GNAT Box®

The Simple,
Powerful,
Affordable

Firewall

User's Guide

Version 3.1

Global Technology Associates, Inc.

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 or 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 consitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

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

Trademarks
GNAT Box is a registered trademark of Global Technology Associates, Incorporated.
Netscape Navigator is a trademark of Netscape Communications Corporation.
Internet Explorer is a trademark of Microsoft Corporation.
WebSENSE is a trademark of Websense, Inc.
All other products are trademarks of their respective companies.

Document Information
GNAT Box Version 3.1.0 August 2000

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

Contact Information
Global Technology Associates, Inc.
3505 Lake Lynda Drive
Suite 109
Orlando, FL 32817 USA
Tel: +1.407.380.0220
Fax: +1.407.380.6080

Electronic Contact Information
GTA Email: info@gta.com
GTA WWW: http://www.gta.com
GNAT Box Email: gb-info@gta.com
GNAT Box WWW: http://www.gnatbox.com

1st Printing August 2000

Contents

Chapter 1: Introduction

Thank-you

Thank-you for purchasing a GNAT Box firewall system product. We hope that the firewall system will provide a simple, powerful and affordable solution for your IP network security, IP network address translation, and remote access requirements.

The GNAT Box firewall system is built around the concepts of simplicity, efficiency, and cost effectiveness. Although GNAT Box firewall system is small and simple, the technology behind the system is not; it's the technological outgrowth of GTA's GFX Internet Firewall System. Through a process of refinement and software innovations the GNAT Box system was born. Originally, the GNAT Box system was to be simply a Network Address Translation (NAT) system, hence the name GNAT (GTA's NAT). However as work progressed our software engineers realized that they could create a fully functional firewall system that was powerful, yet simple to install, configure, and operate.

Since its introduction in 1996 the GNAT Box firewall system has been a software only product that fit entirely on a single 3.5" floppy diskette. In order to provide more capabilities and added functionality to the GNAT Box system, GTA has begun to deliver the GNAT Box firewall system on flash memory based platforms. The flash memory based systems offer new capablities that are not found in the software only product due to space limitations of the 3.5" floppy diskette.

The flash based platforms include:

GB-Flash

The GNAT Box Firewall system on a flash module that installs in your Intel based hardware system.

GB-100 Firewall Appliance

A complete turn key small footprint firewall appliance with 3 built-in 10/100 ethernet interfaces.

GB-1000 Firewall Appliance

A complete turn-key firewall appliance in a 1 RU (1.75") 19" rackmount firewall appliance. The system features four high speed 10/100 ethernet interfaces.

The GNAT Box system is designed to provide:

- Secure IP network connectivity to an external network.
- Network address translation.
- IP pass through (no NAT).
- Virtual Private Networking (VPN)
- Remote access to user designated hosts and services.
- Transparent network access to external and private service networks for TCP, UDP, and ICMP based applications.
- Stateful IP filtering on both inbound and outbound packets.
- DHCP services via built-in DHCP server*
- Domain name sevices via built-in DNS server*
- Internet content filtering via built-in content filtering feature*
- Transparent network access for unusual application protocols such as: FTP, Archie, gopher, RealAudio/RealVideo, StreamWorks, VDOLive, CU-SeeMe, VXtreme, Vosaic, NTT AudioLink, NTT SoftwareVision and RTSP based applications such as Apple Quicktime streaming protocol.

About this Guide

This User's Guide shows you how to install and use the GNAT Box software. It also shows you some of the ways that GNAT Box can be used. This manual is organized to make it easy to use both as a tutorial and as a reference source. It is designed to anticipate the questions that you might ask when you use GNAT Box.

Chapter 1 is this introduction.
Chapter 2 defines terms and concepts.
Chapter 3 explains the hardware requirements.
Chapter 4 describes installation and configuration.
Chapter 5 examines the console user interface.
Chapter 6 explores the web browser interface.
Chapter 7 explains the GBAdmin Win95/NT interface.
Chapter 8 addresses troubleshooting.
Appendix A covers PPP chat scripting.
Appendix B describes the Advanced Configuration interface.
Appendix C provides a listing of common ports and services.
Appendix D lists configuration examples.
Appendix E describes the default filter settings.
Appendix F lists sample reports.
Appendix G is a reference for remote logging.

* Available only on flash based products

Documentation Conventions

The following conventions are used in this guide:

- Terms introduced and explained for the first time and variables are in *italic* type.
- Names of buttons, menu items, and settings have Initial Capitals.
- Text that you type is in bold **Courier** font.
- Text that appears on the screen is in Courier font.
- Name of keys on the keyboard are encased in angle brackets <Return>.

What You Need to Know

Before you begin, you need to know a few basic things:

- Information about network cards that will be used in the system.
- A basic understanding of TCP/IP networking.
- Network IP addresses for all network interfaces used on the GNAT Box.
- Netmasks for each attached network.
- Default route for your external network.
- What services you want to allow inbound (if any).
- What services you want to restrict outbound (if any).

What You Need to Have

The GNAT Box firewall software is a totally self-contained system. It does not run on top of any existing operating system; its integrated operating system is part of the firewall software. The GNAT Box system software requires a dedicated computer system meeting the hardware requirements listed in the table below.

The GNAT Box software is distributed on an ISO 9660 compliant CD-ROM. Since a CD-ROM is not a required component of the GNAT Box runtime system, you will need to have access to a system with a CD-ROM drive in order to create your GNAT Box runtime floppy disk. You can use a DOS, Windows, Windows 95, Windows NT, Macintosh or Unix system to create your runtime floppy disk, as long as the system can mount and read an ISO 9660 CD-ROM.

Requirements Summary

- A dedicated computer system for the GNAT Box runtime system.
- A computer system with a CD-ROM drive to create the GNAT Box runtime diskette.

GNAT Box Runtime Hardware Requirements

Qty	Description
1	Intel or compatible 486, Pentium family, AMD or Cyrix CPUs
1	16 Mbytes - 64 Mbytes RAM
1	1.44 Mbyte 3.5" floppy disk drive
2	Supported network interface cards
1	Basic VGA display adapter
1	Parallel printer port
1	CRT*
1	Keyboard**

* Not required for operation.

** Not required for operation if BIOS supports no keyboard.

Qty	Description
1	Supported network interface card for a Private Service network
1	Serial Port - COM 1-4 (1645x/1655x UARTs only)
1	Async modem for PPP connections or pager
1	ISDN TA with RS-232 interface for PPP connections

Copy Protection

The GNAT Box software is not copy protected directly, so you may make copies of the software for backup purposes. The software based GNAT Box system and GB-Flash system both employ a hardware key block, often called a "dongle," which attaches to a parallel port interface of the target GNAT Box system as a license protection device. If the key block is not attached or incorrectly attached to your GNAT Box system, it will not operate in a fully operational mode, but rather in a demonstration mode.

Many users initially have a strong dislike for hardware key block copy protection devices, for a variety of reasons. The use of a key block on the GNAT Box system, however, is quite different, because:

- The key block is only attached to the GNAT Box system, not to any client workstations.
- The GNAT Box system is a single function device. You can't run any other software on the target system, so it doesn't interfere with other applications.

- It provides a great deal of freedom to upgrade or to change system hardware by simply attaching the key block to the new equipment and booting the floppy diskette.

Activation Codes

The GNAT Box firewall appliance systems GB-100 and GB-1000 use activation codes to protect their software. Both appliances require a registration activation code in order the systems to be fully operational. This activation code is pre-installed on those systems when shipped. The registration activation code is also printed on the packaging and a post card. Please keep this code and your serial number in a safe location.

Feature Codes

Additional features that are available for the GNAT Box system require feature activation codes to unlock the feature and make it active. If you purchase an additional feature for your system you will be provided with a feature unlock code which is entered on the Features screen under the Basic Configuration menu from any user interface. Please keep your feature code in a safe location.

Quick Start

The flash based GNAT Box systems (GB-Flash, GB-100 and GB-1000) are all shipped with the runtime system pre-installed. All that is required is that the system be configured for your local network. Installation and configuration guides are provided separately for these systems.

If you have the software only GNAT Box system and you want to get started right away without reading the manual, then use the following procedure:

On a Windows (95,98,NT, 2000) based system run the GNAT Box installer. It will place the GNAT Box runtime images, remote admin client, utility software and documenation on your workstation. Additionally it will step you through creating the runtime floppy diskette used by your target GNAT Box system.

For other non-Windows OS systems use the following proceedure:

1. Format a 3.5” 1.44Mb floppy diskette.
2. Copy the GNAT Box runtime disk image to the floppy diskette. Use one of the GNAT Box utility programs or one of the other methods described in this guide.
2. Configure your network cards in the GNAT Box system with vendor supplied utility software, if required. Consult the hardware section for details.
3. Boot the floppy disk in your GNAT Box system.

4. The *Setup Wizard* will assist you to configure your GNAT Box system.
5. After configuration with the *Setup Wizard* , the GNAT Box system will continue booting up into full runtime operational mode.

Your GNAT Box system should be up and operational using the default configuration (all unsolicited inbound connections are blocked and all outbound connections are allowed). At this point you may use your web browser (must be frames capable) to access the GNAT Box and perform any additional configuration.

How to Get Technical Support

When you contact us, please have the following ready:

- User's Guide
- GNAT Box serial number
- Hardware information (network cards, CPU, memory)
- System Software Configuration Report
- Hardware Configuration Report

Please be sure that you have sent in your product registration card, either by post or email. Installation support is only available to registered users. Returning your product registration card is the only way that you can be informed of product upgrades and any other pertinent information.

We can be reached electronically at the following addresses:
`gb-support@gta.com` - GNAT Box support
`gb-info@gta.com` - General information

When you send electronic mail, please be sure to include your serial number, hardware description, and configuration information. Describe the problem as complete and precise as possible.

GNAT Box User's List and Forum

A good place to find out more about GNAT Box is to join the GNAT Box users discussion mailing list. This electronic mailing list provides a forum for GNAT Box users to exchange information, ideas, and make suggestions for future software enhancements.

To subscribe: send email to **majordomo@gta.com** and in the body of the email include the line:

```
subscribe gb-users your_email_addres
```

Example:

```
subscribe gb-users jsmith@foo.com
```

An web based GNAT Box user's forum is also available on the GNAT Box website, (http://www.gnatbox.com). To join the GNAT Box user's forum discussions simply register online at the forum home page.

Chapter 2: Terms & Concepts

Introduction

This chapter explains GNAT Box terms, concepts, and how the various system facilities operate. The terms and concepts defined in this chapter are used throughout this guide, so it is important to read this chapter carefully. Some terms and concepts used in this chapter may already be known to you. However, you should make yourself familiar with how these terms and concepts are used in context with the GNAT Box system, as the usage may be slightly different.

Overview

The GNAT Box system only supports IP protocols. Specifically, the IP protocols TCP, UDP and ICMP can be passed through the GNAT Box system in the NAT mode. Additionally the IP protocol GRE is also supported in the NAT mode when Microsoft's PPTP VPN tunneling protocol is authorized. Any IP protocol can be used in the IP Pass Through node (no NAT). This means protocols such as IPX/SPX, NetBEUI, and AppleTalk can be allowed to pass through the system, but only if NAT is not applied. Any IP protocol can be utilized with the built-in IPSec VPN, since it encapsulates and tunnels IP packets.

Terms

A basic unit of the TCP/IP protocol is the IP packet. GNAT Box 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 GNAT Box 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, GNAT Box does not touch the data portion of an IP packet (the packet payload). However, some application protocols embed IP addresses and ports in the data portion and often this information needs to be operated on in the course of network address translation. It is the ability to support such difficult application protocols that makes the GNAT Box network address translation facility so much more powerful than typical “blind NAT” schemes.

External Network

An *External network* is an unprotected network for which no network address translation is performed. An External network is typically connected to the Internet. However, GNAT Box can also be used internally on private networks as an intranet firewall. If connected to the Internet, an external interface must have a registered IP address. GNAT Box provides no security for hosts located on an

External network.

Protected Network

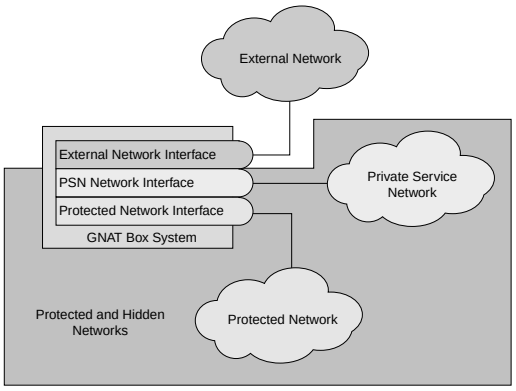
A *Protected network* is a network that is hidden behind the GNAT Box system. The term Protected network is used throughout this manual to refer to a network directly connected to the GNAT Box system. All features and attributes associated with this network also apply to all networks connected to a Protected network. All hosts and IP addresses used on this network are hidden from the External and Private Service networks. Hosts on a Protected Network are not by default accessible from an External network or a PSN network. The Tunnel facility can be used to allow external access to hosts and services on this network.

Private Service Network

A Private Service network (PSN) (often known as a DMZ network) is an optional service network that is located logically between an External network and a Protected network. A PSN isn't actually between a Protected and an External networks, but nearly at a peer level with a Protected network. However, a PSN is untrusted by a Protected network and by default no unsolicited packets are allowed to pass from a PSN to a Protected network. All hosts on a PSN are hidden from an External network, but completely accessible from a Protected network.

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

To create a PSN, add a third supported network card to your GNAT Box and configure it using the PSN network interface type. Since a PSN is hidden, unregistered IP addresses can be utilized.



The Standard GNAT Box System Diagram

Network Interface

A GNAT Box *network interface* (NIC) can be any supported network device operating at any supported speed and utilizing any supported network topography. The GNAT Box system can operate with a combination of different network cards, thus performing network bridging functions between dissimilar networks. GNAT Box requires at least two network interfaces (External & Protected) and supports a maximum of three network interfaces in the standard software release. Any additional network interfaces, more than the basic two, can be defined to be of any type. Thus is possible to have multiple External, Protected or PSN networks.

***Note**: GNAT Box can support up to twelve network interfaces when the optional multi-interface feature is purchased and enabled.*

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 GNAT Box system. Any supported network device can be used as an External Network Interface, (including PPP). More than one External Network Interface may be defined, however only one can be designated as the *Default Route*. An External network interface can have up to 300 IP addresses using *IP Aliasing.*

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 (RFC 1918 addresses are recommended). More than one Protected Network Interface may be defined. The IP Aliasing Facility may be used on a Protected network interface with a maximum of 300 IP aliases.

Private Service Network Interface

A *Private Service network* (PSN) interface is optional. Any supported network device may be used with the exception of the PPP device. However, if you plan to offer public access to servers, such as a web server, it is highly recommended that you install a PSN interface. For many configurations of the GNAT Box, a PSN may not be required, such as on intranets or for outbound access only. A PSN interface does not require a registered IP address (RFC 1918 addresses are recommended). More than one PSN Interface may be defined. The IP Aliasing facility may be used on a PSN interface with a maximum of 300 IP aliases.

Tunnels

A GNAT Box Tunnel is a facility that allows a host on the External or PSN network to be able to initiate a TCP, UDP or ICMP session with an otherwise inaccessible host (on the PSN or Protected networks) for a specific service. (A GNAT Box Tunnel should not be confused with a VPN tunnel, which provides secure gateway to gateway tunneling). This is done by mapping a visible IP address and port (service) to target IP address and port (service). This mapping can be performed for all services (host to host tunneling) or more typically for a given service. Common tunnels include: http (web), FTP, DNS, SQLnet, and telnet. Tunnels can be created to hosts on both the PSN and the Protected network. Only three types of tunnels can be created:

1. From an IP address (can be an IP alias)+port assigned to an External NIC to a host IP address+port on the Private Service network.
2. From an IP address (can be an IP alias)+port assigned to an External NIC to a host IP address+port on the Protected network.
3. From an IP address (can be an IP alias)+port assigned to a Private Service NIC to a host IP address+port on the Protected network.

Before a Tunnel can be accessed either a Remote Access Filter or Automatic Filter must be in place to allow access to the tunnel. Unless the "Hide Source"

option on a Tunnel definition is selected all IP packets will retain their original source IP address and source port number.

Caution: Tunneling to the Protected network can be a security risk, in the case where the Tunnel originates on the External network and the External network is the Internet. Great care should be taken when configuring servers which will be the target of such tunnels. The recommended and secure method of tunneling is to use a PSN.

Note: *A host on the source side of a Tunnel can only see the IP address on that side; the target IP address on the destination side of the Tunnel is always hidden.*

Network Address Translation (NAT)

Network Address Translation, or *NAT*, is one of the primary features of the GNAT Box system. The NAT facility used in the GNAT Box system is always active by default. NAT is applied to outbound packets only:

1. Outbound packets from the Protected Network to the External network.
2. Outbound packets from the Protected Network to the PSN.
3. Outbound packets from the PSN to the External network.

The NAT facility can be bypassed via the IP Pass Through facility, if desired. NAT is available in two forms: *dynamic translation* and *static translation*.

Default NAT

The default NAT form 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 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.

Static Address Mapping

The other form of NAT available is a static translation method, referred to in the GNAT Box system as *Mapping* or *static address mapping*. The Static Address Mapping facility allows the GNAT Box administrator to specify a static mapping address scheme, such that a given address, network or subnet is mapped to a specific IP alias assigned to a specific network interface. Since the default dynamic NAT will translate IP address to the real IP address of the NIC by default, Mapping is only useful if you have assigned an alias(es) to the target NIC.

Static Maps are assigned by associating a source address(es) to an alias assigned to a particular network interface (PSN or External). A netmask (not to be confused with the assigned network netmask) is ANDed with the specified source IP address to yield an IP number that is used for comparisons when applying static mapping.

IP Pass Through

IP Pass Through is essentially the GNAT Box term for "no network address translation." By default, all packets passing through the GNAT Box outbound (to destinations that lie beyond the External or the PSN network interfaces) have NAT applied to them. The IP Pass Through facility provides a means to override the default action of applying NAT and to transfer packets through the GNAT Box without having NAT applied to specific packets. The system creates IP Pass Through tunnels, which are determined by user designated originating IP addresses. These designated IP addresses can be networks, subnets or individual hosts on either a PSN or a Protected networks.

IP Pass Through can be selectively applied to packets based on the destination of the packets. The IP Pass Through facility allows the user to specify which network interface(s) will not have NAT applied for a designated IP address(es). For example, it is possible to apply IP Pass Through for specified packets destined to a host external to a PSN NIC, while packets for a host external to an External NIC still have NAT applied.

The IP Pass Through facility can be defined to operate in the following configurations:

1. For packets from a host(s) on a Protected network outbound through PSN and External NICs.
2. For packets from a host(s) on a Protected network outbound through a PSN NIC only.
3. For packets from a host(s) on a Protected network outbound through an

External NIC only.

