 |
| Comment(s): | I haven't been able to create an inbound tunnel. What am I missing? I thought about filters, but I don't know how to create one that gives Example Widgets the level of security I'm trying to create.<br>--Joe |

*Email Configuration Form*

# 13 System Activity

System Activity provides direct access to firewall status reports. Some System Activity reports appear only when specific features have been activated, therefore some reports listed here may not appear in your product's interface.

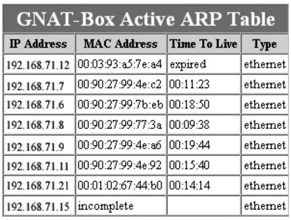
The Web interface is continuously updated, so system activity reports are in real-time. To change the rate at which tables are updated, click **CHANGE REFRESH RATE** on select report screens. In GBAdmin, system activity reports are snapshots of system activity, only available when a connection to the firewall is established. Click the list item to generate an update.



*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 |
|---|---|---|---|
| 192.168.71.12 | 00:03:93:a5:7e:a4 | expired | ethernet |
| 192.168.71.7 | 00:90:27:99:4e:c2 | 00:11:23 | ethernet |
| 192.168.71.6 | 00:90:27:99:7b:eb | 00:18:50 | ethernet |
| 192.168.71.8 | 00:90:27:99:77:3a | 00:09:38 | ethernet |
| 192.168.71.9 | 00:90:27:99:4e:a6 | 00:19:44 | ethernet |
| 192.168.71.11 | 00:90:27:99:4e:92 | 00:15:40 | ethernet |
| 192.168.71.21 | 00:01:02:67:44:b0 | 00:14:14 | ethernet |
| 192.168.71.15 | incomplete |  | ethernet |

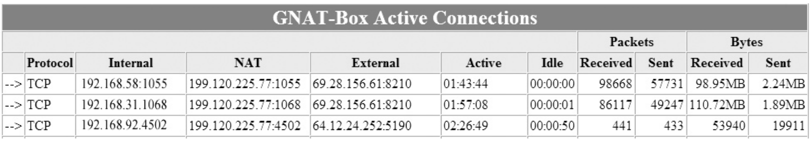
*ARP Table*

# Active Connections

The Active Connections item is used to display a list of currently active inbound and outbound connections. By default, the display is a static snapshot, with the refresh rate set to zero (0) seconds (no automatic updates). If you wish to automatically update the list, adjust the interval using **CHANGE REFRESH RATE**.

## Active Connections List

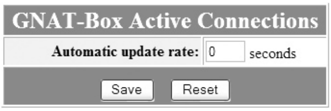
| | |
|---|---|
| (Inbound/Outbound) | Connection Direction: "<--" indicates an Inbound connection; "-->" indicates an Outbound connection. |
| Protocol | Protocol used by the connection. |
| Internal | Internal IP address:port. |
| NAT | NAT IP address:port. |
| External | External IP address:port. |
| Active | Time active. |
| Idle | Time idle. |
| Packets | Number of packets received/sent. |
| Bytes | Number of bytes received/sent. |



GNAT-Box Active Connections

| | | | | | | | Packets | | Bytes | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Protocol | Internal | NAT | External | Active | Idle | Received | Sent | Received | Sent |
| --> | TCP | 192.168.58:1055 | 199.120.225.77:1055 | 69.28.156.61:8210 | 01:43:44 | 00:00:00 | 98668 | 57731 | 98.95MB | 2.24MB |
| --> | TCP | 192.168.31.1068 | 199.120.225.77:1068 | 69.28.156.61:8210 | 01:57:08 | 00:00:01 | 86117 | 49247 | 110.72MB | 1.89MB |
| --> | TCP | 192.168.92.4502 | 199.120.225.77:4502 | 64.12.24.252:5190 | 02:26:49 | 00:00:50 | 441 | 433 | 53940 | 19911 |

*Active Connections*



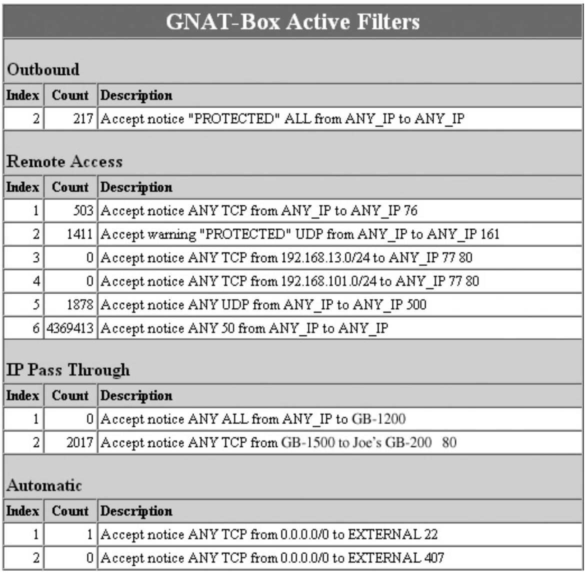
GNAT-Box Active Connections

Automatic update rate: 0 seconds

*Refresh Rate*

# Active Filters

The Active Filters list will create and display a list of filters for each of the four filter types: Outbound, Remote Access, Pass Through and Automatic. Information includes: number of hits (times the filter has been activated) and a description of the filter. Inactive time-based filters have an asterisk '*' next to the entry. By default, the display is a static snapshot, with the refresh rate set to zero (0) seconds (no automatic updates). If you wish to automatically update the list, adjust the interval using **CHANGE REFRESH RATE**.



GNAT-Box Active Filters

Outbound

| Index | Count | Description |
|---|---|---|
| 2 | 217 | Accept notice "PROTECTED" ALL from ANY_IP to ANY_IP |

Remote Access

| Index | Count | Description |
|---|---|---|
| 1 | 503 | Accept notice ANY TCP from ANY_IP to ANY_IP 76 |
| 2 | 1411 | Accept warning "PROTECTED" UDP from ANY_IP to ANY_IP 161 |
| 3 | 0 | Accept notice ANY TCP from 192.168.13.0/24 to ANY_IP 77 80 |
| 4 | 0 | Accept notice ANY TCP from 192.168.101.0/24 to ANY_IP 77 80 |
| 5 | 1878 | Accept notice ANY UDP from ANY_IP to ANY_IP 500 |
| 6 | 4369413 | Accept notice ANY 50 from ANY_IP to ANY_IP |

IP Pass Through

| Index | Count | Description |
|---|---|---|
| 1 | 0 | Accept notice ANY ALL from ANY_IP to GB-1200 |
| 2 | 2017 | Accept notice ANY TCP from GB-1500 to Joe's GB-200 80 |

Automatic

| Index | Count | Description |
|---|---|---|
| 1 | 1 | Accept notice ANY TCP from 0.0.0.0/0 to EXTERNAL 22 |
| 2 | 0 | Accept notice ANY TCP from 0.0.0.0/0 to EXTERNAL 407 |

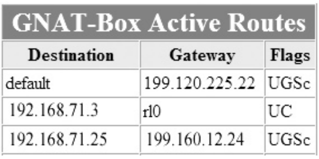
*Active Filters*

## Active Routes

The Active Routes list displays the active routing table. This list can be helpful in troubleshooting routing problems. The list displays destination, gateway and flags. Flags are defined below.

### 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 | Gateway | Flags |
|---|---|---|
| default | 199.120.225.22 | UGSc |
| 192.168.71.3 | rl0 | UC |
| 192.168.71.25 | 199.160.12.24 | UGSc |

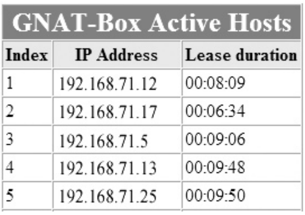
*Active Routes*

## Active Hosts

The Active Hosts list appears only on systems with a restricted number of concurrent users. See your firewall's **Basic Configuration/Features** or the GTA Support center for the number of concurrent users licensed on your firewall.

Active Hosts helps track and regulate outbound access. The number of licenses used is determined by the number of IP addresses from which outbound requests are currently being made. This includes IP addresses connecting from a Protected to External Network; Protected to PSN; PSN to External Network; and outbound connections opened by a Protected Network or PSN when responding to requests.

The record includes the outbound user's IP address and lease duration (time remaining). If the user continues to send outbound requests, remaining active, the lease will renew each time a request is made. If the user remains inactive for the timeout period, the lease duration column will report "expired" until the license is required for another user or the original user renews the lease. The duration of leases is defined in **NAT/Timeouts**.



GNAT-Box Active Hosts

| Index | IP Address | Lease duration |
|---|---|---|
| 1 | 192.168.71.12 | 00:08:09 |
| 2 | 192.168.71.17 | 00:06:34 |
| 3 | 192.168.71.5 | 00:09:06 |
| 4 | 192.168.71.13 | 00:09:48 |
| 5 | 192.168.71.25 | 00:09:50 |

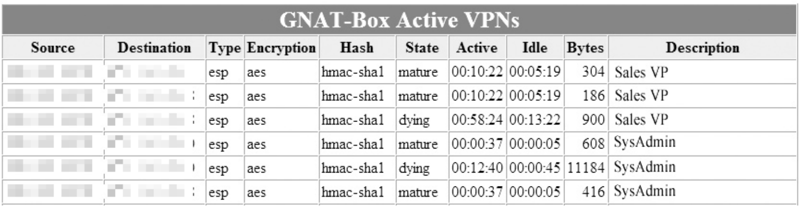
*Active Hosts*

## Active VPNs

The Active VPNs menu item displays all current active VPN connections. There is an inbound and outbound connection for each VPN.