4. For packets from a host(s) on a PSN network outbound through an External NIC only.

By default, IP Pass Through designated IP addresses are configured for outbound use only. This default configuration disallows unsolicited inbound connections. Stateful information is maintained about IP Pass Though 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 inbound connections.

IP Pass Through designated IP addresses can also be configured to allow arbitrary external inbound connections to be initiated, if desired. When configured to allow such inbound connections, IP Pass Through filters need to be created to control inbound access.

IP Pass Through and NAT can operate at the same time. However, a clear understanding of TCP/IP networking is a must, since these types of configurations can become complex and difficult to understand. Unlike the NAT configuration which only supports TCP, UDP and ICMP, IP Pass Through will support any defined IP protocol.

Network Transparency

Network Transparency is a term used to describe the GNAT Box functionality that allows host systems residing on hidden-protected networks (PSN and Protected networks) to send packets and receive replies to/from hosts on external networks in a seemingly transparent manner. Network Transparency is implemented as a part of the GNAT Box stateful packet inspection facility. The state of all connections is maintained by the system in a series of tables, along with other connection information that will insure that only authorized packets are accepted. Network Transparency allows GNAT Box to operate without the need to create permanent holes in the firewall as required by typical IP filtering systems.

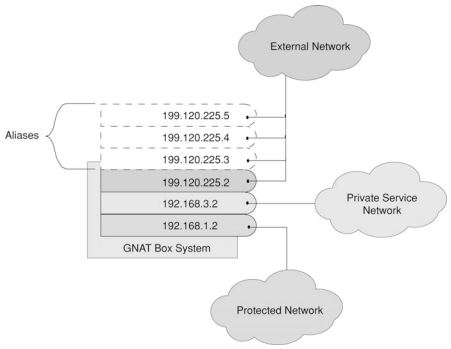
Traditional IP filtering firewalls require that holes be created in the firewall to allow packets to be accepted for arbitrary inbound connections. Since many application protocols create arbitrary secondary inbound connections, additional holes must be created to accept the wide range of possibilities.

Virtual Cracks

The GNAT Box system avoids this security problem through the use of *virtual cracks*. A virtual crack is part of the GNAT Box 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 GNAT Box 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 or timers expire due to inactivity or when the expected protocol event does not occur (i.e. client crash). Some application protocols which use secondary connections and thus virtual cracks, include: FTP, RealAudio, StreamWorks, CU-SeeMe, Net2Phone, Battlenet, and many of the MS Windows NetBIOS facilities.

IP Aliasing

An *IP Alias* is the GNAT Box 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 Tunnel facility (e.g. multiple web servers). This release supports 300 aliases, which can be applied to any network interface.



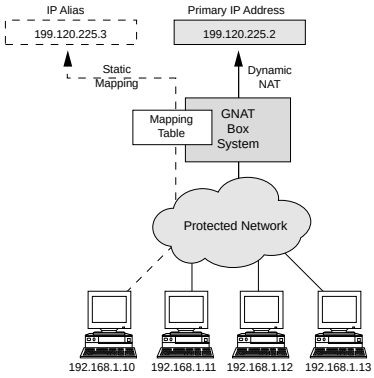
Example of IP Aliases assigned to an External NIC

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.

Static Address Mapping

Static Address Mapping is a GNAT Box facility that allows an internal IP address or subnet to be statically mapped to an external IP address during the network

address translation process. Typically, mapping is used with targets on an External network interface. Mapping is not useful unless IP aliases have been assigned to the target network interface, since by default all IP addresses on a Protected network are dynamically assigned to the real IP address of the outbound network interface. This release supports 300 static outbound maps.



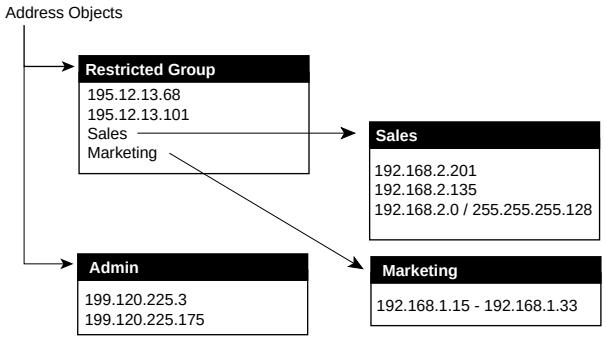
Static Address Mapping Illustration

Address Objects

Address Objects are logical groupings of IP addresses. These Address Objects can be used in various GNAT Box configuration facilities to specify IP Addresses. Traditionally an IP Address+Netmask pair are used in these facilities. The use of Address Objects greatly simplfies the creation of a GNAT Box configuration.

Address Object Rules

1. Each Address Object must have a unique name.
2. An Address Object can have up to 10 members.
3. A maximum of 300 Address Objects are allowed.
4. An Address Object member can be any of the following:
   - A single IP Address
   - A range of IP addresses
   - A subnet
   - An Address Object
5. Any member addition or deletion to an Address Object will be realized anywhere the object is utilized in the GNAT Box configuration.
6. Once an Address Object is created its name should not be changed lightly. Any use of an Address Object whose name is changed will be nullified; since the GNAT Box facilities reference objects by name.



Address Object Example

Filters

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

Basic GNAT Box Filter Concepts

1. Filter order is important, because IP packets are processed against the filter sets sequentially. Therefore, it is very important to arrange your filters in the proper order, otherwise you may not achieve the desired result.
2. Filters are boolean in nature; they can only accept or deny a packet.
3. Outbound Filters control access to IP addresses that reside external to an External network interface from hosts on Protected and PSN networks.
4. Outbound Filters control access to IP addresses that reside external to a PSN network interface from hosts on a Protected network.
5. Remote Access Filters control access for packets that are directed at one of the IP addresses assigned to any GNAT Box network interface.
6. A Remote Access filter must be in place before a Tunnel can be accessed.
7. IP Pass Through filters control access both inbound and outbound to IP Pass Through designated IP addresses, networks, subnets or hosts.
8. IP Pass Through filters support all IP protocols. Remote Access and Outbound filters support only the IP protocols: TCP, UDP and ICMP.
9. Each type of filter set may have up to 400 filters.

Each packet is compared to the appropriate filter set (Remote Access, Outbound or IP Pass Through) starting at filter number one in a specific set. A comparison is performed sequentially against each filter until one of two events occurs:

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

Comparison Parameters

All types of filters (Remote Access, Outbound, and IP Pass Through) use the same filter definition specifications and comparison parameters. The parameters used to perform the filter comparison are:

Source IP Address

The Source IP Address can be specified as an IP address or an Address Object. In the case of the Source IP Address, the IP address is used in conjunction with the Source Netmask to yield an IP number for comparison to the source IP address in the packet being filtered. The Source Netmask is logically ANDed with an IP packet's source address. The result is then compared to the masked Source IP Address parameter. In the case of an Address Object a similar comparison performed for all the elements contained in the Address Object.

Source Netmask

The source netmask used for filter definitions should not be confused with the "network netmask" as they have no relation whatsoever. The source netmask used in a filter definition in conjunction with a Source IP Address and is used in a logical AND operation to yield a set of host IP addresses for comparisons. Specifying a netmask of 255.255.255.255 (all ones) when ANDed with an IP address will yield only that specific address. A netmask specification of 255.255.255.0 will yield a set of 255 addresses. The source netmask is not used when an Address Object is selected for the Source IP Address.

Source Port

The source port can be: a single port, multiple ports or a range of ports. The specified Source Port(s) are compared to the source port of the IP packet to see if a match exist. If no Source Port is specified, any source port is accepted. Typically, the source port for most client protocols is a random value above 1024.

Destination IP Address

The Destination IP Address can be specified as an IP address or an Address Object. In the case of the Destination IP Address, the IP address is used in conjunction with the Destination Netmask to yield an IP number for comparisons to the destination IP address in the packet being filtered. The Destination Netmask is logically ANDed with an IP packet's destination address. The result is then compared to the masked Destination IP Address parameter. In the case of an Address Object a similar comparison performed for all the elements contained in the Address Object.

Destination Netmask

The destination netmask used for filter definitions should not be confused with the "network netmask" as they have no relation whatsoever. The destination netmask is used in a filter definition in conjunction with the Destination IP Address it is used in a logical AND operation to yield a set of host IP addresses for comparison. Specifying a netmask of 255.255.255.255 (all ones) when ANDed with an IP address will yield only that specific address. A netmask specification of 255.255.255.0 will yield a set of 255 addresses. The destination netmask is not used when an Address Object is selected for the Destination IP Address.

Destination Port

The destination port can be: a single port, multiple ports or a range of ports. The specified Destination Port(s) are compared to the destination port of the IP packet to see if a match exists. If no Destination Port is specified, any destination port is accepted. Destination ports are often called services since certain well known services have been assigned dedicated port numbers. Historically, well know services, typically those provided by servers, were defined to be ports in the range from 1 to 1024. However, with the explosive growth of the Internet, this limited range of ports has been exhausted and new services have ports assigned outside this range. A list of common services can be found in Appendix C. An extensive list of services can be found on the GNAT Box web site and on the GNAT Box CD-ROM.

Network Interface

The network interface parameter allows a filter specification to define which network interface the packet must have arrived at in order to be matched. The valid values for the network interface are: "**ANY"** - (Any network interface) and any interface that appears in the interface list, (defined by the user on the

Network Information screen).

Protocol

This parameter allows for the specification of a particular IP protocol to be matched. The valid values for protocol are: **TCP**, **UDP**, **ICMP**, **ALL** and any protocol a user may add to the user specified protocol list. If ALL protocols are specified then no ports (source or destination) may be specified. In the case of NAT any protocol other than (TCP, UDP, ICMP) can only be used with a DENY filter since GNAT Box only supports and routes only TCP, UDP and ICMP. The current use of user specified protocols is to suppress noisy benign protocols (which are implicitly blocked) from filling up log files. This function is accomplished by creating a Deny filter with the “nolog” option selected.

In the case of IP Pass Through any IP protocol added to the Protocol list will be usable for by ACCEPT and DENY filters.

Filter Actions

Filter Actions are not a filter parameter for comparisons; they are actions to be executed if the associated filter is matched. Filter Actions are:

Alarm

If this item is enabled an alarm event will be generated when the filter is matched. Each alarm event increments the alarm count by one. If the alarm threshold is reached within the specified time period an email alarm notification will be sent to the designated email address defined on the Email Server tab. The email message will document all the alarm events that contributed to the alarm notification. Multiple email messages will be sent, if the number of alarm events exceed the maximum alarm count parameter defined in this section.

Optionally, if the pager option is configured, a pager message can be generated when the alarm threshold is reached.

Email

An email message is generated which includes information about the IP packet which matched the filter, a timestamp of the event, and DNS name resolution (if a DNS server has been defined to the GNAT Box and the IP address can be resolved) and is sent to the email address defined in the email preferences section, typically the firewall administrator. If multiple hits on the filter occur within a short span of time, all packets will be detailed in a single email message. The maximum number of events that will be recorded in a single email message

is the same value set for Alarms.

Stop Interface
This action should be used with extreme caution. If the associated filter is matched, the network interface on which the packet arrived will be shut down. No further packets will be received or allowed to be sent out the interface in question. User intervention is required to bring the interface back up. This can be accomplished in two ways: a system reboot or via the Interfaces dialog on either the Command Console User Interface or the web browser user interface.

Pager
This filter action requires that an optional modem be attached to one of the supported serial interfaces (COM 1-4). This modem must be dedicated to the pager function. The modem may be either external or an internal modem card. Only numeric pagers are supported. Because pager systems can vary from country to country there is no guarantee that the pager function will operate in all countries.

If the associated filter is matched and the optional pager facility has been enabled and configured (via the preference dialog), then the defined numeric pager message will be sent by calling the defined telephone number via the pager modem.

SNMP Trap
This filter action will generate a generic SNMP trap and send it to a SNMP management station, if the associated filter is matched. The SNMP option must be enabled (via the preference dialog) for this action to operate. The SNMP management station is defined on the SNMP option dialog screen.

Generate ICMP
This filter action will generate a "service unavailable" ICMP message to the source IP address of the matched packet for the associated filter.

Filter Action Notes
1. Filter actions are not mutually exclusive. You may select none, one or all of the actions on a give filter.
2. It is important to understand clearly what each filter action does, since some actions can be rather severe, i.e. Stop Interface.
3. Filter actions can be selected on both Accept and Deny filters.

Filter Listings

Whenever filters are referenced or listed in a report they will appear in the following format:

```
Index_number  Filter_description
Accept|Deny NIC Proto [log|nolog][filter_actions][timeBased]
  from src_IP_Address/src_netmask port1...port_n
    to dest_IP_address/dest_netmask port1...port_n
       [timeGroup group_name]
actions:=[alarm|email|stopIface|pager|snmp|genICMP]
```

Default Filter Sets

When the GNAT Box is initially configured (or whenever you press the “Default” button on any filter set screen), a set of default filters are generated (for the specific area) based on a predefined security policy and configured preferences. See Appendix E for a discussion of the default security policy and the default filter sets.

Automatic Filters

Automatic Filters have no user configuration facilities. These filters are generated by the system and are transient. An example of automatic filter is the filters created when the Email Proxy is enabled, which allows the GNAT Box system to accept replies from the designated mail server. The only Automatic Filter that is user initiated are those created when
the "Automatic accept all filter" option is enabled on a Tunnel definition. When a configuration report is generated any Automatic Filters currently enabled will be listed.

Remote Access Filters

Remote Access Filters control the access of packets that are directed at an IP address assigned (including IP aliases) to any of the network interfaces on the GNAT Box system. Remote Access Filters are primarily used to control access to Tunnels, since the source side of a tunnel is always an IP address assigned to a GNAT Box network interface (EXT or PSN types). Remember, a Tunnel is only a conduit that associates a Protocol, an IP address assigned to a GNAT Box NIC, and a port number to an internal IP address (on a PSN or a Protected network) and port number. The Remote Access filter is the facility which accepts or denies access to the Tunnel.

Remote Access filters also process packets destined for services on the GNAT Box, such as the web browser user interface and proxy services (email and URL

blocking), if enabled. This release supports 400 Remote Access Filters.

Outbound Filters

Outbound Filters control access of packets directed to IP addresses on an External network (typically the Internet) and to a PSN (if one exists). As mentioned previously, the implicit filter rule is "that which is not expressly permitted is denied" applies to outbound packets as well as inbound packets. When the GNAT Box is initially configured, default Outbound filters will be created. The default Outbound filter allows all IP addresses on a Protected network to access any IP address and any service external to a Protected network. If a PSN network interface exists, an Outbound filter will be created that allows all access to the External network(s) (typically the Internet) from a PSN. These filters can be modified or deleted to suit the local network security policy for external network access.

To allow only specific external services to be accessed, simply remove the default Outbound filter(s) and add filters for the allowed services. Any packet destined for a service not matching the allowed services will be rejected by the implicit rule. This release supports 400 Outbound Filters.

Outbound Filter Example

1. All users are allowed to access world wide web services.
2. All users are allowed to access RealAudio services.
3. All users are allowed to perform DNS lookups.
4. SMTP is only allowed to be sent from the mail server.
5. All other outbound services are denied.
6. Log any attempts to access FTP servers.

Outbound Filter Set

```
1. Allow all user access to WWW and RealAudio
Accept PRO TCP
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0 80 7070

2. Allow mail server to send email outbound.
Accept PRO TCP
192.168.1.50/255.255.255.255
0.0.0.0/0.0.0.0 25

3. Allow DNS lookups
```

```
Accept PRO UDP
0.0.0.0/0.0.0.0 53
0.0.0.0/0.0.0.0 53

4. Log any attempt to access a FTP server.
Deny PRO TCP log
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0 21
```

IP Pass Through Filters

IP Pass Through Filters control access to and from IP addresses that have been specified as IP Pass Through addresses. IP Pass Through filters, although similar to the other two filter types (Remote Access and Outbound), are a bit different since they control both inbound and outbound access to/from the designated IP Pass Through addresses. Since IP Pass Through addresses are not translated, the GNAT Box functions as a gateway for these addresses. Therefore, the IP Pass Through Filters utilize IP Pass Through addresses in the filter definitions not GNAT Box NIC addresses.

If IP Pass Through host/networks are defined, pressing the “Default” button on the IP Pass Through filter screen will create a set of filters based on the IP Pass Through addresses defined. Since IP Pass Through host/networks can be defined in a variety of different combinations, the default filters will vary according to options selected. These generated filters are quite general and should be modified to match your security requirements. This release supports 400 IP Pass Through filters.

Time Groups

Time Groups are user defined time schedules, that can be associated with any type of filter. Time Groups provide the firewall administrator with the ability to control access (both inbound or outbound) based on the time of day and day of the week. A filter that has an associated Time Group will only be in effect during the defined time period. The time granularity is based on 10 minute increments. Time Groups can provide a great deal of flexibility, especially when multiple filters are involved. This release supports 100 Time Groups.

1. All normal filter functions apply, and a filter may be an Accept or a Deny.
2. Often negative logic can be used to exclude and may be your best filter solution.
3. 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.

Time Groups Example

1. Allow users access to Internet Relay Chat only after normal working hours.
2. Allow access to a public FTP server on a PSN after 19:00 hrs on weekdays.
3. Deny all outbound services except email during the weekend.

```
Weekend      Sat 00:00-23:50, Sun 00:00-23:50
Workday      Mon-Fri 08:00-18:00
No FTP Time  Mon-Sun 0800-19:00
```

Outbound Filters

```
1. Deny IRC during working hours
Deny Pro TCP
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0 111 timeGroup Workday

2.  Block everything on the weekend except email
Deny Pro TCP
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0 25 timeGroup Weekend

3. Allow access to all services.
Accept Pro ALL
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0
```

Remote Access Filters

```
1. Deny FTP during the daytime
Deny Ext TCP
0.0.0.0/0.0.0.0
199.120.225.2/255.255.255.255 21 timeGroup No_FTP_Time
```

Note: *All Remote Access filters are not listed in this example, only the Time Group examples.*

VPN

GNAT Box is provided with a built-in Internet Engineer Task Force (IETF) IP Security (IPSec) standard VPN facility. Since the GNAT Box 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. The remote gateway can be another GNAT Box system or another compatible security gateway. The GNAT Box VPN provides support for any IP protocol to be pass 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 implicit rule also applies to VPN tunnels; "that which is not explicitily 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. For a complete discussion of the GNAT Box VPN see chapter 9 in this user's guide.

DNS

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

Built-in DNS Server

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

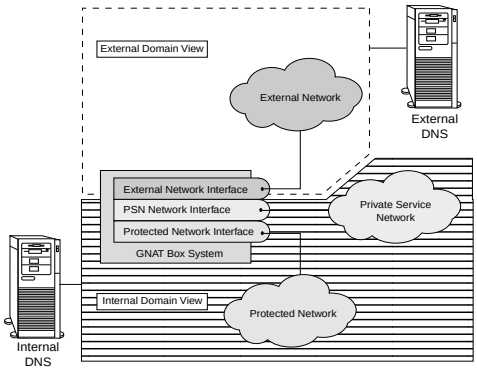
DNS & Small Networks

Small networks typically neither have nor require a dedicated internal DNS server. An external DNS server (often located at your ISP) can be used for address resolution on an External network (typically the Internet). If some internal hosts need to be referenced by name (for TCP/IP services), the use of a local "host file" on client systems may be utilized. The host file name and location varies depending upon the operating system. Host file loca-

tions for some common systems are:

Windows95/NT - /Windows/Hosts
Macintosh - System Folder/Mac TCP DNR
Unix/Linux - /etc/hosts

Note: *Sample host files are typically provided with the above mentioned operating systems.*



DNS Domains Illustration

DNS & Larger Networks

If DNS is used for IP address resolution for internal hosts, a split DNS scheme should be used with the GNAT Box system. That is, a DNS server can operate on a Protected network serving DNS information for and about a Protected network. Hosts on a Protected network should reference the internal DNS server, as it will provide address resolution for external as well as internal hosts. Information about hosts on a PSN may also be provided by this DNS server for use by hosts on a Protected network (hosts on a PSN would not have access to this server unless you created a tunnel to a Protected network from a PSN on port 53/UDP). A separate DNS server should be used to provide DNS information for users on an External network (the Internet). This external DNS server can reside anywhere that is accessible by external users. This DNS server can be located at your Internet Service Provider, on an external host (in the case of an Intranet) or often on the PSN with Tunnels on port 53 for both TCP and UDP.

A Dual DNS Configuration Scheme

Often a split DNS scheme is desired, but the resources for two DNS servers may not be available. It is possible to operate two separate DNS servers on the same host by being a little creative. As most DNS servers run on hosts using Unix or a Unix like system (Linux) this scheme only addresses a Unix configuration.
The objective is to configure a Unix system located on a PSN network to provide DNS services about your domain for users on the external network (Internet) and DNS services for your internal users (located on Protected and PSN networks).

Example Internal DNS Server Configuration

1. Configure the Unix host on the PSN as a normal DNS server. Configure the DNS information using your hidden/unregistered IP addresses. Your internal domain will most likely include at least two sets of networks (IP addresses from a Protected network as well as from a PSN). The DNS server typically will contain information for hosts on a PSN such as web and FTP servers (using their unregistered IP addresses).

2. Have your internal users reference the Unix host on a PSN as their DNS server. This server will resolve all local addresses and external addresses. Remember, if an external address needs to be resolved and that information does not reside in the DNS servers cache, a lookup on an external network (the Internet) will be performed transparently.

Example External DNS Server Configuration

1. Create a new directory for the external DNS server.
   For example: /etc/namedb2

2. In the new directory, create your DNS domain and reverse lookup files. Only registered IP addresses should appear in these files. The IP addresses for email, web, FTP and DNS servers will either be an External NIC IP address or aliases assigned to an External NIC (assuming you have created tunnels for these services).

3. In the /etc directory, create an additional DNS boot file (/etc/named.boot2) for your external DNS server. This file should be created as a normal “named.boot” file yet reference files in the external DNS directory (/etc/namedb2).

4. In the appropriate “rc” file, add an additional entry to start-up a second

copy of the DNS server (typically called "named"). This second copy of the DNS server should be invoked with a port parameter of 54 (-p 54) and an alternative boot file name (-f /etc/namd.boot2).

5. Create two tunnels on the GNAT Box for the external DNS server: one for DNS lookups (UDP/53) and one for zone transfers by a secondary DNS server (TCP/53). These tunnels should have the source side of the tunnel set for port 53 and the destination set for port 54.

6. Create Remote Access filters which will allow the tunnels to be accessed by the appropriate users.

Example Configuration

```
GNAT Box
EXT: 199.120.225.2
PRO: 192.168.2.2
PSN: 192.168.3.2
DNS Server  192.168.3.20

Tunnels
UDP 199.120.225.2 53  192.168.3.20 54
TCP 199.120.225.2 53  192.168.3.20 54

Remote Access Filters
1. Allow DNS lookups from the Internet
Accept UDP EXT
From: 0.0.0.0/0.0.0.0 53
To: 199.120.225.2/255.255.255.255 53

2. Allow DNS zone transfers by our secondary
Accept TCP EXT
From: 204.96.116.2/255.255.255.255
To: 199.120.225.2/255.255.255.255 53
```

In the above configuration example, the domain's name server would be listed as 199.20.225.2 and users from the Internet would access this IP address to reference DNS information about the domain. Internal users would reference 192.168.3.20 as their DNS server.

What Does GNAT Box Do?

Firewalling - It prevents unauthorized access to Protected and Private Service networks, while allowing authorized outbound connections to operate transparently. It acts as a choke point to control outbound access and it protects against denial of service and spoofing attacks.

A network address translation (NAT) system. Unregistered IP addresses may be used on the Protected and the PSN networks. All IP addresses are hidden from the External network and are translated to the primary IP address of the external network interface.

Powerful - It supports up to 32,768 concurrent sessions.

Flexible - It can be configured for a variety of network scenarios and supports many popular nonstandard application protocols, such as streaming, audio/video, multimedia.

Network Bridge - It can function as a link between different network topographies (e.g. 10Mbps to gigabit) and replace a router in the case of the PPP configuration.

VPN - It can provide a Virtual Private Network between two networks using the IPSec VPN standards.

DNS - GNAT Box has a built-in DNS server. (Only available on GB-Flash, GB-100 and GB-1000 systems).

DHCP - GNAT Box has a built-in DHCP server. (Only available on GB-Flash, GB-100 and GB-1000 systems).

We believe that you shouldn't have to pay for security features that you will probably not use or need. GNAT Box was developed to provide a powerful, simple, and affordable IP network security solution to organizations that would otherwise be forced to purchase an expensive solution or do without IP security altogether. This release of the GNAT Box software does not directly support:

- Remote user authentication.

Note: *The GNAT Box does support many third party VPN products transparently, such as Microsoft Corporation's PPTP and Data Fellows SSH (http://www.datafellows.com) and many other third party IPSec VPN implementations.*

What Doesn't GNAT Box Do?

The GNAT Box system is **NOT** a general purpose computer system. It is dedicated to network security, therefore:

- You can't log on to it (there is no user shell), except for the console interface for configuration purposes.
- You can't telnet to it.
- You can't use it for a mail server.
- You can't use it for a web server.
- You can't run any other applications on it.

How Does GNAT Box Work?

The GNAT Box system is **Not** a Unix system, although it uses core technology from the BSD Unix operating system.

At the heart of GNAT Box is GTA's network address translation and stateful packet inspection engine. This facility was originally developed and used in GTA's turnkey, dual-wall GFX Internet Firewall System. The stateful packet inspection facility monitors every IP packet passing through the GNAT Box to guarantee that:

- Network address translation is performed for all packets passing through the GNAT Box system outbound (unless overridden by the IP Pass Through facility).
- Only valid response packets or packets passing through user defined tunnels are allowed to reach hosts on the Protected or PSN networks from the External network.

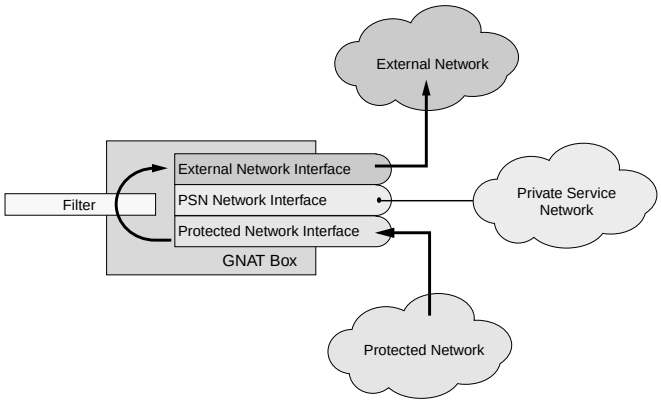
The NAT and stateful packet inspection facilities are tightly integrated into the GNAT Box's network layer to guarantee maximum data throughput.

Eight GNAT Box Concepts

The following section describes and illustrates basic concepts of the GNAT Box system operation.

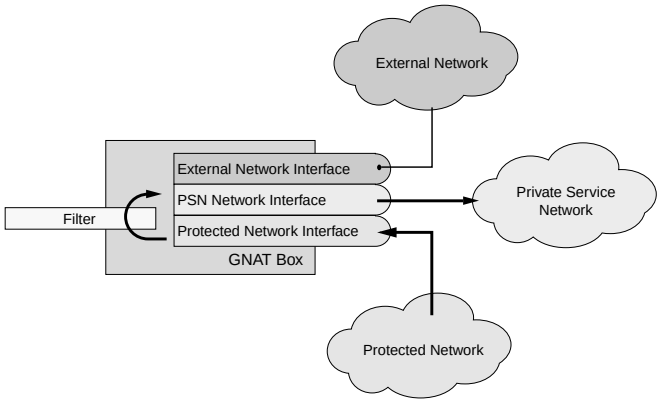
Concept 1

Outbound packets originating from a Protected network pass transparently through the GNAT Box to an External network and return. Network address translation is performed on the packet header (and its payload if required) resulting in the source IP address of an External network interface. A new source port is also assigned.



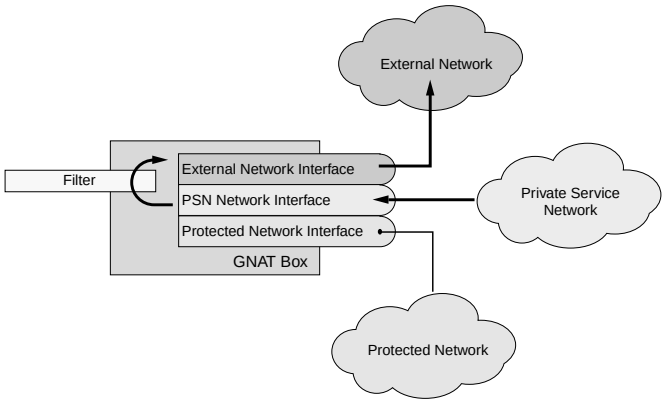
Concept 2

Outbound packets originating from a Protected network can pass transparently through the GNAT Box to a PSN and return. Network address translation is performed on the packet header (and its payload if required) resulting in the source IP address of a PSN network interface. A new source port is also assigned.



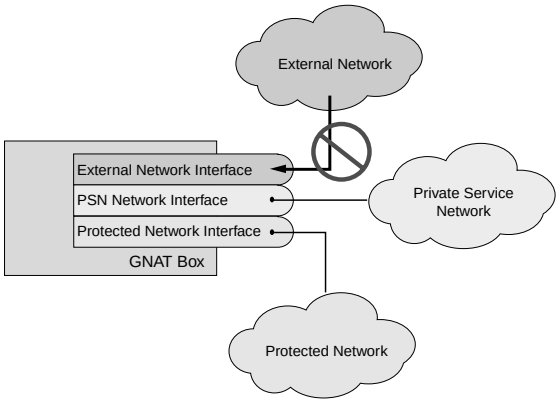
Concept 3

Outbound packets originating from a PSN can pass transparently through the GNAT Box to an External network and return. Network address translation is performed on the packet header (and its payload if required) resulting in the source IP address of an External network interface. A new source port is also assigned.



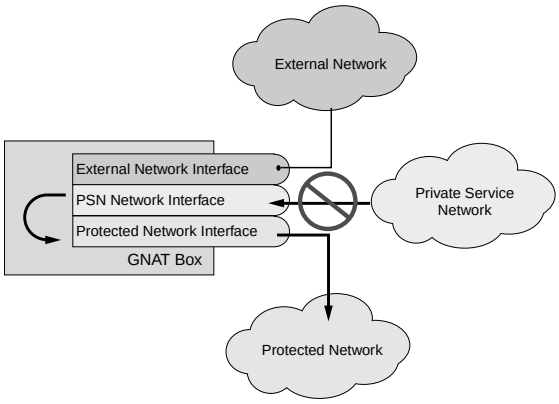
Concept 4

Unsolicited packets arriving on an External network interface are blocked. The event is logged with detailed information about the attempt to the GNAT Box console and log host, if one is defined. An alarm notification (via email, SNMP Trap, or pager) is sent to the designated administrator if the alarm facility is enabled.



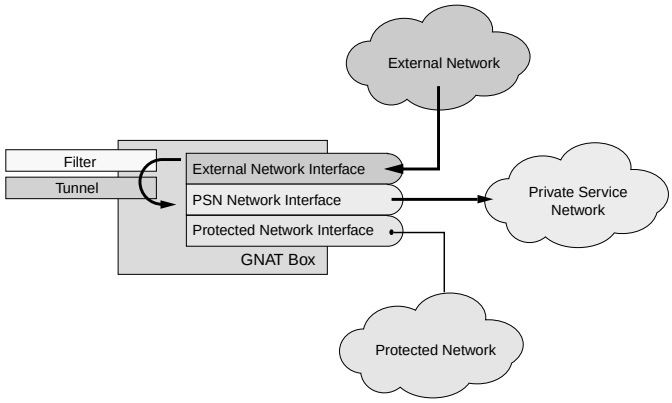
Concept 5

Unsolicited packets arriving on a PSN network interface, destined for a Protected network, are blocked. The event is logged with detailed information about the attempt to the GNAT Box console and log host, if one is defined. An alarm notification (email, SNMP Trap, or pager) is sent to the designated administrator if the alarm facility is enabled.



Concept 6

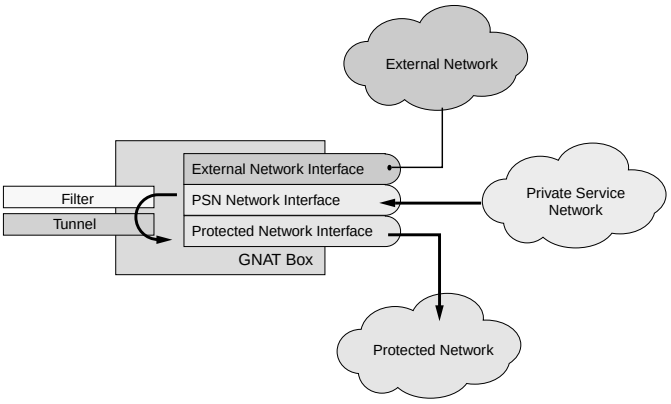
Packets originating from an External network may be directed to an IP address/ Port combination on a PSN when an appropriate GNAT Box Tunnel and Remote Access Filter are in place. If NAT logging is enabled, the event is logged with detailed information about the opened connection. When the connection is closed, the event is logged with summary information about data transfers (if enabled).



Concept 7

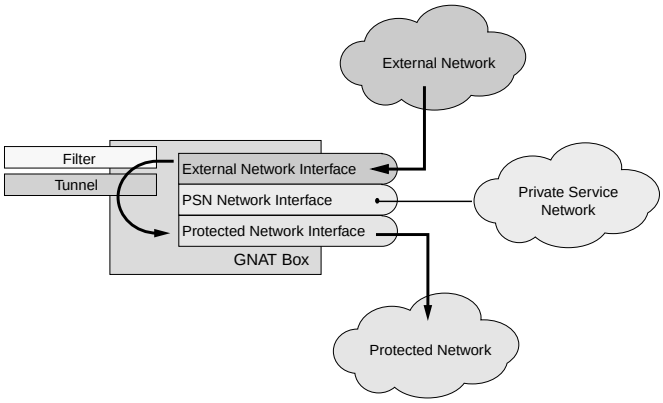
Packets originating from a PSN may be directed to an IP address/Port combination on a Protected network, when an appropriate GNAT Box Tunnel and Remote Access Filter are in place. If NAT logging is enabled, the event is logged with detailed information about the opened connection. When the connection is closed, the event is logged with summary information about data transfers (if

enabled).



Concept 8

Packets originating from an External network may be directed to an IP address/ Port combination on a Protected network, when an appropriate GNAT Box Tunnel and Remote Access Filter are in place. If NAT logging is enabled, the event is logged with detailed information about the opened connection. When the connection is closed, the event is logged with summary information about data transfers (if enabled).



Outbound Packets from a Protected Network

When an IP packet arrives on a GNAT Box Protected network interface, and the packet is destined for an IP address that resides external to an External or a PSN NIC and the packet did not originate from an IP Pass Through host/network, it is considered to be an outbound packet. Outbound packets are processed

against the Outbound Filter set. If the packet is accepted by an Outbound filter, the system determines where the packet should be sent and performs the necessary modifications and processing on the packet (i.e. network address translation, special application modification), if required.

If the packet originates from an IP Pass Through host/network, then IP Pass Through filters are applied to the packet. If the packet is accepted, a check is made to determine which interface the packet will be sent out and if IP Pass Through has been enabled for the interface. If IP Pass Through is not in enabled for the exit interface, then the packet falls into the NAT processing cycle.

If the packet has NAT applied to it, a check is made to determine if the default dynamic NAT should be applied or if a static mapping is defined for the packet. The system then routes the packet to the correct network interface.

Information about the packet (original packet configuration, state information, special processing, etc.) is maintained for all active connections. Network transparency and virtual cracks are configured and activated, if required.

Packets that are directed at a Protected network interface are not considered outbound packets, since they are directed to an IP address that resides on a Protected network. These packets are discussed in the section Inbound Packets from a Protected Network Interface.

Outbound Packets from a Private Service Network

Outbound packets from a Private Service network follow the same processing as packets from a Protected network, except outbound packets can only have a destination IP address that is external to an External NIC.
Packets that are directed at a PSN network interface are not considered outbound packets, since the IP address is on the same network. This packet processing is discussed in the section titled Inbound Packets from a PSN.

Inbound Packets from the External Network

In its default configuration, the GNAT Box system does not listen for any unsolicited inbound packets. It only responds to reply packets (those packets which are returning in response to packets that originated from a Protected or PSN) and secondary connection packets processed through the use of virtual cracks.

When a response packet returns to the GNAT Box, the packet is inspected to determine if the packet is in fact a response on an active transparency circuit. If

the packet is accepted, it is then modified with the originating reply IP address and routed to the appropriate network. If the packet is a secondary connection, it is accepted via a virtual crack and processed according to information stored when the initial connection was established. Since response packets and secondary connections are handled by the GNAT Box network transparency and virtual crack technology, no filters are involved in processing these packets.