### VPN Information

| | |
|---|---|
| Source | Source IP address of the gateway. |
| Destination | 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. |
| Active | Time the VPN has been connected. |
| Idle | Idle time of the VPN. |
| Bytes | Number of bytes transferred by the connection. |
| Description | Identifying name for the VPN. |



GNAT-Box Active VPNs

| Source | Destination | Type | Encryption | Hash | State | Active | Idle | Bytes | Description |
|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | esp | aes | hmac-sha1 | mature | 00:10:22 | 00:05:19 | 304 | Sales VP |
| [redacted] | [redacted] | esp | aes | hmac-sha1 | mature | 00:10:22 | 00:05:19 | 186 | Sales VP |
| [redacted] | [redacted] | esp | aes | hmac-sha1 | dying | 00:58:24 | 00:13:22 | 900 | Sales VP |
| [redacted] | [redacted] | esp | aes | hmac-sha1 | mature | 00:00:37 | 00:00:05 | 608 | SysAdmin |
| [redacted] | [redacted] | esp | aes | hmac-sha1 | dying | 00:12:40 | 00:00:45 | 11184 | SysAdmin |
| [redacted] | [redacted] | esp | aes | hmac-sha1 | mature | 00:00:37 | 00:00:05 | 416 | SysAdmin |

*Active VPNs*

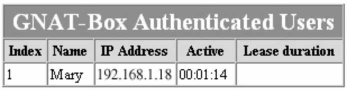
## Authenticated Users

The Authenticated Users report helps track access by users authenticated thorugh GBAuth for GTA, LDAP and RADIUS authentication. The record includes the outbound user's name as indicated in User Authorization, the LDAP configuration or the RADIUS configuration, and reflected in the GBAuth IDENTITY field; the source IP address; and the number of minutes the user has been active.

The last column, lease duration (time remaining), applies only to mobile VPN users. If a VPN client user is actively connected, the lease will renew each time a request is made. If the user remains inactive for the timeout period, the lease duration column will report "expired" until the license is required for another user or the original user renews the lease. The duration of leases is defined in **NAT/Timeouts**.

### Authenticated Users List

| | |
|---|---|
| Index | Rule line. |
| Name | Identifying name of the user. |
| IP address | IP address from which the connection is made. |
| Active | Time the connection has been in use. |
| Lease Duration | For mobile VPN users, the time remaining before the connection expires, and the lease must be renewed. |



GNAT-Box Authenticated Users

| Index | Name | IP Address | Active | Lease duration |
|---|---|---|---|---|
| 1 | Mary | 192.168.1.18 | 00:01:14 | |

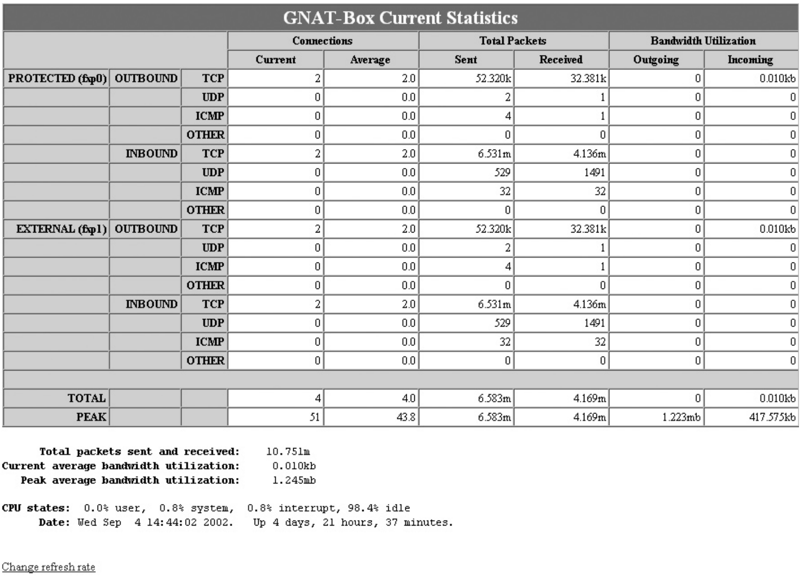
*Authenticated User*

## Current Statistics

The Current Statistics report provides access to the GTA Firewall's statistics display. Statistics are for both connections and packets of the TCP, UDP, ICMP or other protocol. A summary of the information appears at the bottom of the list, including total packets, current average packets, peak average packets, date, time, uptime and CPU states – % user process, % system process, % interrupt, and % idle. To automatically update the list, adjust the interval using **CHANGE REFRESH RATE**.

### Current Statistics List

| | |
|---|---|
| Interface | Interface on which the connection is being made. |
| Connection Direction | Inbound or Outbound. |
| Protocol | List items for TCP, UDP, ICMP and other protocols. |
| Connections | Current and average number of connections for each protocol and connection direction. |
| Total Packets | Packets sent and received for each protocol and connection direction. |
| Bandwidth Utilization | Bandwidth for each protocol and connection direction. |
| Total | Summary line that displays the totals for each column. |
| Peak | Summary line that displays the peak for each column. |



**GNAT-Box Current Statistics**

| | | | Connections | | Total Packets | | Bandwidth Utilization | |
|---|---|---|---|---|---|---|---|---|
| | | | Current | Average | Sent | Received | Outgoing | Incoming |
| PROTECTED (fxp0) | OUTBOUND | TCP | 2 | 2.0 | 52.320k | 32.381k | 0 | 0.010kb |
| | | UDP | 0 | 0.0 | 2 | 1 | 0 | 0 |
| | | ICMP | 0 | 0.0 | 4 | 1 | 0 | 0 |
| | | OTHER | 0 | 0.0 | 0 | 0 | 0 | 0 |
| | INBOUND | TCP | 2 | 2.0 | 6.531m | 4.136m | 0 | 0 |
| | | UDP | 0 | 0.0 | 529 | 1491 | 0 | 0 |
| | | ICMP | 0 | 0.0 | 32 | 32 | 0 | 0 |
| | | OTHER | 0 | 0.0 | 0 | 0 | 0 | 0 |
| EXTERNAL (fxp1) | OUTBOUND | TCP | 2 | 2.0 | 52.320k | 32.381k | 0 | 0.010kb |
| | | UDP | 0 | 0.0 | 2 | 1 | 0 | 0 |
| | | ICMP | 0 | 0.0 | 4 | 1 | 0 | 0 |
| | | OTHER | 0 | 0.0 | 0 | 0 | 0 | 0 |
| | INBOUND | TCP | 2 | 2.0 | 6.531m | 4.136m | 0 | 0 |
| | | UDP | 0 | 0.0 | 529 | 1491 | 0 | 0 |
| | | ICMP | 0 | 0.0 | 32 | 32 | 0 | 0 |
| | | OTHER | 0 | 0.0 | 0 | 0 | 0 | 0 |
| | | | | | | | | |
| TOTAL | | | 4 | 4.0 | 6.583m | 4.169m | 0 | 0.010kb |
| PEAK | | | 51 | 43.8 | 6.583m | 4.169m | 1.223mb | 417.575kb |

```
      Total packets sent and received:    10.751m
Current average bandwidth utilization:     0.010kb
   Peak average bandwidth utilization:     1.245mb

CPU states:  0.0% user,  0.8% system,  0.8% interrupt, 98.4% idle
      Date: Wed Sep  4 14:44:02 2002.   Up 4 days, 21 hours, 37 minutes.
```

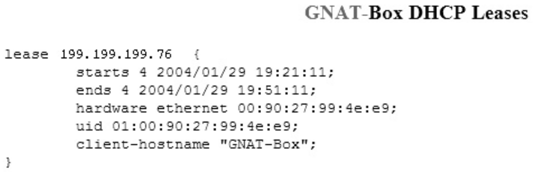
Change refresh rate

*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.



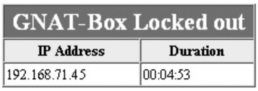
**GNAT-Box DHCP Leases**

```
lease 199.199.199.76  {
        starts 4 2004/01/29 19:21:11;
        ends 4 2004/01/29 19:51:11;
        hardware ethernet 00:90:27:99:4e:e9;
        uid 01:00:90:27:99:4e:e9;
        client-hostname "GNAT-Box";
}
```

*DHCP Leases*

## Locked Out

The table shows the IP address from which a logon was attempted that exceeded the threshold number of attempts set in the LOCKOUT THRESHOLD field in Admin Accounts in **Chapter 4 – Authorization**. A failed logon attempt is one in which the wrong user name and/or password has been entered. The duration shows how long the IP address 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 logon from the IP address. When the lockout time is up, the IP address will drop from the table.



GNAT-Box Locked out

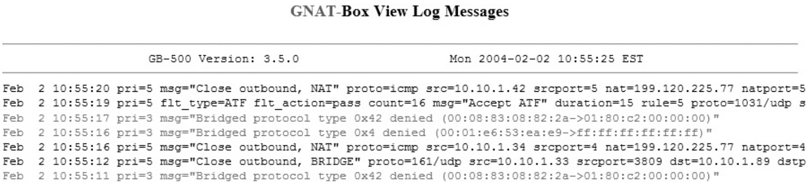
| IP Address | Duration |
|---|---|
| 192.168.71.45 | 00:04:53 |

*Lockouts*

## View Log Messages

Recent events are kept locally in a buffer on the firewall system. The size of the buffer is dependent on the system and memory configuration. When the buffer is filled, it will begin writing over older data. Log messages are displayed in reverse order, with the most recent message appearing at the top. The display is static and must be refreshed in order to display new activity.

Data is written in the standard WebTrends Enhanced Log Format (WELF). Warning messages are displayed in red. See **Appendix B–Log Messages** for more about Log Messages. See Remote Logging in **Chapter 3 – Services** for more about WELF.



GNAT-Box View Log Messages

```
                    GB-500 Version: 3.5.0                   Mon 2004-02-02 10:55:25 EST

Feb  2 10:55:20 pri=5 msg="Close outbound, NAT" proto=icmp src=10.10.1.42 srcport=5 nat=199.120.225.77 natport=5
Feb  2 10:55:19 pri=5 flt_type=ATF flt_action=pass count=16 msg="Accept ATF" duration=15 rule=5 proto=1031/udp s
Feb  2 10:55:17 pri=3 msg="Bridged protocol type 0x42 denied (00:08:83:08:82:2a->01:80:c2:00:00:00)"
Feb  2 10:55:16 pri=3 msg="Bridged protocol type 0x4 denied (00:01:e6:53:ea:e9->ff:ff:ff:ff:ff:ff)"
Feb  2 10:55:16 pri=5 msg="Close outbound, NAT" proto=icmp src=10.10.1.34 srcport=4 nat=199.120.225.77 natport=4
Feb  2 10:55:12 pri=5 msg="Close outbound, BRIDGE" proto=161/udp src=10.10.1.33 srcport=3809 dst=10.10.1.89 dstp
Feb  2 10:55:11 pri=3 msg="Bridged protocol type 0x42 denied (00:08:83:08:82:2a->01:80:c2:00:00:00)"
```

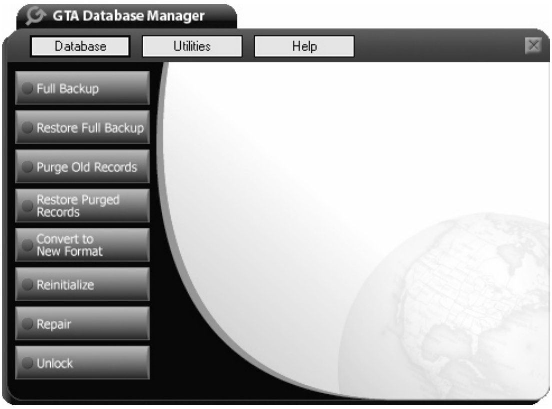
*View Log Messages*

# 14 Utilities

## DBmanager

DBmanager contains an interface for GTAsylog and the LogView utility and verifies installation success for GTAsyslog. For GTA Reporting Suite and GB-Commander, DBmanager verifies installation success and maintains ODBC-compliant databases by performing backups, data purges, data restores, log imports, format conversions, reinitializations, unlocking and repairs. Functions specific to GTA Reporting Suite and GB-Commander are covered in those products' guides; only functions used by the GTA Firewall and GTAsyslog are covered in this guide.

Select DBmanager from the **GTA** sub-menu of the **Windows Start Menu**.



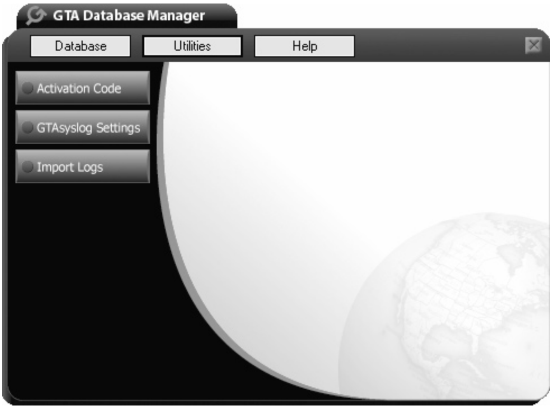
*DBmanager*

### Database Maintenance

The database maintenance functions under the **Database** menu are intended for use with GTA Reporting Suite and GB-Commander and will not function without a license for one of these products. It contains facilities for purge and backup, database conversion, reinitialization and repair, and a facility to unlock the database. See the GTA Reporting Suite and GB-Commander product guides for more information.

## Utilities

The **Utilities** menu in DBmanager contains the GTA Reporting Suite Activation Code interface; an interface for configuring the GTAsyslog for GNAT Box System Software and GTA Reporting Suite; and the Import Logs function to import old logs into the GTA Reporting Suite or GB-Commander database. Activation Code, Import Logs and the Firewall Monitoring List under GTAsylog will not function without a license for GTA Reporting Suite or GB-Commander.



*DBmanager – Utilities Tab*

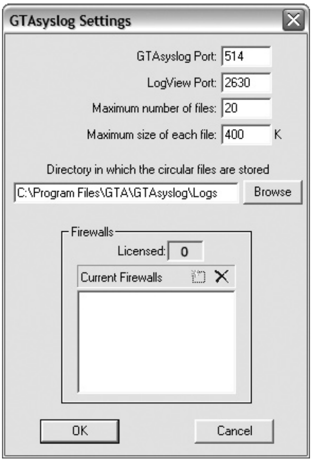
### GTAsyslog Settings

The GTAsyslog dialog allows the user to select how GTAsyslog operates, how GTA Reporting Suite accesses recorded data, and which port will be used by the LogView utility.

GTAsyslog automatically writes log data to a circular file. The file buffer size is dependent on the system and memory configuration. When the buffer is filled, GTAsyslog begins writing over older data. Log messages are displayed in reverse order, with the most recent message appearing at the top. The display is static and must be refreshed in order to display new activity. Data is written in the standard WebTrends Enhanced Log Format (WELF). See Remote Logging in **Chapter 3 – Services** and **Chapter 13 – System Activity** for more about Logging.

## GTAsyslog Fields

| | |
|---|---|
| GTAsyslog Port | Default 514. |
| LogView Port | Default 2630. |
| Max number of files | Log entries retained before overwriting. Default 20. |
| Max size of each file | Maximum file size for each log. Default – 400 K. |
| File Directory | Circular log file name. Default C:\GTA\GTAsyslog\Logs. |
| Current Firewalls | Host names of firewalls monitored by GTAsyslog for GTA Reporting Suite. |



GTAsyslog Settings

GTAsyslog Port: 514

LogView Port: 2630

Maximum number of files: 20

Maximum size of each file: 400 K

Directory in which the circular files are stored

C:\Program Files\GTA\GTAsyslog\Logs

Firewalls

Licensed: 0

Current Firewalls

*GTAsyslog*

## Help

Verify Installation for GTAsyslog, GB-Commander and GTA Reporting Suite, and the About dialog box are found under DBmanager's **Help** menu.

### Verify Installation

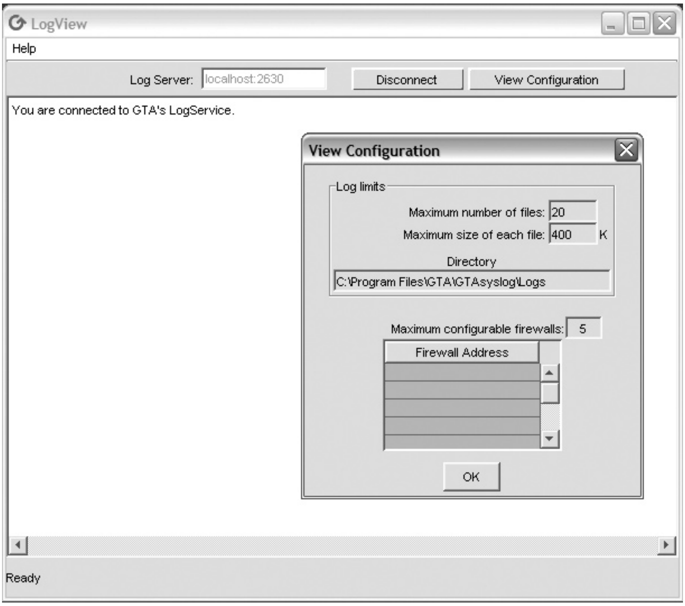
Verify Installation provides a list of general information about your workstation computer. It also provides a list of serial numbers; number of firewalls licensed; and database information, including tables and DSNs for GB-Commander and GTA Reporting Suite, when installed.

Verify Installation also indicates whether the GTAsyslog utility is running. For more about using Verify Installation with GTA Reporting Suite and GB-Commander, see the individual product guides.

## LogView

LogView is a versatile viewer that gives read-only access to logs for up to 10 workstations. Users equipped with LogView can review the streaming log file data as it is written to the circular file from anywhere on the network.

Enter the location of your syslog server in the Log Server field. By default, this is hostname/port number `localhost:2630`. Click the **CONNECT** button to use LogView. Click **DISCONNECT** to stop viewing the log files.



Log Server: localhost:2630

You are connected to GTA's LogService.

Maximum number of files: 20

Maximum size of each file: 400 K

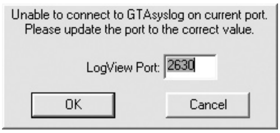
Directory

C:\Program Files\GTA\GTAsyslog\Logs

Maximum configurable firewalls: 5

*Log Viewer with View Configuration*

If an error message appears indicating that the port number may be incorrect, GTAsyslog may not be running. Check the Windows system Services to verify that GTA syslog is installed and running, or use Verify Installation in DBmanager.