Unsolicited packets are always directed to an IP address assigned to the network interface. If a Tunnel is in place for the target IP address+port on the External network interface, the packet is passed to the Remote Access filter processing. If the packet is accepted by a Remote Access filter, its destination IP address is modified to that of the destination IP address of the specific tunnel definition. The packet is then directed out through the appropriate NIC to the destination IP address of the Tunnel.

Inbound Packets from a PSN Network

Packets that are destined for IP Pass Through hosts are processed a bit differently, since no network address translation is applied to these packets. If an IP Pass Through host is allowed to receive inbound connections, then the GNAT Box system functions only as a filtering gateway. The packets that are directed to the External network interface are packets that are to be forwarded to the target IP Pass Through host on either a PSN or a Protected network. If the packet is a response packet, it is processed in the same manner as described above, except the packet is not modified in any way. If the packet is unsolicited, it is processed against the IP Pass Through filter set. If the packet is accepted by a filter, it is directed out the appropriate network interface to the target IP Pass Through host.

Inbound Packets from A PSN Network

Packets that are sent to a PSN network interface are either directed to a Tunnel (in which the **only** case can be a destination on a Protected network), or a service running on the GNAT Box (Web browser or RMC user interfaces). By default, the Web browser or the RMC user interfaces are not enabled for a PSN network interface. Remote Access filters must be explicitly configured to allow these types of connections.

Packets arriving on a PSN network interface for a Tunnel are processed by the Remote Access filter set. If the packet is accepted by a filter and a Tunnel is in place, the packet's destination IP address is modified to reflect the destination IP address defined by the Tunnel. The packet is then routed out a Protected network interface to the target host.

Inbound Packets from a Protected Network

Packets inbound to the GNAT Box from a Protected Network interface will be either for the Web browser interface or the URL blocking proxy. The packet cannot be for a Tunnel, since Tunnels are not allowed on a Protected network interface. In either case, the packet is processed against the Remote Access filter set. If the packet is accepted, it is then passed to the appropriate service: Web browser interface or URL blocking proxy.

How Tunnels Work

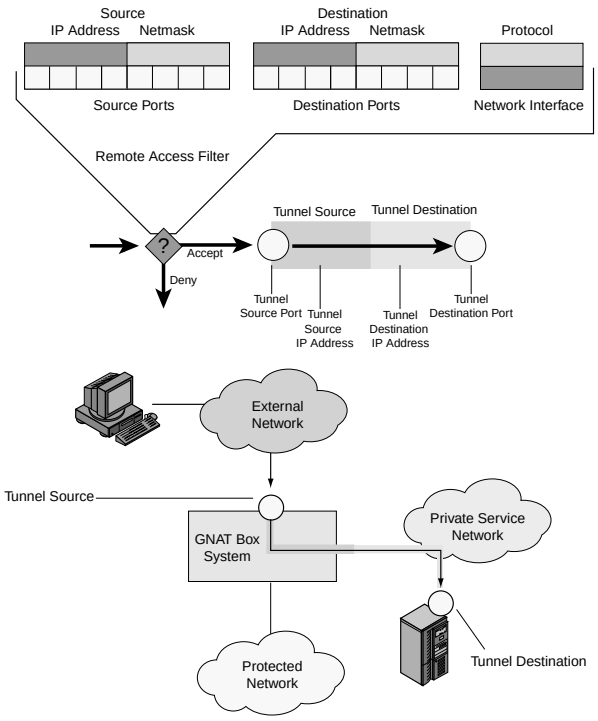
It is important to remember three key points when working with Tunnels.

1. Tunnels are only used for inbound unsolicited connections.
2. Reply packets and outbound packets do not use the Tunnel facility.
3. Hosts on the Protected network should not access Tunnels (although it is allowed), since all target IP addresses of Tunnels are directly accessible to these hosts.

Tunnels can **only** be created for the following configurations:

1. From an IP address assigned to an External network interface to a port (service) on a host on a Private Service network.
2. From an IP address assigned to an External network interface to a port (service) on a host on a Protected network.
3. From an IP address assigned to a Private Service network interface to a port (service) on a host on a Protected network.

When an inbound, non-response IP packet arrives at one of the GNAT Box's network interfaces (External or PSN types) and the Remote Access Filter rules allow the packet, it is compared against the defined set of Tunnels. If the destination IP address and port match the source side of a Tunnel, then a new connection is created. This new connection will have the destination address and port of all packets arriving on this connection automatically changed to the values of the destination side of the Tunnel. Additionally, all response packets originating from the Tunnel's destination host will have the source address and port changed back to the Tunnel's source values as the packets are transmitted back to the originating host.



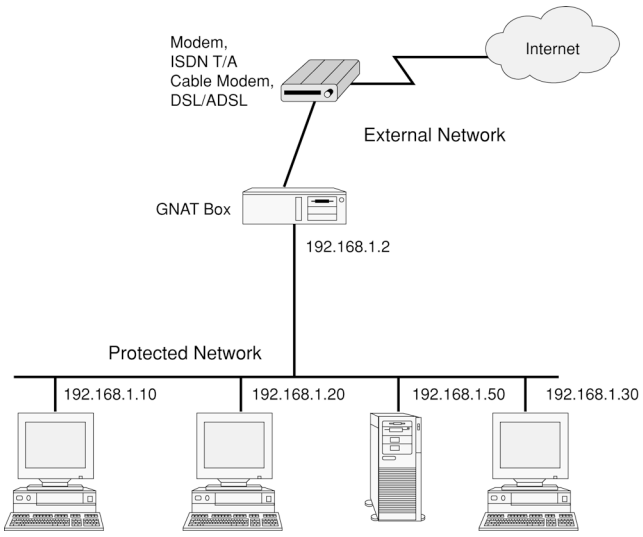
Tunnels are only the conduit portion of an inbound connection. Every defined Tunnel requires at least one Remote Access Filter that permits use of the Tunnel. A Tunnel will not be usable, unless a Remote Access Filter is in place.

The two network illustrations in this section represent sample GNAT Box network configurations that are used throughout this guide in examples and illustrations. The first example is a typical GNAT Box configuration with the addition of a remote network attached via a WAN on the Protected network.

1. Gateway (default route) for hosts on the 192.168.1.0 network is 192.168.1.2.
2. Gateway (default route) for hosts on the 192.168.2.0 network is 192.168.2.2.
3. Gateway (default route) for hosts on the 192.168.3.0 network is 192.168.3.2.
4. Default route for the GNAT Box is 199.120.225.1.
5. A static route installed on the GNAT Box for the remote network 192.168.2.0 is 192.168.1.254.

The second network configuration represents a GNAT Box network that utilizes a PPP, cable modem, or xDSL external network connection.

GNAT Box PPP/Cable/xDLS Configuration



1. Gateway (default route) for hosts on the 192.168.1.0 network is 192.168.1.2.
2. The default route for the GNAT Box is not specified if the connection is a PPP dialup.
3. The default route for the GNAT Box typically is dynamically assigned (via DHCP) for cable modems and xDSL installations.

Chapter 3: Hardware

System Requirements

The hardware requirements are few. It is best to have only the required components installed in the system. Devices such as SCSI controllers, sound cards and IDE hard disks, etc., only tend to confuse the initialization software. It is best to leave these unused devices out of the system.

Required System Hardware Components

Qty	Description
1	Intel or compatible 486, Pentium family, AMD or Cyrix CPUs
1	16 - 64 Mbytes RAM (32 Mb typical)
1	1.44 Mbyte 3.5” floppy disk drive
2	Supported network cards
1	Basic VGA display adapter
1	Parallel printer port
1	IDE controller (GB-Flash only)
1	CRT*
1	Keyboard**

* Not required for operation.

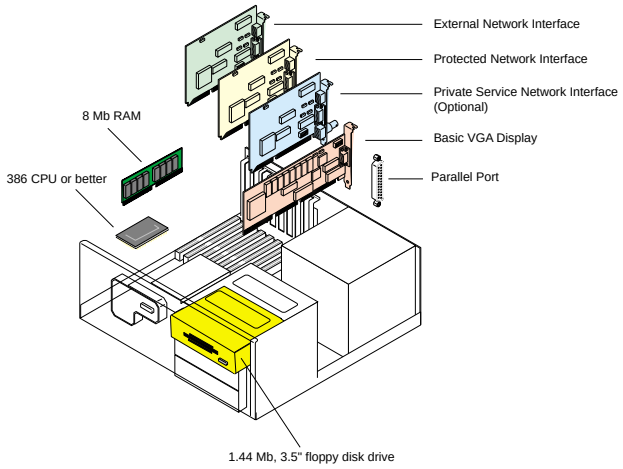
** Not required for operation if BIOS supports no keyboard.

Optional System Hardware Components

Qty	Description
10	Additional network interface cards***
1	Serial Port - COM 1-4 (1645x/1655x UARTs only)
1	Async modem for PPP connections
1	ISDN TA with RS-232 interface for PPP connections

*** Multi-interface software option supports up to 12 NICs

The following tables list network interface cards supported by the GNAT Box. Cards that are not explicitly listed may be supported; check the chipset family listing to see if your network card’s chipset is listed. If so, it is most likely supported.



Supported Network Interface Cards

10Mbps Ethernet Cards

Description	NIC Name
3Com 3c509 Etherlink	ep
3Com 3c900, 3c900B EtherLink XL PCI	xl
3Com 3c589c/3c589d Etherlink III PCMCIA	zp
Compaq NetFlex-3/P card and Integrated	tl
Compaq NetFlex 3/P with BNC	tl
Compaq Nettelligent 10 T/2 PCI UTP/Coax	tl
DEC EtherWORKS II (DE200, DE201, DE202, DE422)	le
DEC EtherWORKS III (DE203, DE204, DE205)	le
IBM Ethernet II PCMCIA (NS chipset)	ze
Intel EtherExpress PRO/10+ (PCI only)	fxp
Kingston Technology EtheRx KNE40x	de
Novell NE-2000, NE-2100 and compatibles	ed
Olicom OC-2183/2185	tl
Olicom OC-2325	tl
SMC Etherpower Series (SMC 9332)	de
SMC Etherpower2 (SMC 8432, 8434)	de
SMC Elite Ultra	de
SMC 8416 EtherEZ series	ed
Most PCMCIA Ethernet cards using the NS chipset	ze

10/100 Mbps Ethernet Cards

Description	NIC Name
3Com 3c595 EtherLink XL PCI	vx
3Com 3c905 and 3c905B	xl
3Com 3c980-TX	xl
3Com 3cSOHO100-TX	xl
Accton ENI1203	de
Allied Telesys AT 2500	rl
ASUS PCI-L101-TB	de
Cogent EM960PCI	de
Compex CPXPCI/32C	de
Compaq Netellignet 10/100	tl
Compaq Netellignet 10/100 Proliant	tl
Compaq Netelligent 10/100 Embedded UTP	tl
Compaq Netelligent 10/100 TX PCI UTP	tl
Compaq Netellignet Dual 10/100 TX PCI UTP	tl
Compaq Netellignet 10/100 TX PCI Intel UTP	fxp
Compaq NC3121 Fast Ethernet NIC	fxp
Compaq NC3122 Dual Port Fast Ethernet NIC	fxp
Dell Optiplex GX1 on-board 3c918	xl
Dell Precision on-board 3c905B	xl
Dell Latitude laptop docking station embedded	xl
D-Link DE-530	de
D-Link DFE-500TX	de
Danpex EN-9400P3	de
DC Communications 100TX	rl
DEC DE500-AA	de
DEC DC435	de
Encore 832-TX 10/100 M PC	rl
Genius GF100TX (RT8139)	rl
Intel EtherExpress PRO/100B, PRO/100+	fxp
Intel EtherExpress	fxp
JCIS Condor JC1260	de
Kingston KNE100TX	de
KTX-9130TX 10/100 Fast Ethernet	rl
Linksys EtherPCI	de
Lite-O 82c168/82c169	pn
Lonshine CS-8038TX-R	rl

Description	NIC Name
Macronix 98713, 98715, and 98725 based cards	mx
Mylex LNP101	de
Olicom OC-2326 10/100 TX UTP	tl
Ovisink F-8129TX,F-8139TX	rl
SMC EtherPower 10/100 (9332, 9334)	de
SMC EtherPower 10/100 (SMC 9432)	tx
Tektronix nc. A-1210 ethernet 10/100	rl
Zynx ZX314	de
Zynx ZX342	de
Gigabit Ethernet Cards	
Alteon AceNIC V	ti
3Com 3c985-SX	ti
Netgear GA620	ti
FDDI Cards	
DEC DEFPA PCI FDDI (SAS & DAS MMF, SAS UTP)	fpa
Cards Known Not Compatible	
Cogent EM110-TX-PCI	
Intel EtherExpress ISA based cards	
Intel EtherExpress PRO/10+ (ISA based cards)	

The following table lists most chipset families that are supported by GNAT Box. Some network interface cards that utilize a supported chipset may not actually be supported, due to implementation and/or design issues with the card.

Chipset Families

ax

ASIX Electronics AX88140A fast ethernet controller chip

ASIX Electronics AX88141 fast ethernet controller chip

de

DEC 21040 controller chip

DEC 21041 controller chip

DEC 21140 fast ethernet controller chip

DEC 21141 fast ethernet controller chip

DEC 21142 fast ethernet controller chip

DEC 21143 fast ethernet controller chip

fxp
Intel i82557 fast ethernet controller chip
Intel i82558 fast ethernet controller chip
mx
Macronix 98713 fast ethernet controller chip
Macronix 98713A fast ethernet controller chip
Macronix 98715 fast ethernet controller chip
Macronix 98715A fast ethernet controller chip
Macronix 98725 fast ethernet controller chip
pn
Lite-On 82c168 PNIC fast ethernet controller chip
Lite-On 82c169 PNIC fast ethernet controller chip
rl
RealTek 8129 fast ethernet controller chip
RealTek 8139 fast ethernet controller chip
Texas Instruments ThunderLAN ethernet controller chip
tx
SMC83c170 EPIC chip
vr
VIA Technologies VT3043 Rhine I fast ethernet controller
VIA Technologies VT86C100A Rhine II fast ethernet
wb
Winbond W89C840F fast ethernet controller chip
xl
3Com boomerang bus-master Etherlink XL chip
3Com cyclone bus-master Etherlink XL chip

Network Card Configuration

1. Prior to use in a GNAT Box system, each network interface card should be configured with the network card vendors configuration software. Very often, the vendors software has an automatic configuration option that will set IRQs, I/O ports, and memory addresses to values that will not conflict with other devices installed in the system.

2. The suggested method of network interface configuration is to perform the configuration on the actual GNAT Box system with all network interface cards installed that will be used in the run time system. Cards configured in another system and then installed in the GNAT Box run time system may be incorrectly configured and may conflict with other devices.

3. A simple method to configure network interface cards in the run time GNAT Box system is as follows:
   3.1 Create a bootable DOS diskette.
   3.2 Install all the network interface cards in the GNAT Box run time system.
   3.3 Boot DOS from the bootable diskette.
   3.4 With the system up and running under DOS, remove the DOS boot diskette and insert the network interface card vendor's configuration diskette.
   3.5 Run the network interface card vendor's configuration/diagnostic program and configure your network cards. Do this for each different card in the system.

4. Once the network interface cards have been configured, the GNAT Box system software should be able to use the configuration. Items such as media type, speed, etc. can be overridden on the GNAT Box Network Information configuration area.

5. Some network interface cards that offer an "auto sense" option need to be set to a specific value (e.g.. UTP, AUI, BNC). If you are unsure, watch the boot messages on the GNAT Box console for any warning messages about a particular network interface card and its configuration. Generally the warning messages provide enough information for a user to easily understand and correct the problem.

Ethernet Card Notes

Network interfaces are addressed by their two or three character device identifier and a positional number starting at zero. The first card of a specific type identified by the system will have a positional identifier of zero (e.g. de0). If a second card of the same type as the first is found, it will have a positional identifier of one (e.g. de1) and a third card will have a positional identifier of two (e.g. de2). Each new type of card identified in the system will begin with a base identifier of zero. This naming scheme does not apply to cards that must be configured to specific values listed below.

ISA Cards

1. Network cards do not have to be of identical make and/or manufacturer.
2. Configure the network cards using the configuration programs supplied with the network cards. It is very important that you configure the cards correctly, otherwise you may have problems later. Remember to:

- Turn off plug and play.
- Configure the interface type (UTP, BNC, etc,)
- Use the listed IRQ, PORT and memory address (if required).

3. ISA cards must be configured to operate in the 16 bit mode.

PCI Cards

PCI cards are self configuring and do not need to be configured. However, some older PCI motherboards require that the IRQ's used on the PCI bus be allocated and enabled in the BIOS setup. Some early PCI motherboards have problematic PCI bus implementations.

NE-2000 and Compatibles

1. The card must be a 16 bit card and operate in the 16 bit mode.
2. The card must be configured to one of the configurations in the table below and must not conflict with any other card. Cards will be mapped to the associated device name listed in the configuration section below. For example, if you only have one NE-2000 or compatible card and select I/O 320h with IRQ 11, that card will be addressed as device "ed2," even though you may not have a ed0-ed1.

Note: *PCI based cards that emulate the NE-2000 generally have no external method to configure the card, since they rely on "plug and play." Since the GNAT Box does not support "plug and play," these cards tend to get assigned device names that begin after the official device list ends. So cards of this type will appear beginning at device "ed5". The same behavior is exhibited by on-board NE-2000 ethernet interfaces.*

Card	Device	I/O	IRQ
1st	ed0	280h	10
2nd	ed1	300h	5
3rd	ed2	320h	11
4th	ed3	340h	12
5th	ed4	360h	15

1. The card must be a 16 bit card and operate in the 16 bit mode.
2. The card must be configured to one of the following configurations and must not conflict with any other card. Cards will be mapped to the associated device name listed in the configuration section below.

DEC EtherWorks3 & Compatibles

Card	Device	I/O Port	IRQ	IOMEM
1st	le0	300h	5	D0000
2nd	le1	280h	10	D0800
3rd	le2	320h	11	D1000
4th	le3	340h	15	D1800

3Com 3c509

Boot DOS and run the 3Com utility software, 3C5X9CFG.EXE

Remember to:

- Disable plug and play.
- Configure each card using the "auto configuration" option

3Com Etherlink III PCMCIA Card (3c589)

Configure the cards under DOS using the settings in the table below.

Card	Device	I/O	IRQ	IOMEM
1st	zp0	0x300	10	0xD8000
2nd	zp1	0x280	5	0xD0000

PPP Hardware Requirements

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

Supported PPP Hardware

- Any external asynchronous modem. COM ports 1-4 are supported and only COM ports based on the 1645x/1655x UARTs are supported.
- Any internal asynchronous modem. Only modems that use 1645x/1655x compliant UARTs are supported.
- Any ISDN external modem/terminal adapter. COM ports 1-4 are supported. Only COM ports based on the 1645x/1655x compliant UARTs are supported.