Unable to connect to GTAsyslog on current port.
Please update the port to the correct value.

LogView Port: 2630

*Port Number Error*

# GBAuth User Authentication

If Authentication is required by a filter or tunnel, a user accessing the GTA Firewall must enter the GTA Authentication, LDAP or RADIUS name and password into the GBAuth utility before initiating a connection. The Authentication feature desired must be enabled and configured and a user authentication Remote Access Filter must be configured to use authentication. See **Chapter 4 – Authorization** for information on configuring authentication for GTA, LDAP and RADIUS and on users and VPNs.

GBAuth can be installed as a Windows or a cross-platform Java-based service. Install the appropriate application on the computer from which authentication will be initiated. When the service is started, a GBAuth icon will appear in the system tray. By right-clicking on the GBAuth icon, you can display the authentication dialog, close the utility, or view the About box.

As long as data is being exchanged, GBAuth automatically re-authenticates. If data is not being exchanged, a the connection closes after 10 minutes of inactivity. To close GBAuth, right-click on the icon and select **Close**.

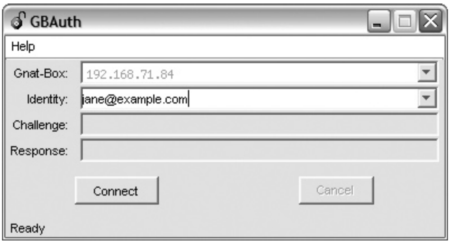
## Using GBAuth for GTA Authentication

To use GTA authentication, the Authentication feature must be enabled; a user authentication Remote Access Filter must be configured; and users must be created. To authenticate to the firewall using GBAuth, users enter the values from Users Authorization.

**GBAuth GTA Authentication Fields**

| | |
|---|---|
| GNAT Box | Name or IP address of the GTA Firewall. |
| Identity | Login data provided to the user: the value from the Users Authorization LOCAL IDENTITY field. Maximum, 127 characters. Case-sensitive. |
| Challenge | N/A |
| Response | Alphanumeric password from the Users Authorization PASSWORD field. |

Enter the name or IP address of the GTA Firewall in the GNAT BOX field or select it from the dropdown box. Enter the identity in email address format specified in User Authorization in the IDENTITY field, then click **OK**.



GBAuth

Help

Gnat-Box: 192.168.71.84

Identity: jane@example.com

Challenge:

Response:

Ready

*GBAuth using GTA Authentication*

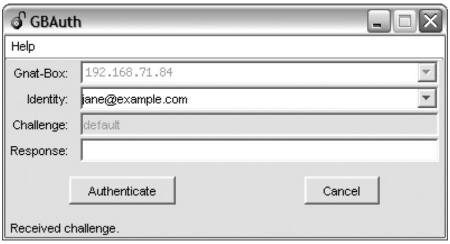
If the information is correct, an unlock icon should appear in the system tray.

*Authentication Unlocked Icon*

***Note***

> The Unlocked icon indicates that authentication has begun; the Locked icon indicates that the user has successfully authenticated.

The cursor will move to the Response field. Enter the password from Users Authorization, then click **OK**.



GBAuth

Help

Gnat-Box: 192.168.71.84

Identity: jane@example.com

Challenge: default

Response:

Received challenge.

*GBAuth Challenge & Response*

If the identity or password is not recognized, an "Authentication failed" box will appear. If the information is correct, the lock icon appears in the system tray, and you can initiate a VPN connection through the firewall.

*Authentication Locked Icon*

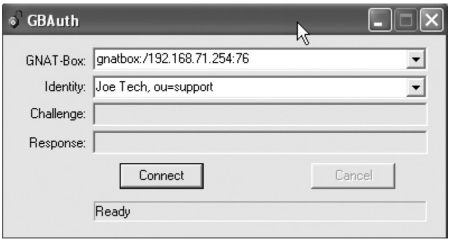
## Using GBAuth for LDAP Authentication

To use LDAPv3 authentication, the Authentication and LDAPv3 features must be enabled; a user authentication Remote Access Filter must be configured; and the LDAP server must be configured.

## GBAuth LDAP Fields

| | |
|---|---|
| GNAT Box | Name or IP address of the GTA Firewall. |
| Identity | Login data provided to the user: cn (common name) and ou (organizational unit) combined. Do not enter the “cn=” identifier; this will be prepended when the data is sent to the LDAP server. Maximum, 127 characters. The cn is case-sensitive. |
| Challenge | N/A |
| Response | Alphanumeric password specified for the user on the LDAP server. Case-sensitive. |

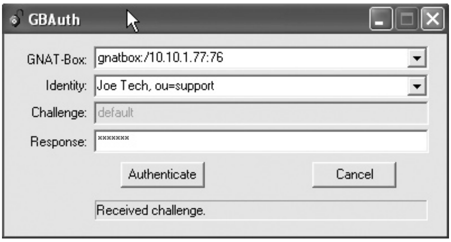
Enter the name or IP address of the GTA Firewall in the GNAT Box field or select it from the dropdown box. Enter the cn and the ou identifier plus value in the Identity field using the format `User Name, ou=organization unit`, then click **OK**.



GNAT-Box: gnatbox:/192.168.71.254:76
Identity: Joe Tech, ou=support
Challenge:
Response:
Ready

*GBAuth using LDAP Authentication*

If the information is correct, a GBAuth unlock icon should appear in the system tray. The cursor will move to the Response field. Enter the password set up for the user on the LDAP server, then click **OK**. (The Authentication Base DN field values are appended to the data, creating the dn string that is sent by GBAuth to the LDAP server.)



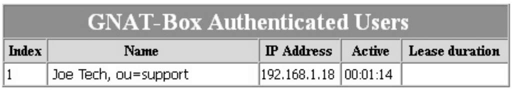
GNAT-Box: gnatbox:/10.10.1.77:76
Identity: Joe Tech, ou=support
Challenge: default
Response: *******
Received challenge.

*GBAuth Challenge & Response*

If the identity or password is not recognized, an "Authentication failed" box will appear. If the information is correct, a lock icon appears in the system tray, and you can initiate a connection to or through the firewall.

### Authenticated Users

Below is an example of a user authenticated with LDAP. The Authenticated Users screen is located in **System Activity/Authenticated Users**. By default, the firewall will log both successful and unsuccessful authentication attempts. See **Chapter 13 – System Activity** for more information about the Authenticated Users screen.



GNAT-Box Authenticated Users

| Index | Name | IP Address | Active | Lease duration |
|---|---|---|---|---|
| 1 | Joe Tech, ou=support | 192.168.1.18 | 00:01:14 | |

*Authenticated Users for LDAP*

## Using GBAuth for RADIUS Authentication

To use RADIUS authentication, the Authentication and RADIUS features must be enabled; a user authentication Remote Access Filter must be configured; and the RADIUS server must be configured.

Enter the name or IP address of the GTA Firewall in the GNAT Box field or select it from the dropdown box. Enter the RADIUS identity and password in the appropriate fields. If the information is correct, a lock icon appears in the system tray, and you can initiate a VPN connection through the firewall.

User names are specified on your RADIUS server; the response or password is configured in the RADIUS section of the Authentication service on the GTA firewall.

### GBAuth RADIUS Fields

GNAT Box — Name or IP address of the GTA Firewall.

Identity — Login data provided to the user, specified on the RADIUS server. Maximum, 127 characters. Case-sensitive.

Challenge — N/A

Response — Alphanumeric preshared secret (password) specified for the user in the RADIUS section of Authentication. Case-sensitive.

# 15 Troubleshooting

## Troubleshooting Basics

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? (Firewall Appliances)

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.

### 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 (firewall to host or router) you need a cross-over cable.
- For a connection to a hub or switch you need a straight-through cable.

***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 (Primary Domain Controller) 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 a “bridging loop” error message when I am in bridging mode.

A bridging loop message indicates a physical loop in the network cabling.

```
Feb 2 02:04:30 pri=4 msg=”Bridging loop (13) 00:00:5e:00:01:
60->01:00:5e:00:00:12 fxp1->fxp0 (muted)” src=199.120.225.53
dst=224.0.0.18
```

Check physical wiring of hubs and switches to be sure no wire is crossed. Bridged networks must be physically isolated.

### 11. I get an “alarm: Interface down” message.

An Interface down error message indicates that an interface has failed.

```
Feb 2 13:44:18 pri=4 msg=”alarm: Interface EXTERNAL (rl1) down”
type=mgmt
```

This could be caused by a loose or disconnected cable.

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

You may have the wrong cable for your connection.

- For a direct connection (GNAT Box System to host or router) you need a crossover cable.
- For a connection to a hub or switch you need a straight-through cable.

A yellow crossover cable and grey straight-through cable are included with hardware appliances.

***Note***

Distinguish between crossover cables and straight-through cables by comparing 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.

**13. I lost my user name and/or password. How can I log on to my firewall ?**
**-or- Resetting to Factory Defaults (not available on some versions prior to 3.5).**

If login information has been irretrievably lost, a firewall can be reset to factory defaults, erasing all configuration data from the currently used memory partition and resetting the user name and password to `gnatbox/gnatbox`. The configuration data can only be restored by loading a saved configuration with a known user name and password, or by manually entering the information.

To reset your firewall to factory defaults, attach either a terminal (using a serial console cable), or a workstation with terminal emulation software (using a DB9 null modem cable). Enter these settings for the console connection:

| | |
|---|---|
| Emulation | VT 100 |
| Port | COM port used on the system. |
| Baud Rate | 38400 |
| Data | 8 |
| Parity | None |
| Stop | 1 |
| Flow control | Hardware* |

* Set flow control to “None” as an alternative to hardware flow control.

Power on the GTA Firewall. The following words will display:

`GNAT Box System Software 3.5.0` (your version number)

`loading...`

When the word “`loading`” appears, immediately press <**Control R**>. The system will begin to load, and configuration and hardware data will appear on screen. Finally, a confirmation question displays:

`Are you sure you want to reset your` (GTA Firewall) `configuration?: (“yes” or “no”)`

To reset to factory defaults, type the word “`yes`” in ***lower case*** letters. Typing any other key will reboot the system without resetting to defaults. There is no time out; the reset confirmation question will remain until a key is pressed.

### 14. How do I revert to my previous configuration after a version upgrade? (The memory slice feature is not available on versions prior to 3.4.)

The GNAT Box system's flash memory is in two sections; one contains the current software version plus any saved configuration, the other contains the previous software version and configuration. A new GNAT Box system has two identical slices.

When the GNAT Box system is upgraded to a new runtime, the upgrade process automatically overwrites the memory slice not in use with the new software version and the existing configuration, leaving the production firewall version and configuration intact. When the firewall is rebooted, the updated memory slice will load by default.

To select a memory slice other than the default, set up the console interface as described in the previous Troubleshooting question, Resetting to Factory Defaults.

When the system boots up, the memory slice information will load. When the word "`Default`" appears, immediately type the number of the slice you wish to load.

```
1 GNAT Box slice 1

2 GNAT Box slice 2

Default: 1
```

### 15. How do I use the memory slice feature for live configuration testing? (The memory slice feature is not available on versions prior to 3.4.)

The memory slice feature can be used to test a new firewall configuration in production while preserving the current configuration in the opposite memory slice. In the following example, memory slice 1 contains the production configuration, and memory slice 2 is used for test a configuration.

1. Save a copy of the current configuration.
2. Reboot the firewall using the console interface.
3. Select and boot memory slice 2.

***Caution***

The test configuration will now be your active firewall.

4. Upload the configuration saved in step #1.
5. Switch to the Web interface or GBAdmin to make advanced configuration changes; the slice will load by default until another is selected.
6. To revert to the production configuration, reboot the firewall using the console interface and select memory slice 1.

# Appendix A Ports and Services

## GTA Ports & Services

Port Numbers are divided into three ranges:

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

GTA generally uses well-known ports for standard services. For GTA services, appropriate ports are supplied by default. Default ports can be changed, but must be matched to references to the port within filters and services.

The following ports are the default for GTA services; some are standard, others are private ports for a specific GTA or third-party service. This list is provided for reference only and should not be considered definitive. Default ports for services may change. Consult documentation for your product for the latest information. Some ports are used for more than one service.

**GTA Default & Standard Port Assignments**

| Service | Port/Protocol | Description |
|---|---|---|
| GB-C, encrypted | 76/TCP | Communication with GB-Commander Server (SSL) |
| RMC | 77/TCP | Firewall Administration using GBAdmin |
| GB-C Client | 78/TCP | Client communication with GB-Commander Server |
| http | 80/TCP | Firewall Administration using HTTP |
| ntp | 123/UDP | Used for NTP in the Network Time Service |
| ldap | 389/TCP | LDAP service for dynamic DNS |
| https | 443/TCP | Encrypted administration via the Web |
| logging | 514/TCP | Remote Logging |
| radius | 1812/TCP | RADIUS service for dynamic DNS |
| http proxy | 2784/TCP | HTTP proxy default port |

## Well-known Ports and Services

Well-known (common) ports 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. Here is a brief list of these common services and port numbers.

### Well-known Port Assignments

| Service | Port/Protocol | Description |
|---|---|---|
| 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 | |

# Appendix B Log Messages

In order to use the remote logging facility of the GNAT Box System the remote logging service must be configured on the Remote Logging screen, where the user defines the remote host, log facilities, and the data that will be transmitted. Log messages can be viewed from View Log Messages (see **Chapter 13 – System Activity**), from the LogView utility (see **Chapter 14 – Utilities**), as a log file in a text utility such as Notepad or TextEdit, or using the GTA Reporting Suite application.

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

## Default Logging

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
```

# Log Messages

## Permitted Inbound Request

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, enable the TUNNEL OPENS field in Filter Preferences.

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 created only when the session is closed. To generate a log message when an outbound session is created, enable the TUNNEL CLOSES field in Filter Preferences (enabled by default).

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 explicitly allowed 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 verification 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=/ duration=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 duration=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 duration=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 dura-
tion=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@hacker.net”
src=199.120.220.100 srcport=1034 dst=199.120.225.80 dstport=25 dura-
tion=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 interface 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

### 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 connec-
tions. 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
```

## Authentication Messages

Log messages for authenticated users and active hosts (limited user license products).

### Authenticated User

```
Jun 13 11:06:52 pri=6 msg=”RMCauth: Allow ‘support@gta.com’,
authentication successful.” type=mgmt src=192.178.71.254
srcport=3630 dst=10.10.1.84 dstport=76 duration=7 Jun 13 11:06:52
pri=5 msg=”AUTH: Assign 192.178.71.254, to ‘Mary’” type=mgmt Jun
13 11:06:46 pri=5 msg=”RMCauth: Accepted connection” type=mgmt
src=192.178.71.254 srcport=3630 dst=10.10.1.84 dstport=76 duration=1
```

### Authenticated User Close

```
Jun 13 11:18:00 pri=5 msg=”RMCauth: Close connection” type=mgmt
src=192.178.71.254 srcport=3630 dst=10.10.1.84 dstport=76 dura-
tion=675 Jun 13 11:18:00 pri=5 msg=”AUTH: Release 192.178.71.254,
from ‘Mary’” type=mgmt
```

### Authenticated User Denied

```
Jun 13 11:04:39 pri=5 msg=”RMCauth: Close connection”
type=mgmt src=192.178.71.254 srcport=3569 dst=10.10.1.84
dstport=76 duration=17 Jun 13 11:04:38 pri=4 msg=”RMCauth:
Deny ‘support@gta.com’, authentication failure.” type=mgmt
src=192.178.71.254 srcport=3569 dst=10.10.1.84 dstport=76 dura-
tion=16 Jun 13 11:04:22 pri=5 msg=”RMCauth: Accepted connection”
type=mgmt src=192.178.71.254 srcport=3569 dst=10.10.1.84 dstport=76
```

### Tunnel Access after Authentication

```
Jan 6 17:36:04 pri=5 msg=”Open inbound, NAT tunnel” proto=smtp
src=199.120.225.20 srcport=1806 user=”Nick” nat=199.120.225.78
natport=25 dnat=10.10.1.78 dnatport=1806 dst=10.10.1.9 dstport=25
rule=1
```

### Remote Access Filter without Authentication

```
Jun 4 13:27:08 pri=4 flt _ type=RAF flt _ action=block msg=”Rejecting
unathenticated access (1)” rule=1 proto=25/tcp src=199.120.225.77
srcport=1700 dst=199.120.225.78 dstport=25 interface=sis1 flags=0x2
```

### Remote Access Filter with Authentication

```
Jun 4 13:31:50 pri=5 msg=”Open inbound, NAT tunnel” proto=smtp
src=199.120.225.77 srcport=1753 user=”Nick” nat=199.120.225.78
natport=25 dnat=10.10.1.78 dnatport=1753 dst=10.10.1.9 dstport=25
rule=1
```

### Attempt at Mobile VPN Without Authentication

```
Jan 11 14:20:09 pri=4 msg=”Authentication needed, access for
‘support@gta.com’ denied.” type=mgmt,vpn src=65.33.234.134
dst=199.120.225.78
```

### Released User

User must authenticate again to gain access to restricted areas.

```
Jan 6 17:59:19 pri=5 msg=”USER: Release 199.120.225.20, from
‘Nick’” type=mgmt
```

## Automatic Filter Messages

Automatic Accept All filters can be logged by activating Automatic Filter logging in Filter Preferences. When activated, automatic filters will be recorded in the Active Filters table of the System Activity section.

```
Automatic Filter Example - Dec 2 10:23:33 pdbtest78.gta.com
FILTER: ATF (5) accept - notice ICMP [192.168.1.12:3]-
>[192.1168.1.78:3] fxp0 l=32 f=0x3.
```

### Invalid Packets

```
Dec 2 10:30:59 pdbtest78.gta.com FILTER: Rejecting invalid packet:
warning TCP [10.10.1.98:0]->[10.10.1.78:0] fxp0 l=20 f=0x0
```

### Active Host

```
Jan 9 01:14:22 pri=5 msg=”Accept outbound, NAT” cat _ action=pass
dstname=www.eweek.com proto=http src=10.10.1.82 srcport=1658
nat=199.120.225.72 natport=1658 dst=63.87.252.160 dstport=80 rule=2
duration=349 sent=2480 rcvd=11842 pkts _ sent=18 pkts _ rcvd=17
op=GET arg=/util/css/eweek.css Jan 9 01:14:07 pri=5 msg=”Accept
outbound, NAT” cat _ action=pass dstname=www.eweek.com proto=http
src=10.10.1.82 srcport=1657 nat=199.120.225.72 natport=1657
dst=63.87.252.160 dstport=80 rule=2 duration=334 sent=2709
rcvd=24433 pkts _ sent=24 pkts _ rcvd=25 op=GET arg=/print _
article/0,3668,a
```