Serial Ports

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

Modem/ISDN TA Configuration

It is best to configure the modem or ISDN TA on some other system prior to installing it on the GNAT Box system. Most modems allow for the storage of a user configuration and the recall of this configuration using a specific command (i.e. ATZ). The Dial Script data entry field can be used to configure the modem, but it is generally best to be able to recall a configuration and set the modem to a known state with a few commands.

Note: *The default configuration for most modern modems generally should work without problems.*

It's probably best to configure the modem to use a fixed DTE speed (the speed at which the computer talks to the modem, not the speed at which the modem communicates with another modem). If the modem supports high DTE speeds such as 38400 and 57600, use one of these values to insure the highest throughput. Make sure that you configure your serial port to the highest possible speed when using an ISDN TA. Unless you expressly wish to connect to the remote modem at a specific speed, set your DCE speed (speed at which the modem talks to the remote modem) to auto negotiate any speed.

Cable Modems and xDSL Configurations

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

Memory Requirements

The GNAT Box system can operate with a memory size as small as 16 megabytes. However, you should consider certain factors when selecting a memory configuration for your GNAT Box system. The table below list the maximum concurrent sessions possible for a given memory configuration.

Memory and Concurrent Connections

RAM	Concurrent Connections
16	16,384
24	24,576
32	32,768
64	32,768

Other factors that should be considered when selecting a memory configuration

are: if the URL blocking and or email proxy facility will be utilized 32 Mb is recommended when utilizing these features on a heavily loaded network. If you are running a GB-Flash based system and utilizing the additional features (DNS Server, DHCP server and content filtering) then 64MB of RAM is required.

Hardware Selection and Performance

The GNAT Box system is designed to be very efficient and to operate on a broad spectrum of hardware configurations. The hardware you select will have an impact on the GNAT Box system's performance, due to the system architecture. This is especially true when the GNAT Box is used in an Intranet configuration with full network speeds on all interfaces. The best possible performance can be obtained by using a Pentium CPU with PCI based network cards. Most organizations with low speed (56Kb or less) Internet connections will find that 486 ISA based systems will perform quite well.

Performance of the GNAT Box is generally not an issue for most organizations connected to the Internet. The bottle neck usually occurs at the WAN connection to the Internet, where 56K or T-1 connectivity is common. The GNAT Box can easily provide enough throughput with 10Mbps ethernet cards for network connectivity up to T-1 speeds (1.5 Mbps). When the WAN connectivity is a T-3 or faster, it is recommended that 100Mbps or FDDI network cards be utilized in the GNAT Box.

If your GNAT Box PCI system is performing poorly, randomly crashing or exhibiting unusual behavior check your motherboard and IRQ assignments. Make sure any unused devices, such as IDE and SCSI controllers, sound cards and serial ports are disabled. You should also run the hardware configuration report and scan it for any warning or error messages. Often the cause of the problem is indicated in this report.

Since the GNAT Box performs a network role, selection of network interface cards is important. Although the GNAT Box supports a wide variety of network interface cards, some perform better than others. Cards based on the RealTek and the VIA Rhine chipsets tend to have poor performance when compared to other PCI based implementations, although cards based on these chipsets perform better than ISA based cards. Cards based on these chipsets should be avoided if performance is a concern.

It should be noted that even if the selected hardware operated correctly under another operating system, it doesn't necessarily mean that it will operate cor-

rectly with the GNAT Box system. The GNAT Box system has its own drivers and operating system and tends to push the hardware beyond what most desktop operating systems can achieve.

Note: *Beware of mother boards with early PCI implementations. Many of the early PCI based systems had problematic BIOS and/or PCI chipsets. These systems tend to be older 486 and early Pentium (50-100 Mhz) based PCI systems. If you are using such a motherboard and your system is not operating correctly or randomly crashing, you should replace the motherboard.*

Chapter 4: Installation & Configuration

Installation

In keeping with the basic GNAT Box philosophy of "keep it simple," installation and configuration is not complex. But some knowledge of IP networking is required to understand the implications of GNAT Box integration into your network.

Prior to installation you should have the following:

- The required GNAT Box system hardware (configured).
- A computer system that will be used to create the GNAT Box boot/ runtime diskette (DOS/Win/Win95, Unix or Mac).
- Network address information.
- IP address and netmask for the External network interface.
- IP address and netmask for the Protected network interface.
- IP address and netmask for the PSN interface (optional).
- IP address of the default route (to the Internet).
- IP address of a DNS server (optional).
- IP address of your mail server (optional).
- PPP dialup information (phone number, passwords, PAP/CHAP information, etc.), if PPP will be used.
- Configured network interface cards and/or modem/ISDN TA per the instructions in the hardware section of this guide.

Software Installation

Software installation consists of three parts:

1. Installation of GNAT Box runtime diskette image and utility software on your workstation's hard disk.
2. Creation of the GNAT Box runtime diskette.
3. Configuration of your GNAT Box system.

The GNAT Box system can be configured from a variety of operating system platforms: Unix, Win95/NT, Win3.x, DOS and Macintosh. The tools and methods for configuration vary depending upon the OS platform. The Windows95/98/NT environment has some additional configuration tools not available under other OS platforms. However, installation and configuration is rather simple on any supported platform.

Although the GNAT Box software is supplied on CD-ROM, the system actually

boots and runs off a 3.5" floppy diskette and requires the creation of a GNAT Box runtime system diskette (not performed on your runtime system). The CD-ROM is a hybrid/ISO 9660 format disc and should be readable by most modern operating systems (DOS/Win, Unix and Macintosh). If you cannot read the CD-ROM, please contact technical support and the software will be supplied in an alternate format.

***Note**: If you have obtained the GNAT Box software via the Internet, simply skip the references to the CD-ROM and begin following the procedure after the software has been extracted from the CD-ROM. If you received the GNAT Box software on diskette then there is nothing to do, as the diskette is ready to run. However, you may want to make a backup of the runtime diskette using one of the GNAT Box utilities (GBadmin.exe, GBREAD.EXE, GBUTIL.EXE, etc.).*

Windows 95/98/NT Installation

The following sections describe the installation and configuration procedure for various OS platforms. Find the section for your workstation platform and follow the instructions.

1. Insert the CD-ROM into your CD drive, the installer will startup automatically.
2. If the installer doesn't "autostart" then double click on the "My Computer" icon to open it.
3. Double click on the GNAT Box CD icon to open it.
4. Double click the Install icon, which will launch the installer application.

The installation process will offer you a choice of software packages to install; from a complete install of all GNAT Box software to only copying the GNAT Box runtime diskette image to your hard disk. At a minimum, select the GNAT Box runtime and the GBAdmin program. A complete installation would include the GNAT Box runtime, GBAdmin, the remote logging client, on-line manual, and sample files.

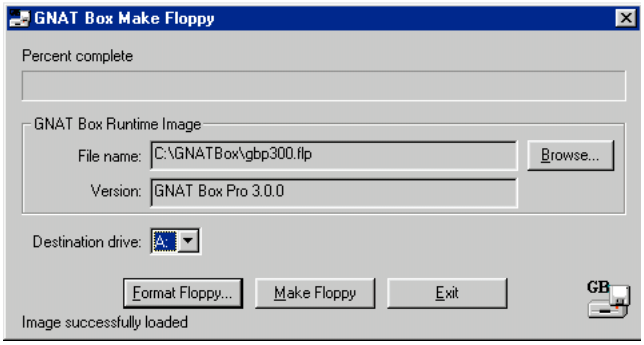
The installation process provides you with an option to create a GNAT Box runtime diskette after the installation process is complete. Choosing this option insures that you will have a bootable runtime system diskette. You may also choose to run gbMakeFloppy and/or GBAdmin after the installation process completes and create a runtime diskette with these applications.

gbMakeFloppy

The **gbMakeFloppy** utility provides a convient method for making runtime floppy

diskette images. The program is installed under the GNAT Box group in the Start menu.

If you wish to make a clean unconfigured runtime diskette, simply click the **gbMakeFloppy** menu item or the program icon. The menu item installed in the Start menu is pre-loaded with a specific GNAT Box runtime diskette image (Pro, Demo or Light). Launching the program from the Start menu will load the specified runtime image automatically into **gbMakeFloppy**. The runtime image version information is displayed in the Version field.

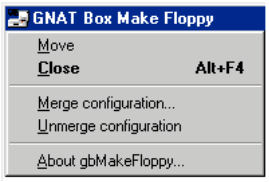


To make a runtime diskette:

1. Insert a 3.5” 1.44Mb diskette into your floppy drive.
2. Select the destination drive from the “Destination Drive” pull down choice list.
3. If the diskette is not formatted use the “Format Floppy...” button to format the diskette.
4. After the diskette is formatted, click the “Make Floppy” button to copy the runtime image to your diskette. A progress bar at the top of the application window will display the percentage of data copied.
5. When the data copy has completed you may remove the diskette and insert it into your target GNAT Box system.
6. Boot the diskette and use the Setup Wizard to perform the initial configuration of your system.
7. Once the system is up and running use either a web browser or GBAdmin to adjust the system configuration for your site. See chapters 6 and 7 for the operation of these user interfaces.

Merging Configuration Data

You can also use gbMakeFloppy to merge a previous GNAT Box configuration with a runtime image, (check the release notes for which previous system versions are readable by the current runtime system). Clicking the icon in upper left hand corner of the titlebar will display a menu. Select the "Merge configuration" menu item, then select the GNAT Box configuration file you wish to merge.



The file should only contain GNAT Box configuration data, not a complete runtime diskette image. You configuration data will then be merged with the runtime image. Clicking "Make a Floppy" will create a runtime diskette with the runtime and specified configuration data.

Note: *Use the "Save As..." file menu in **GBAdmin** and only select "Configuration data" in the "Data to Save" section to generate a file that only has configuration data.*

GBAdmin

The **GBAdmin** utility provides many functions from diskette creation, to complete system configuration, validation and remote system management. The procedure in the following section describes simply how to create a bootable unconfigured GNAT Box floppy diskette using GBAdmin. Complete configuration using GBAdmin is described later in this guide. Please see chapter 7 for a complete reference to the GBAdmin software.

Windows 3.x Installation

1. Insert the CD-ROM into your CD drive.
2. Double click on the GNAT Box CD icon to open it.
3. Open the Win3.x folder and double click the Install icon. This will launch the installer application for Windows 3.x/Windows for Workgroup.

The installation process will offer you a choice of software packages to install; from a complete install of all GNAT Box software to only copying the GNAT Box runtime diskette image to your hard disk. At a minimum, select the GNAT Box runtime and the **GBUtil** program. A complete installation for a Windows 3.x system would include the GNAT Box runtime, **GBUtil**, the command line utility

programs, and sample files.

***Note**: Before starting the installation process you should format a 3.5" 1.44Mb floppy diskette and have it available for the installation process.*

GBUtil

You may use the Windows 3.x application **GBUTIL.EXE** program to copy the runtime diskette image (GBPnnn.FLP where nnn is the version number) to a formatted floppy diskette.

GBWRITE

You may also choose to use the command line program **GBWRITE.EXE**, which will copy the runtime diskette image to your formatted floppy diskette. The **GBWRITE.EXE** program will prompt you for the target diskette drive letter and the name of the GNAT Box runtime diskette image file.

DOS Installation

1. Insert the CD-ROM into your CD drive.
2. Change directory on the CD-ROM to the DOS directory.
3. Make a directory on your hard disk called GNATBOX
4. Copy the contents of the DOS directory on the CDROM to the GNATBOX directory on your hard disk.

Use the command line program **GBWRITE.EXE**, which will copy the runtime diskette image to your formatted floppy diskette. The **GBWRITE.EXE** program will prompt you for the target diskette drive letter and the name of the GNAT Box runtime diskette image file.

Example: `GBWRITE A GBP220.FLP`

Unix/Linux Installation

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

Use the following procedure:

1. Create a directory where you want to install the GNAT Box software.

2. Format a 3.5" 1.44Mb diskette.
3. Mount the GNAT Box CD-ROM as a ISO 9660 filesystem (e.g. SunOS mount -r -t hsfs /dev/sr0 /cdrom).
4. Change directory to the Unix directory on the CD-ROM (e.g. cd /cdrom/unix).
5. Copy the contents of the Unix directory to the directory you created on your Unix system.
6. Insert the formatted floppy diskette into your Unix system.
7. Use the Unix "**dd**" command to copy the GNAT Box runtime image to the floppy diskette.

Examples:

Write a GNAT Box diskette:

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

Read a GNAT Box diskette:

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

Read only the configuration data from a diskette:

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

Write only the configuration data from to diskette:

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

Note: *these examples are for FreeBSD your raw floppy diskette device may have a different name.*

Macintosh Installation

The GNAT Box CD-ROM is a hybrid ISO 9660/Mac CD-ROM. Macintosh users should have no problem mounting the disc. This release does not include utilities to read/write the GNAT Box runtime image to floppy disk, but a GNAT Box boot/runtime disk image has been provided in the runtime folder. This file is provided as an image file in Apple Disk Copy format. Although the image file cannot be mounted with Apple Disk Copy, a floppy diskette can be created using the image file. Disk Copy is available from the Apple software update site at: http://swupdates.info.apple.com.

Another alternative to Disk Copy is to use the shareware program "DiskDup+". This program can be used to write the GNAT Box runtime disk image to a formatted (DOS formatted) floppy diskette. DiskDup+ only recognizes it's own

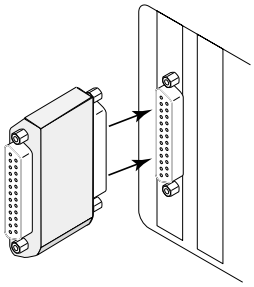
file format. You will need to use a filetyper utility to change the diskette image file type and creator. Use the following settings:

```
Type: DDim  Creator: DDp+
```

Once you have created the floppy diskette, you will have a GNAT Box runtime diskette (unconfigured) ready to boot in your GNAT Box system.

Hardware Keyblock

The GNAT Box system uses a hardware key block (often referred to as a "dongle") to prevent unauthorized use of the GNAT Box software.



Installation of the Hardware Keyblock

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

***Note**: If you have not purchased the GNAT Box software, but have received a demo disk or downloaded the software from the GNAT Box web server, you will not have the required hardware key block. Without the hardware key block the GNAT Box software will be operational for a limited time (starts at 180 minutes then decreases by 30 minutes at each re-boot), before it automatically halts.*

Initial Configuration

Insert the GNAT Box diskette into the 3.5" 1.44Mb floppy disk drive of your target GNAT Box system. Make sure the floppy diskette is not write protected as your configuration parameters need to be written to this diskette. Apply power and let the GNAT Box system boot from the floppy disk. The GNAT Box system will load from the floppy disk into memory by its bootstrap loader and display a series of

console messages as it begins to load.

Once the GNAT Box system kernel is loaded, it will begin to probe the system hardware. You should monitor the console messages to see if the system has discovered and recognized your network cards. If the messages scroll off the screen too quickly, you can press the <Scroll Lock> key and then use the <UP> and <DOWN> arrow keys to scroll the console messages into view. Remember to press <Scroll Lock> to disengage the Scroll Lock otherwise the console will not respond to other key strokes.

Quick Start with the Installation Wizard

If your hardware was configured correctly and the system did not encounter any problems, you will see the GNAT Box About window displayed on your console and you are ready to begin the initial system configuration.

***Note**: Prior to installation it is a good idea to record the MAC address and location of each card installed in the system for easy identification and selection.*

Keystroke Guide for the Installation Wizard

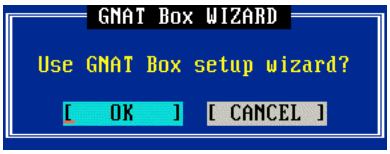
Function	Keystroke
Clear field	<F6>
Previous field	<F7>
Next field	<F8> or <Tab>
Delete/Backspace	<Del> or <Backspace>
Toggle choice list	<Space Bar>
Choice list	<F2>
Toggle Color on/off	<F12>
Save	<F10>
Select a button	<Space Bar>

It is assumed that you have successfully booted your GNAT Box runtime diskette and the GNAT Box About window has been displayed on the console.

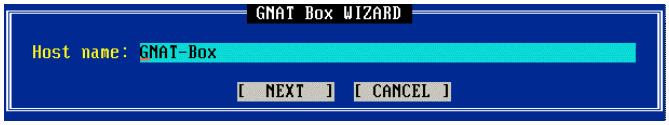
1. Press the space bar to acknowledge the About screen.

2. The GNAT Box Licensing Agreement dialog box will be displayed next. Move the cursor to "View License" to view the license. Once you're finished reading the licensing terms, press the "Esc" key to return to the previous display. Use the <Tab> key to move to the "Accept" button and press the

space bar. If you don't accept the licensing terms move to the "Do Not Accept" button and press the space bar, which will terminate the software installation.

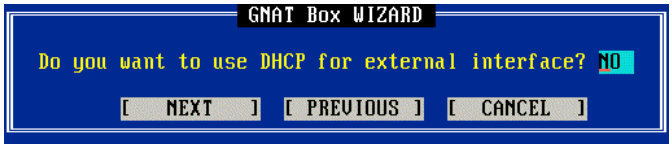


3. The next displayed dialog box will prompt you to use the GNAT Box Wizard. Select "OK" by moving to the "OK" field and pressing the space bar. If you choose not to use the Wizard by pressing the "Cancel" button, the system will drop you into an empty "Network Information" screen from the Console Command interface. You will need to complete the "Network Information" before the GNAT Box system will complete booting to its full runtime state. Please consult chapter 5 for a complete reference on the Console Command Interface.



4. Assuming you have chosen to use the Wizard, the next dialog displayed will prompt you for the Host Name of your GNAT Box. This name is not a fully qualified domain name and has nothing to do with DNS. It is merely a means of identifying your GNAT Box system. Once you key in a name, select the Next button by pressing the space bar.

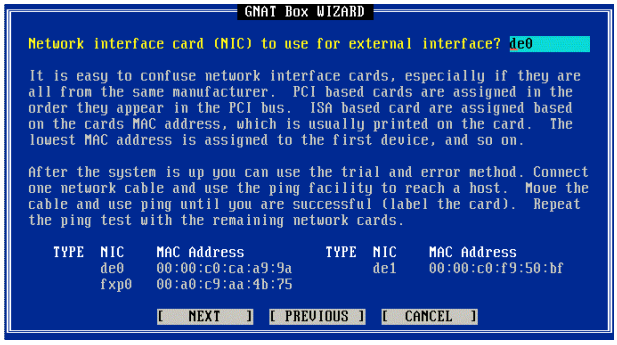
5. The next dialog box will ask you wether or not you will be using PPP on the external interface. Select "No" here if you will not be using PPP, otherwise select "yes" by toggling the field value (space bar or F2) and press the "Next" button. The remainder of this section will address a non-PPP configuration. A PPP configuration will be discussed in a later section.