### Access Control List with Surf Sentinel Allowed

```
Oct 29 14:24:18 acmefirewall id=firewall time=”2002-10-29 14:24:18”
fw=”acmefirewall-ha-1” pri=5 msg=”Accept outbound NAT”
cat _ action=pass cat _ site=”Web Communications”
dstname=www.leadcart.com proto=http src=192.168.71.97 srcport=2661
nat=199.120.225.3 natport=2661 dst=205.138.3.133 dstport=80 rule=2
duration=23 sent=536 rcvd=537 pkts _ sent=6 pkts _ rcvd=5 op=GET
arg=/ads1/images/digits/n7.gif
```

### Local Content List Denied

```
Oct 29 14:24:26 acmefirewall id=firewall time=”2002-10-29 14:24:26”
fw=”acmefirewall-ha-1” pri=4 msg=”Block outbound NAT”
cat _ action=block cat _ site=”Local Deny” dstname=ad.doublclk.net
proto=http src=src=192.168.71.33 srcport=4991 nat=199.20.136.33
natport=4991 dst=205.138.3.82 dstport=80 rule=2 duration=22
sent=861 rcvd=60 pkts _ sent=3 pkts _ rcvd=1 op=GET arg=/adi/
caranddriver.lana.com/kw=;;ord=180587622710292244
```

## Bridging Error Messages

Indicates a physical loop in the cabling of the network. Check physical wiring of hubs and switches to be sure no wire is crossed. Bridged networks must be physically isolated.

### Physical Loop

```
Feb 2 02:04:30 pri=4 msg=”Bridging loop (13) 00:00:5e:00:01:
60->01:00:5e:00:00:12 fxp1->fxp0 (muted)” src=199.120.225.53
dst=224.0.0.18
```

### Denied Protocol

Only displayed when logging options set to log invalid packets. One can allow these packets through by adding them to the Bridged protocol list.

***Caution***

No filtering will then be done on this. Great care should be taken in allowing these packets through.

```
Feb 2 13:28:53 pri=3 msg=”Bridged protocol type 0x42 denied (00:
08:83:08:82:2a->01:80:c2:00:00:00)”
```

## Surf Sentinel

### Saving Content Filtering Preferences

```
Feb 2 13:28:52 pri=5 msg=”proxyWWW: Surf Sentinel successfully
initialized” type=mgmt
```

```
Feb 2 13:28:53 pri=6 msg=”proxyWWW: Listening at port 2784.”
type=mgmt
```

```
Feb 2 13:37:40 pri=6 msg=”proxyWWW: Reinitializing.” type=mgmt
```

```
Feb 2 13:37:40 pri=5 msg=”WWWadmin: Update of ‘URL Access
Lists’.” type=mgmt src=192.168.71.243 srcport=2447 dst=192.168.71.77
dstport=443
```

### Saving Content Filtering Access Control Lists

```
Feb 2 13:37:40 pri=5 msg=”WWWadmin: Update of ‘URL Access
Lists’.” type=mgmt src=192.168.71.243 srcport=2447 dst=192.168.71.77
dstport=443
```

```
Feb 2 13:37:40 pri=6 msg=”proxyWWW: Reinitializing.” type=mgmt
```

### Saving Content Filtering Local Content Lists

```
Feb 2 13:39:23 pri=5 msg=”WWWadmin: Update of ‘Local Content
Lists’.” type=mgmt src=192.168.71.243 srcport=2460 dst=192.168.71.77
dstport=443
```

```
Feb 2 13:39:23 pri=6 msg=”proxyWWW: Reinitializing.” type=mgmt
```

### Block Message

```
Feb 2 13:33:49 pri=4 msg=”Block outbound, NAT” cat _ action=block
cat _ site=”Adult/Sexually Explicit” dstname=www.playboy.com
proto=http src=192.168.71.243 srcport=2399 nat=199.120.225.77
natport=2399 dst=209.247.228.201 dstport=80 rule=2 duration=22
sent=676 rcvd=44 pkts _ sent=3 pkts _ rcvd=1 op=GET arg=/
```

### Accept Message

```
Feb 2 13:34:45 pri=5 msg=”Accept outbound, NAT” cat _ action=pass
cat _ site=”Games” dstname=1118.ign.com proto=http src=192.168.71.95
srcport=1813 nat=199.120.225.77 natport=1813 dst=216.35.123.118
dstport=80 rule=2 duration=22 sent=1279 rcvd=450 pkts _ sent=5
pkts _ rcvd=5 op=GET arg=/event-ng/Type
```

## Miscellaneous

Interface is down; indicates an interface has failed. This could be caused by a loose or disconnected cable.

```
Feb 2 13:44:18 pri=4 msg=”alarm: Interface EXTERNAL (rl1) down”
type=mgmt
```

## Saving GB-Commander on Firewall

```
Feb 2 14:22:19 pri=5 msg=”WWWadmin: Update of ‘GBC’.” type=mgmt
src=192.168.71.243 srcport=2759 dst=192.168.71.77 dstport=443
```

```
Feb 2 14:22:19 pri=6 msg=”gblogd: Reinitializing.” type=mgmt
```

```
Feb 2 14:26:21 pri=5 msg=”GBC: Connected to server success-
fully” type=mgmt src=199.120.225.77 srcport=2268 dst=204.94.136.20
dstport=76
```

OR

```
Feb 2 14:22:19 pri=5 msg=”GBC: Already connected to server”
type=mgmt src=199.120.225.77 srcport=2267 dst=204.94.136.20
dstport=76
```

# Appendix C User Interfaces

GNAT Box System Software includes two primary interfaces: the Web interface and GBAdmin. Both user interfaces provide comprehensive administrative access and user-friendly, browser-based Help.

A third interface, the Console, is primarily a fail-safe,. It is used to reset a misconfigured firewall to default, to recover a GTA Firewall and can be used for basic configuration. The Console has limited functions on GB-Light. See the **Console Interface User's Guide** at www.gta.com for more information.

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 other basic and advanced configuration.

## Web Interface

The Web interface is platform-independent and can be used on any compatible browser, including Internet Explorer, Netscape Navigator, Mozilla, Opera and the text-based Lynx browser, running on platforms such as Windows, Unix and Mac; caveats are noted in guides and release notes.

The GTA Firewall can be remotely administered using the Web interface on a frames-capable web browser, allowing administration of the GTA Firewall from Windows, Unix, X-Windows and Macintosh platforms.

### Exclusive Features

- SSL encryption option.
- Secure administration from any location connected to the Internet.
- Intuitive browser-based user interface.
- Platform-independent, compatible with most browsers and platforms.
- Immediate modification as changes are saved to the firewall.

## 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 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.

### 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.”

### How to Access the Web Interface

Start a frames-capable web browser.

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., https://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.

***Caution***

Firewall login persists until the user logs out or quits the browser application. To prevent unauthorized access, remember to log off the firewall or quit the browser application.

## Navigation and Data Entry

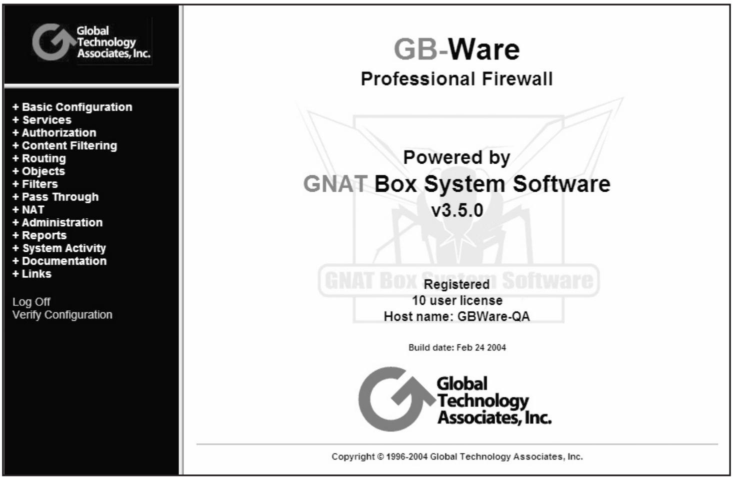
The Web interface uses HTML frames to subdivide the browser's display. The main parts of the Web interface navigation screen are:

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-Ware
Professional Firewall

Powered by
GNAT Box System Software
v3.5.0

Registered
10 user license
Host name: GBWare-QA

Build date: Feb 24 2004

Global Technology Associates, Inc.

Copyright © 1996-2004 Global Technology Associates, Inc.

*Web Interface Opening Screen*

### 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.

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.

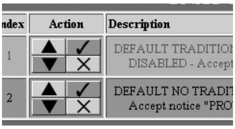
### Buttons and Fields

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

## Navigation Buttons

| | |
|---|---|
| Reset | Return screen to previous state. |
| Submit | Submit entries made in the current function. |
| Copy | Copy filters or other items. |
| Paste | Paste copied items into a new screen. |
| Default | Make the configuration screen items conform to the default security policy for the current configuration. |
| Back | Go back to the previous screen without saving. |
| Save | Save this screen or item. |
| 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.

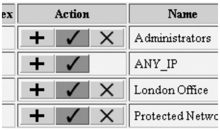


| ndex | Action | Description |
|---|---|---|
| 1 | ▲ ✓<br>▼ × | DEFAULT TRADITIOI<br>DISABLED - Accept |
| 2 | ▲ ✓<br>▼ × | DEFAULT NO TRADIT<br>Accept notice "PRO |

*Filter Icon Buttons*

## Filter Icon Buttons

| | |
|---|---|
| Up/Down Arrow | Add a line (e.g., filter) above/below the selected item. Used where order ***is*** important. |
| ×/Delete | Delete the selected line item. |
| √/Check Mark | Edit the selected line item. |



| ex | Action | Name |
|---|---|---|
| | + ✓ × | Administrators |
| | + ✓ | ANY_IP |
| | + ✓ × | London Office |
| | + ✓ × | Protected Netwo |

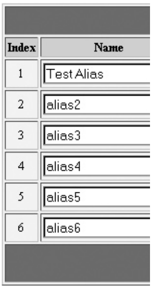
*Object Icon Buttons*

## Object Icon Buttons

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

Specialized buttons such as **SET TIMEZONE** 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.

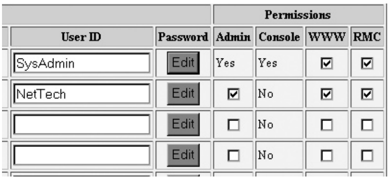


| Index | Name |
|---|---|
| 1 | Test Alias |
| 2 | alias2 |
| 3 | alias3 |
| 4 | alias4 |
| 5 | alias5 |
| 6 | alias6 |

*Index Fields*

Checkboxes 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.



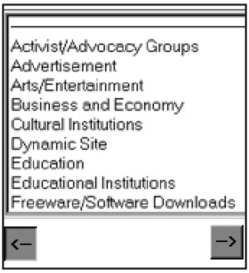
| | | Permissions | | | |
|---|---|---|---|---|---|
| User ID | Password | Admin | Console | WWW | RMC |
| SysAdmin | Edit | Yes | Yes | ☑ | ☑ |
| NetTech | Edit | ☑ | No | ☑ | ☑ |
| | Edit | □ | No | □ | □ |
| | Edit | □ | No | □ | □ |

*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.

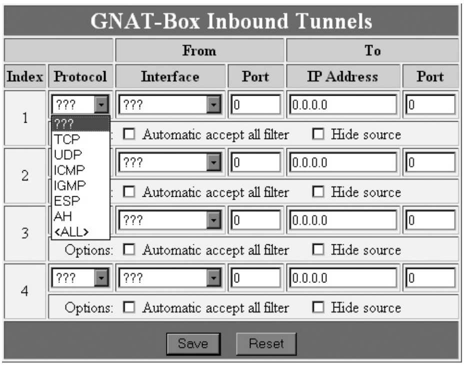
**–>** A right-pointing arrow moves the selected item from the list on the left to the list on the right.



Activist/Advocacy Groups
Advertisement
Arts/Entertainment
Business and Economy
Cultural Institutions
Dynamic Site
Education
Educational Institutions
Freeware/Software Downloads

*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.



GNAT-Box Inbound Tunnels

| | | From | | To | |
|---|---|---|---|---|---|
| Index | Protocol | Interface | Port | IP Address | Port |
| 1 | ??? | ??? | 0 | 0.0.0.0 | 0 |
| | : □ Automatic accept all filter | | | □ Hide source | |
| 2 | | ??? | 0 | 0.0.0.0 | 0 |
| | : □ 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 | |

*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 a Windows-only interface that allows access from a local workstation that can be operated without access to the Internet. The program uses standard Windows commands and conventions. It requires a Windows-based computer or workstation and Internet Explorer, version 5.0 and up.

## 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. This allows using verification and configuration reports to adjust settings before committing a new configuration to the production 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.

### Characteristics

GBAdmin data are not saved to the currently loaded configuration file, remote GTA Firewall or floppy disk, until: a configuration 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."

### How to Access GBAdmin

Click the GBAdmin icon on the desktop if one was created during installation; optionally, open the **Windows program menu/GTA GNAT Box folder** and click the program icon.

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 GTA Firewall configuration loaded, an unauthorized user could gain access. To prevent unauthorized access, remember to log off.

## 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.

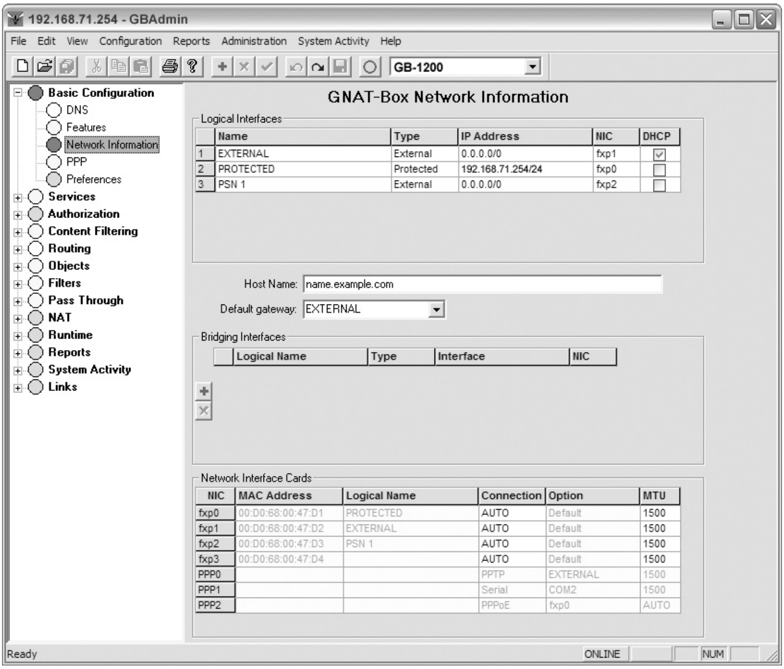
Toolbar: Tools which provide quick access to GBAdmin's most used features.

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.



GNAT-Box Network Information

Logical Interfaces

| | Name | Type | IP Address | NIC | DHCP |
|---|---|---|---|---|---|
| 1 | EXTERNAL | External | 0.0.0.0/0 | fxp1 | ☑ |
| 2 | PROTECTED | Protected | 192.168.71.254/24 | fxp0 | ☐ |
| 3 | PSN 1 | External | 0.0.0.0/0 | fxp2 | ☐ |

Host Name: name.example.com

Default gateway: EXTERNAL

Bridging Interfaces

| | Logical Name | Type | Interface | NIC |
|---|---|---|---|---|

Network Interface Cards

| NIC | MAC Address | Logical Name | Connection | Option | MTU |
|---|---|---|---|---|---|
| fxp0 | 00:D0:68:00:47:D1 | PROTECTED | AUTO | Default | 1500 |
| fxp1 | 00:D0:68:00:47:D2 | EXTERNAL | AUTO | Default | 1500 |
| fxp2 | 00:D0:68:00:47:D3 | PSN 1 | AUTO | Default | 1500 |
| fxp3 | 00:D0:68:00:47:D4 | | AUTO | Default | 1500 |
| PPP0 | | | PPTP | EXTERNAL | 1500 |
| PPP1 | | | Serial | COM2 | 1500 |
| PPP2 | | | PPPoE | fxp0 | AUTO |

*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.

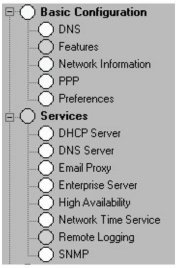
In GBAdmin, clicking on the Scrolling Menu title will display an HTML version of the material available in this guide for each menu title.

### Keys

Familiar keyboard keys used in Windows are also used in GBAdmin: arrow keys 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.

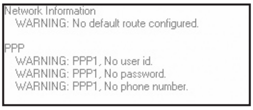


*Scrolling Menu Example*

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

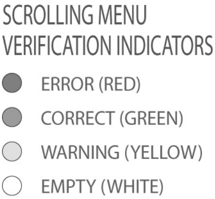
A feature of GBAdmin is the instant verification provided for a configuration. If the function has not been configured correctly or completely, a Pop-up Verification Note is created. The notes appear in front of the section when the user "hovers" the mouse by resting the cursor over the section label. There are two kinds of note: Warning, reporting a possible problem, and Error, reporting 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*

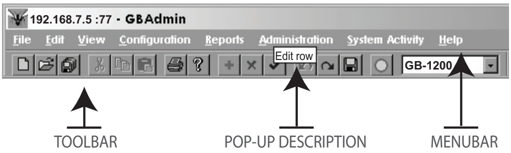
Indicator Dots (also called "lights" or "buttons") give the user an instant impression of whether the section or function is configured correctly.



*Indicator Dots*

### Menubar

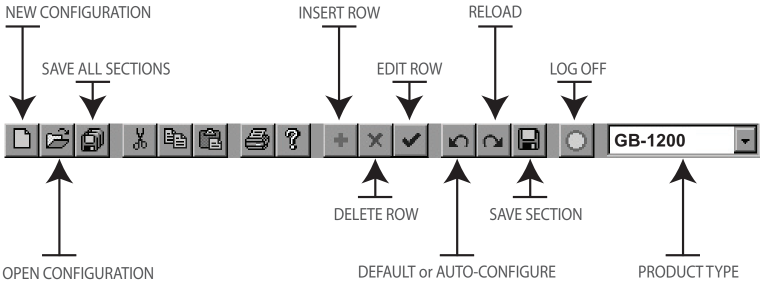
The Menubar contains all the same functions as the Scrolling Menu, plus the Administration menu and many of the familiar Windows functions.


192.168.7.5 :77 - GBAdmin
File Edit View Configuration Reports Administration System Activity Help
Edit row
GB-1200
TOOLBAR
POP-UP DESCRIPTION
MENUBAR

*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 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.