6. The next dialog box will offer you the option to run DHCP on the External network interface (typically cable modem, xDSL sites use DHCP for address assignment). If your system will utilize DHCP for the External network interface assignment select, "Yes" on this screen, otherwise select "No".

7. If you will not be using DHCP on the External interface, the next two dialogs will prompt you for the IP address and the netmask of the external interface. This IP address should be a valid registered IP address, if you are connected to the Internet.

8. The next dialog screen will allow you to select an available network interface card to be assigned to the External interface. Use the F2 or the space bar to select from the available device list. Each identified network interface card is identified and listed with its MAC address at the bottom of the display.



9. After the device selection for the External interface, the next set of dialogs will step you through IP address, netmask and device assignment for the Protected and PSN (if available) network interfaces. These sets of dialogs are identical to the previous displays used for the External network interface.

   Since one of the primary features of the GNAT Box system is network address translation, the IP address and any network addresses behind (on or attached to either the Protected network or PSN) the GNAT Box can be unregistered addresses. If you are setting up a new network, it is a good idea to choose network addresses described in RFC-1918. The Internet Assignment Numbers Authority (IANA) has specified network addresses in RFC-1918 that have been designated for use as private networks. These networks will never be issued for use on the Internet.

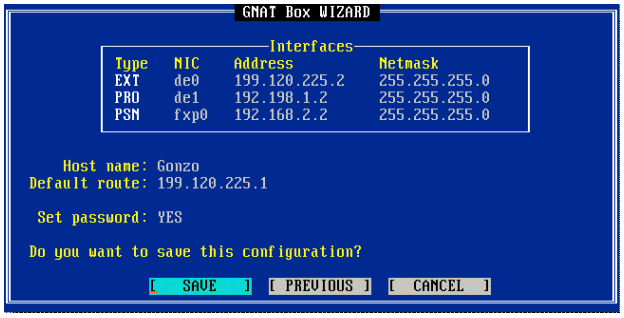
IANA Private Networks

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

An important point that should be obvious, but is sometimes overlooked, is that networks attached on each interface of the GNAT Box system need to be on logically different networks.

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

11. The next dialog will asks you to assign a password to your GNAT Box system (a requirement). The dialog will provide data entry fields for the password assignment. At this time the User ID is set to "gnatbox", however, it can be changed later in the Admin Accounts section of the Authorization facility.

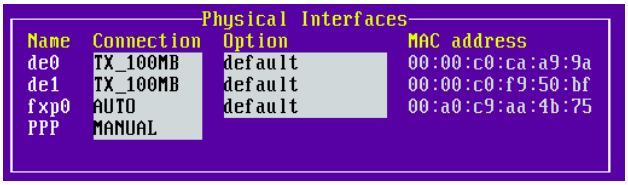


12. The final dialog displayed in the summary screen displays all your configuration settings. Please review the settings in this display. If changes need to be made, use the "Previous" button to move back to the desired dialog and make corrections. You cannot make changes directly to the summary screen. Once you are satisfied with your settings, press the "Save" button to commit your settings and allow the GNAT Box system to boot up into a fully operational mode.

If your system utilizes DHCP for IP address assignment on the External network interface (cable modem, xDSL users typically), you may want to watch the main console after exiting the Setup Wizard for the DHCP address negotiation and assignment. The negotiation messages can be helpful in determining problems.

13. After the system has completed the boot process, switch to the Command Console interface (ALT-F2). Login using the User ID of "gnatbox" and the password you assigned during the installation process.

14. Select the Network Information screen and make any adjustments to your devices in the Physical Interfaces section.



In the Physical Interfaces section, you can select the type of network connection and options for each physical device. The type of connection and options will vary depending upon the type and capabilities of each device. Some devices have only a single network connection type and no options. Frequently, a family of network cards will be available in various connection configurations. However, some of these connection types may not be available on a given card although all connection types will appear in the choice list for that device. Common sense should be exercised in these situations (e.g. don't select BNC if your network card only has a UTP interface).

Select the connection type and options for each network interface.

AUTO - The card will auto select the active network connection.

MANUAL - The card will use the network connection configured by the vendor's software or jumper selections.

UTP_10 - The card will use the unshielded twisted pair interface at 10Mbps.

BNC_10 - The card will use the BNC interface at 10Mbps.

AUI_10 - The card will use the AUI interface at 10Mbps.

TX_100 - The card will use the unshielded twisted pair interface at 100Mbps.

Default - The card will use the default option setting.
Full Duplex - The card will operate in the full duplex mode.
Half Duplex - The card will operate in the half duplex mode.

15. After making adjustments, your GNAT Box should be operational in the default configuration. After testing your connectivity, you should use the web browser or GBAdmin interfaces to modify the system configuration to your local requirements.

Testing Your Configuration

1. Use ping to test network connectivity. Press <ALT-F2> to switch to the console user interface. Select the Ping command from the Admin menu then:
   a. Ping your default route (typically a router).
   b. Ping a known host on a Protected network.
   c. Ping a known host on a PSN (if one exist).
   d. Ping a host on an external network (Internet).

2. Host access through the GNAT Box. Try to access a host on the External network (Internet) from a host on the Protected network and a host the PSN (if one exists). Make sure that the default route (gateway) is set correctly for the host. For a host directly connected to the Protected network, the default route should be the IP address of the Protected network interface on the GNAT Box system. For a host directly connected to the PSN, its default route should be the IP address assigned to the PSN network interface on the GNAT Box system. If the hosts are not directly connected, see the Troubleshooting section of this guide addressing routing issues.

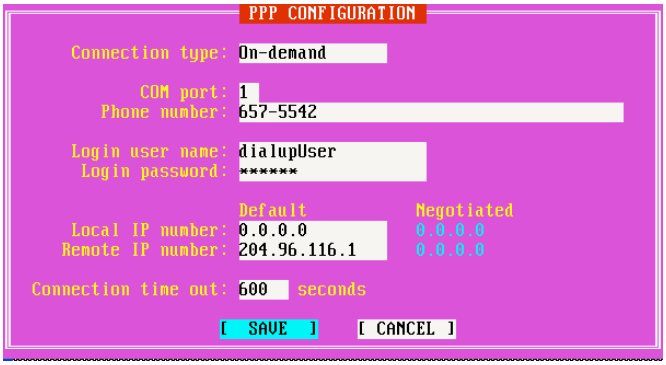
3. Access the GNAT Box web server. Start a frames capable web browser on a host connected to the Protected network. Point the browser at the IP address of the Protected network interface of the GNAT Box system (i.e. http://192.168.1.2/). Read the chapter on the web browser based user interface for more information.

4. If your connectivity tests prove successful, it is a good idea to make a copy of your GNAT Box runtime diskette. Use one of the GNAT Box utility programs to copy the diskette and save a copy on your workstation's hard disk, as well as making a backup floppy diskette.

PPP Configuration Procedure

As an alternative to the typical external network configuration that uses a network interface card and a stand alone router, the GNAT Box system can be configured to use a serial PPP interface for the External network interface. As described in the Hardware section of this guide, the PPP interface can utilize: internal async modems, external async modems, and external ISDN TAs. It is assumed that you have configured and installed your communications device (modem or ISDN TA) as per the instructions in the Hardware section of this manual.

This section continues from item 5 under the "Quick Start with the Install Wizard", if you selected PPP for the External interface. The next dialog that will be displayed is the PPP Configuration screen.



The PPP Configuration Screen is used to perform the basic PPP setup and configuration. Additional configuration options are available via the web browser or GBAdmin interfaces.

1. Select the PPP connection type. Use the <space bar> to select the desired connection type from the choice list.

On-Demand

This connection type will initiate and establish a PPP connection (if the link is down) with the remote site, whenever a packet arrives on the Protected or PSN interfaces and is destined for the External network. The PPP link will stay up as long as packets are received before the specified time-out period has expired.

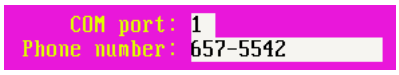
On-Enabled

This type of connection requires the GNAT Box administrator to manually enable the External network interface, which will then initiate a PPP session and establish a link with the remote site. The External network interface may be enabled either from the Interfaces option under the Admin menu on the console interface, or from the Interfaces menu item on the web browser admin interface. The PPP link will stay established until manually disabled by the GNAT Box administrator.

Dedicated

This type of connection means that a PPP link will be established when the GNAT Box system boots up. The PPP link will remain up until the GNAT Box administrator manually disables the interface, or the system is halted.

2. Select the COM Port. Use the <space bar> to select the COM port which will be used for the PPP interface. COM ports 1-4 are allowed. The COM port may be an internal modem card or a serial interface.



3. Enter the telephone number of the remote site. The telephone number should contain any special access codes or dialing directives required to call the remote site. Special characters used for pauses and secondary dial tones can be used. Consult your modem or ISDN TA manual for dialing codes.
4. Enter the login user name and password. Enter the user id used for remote PPP access. This is the user id issued by the remote site. Key in the password associated with the user id. The password is obscured in the data entry field. If the remote system uses CHAP or PAP you will have to configure those parameters either from the console interface, or the web browser interface once your GNAT Box system has completed booting up.

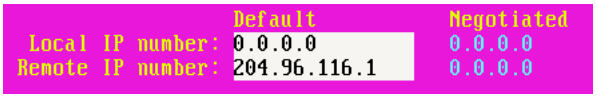
5. Assign IP numbers. A PPP link uses two IP addresses: one is local and one is remote. The GNAT Box PPP facility has the capability to negotiate the local and remote address dynamically, if the remote site supports dynamic address assignment (generally the default for most ISPs and remote sites). Dedicated IP addresses are supported for either or both sides of the PPP connection as well.

If your remote site uses dynamic address assignment, use the following configuration:

Dynamic IP Address Assignment

1. Leave the Local IP number set to 0.0.0.0; the default.

2. In the Remote IP number field, enter an IP address that may be assigned dynamically. It is not really important that the specified IP number will actually be assigned, since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote network. Very often, a good choice for this number is the remote system's router IP address or DNS server IP address.



Static Address Assignment

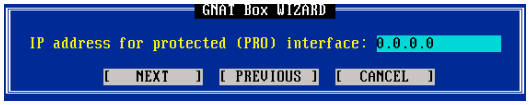
If you have a dedicated Local and/or Remote IP address, enter the IP address of the dedicated IP addresses in the appropriate fields. If you have a dedicated Local IP address, but the Remote side is dynamic, use the technique described in Dynamic Address Assignment for the Remote IP address. If your Remote IP address is static, simply leave the Local IP number set to: 0.0.0.0.

Note: *The IP address assignment for PPP connections has more options available under the Advanced Configuration section of the Console Command interface, Web browser interface or GBAdmin.*

6. Set the Connection time out value. Set the number of seconds of inactivity that the PPP link should wait before taking down the connection. Setting the time out to a value of zero indicates that no time out should be used.

7. Commit your PPP configuration. Tab to the Save button and press the **<space bar>** to save your PPP configuration.
8. The next set of dialogs will step you through IP address, netmask and device assignment for the Protected and PSN (if available) network interfaces. These sets of dialogs are identical to the previous displays used for the External network interface.

Since one of the primary features of the GNAT Box system is network address translation, the IP address and any network addresses behind (on or attached to either the Protected network or PSN) the GNAT Box can be unregistered addresses. If you are setting up a new network, it is a good idea to choose network addresses described in RFC-1918. The Internet Assignment Numbers Authority (IANA) has specified network addresses in RFC-1918 that have been designated for use as private networks. These networks will never be issued for use on the Internet.



IANA Private Networks

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

An important point that should be obvious, but is sometimes overlooked, is that networks attached on each interface of the GNAT Box system need to be on logically different networks.

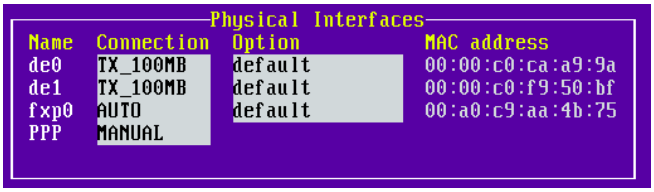
9. Once the IP address, netmask, and device assignment have been made you will be prompted for the default route for your GNAT Box system. The Wizard will have already determined the network portion of the IP address and only the host portion needs to be entered.

10. The next dialog will ask if you would like to assign a password to your GNAT Box system (a good idea). If you answer yes, the next dialog will provide data entry fields for the password assignment. At this time the User ID is set to, “gnatbox”. However, it can be changed later using the password dialog screen on one of the available interfaces.

11. The final dialog displayed is the summary screen, listing all your configuration settings. Please review the settings in this display. If changes need to be made, use the “Previous” button to move back to the desired dialog and make corrections. You cannot make changes directly to the summary screen. Once you are satisfied with your settings, press the “Save” button to commit your settings and allow the GNAT Box system to boot up into a fully operational mode.

12. After the system has completed the boot process, switch to the Command Console interface (ALT-F2). Login using the User ID of “gnatbox” and the password (if you assigned one) from the installation process.

13. Select the Network Information screen and make any adjustments to your devices in the Physical Interfaces section.



In the Physical Interfaces section you can select the type of network connection and options for each physical device. The type of connection and options will vary depending on the type and capabilities of each device. Some devices have only a single network connection type and no options. Frequently, a family of network cards will be available in various connection configurations. However some of these connection types may not be available on a given card, although all connection types will appear in the choice list for that device. Common sense should be exercised in these situations (e.g. don't select BNC if your network card only has a UTP interface).

Select the connection type and options for each network interface.

AUTO - The card will auto select the active network connection.

MANUAL - The card will use the network connection configured by the vendor's software or jumper selections.

UTP_10 - The card will use the unshielded twisted pair interface at 10Mbps.

BNC_10 - The card will use the BNC interface at 10Mbps.

AUI_10 - The card will use the AUI interface at 10Mbps.

TX_100 - The card will use the unshielded twisted pair interface at 100Mbps.

Default - The card will use the default option setting.

Full Duplex - The card will operate in the full duplex mode.
Half Duplex - The card will operate in the half duplex mode.

14. After making any adjustments to the physical devices, your GNAT Box should be operational. However, your EXTernal network interface (PPP) may not be up depending on the type of connection you have specified.

Test the Configuration

1. Use ping to test network connectivity. Press <ALT-F2> to switch to the console user interface. Select the Ping command from the Admin menu then:
   a. Ping your default route. If you have selected an “On-demand” PPP connection, the ping command should cause a PPP session to be initiated. Since the time it takes to establish a PPP session is much longer than the time-out for a ping reply, your initial ping attempt should fail. After the PPP session has been established, attempt the ping test again. If your PPP session was not established, even after retries, you may need to make some adjustments to your PPP configuration. It is best to use the web browser interface for this purpose, since the interface provides easy to use cut and paste capabilities. See the Troubleshooting section of the manual for further information about setting up your PPP configuration. You might also review Appendix A for a discussion of PPP chat/login scripting. If your PPP session was established and the ping to the default route was successful, try the following tests:

   b. Ping a known host on the Protected network.
   c. Ping a known host on the PSN (if one exist).
   d. Ping a host on the external network (Internet).

2. Host access through the GNAT Box. Try to access a host on the External network (Internet) from a host on the Protected network and a host on the PSN (if one exist). Make sure to set the default route for the hosts correctly. For a host directly connected to the Protected network, the default route should be the IP address of the Protected network interface on the GNAT Box system. For a host directly connected to the PSN, its default route should be the IP address assigned to the PSN network interface on the GNAT Box system. If the hosts are not directly connected, see the Troubleshooting section of this guide addressing routing issues.

3. Access the GNAT Box web browser admin interface. Start a frames capable web browser on a host connected to the Protected network. Point the browser at the IP address of the Protected network interface of the GNAT Box system (i.e. **http://192.168.1.2/**). Read the chapter on the web browser admin interface for more information about its use and operation.

Routing Issues

One of the most common GNAT Box installation problems is not with the GNAT Box system itself, but with routing issues. Although the GNAT Box system is a gateway (it routes packets), it is first a firewall and is rather conservative about routing packets. By default, GNAT Box neither listens, broadcasts nor supports any routing protocol (i.e. RIP, BGP, EGP, etc.). The system routes packets:

1. Between any locally attached networks (after being processed and authorized by the internal GNAT Box facilities).
2. Between any locally attached networks and an IP address that has a static route installed on the GNAT Box system (after being processed and authorized).
3. From the Protected or PSN networks to the default route, if the packet is not locally routed or a static route is not installed for the destination IP address.

RIP

GNAT Box provides support for the RIP routing protocol as a user configurable option. RIP may be enabled from the RIP configuration screen in the Routing configuration section. The GNAT Box can be configured to listen to and/or broadcast RIP information on any or all network interfaces. Additionally, RIP can be configured to broadcast the default route on the Protected network. Extreme caution should be exercised with regard to enabling RIP on the External network interface, especially if connected to the Internet. It is recommended that RIP not be enabled on the External network interface, if connected to the Internet.

If you choose to enable RIP, you will need to add Remote Access filters to allow the GNAT Box system to accept RIP packets. The easiest way to add these filters is to configure your RIP settings and then use the “Default” button on the Remote Access filter screen to generate the appropriate filters for your configuration.

Host Routing Configuration

Routing is the process of selecting the correct interface and the next “hop” for a

packet being forwarded. In order for a host on the Protected network to be able to send packets to the Internet, they must have a default route defined--the IP address assigned to the Protected network interface of the GNAT Box. The default route will direct all packets from the host though the GNAT Box.

Hosts on a Protected Network

Hosts directly attached to a Protected network need to set their default route (gateway) to the IP address of a GNAT Box Protected network interface. Routers attached directly to the Protected network need to set their default route to the IP address of a GNAT Box Protected network interface.

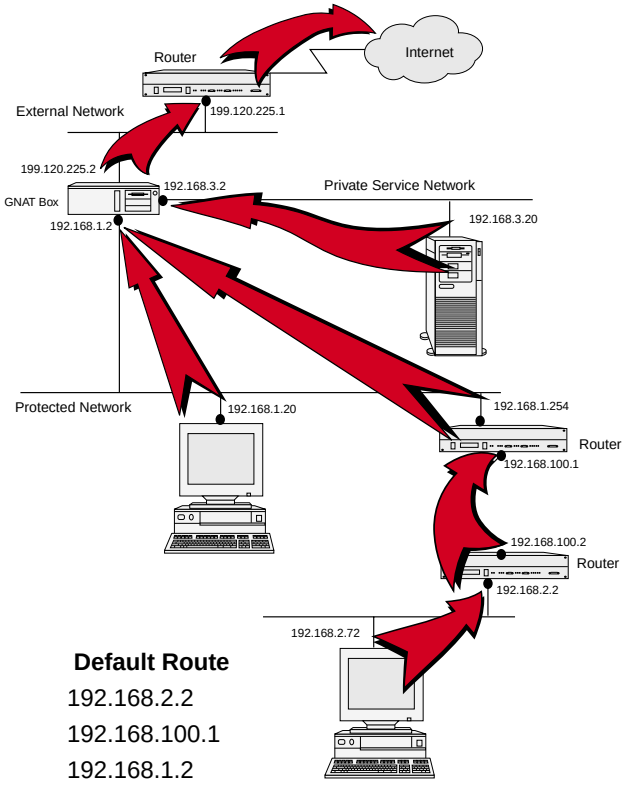
Hosts on a Private Service Network

Hosts directly attached to a PSN need to set their default route (gateway) to the IP address of a GNAT Box PSN network interface. Routers attached directly to a PSN need to set their default route to the IP address of a GNAT Box PSN network interface.