# Appendix D GNAT Box Terms

This section defines terms used in GNAT Box System Software and documentation. These terms, along with a collection of other relevant GNAT Box and industry 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 13 – 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. Common tunnels include: HTTP, FTP, DNS, SQLnet, and telnet.

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.

## Network Transparency

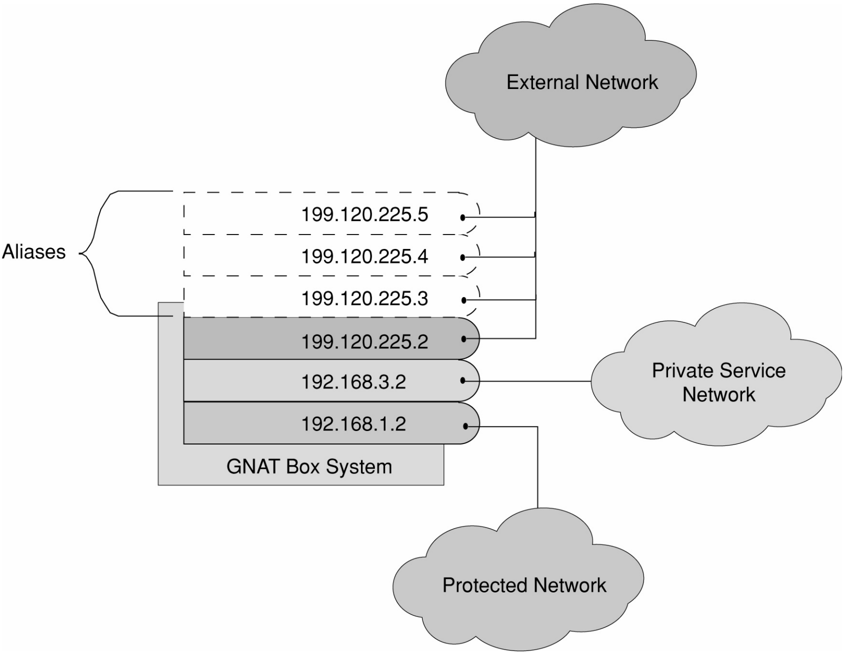
Network Transparency is used to describe the function that allows host systems residing on the PSN and Protected Network to send packets to and receive replies from hosts on external networks in an apparently transparent manner. Network Transparency is implemented as a part of Stateful Packet Inspection. 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.

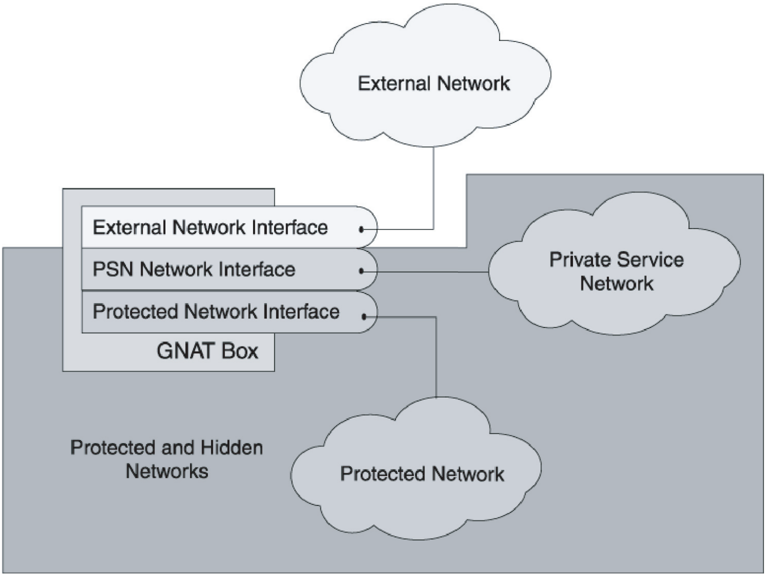


*Example of IP aliases assigned to an External Network interface*

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 (**D**e**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. GTA's firewalls for 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 eight (8) physical network ports (with the optional multi-interface option), and on select firewalls, and unrestricted number network interfaces. Interfaces beyond the required two may be defined as any of the three types; it is possible to have multiple External, Protected or PSN networks.

## 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 one Protected Network to another Protected Network.

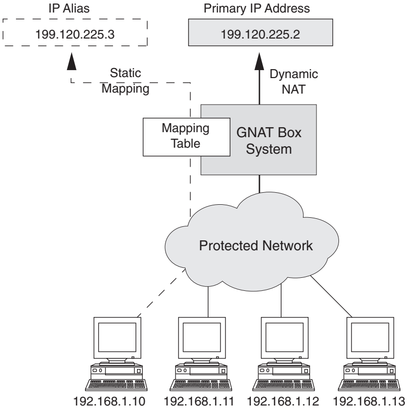
### Default NAT (Dynamic NAT)

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.

### 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. IP Pass Through 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. 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 9 – 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 object (address, interface, etc.) is changed, references to it ***must be changed*** to reflect the new name.

## 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.

Four VPN objects are created by default: an IKE, Manual, Mobile and Dynamic VPN Object.

# Filters

Filter 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 implicit rule for GTA Firewalls is: “That which is not explicitly allowed is denied.” Therefore, if no filters of any type were defined, packets would not be allowed to flow to or through (inbound or outbound) the GTA Firewall system. See individual product guides for the number of filters available on a specific GTA Firewall.

## Filter Sets

When you use the **DEFAULT** button in a filter section, auto-configured filters are generated based on the configuration, security policy and preferences. For new installations, these are the factory set policy and preferences. See the **Appendix E – Default Settings** for a description of the factory set defaults.

## Filter Types

The GTA Firewall system supports four types of filters. The first three types, Remote Access Filters, Outbound Filters and IP Pass Through Filters are configured in a similar way. They can be defined by the user, either by creating custom filters or by using the **DEFAULT** button to auto-configure the filter set.

### Automatic Filters

The fourth type of filter, Automatic Filters, has priority over the other filter types. Automatic Filters are generated by the system for transient events, i.e., a packet sent in response to a request from behind the firewall; connections triggered by selecting Automatic Accept All for an inbound tunnel; and Stealth mode. When Outbound, Remote Access and IP Pass Through filters are active, they will be listed under Automatic Filters in the Active Filters list.

### Stealth Mode

Stealth mode is the factory set default for new GTA Firewall systems. In Stealth mode, the firewall will not respond to ICMP ping requests, ICMP traceroute requests nor UDP traceroute requests. In addition, the firewall will not respond with an ICMP message when a packet arrives for a port without a tunnel or service set on any External Network interface. Because it is activated at the system kernel level, Stealth mode will not appear in the Active Filters list. Stealth mode does not affect Protected Network or Private Service Network interfaces.

## 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 in the ESP tunnel mode. To learn how VPN users and objects are defined, see VPNs in **Chapter 4 – Authorization** and VPN Objects in **Chapter 7 – Objects**. For more information about the GNAT Box VPN and the VPN Client option, see the **GNAT Box VPN Feature Guide**.

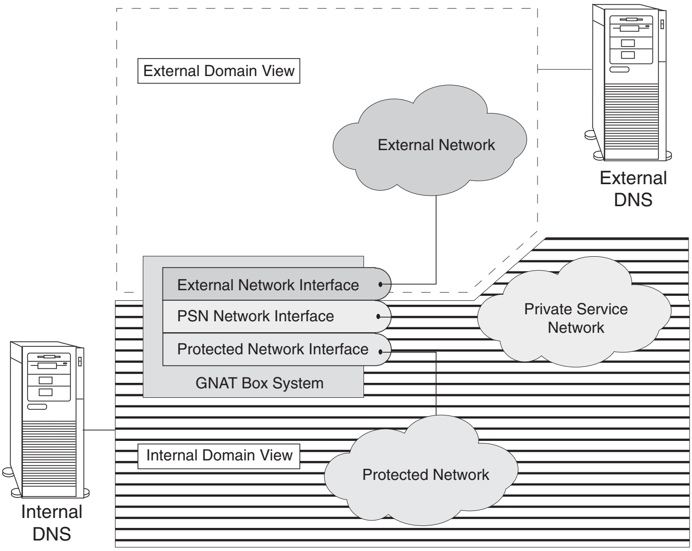
# DNS

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 DNS server on the external network for address resolution. However, the DNS server on the external network cannot be used by hosts on the external network to resolve protected hosts. NAT 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.

Before configuring DNS, you should understand how the domain name system functions. A good reference book on DNS is: **DNS AND BIND, 3RD EDITION** by Paul Albitz & Cricket Liu, published by O'Reilly and Associates.

## Built-in DNS Server

A built-in DNS server that can host multiple domains is available on most GTA Firewalls. The GNAT Box DNS server functions as a primary (not a secondary) Domain Name System server.



*Domain Name System (DNS)*

# Appendix E 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 explicitly allowed 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: allow access to DNS by traditional WWW proxy users.
Accept notice "PROTECTED" UDP coalesce(all) trafficShaping
<DEFAULT> weight 5 from ANY _ IP to ANY _ IP 53

2 #DEFAULT: Allow protected interface access to anywhere. Accept
notice "PROTECTED" ALL coalesce(all) trafficShaping <DEFAULT>
weight 5 from ANY _ IP to ANY _ IP

3 #DEFAULT: Block with alarm everything.
Deny warning ANY ALL alarm coalesce(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

# Index