Static Routes

Conversely, the GNAT Box needs a way to get reply packets back to the originating host. If the host is on the same logical network as the GNAT Box, nothing needs to be done. However, if the host is behind a router (i.e. on a remote WAN network) a static route must be added to the GNAT Box. This static route will tell the GNAT Box which router to use to route replies back to the originating host. Use the Web browser, GBAdmin or the Advance User interface to assign static routes if needed.

Default Route Example



Host	Default Route
192.168.2.72	192.168.2.2
192.168.100.2	192.168.100.1
192.168.1.254	192.168.1.2
192.168.1.20	192.168.1.2
192.168.3.20	192.168.3.2
199.120.225.2	199.120.225.1

Chapter 5: The Console User Interface

The GNAT Box system provides three user interfaces: the **Console Interface**, **Web Browser Interface** and **GBAdmin Interface** (only for Win95/98/NT). The console interface is always available for use, since it runs on the GNAT Box system console. Alternatively, the Web Browser interface and the on-line portion of the GBAdmin interface are only available after you have initially configured the GNAT Box system and have it up and running.

About the Console Interface

The Console interface is a simple GUI based interface of hierarchical menus. As the name implies, the Console interface only operates on the GNAT Box console; you cannot access it via any other method. The console user interface only runs on the second virtual console. Use the key combination <ALT><F2> to select this console. The hot keys for switching virtual consoles are always active, making it possible to switch back to the primary console (<ALT><F1>) or the statistics console (<ALT><F3>). To enter the console user interface menu system you must supply the authorized administrator's User ID and password at the login and password prompts. Initially the administrator's user ID is set to "gnatbox". However, this can be changed on the Administrative Accounts screen.

The console user interface consists of drop down menus and popup windows. Navigating the interface is quite simple. Use the keystroke reference guide below for navigation and data entry while using the standard console user interface. The Console interface was designed for use with a color display. However, it will also operate on grayscale and TTL displays. The function key F-12 will toggle the display mode between color and black & white.

Note: *The black & white mode can run on a color display, which is useful for users who are color blind.*

Keystroke Guide for the Console Interface

Function	Keystroke
Exit/Abort	<Esc>
Clear field	<F6>
Previous field	<F7>
Next field	<F8> or <Tab>

OK/Save	<F10>
Delete/Backspace	<Del> or <Backspace>
Toggle choice list	<Space Bar>
Display choice list	<F2>
Toggle color display	<F12>
Insert	<Insert Key>
Select a button	<Space Bar>

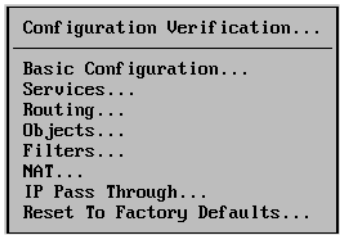
Introduction

The console user interface can be used to perform all configuration tasks, although it is best suited for initial configuration and administrative tasks when the other remote user interfaces (web or GBAdmin) are not available. Most of the tasks that need to be performed on the console are accessed via the drop down menus and popup windows.

It is important to note that when the administrator logs on to the console interface, the GNAT Box configuration data is read from the floppy diskette. This is the only time that data is read by the console user interface. If the GNAT Box system data is modified via one of the remote user interfaces while a console user interface session is in progress, the updates will not be reflected on the console. Any subsequent changes made from the console interface will overwrite the remote changes.

The Configuration Menu

The Configuration Menu contains commands that are related to the configuration and setup of the GNAT Box system. Some items in the Configuration Menu and its sub-menus are optional and need not be completed.



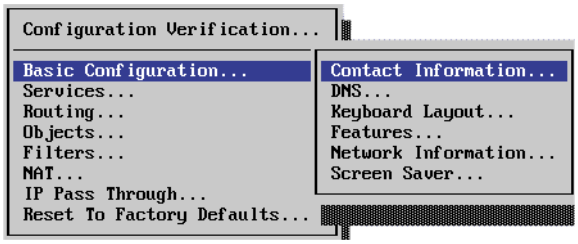
Configuration Verification

Configuration Verification... menu item runs verification checks on your GNAT Box software configuration. A verification report is displayed showing each

section checked and any errors or warnings found in each section. It is important to run verification each time you make changes to the system, since many facilities are interrelated and an incorrect value in one area can cause problems in another. All errors and warnings should be cleared. Running your GNAT Box system with validation error or warning messages may cause erratic or nonoperating conditions.

Basic Configuration

The Basic Configuration Menu consists of the functional areas that are typically required for basic operation and setup of the GNAT Box system. Some areas in this section are optional and are not required for operation of the GNAT Box system.



Contact Information

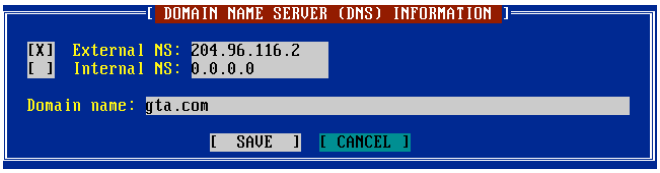
The Contact Information... menu provides data entry fields that store information about the GNAT Box installation, including serial number and contact information. This information is used by the "Email Configuration" facility and other reporting functions.

Name - Primary contact name.
Company - The name of your company or organization.
Email address - The email address of the primary contact.
Phone number - The telephone number of the primary contact.
Serial number - Your GNAT Box serial number. This can be found in several different locations: registration card, software box and on the license certificate.
Support email address - The email address of your support organization. If

you have a support contract, your reseller should provide you with an email address for this field. By default this is "gb-config@gta.com".

DNS

The DNS... menu item displays the Domain Name Server popup window, which provides the user with a means of specifying the IP address of a DNS server that will be used to resolve host names to IP addresses. If the site has a DNS server for the internal hidden network, it is recommend that this server be specified since it will be able to resolve both internal and external IP addresses. If an internal DNS server is not available, use the IP address of the external DNS server.



The primary domain field is used to specify the DNS domain of the site. If multiple DNS domains are used, simply specify the primary DNS domain.

The primary domain field is used to specify the DNS domain of the site. If multiple DNS domains are used, simply specify the primary DNS domain.

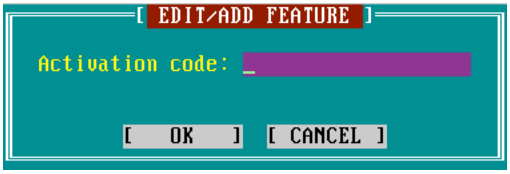
Keyboard Layout

The Keyboard Layout... menu item displays a configuration form that allows the administrator to select a keyboard layout that can be used with localize keyboards for operations on the console. This facility only provides a means to map the standard ASCII characters to their correct locations on the keyboard. It does not enable support for localized characters, such as Japanese Kanji and Swedish characters.

Features

Selecting this menu item displays a scrolling list of enabled features (including system registration code). The list displays the activation code and a description of the features.

To add a feature press the <Insert> key to display an Edit/Add Feature data entry dialog. In the "Activation code" field enter the activation code you receive for the specific feature. Move the cursor to the OK button and press the <Spacebar>. The new feature should now be added to the scrolling feature list. If the feature description is displayed as "????" then either the activation code was enter incorrectly or the activation code is not correct for the current GNAT Box system. Move the cursor to the Save button and press the spacebar to save the list and enable the new feature.



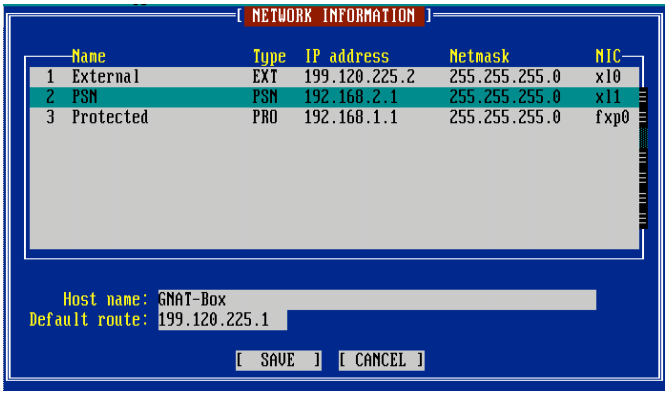
> **Note:** *In order for the activation code to function properly the system serial number must have been entered on the Preferences data entry form.*

Network Information

The Network Information form allows the administrator to assign IP addresses, netmasks, default route, network interface card options and associate logical

interfaces with physical NICs installed in the system. The scrolling list summaries the network interfaces and their configuration.

To modify an interface's configuration move the cursor to the desired interface in the scrolling list and press the <Return> key.



In standard GNAT Box system a maximum of three network interfaces will be displayed in the Network Information scrolling list, regardless of how many physical NICs are installed in the system.

Note: *The GNAT Box Multi-interface option allows a system to utilize up to 16 network Interfaces of any supported type.*

Host Name

This name is used to tag log messages. It is not a DNS host name, although you can use such a name if desired.

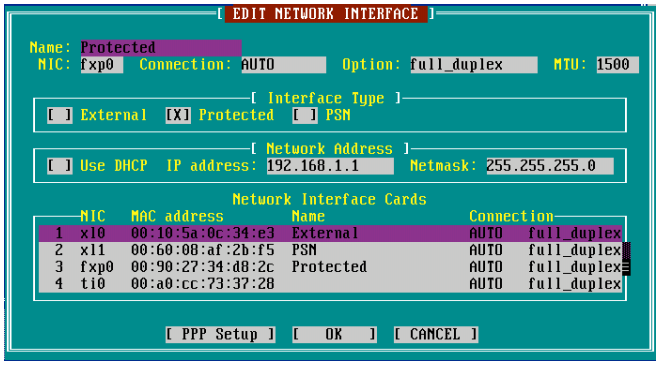
Default Route

The default route is generally the IP address of your router that connects your network to the Internet. The default route is the gateway where any non-local IP packets are sent.

When the PPP interface has been assigned to the logical External network interface in the Logical Interface section, the **Default route** field is set to the value PPP and becomes a protected field. Since the default route is dependent on the PPP negotiations, this field is not available for user data entry.

It is important to remember that a default route must always be on the same logical network as the External network interface. The only exception to this rule is a GNAT Box PPP connection.

Edit Network Interface Form



Name

The Name field allows the administrator to name each interface to suit local conventions.

NIC

The NIC field is a choice list, which is accessed by pressing F2 for a choice list or the <space bar> to toggle through the list. The NIC names are dependent on the type of network interface cards that are present in the system. A list of the NIC device names can be found in the hardware section of this manual. The display of "**???**" means no device is assigned. The special case of the **PPP** device is only valid for use on the External network interface.

Connection

This field is a choice list (F2 or <space bar>) of the possible connection types available for the specified network interface. The choice list for a particular network card might include connection options that are not available on all versions of the card.

AUTO - The card will auto select the active network connection.

MANUAL - The card will use the network connection configured by the vendor's configuration software or jumper selections.

UTP_10 - The card will use the unshielded twisted pair interface at 10Mbps.

BNC_10 - The card will use the BNC interface at 10Mbps.

AUI_10 - The card will use the AUI interface at 10Mbps.

TX_100 - The card will use the unshielded twisted pair interface at 100Mbps.

Option

This field is a choice list (F2 or <space bar>)of the possible options available for the specified network interface.

Default - The card will use the default option setting.

Full Duplex - The card will operate in the full duplex mode.

Half Duplex - The card will operate in the half duplex mode.

MTU

The MTU (maximum transmission unit) is used to limit the size of packets that are transmitted on an interface. The default is 1500. This value can be adjusted but you can cause your GNAT Box to perform poorly or not at all if you set this value incorrectly. Generally the default value should not be changed. The one exception is for gigabit network cards, where it may be desirable to use jumbo packets.

Interface Type

The **Type** column lists the possible logical network interface types that are available on the GNAT Box system. There are three logical interfaces available on a GNAT Box system:

External network interface.
Protected network interface.
PSN (Private Service Network) interface.

The minimum GNAT Box configuration requires that both an External and a Protected network interface be present and configured.

Network Address Section

This section provides data entry fields to setup IP address assignment for the select network interface card.

Use DHCP

The DHCP (Dynamic Host Configuration Protocol) field, when checked, utilizes the DHCP protocol to obtain an IP address for the specified network interface. When the DHCP field is checked, the IP and netmask fields are protected from user input. The assigned DHCP IP address/netmask will be displayed in these protected fields, after assignment. DHCP may be use: on External, Protected and PSN network interfaces. Typically sites that use cable modems require the use of DHCP on the External network interface

since dynamic IP address assignment tends to be the standard. Sites which use xDSL and don't have a dedicated IP address may require DHCP for the External network Interface IP address assignment.

Note: *The default route will be assigned automatically if DHCP is selected for an External network interface.*

IP Address

The IP address of the logical network interface. The IP address is entered in standard "dotted decimal" notation. An IP address must be entered for each active network interface. In the case of a PPP connection, the IP Address field is protected and no value may be entered since the system uses the PPP setup to configure the External network interface.

Netmask

Each active network interface must have a netmask. The value of the netmask is dependent on the network the interface will be attached to. Some common netmasks are:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Network Interface Cards Section

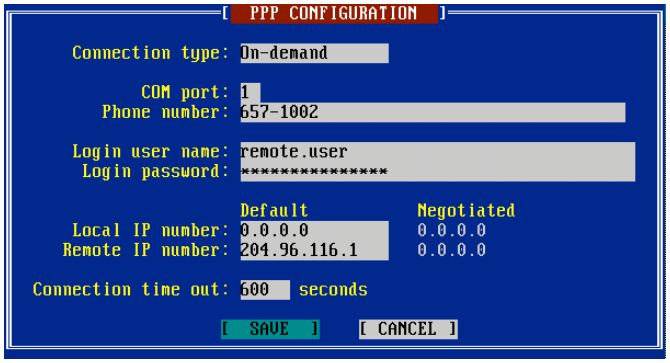
This section displays a scrolling list of all network interface cards detected by the system at boot time. The any of the NICs in this list are available for use by the GNAT Box system, however the basic GNAT Box system is restricted to the use of three network interfaces. If you wish to use more than three network interfaces at a time the muli-network interface option must be enabled. The scrolling list displays: NIC Device, MAC address, assigned logical name and connection options.

PPP Setup, Save and Cancel Buttons

The PPP setup button is normally inactive unless the logical External network interface has been assigned to the PPP device. When the PPP setup button is active, selecting it and pressing **<space bar>** will display the PPP Configuration window. Pressing the **<space bar>** on the Cancel button will discard any changes to the currently selected network interface card and return to the Network Information screen.

PPP Configuration

If the External network interface device is set to PPP then the PPP setup button is activated. Press this button will display the PPP Configuration screen. A basic PPP configuration can be setup using this screen, however using either the web browser or GBAdmin interfaces will allow much finer control and specification of PPP options.



Connection Type

Use the **<space bar>** to select the desired connection type from the choice list.

The available connection types are:

On-demand

This connection type will initiate and establish a PPP connection (if the link is down) with the remote site, whenever a packet arrives on the Protected or PSN interfaces and is destined for the External network. The PPP link will stay up as long as packets are received, before the specified time-out period has expired.

On-enabled

This type of connection requires the GNAT Box administrator to manually enable the External network interface, which will then initiate a PPP session and establish a link with the remote site. The External network interface may be enabled either from the Interfaces option under the Admin menu on the Console interface, or from the Interfaces menu item on the web browser admin interface. The PPP link will stay

established until manually disabled by the GNAT Box administrator.

Dedicated

This type of connection means that a PPP link will be established when the GNAT Box system boots up. The PPP link will remain up until the GNAT Box administrator manually disables the interface, or the system is halted.

COM Port

Use the **<space bar>** to select the COM port which will be used for the PPP interface. COM ports 1-4 are allowed. The COM port may be an internal modem card or a serial interface.

Phone Number

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

Login User Name & Password

Enter the user id used for remote PPP access. This is the user id issued by the remote site. The password is obscured in the data entry field. If the remote system uses CHAP or PAP you will have to configure those parameters either from the Advance Options section of the Console interface or use the Web Browser interface once your GNAT Box system has completed booting up.

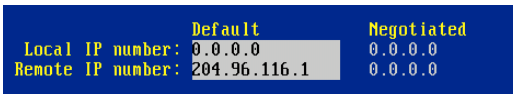
Local and Remote IP Numbers

A PPP link uses two IP addresses, one is local and the other is remote. The GNAT Box PPP facility has the capability to negotiate the local and remote address dynamically, if the remote site supports dynamic address assignment (generally the default for most ISPs and remote sites). Dedicated IP addresses are also supported for either. The Save button will commit the data on the Network Information screen to the floppy diskette and apply any changes immediately.

Dynamic Address Assignment

If your remote site uses dynamic address assignment use the following configuration:

1. Leave the Local IP number set to 0.0.0.0; the default.
2. In the Remote IP number field enter an IP address that may be assigned dynamically. It is not important that the specified IP number will actually be assigned since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote network. Very often a good choice for this number is the remote system's router IP address or DNS server IP address.



Static Address Assignment

If you have a dedicated Local and/or Remote IP address enter the IP address of the dedicated IP addresses in the appropriate fields. If you have a dedicated Local IP address, but the Remote side is dynamic, use the technique described in Dynamic Address Assignment for the Remote IP address. If your Remote IP address is static, simply leave the Local IP number set to the default value of: 0.0.0.0.

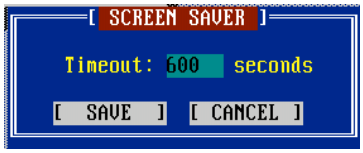
Connection Time Out

Set the number of seconds of inactivity that the PPP link should wait before taking down the connection. Setting the time out to a value of zero indicates that no time out should be used.

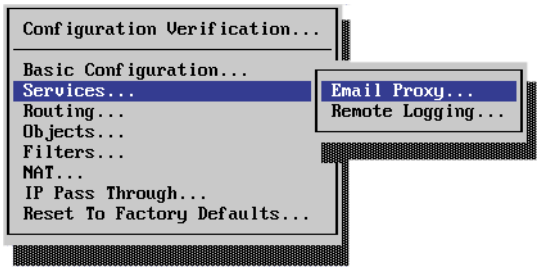
Note: *The Web Browser interface, Console Advanced menu interface or the GBAdmin Win95/98/NT software offer more extensive PPP configuration options. The console PPP configuration is designed to provide the user with a typical PPP configuration.*

Screen Saver

The Screen Saver... menu item will display a popup window which accepts a time out parameter for the built-in screen saver.



Services



Email Proxy

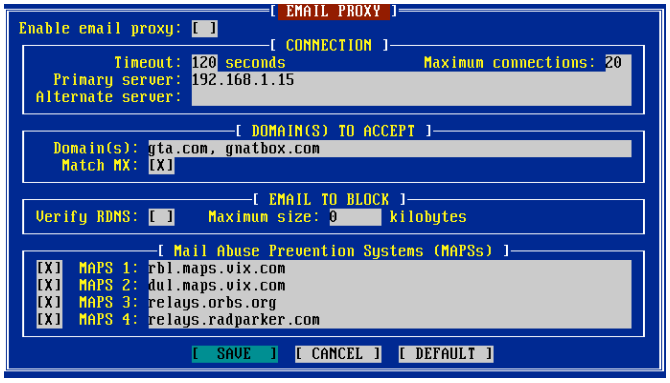
The Email Proxy dialog is used to configure the GNAT Box Email Proxy. The Email Proxy is an SMTP (TCP/25) proxy which is used to proxy inbound email connections. The Email proxy will answer on any IP address assigned to the External NIC, unless there is a tunnel created on port 25/TCP which will then override the proxy startup on the IP address in question. The GNAT Box email proxy shields your internal email server from unauthorized access attempts through SMTP exploits. Additionally, the GNAT Box email proxy provides facilities to reduce and possibly eliminate unsolicited email (known as “SPAM”).

Enable email proxy

To enable the email proxy this checkbox must be selected. To disable the email proxy deselect this item.

Connection Section

In this section, the administrator provides data for parameters involved with the email proxy connection.



The time value is the number of seconds to wait between each SMTP command exchange.

Maximum Connections

This parameter is the maximum number of simultaneous SMTP connections you wish to run on the GNAT Box. If additional connections are attempted once this maximum limit has been reached, the additional connections will be deferred, until a connection slot becomes available. Each simultaneous connection invokes a copy of the SMTP proxy program.

Primary email server

This field should contain the host name (if DNS has been configured on your GNAT Box system) or IP address of your email server. The primary email server must reside either on the PSN or Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.

Alternate email server

This field should contain the host name (if DNS has been configured on your GNAT Box system) or IP address of a backup or secondary email server if you have one. The secondary email server, must reside either on the PSN or Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.

Domain(s) to Accept

The GNAT Box Email Proxy will only accept SMTP connections for specific domains. The domains are either explicitly specified manually in the Domain list

and/or rely on the DNS MX records that are assigned to the IP Address(es) on the EXTernal NIC of the GNAT Box.

Domain list
Enter your primary and any additional email domains which you wish to accept email. The domains should be separated by a whitespace (blank, tab), or comma. This field may be used in conjunction with the MX (DNS Mail Exchanger Record) match option. This facility prevents your site from being used to relay email to other sites.

Macth against MX
If this item is enabled, the GNAT Box Email proxy will make a DNS MX record query to determine if the domain(s) assigned to the IP Address on which the proxy answered matches the domain in the "To:" portion of the email header. If there is no match, the email is rejected. This facility prevents your site from being used to relay email to other sites.

Email to Block
This section allows the administrator the ability to impose additional controls over inbound SMTP connections.

Verify RDNS
If this item is enabled then the GNAT Box Email proxy will perform a reverse DNS lookup on the IP address of the remote host attempting to make the SMTP connection. A DNS lookup is then performed on the returned host name to see if it matches the IP address of the remote host. If these lookups fail or don't match the connection is refused. This facility imposes a stringent requirement on all hosts wishing to deliver email to an address in your domain. Although all hosts on the Internet should be correctly defined in DNS, many sites have improper or mis-configured DNS entries. If you chose toenable this facility legitimate hosts which are not properly defined in DNS will not be able to deliver email to your domain.

Note: *If a DNS server has not been defined in the DNS configuration section this facility will not function correctly.*

Maximum Size
This parameter controls the maximum size (in kilobytes) of an email message that will be accepted by the proxy. A value of zero (0) means no size restrictions. This facility is designed to prevent "email bombs" (extremely large attachments

that consume disk space and cause problems for email clients).

Mail Abuse Prevention System

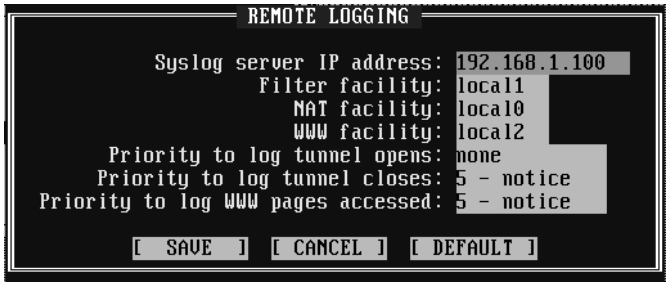
The Mail Abuse Prevention System (MAPS) - Realtime Blackhole List (RBL) is a list that consists of hosts and domains that have been documented as transmitting and/or generating unsolicited email (SPAM).

MAPS1-4

Each of these items enable a specific MAPS Realtime Blackhole List server. The specified server will be utilized to block email from known SPAM sites (those who send bulk unsolicited email). Four sites are listed, you may use any or all of the four listed sites; or enter the domain name of alternative MAPS sites you wish to utilize. Please check the RBL website: `http://www.maps.vix.com` for updated site information.

Remote Logging

The Remote Logging... menu item displays the Remote Logging popup window, which provides a means to configure how and where log information is sent.



The GNAT Box system sends logging information to a remote host using the syslog protocol. If you wish to enable remote logging, simply enter the IP address of the host system that will receive the syslog data. Unix and Linux systems have a syslog facility as a standard feature. For sites that use Windows NT or Windows95/98, the GNAT Box Logger software can be used to receive the remote logging data.

Syslog server IP address

This is the IP address of a host system that will be accepting the remote logging data. Remote logging data can be accepted by the standard Unix syslogd program, the supplied Win95/NT syslog client or any client program that can accept the syslog protocol.

Filter Facility

The Filter Facility field is a choice list accessed by pressing the **<space bar>** to cycle through the list of options. The option list contains all the standard Unix syslog facilities, some of which have no context for the GNAT Box. However, all of the facilities are available to use. The Filter Facility is the syslog stream which logs information associated with any filter that has logging enabled. Additionally, the default logging configuration is set to log any rejected packets to this log stream. This means any attempts at unauthorized access will be logged to the Filter Facility log stream. This facility may be disabled by selecting “none” in the choice list.

NAT Facility

The NAT Facility field is a choice list accessed by pressing the **<space bar>** to cycle through the list of options. The option list is the same list used by the Filter Facility field. The NAT Facility is the syslog stream which logs information associated with any network address translation, which essentially means “outbound packets.” Selecting “none” will disable the remote logging of NAT packets.

Priority for Tunnels Open/Closes

The Tunnel Open and Close fields are choice lists accessed by pressing the **<space bar>** to cycle through the list of options. The option list contains all the standard Unix syslog priorities, some of which have no context for the GNAT Box. However, all of the priorities are available to use. Whenever a network connection is initiated, an “open” log record will be generated. If you wish to log these “open”, then select a priority other than “**none**.” A “close” record will be generated when a network connection is terminated. In addition to the standard log information, “close” records contain the number of packets and bytes sent and received. To disable the generation of remote “close” log records, set the priority to “**none**.”

Priority to log WWW Facility

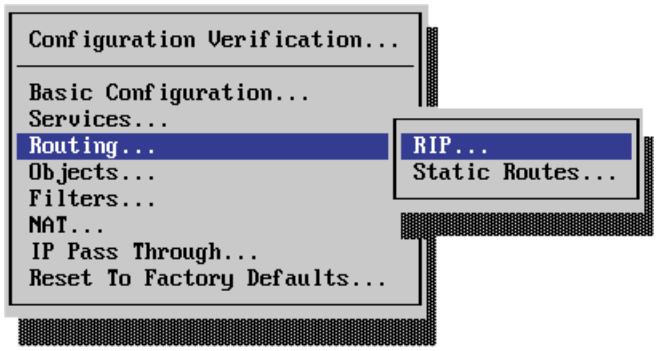
The WWW Facility field is a choice list accessed by pressing the **<space bar>** to cycle through the list of options. The option list is the same list used by the Filter Facility field. The WWW Facility is the syslog stream which logs all URLs accessed through the GNAT Box system. Selecting “none” will disable the remote logging of URL information.

All other log data is sent to the “daemon” facility. This data includes:

- Audit trails of all modifications made to the GNAT Box system.
- Remote administration access from either the web browser or GBAdmin.
- Console administration access.
- Startup messages.
- System warning and diagnostic messages.

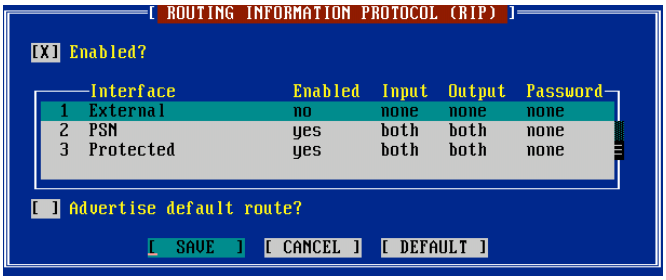
Routing

This section provides the administrator screens that address the routing facilities on the GNAT Box system. This menu section provides configuration dialogs for RIP and static routes.



RIP

The RIP.. menu item displays the Routing Information Protocol window, which provides a means to enable and configure the RIP protocol on a per network interface basis. The GNAT Box like any good firewall does not accept routing information from external sources to redirect packets through the firewall. However, if desired, the GNAT Box can enable the capability to receive as well as broadcast, routing information via individual interfaces.



The scrolling list displays all configured authorized network interfaces in the

GNAT Box system. To enable RIP on an interface first the **Enabled** checkbox must be selected. Next tab to the scrolling list and select the network interface to be configured for RIP, and press return to display the **Edit RIP Interface** window.

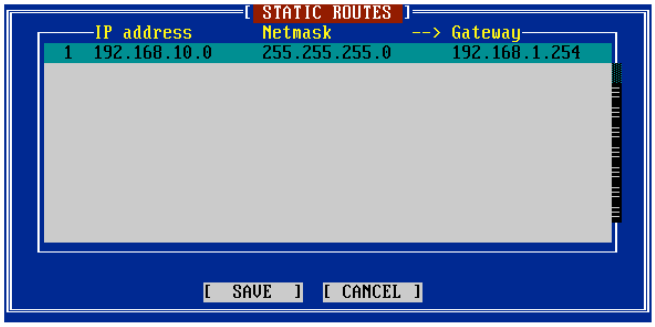
How to enable RIP on an Interface

1. In the Edit RIP Interface window, select the Enabled checkbox.
2. In the Input and Output fields use the <spacebar> to toggle the RIP protocol choices (Version 1, Version 2, both or none).
3. If RIP version 2 is select you have the option of enabling a password. Toggle the password on with the <spacebar> then enter the desired password.
4. Move to the “OK” button and press <spacebar> or Press F10 to save the settings.
5. Repeat the process for other interfaces.

Static Routes

The Static Routes menu item provides access to the Static Routes form. This form provides a means for the administrator and to define static routes on the GNAT Box system. Because the GNAT Box system is a firewall it does not normally listen to routing protocols such as RIP. Consequently it is sometimes necessary to define a static routes on the GNAT Box system.

Static routes are quite often used defined the routes to remote networks that are located somewhere beyond a local router on a Protected network. These static routes override the default routing rules and explicitly define a routing path for a particular host or network.

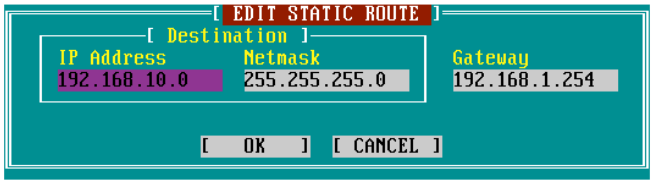


Defining a Static Route

Use the following procedure to define a static route:

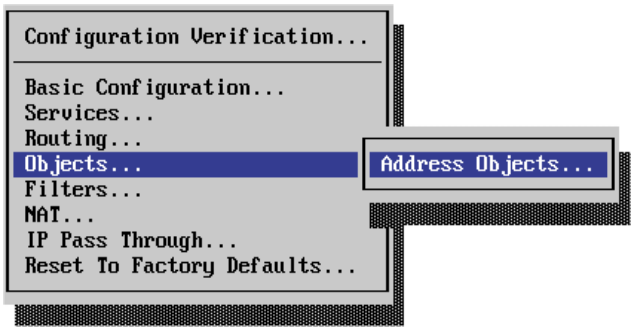
1. Press <Return> with the cursor on the Static Routes menu item.
2. Press the <Insert> key to display the Edit Static Route form. Or you can position the cursor on an existing definition and press <Return> to edit the definition.
3. In the IP Address field enter the IP address, subnet or network address.
4. In the Netmask field enter the netmask which is associated with the IP address.
5. In the Gateway field enter the IP address of the gateway to the Address, subnet or network defined in the destination section.
6. Tab to the "Save" button and press the <space bar> or F10 to save the definition.

The GNAT Box system supports 300 static routes.



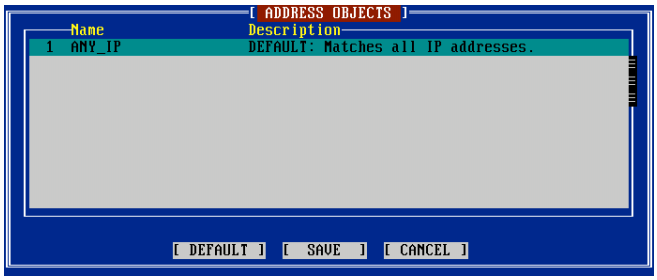
Objects

The Objects section currently contains a single item: Addresses. Future releases of GNAT Box will add more object types to this menu section.



Addresses

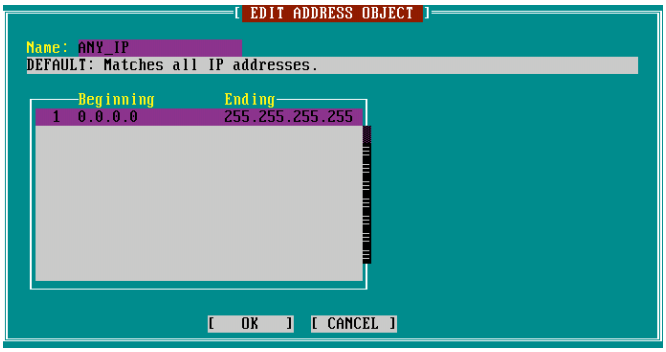
Clicking on the Addresses item will invoke the GNAT Box Address Object list. The list displays the name and description of all defined GNAT Box Address Objects.



A maximum of 300 Address Objects may be defined, with an Address Object having a maximum of 10 members. The members may be either a single IP address, a range of IP addresses, a subnet specified by an IP address and netmask, or a previous defined Address Object.

How to Add an Address Object

1. Press the <Insert> key to display the Edit Address Object screen.
2. Enter a name for the Address Object by which it will be referenced. The name must be unique.
3. In the next field enter a description for the Address Object.



4. Tab into the scrolling element list and press the <Insert> key to add an element. The Edit Address Object screen will then be displayed.

5. Press the <F2> key to display a choice list in the **Object** field. The member may be defined by either selecting a previously defined Address Object to included in the new Address Object definition or by selecting <USE IP ADDRESS> item to define the member by using IP Addresses.

If you choose to use another Address Object as a member of the current Address Object, then there is nothing else to do to define the member.

If you choose to define the new member with an IP Address select the type of definition in the IP Address section. Your choices are:

Host
Use a single IP address. Simply enter an IP address in the Beginning Address field. Leave the Ending Address field empty.

Range

Use a range of IP addresses. Enter the beginning IP address in the Beginning Address field and the last address in the Ending Address field.

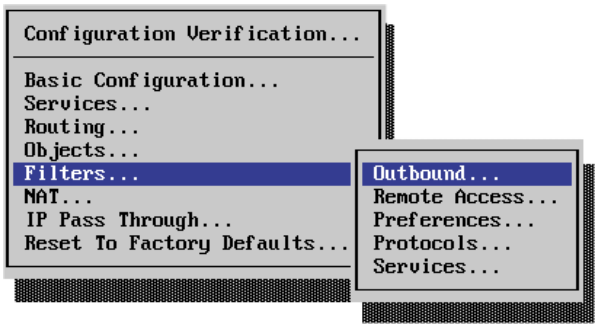
Mask

Use an IP Address and a netmask to specify the desired IP addresses.

5. Repeat step 4 until all the empty rows have been used or until you have added all the members you desire. If you need to enter more members, simply press the "OK" button then click the Edit icon of the Address Object again and additional empty rows will be provided on the Edit Address Object form.

Filters

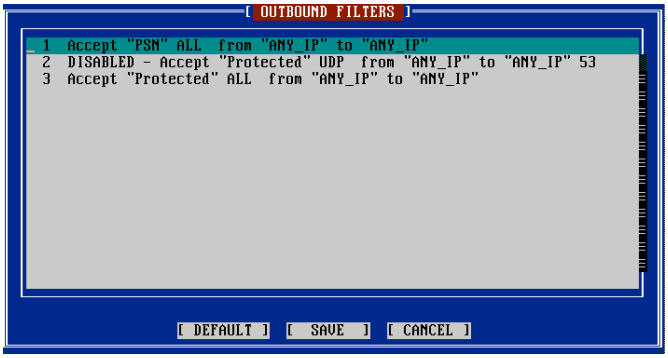
The Filter... menu item displays a submenu of items used to define and configure filters.



Outbound

Outbound Filters control access to the External network (typically the Internet) and to the PSN (if one exists). As mentioned previously, the implicit filter rule is "**that which is not expressly permitted is denied.**" It applies to outbound packets as well as inbound packets. When the GNAT Box is initially configured, a default Outbound Filter will be created dynamically, but not saved. The default filter allows all IP addresses on the Protected network to access any IP address and any service external to the Protected network. If a PSN network interface exists, a similar default Outbound Filter will be created that allows all access to the External network (typically the Internet). These filters can be modified or deleted to suit the local network security policy for external network access. An example of the default Outbound filters can be found in Appendix E.

This release supports 400 Outbound Filters.



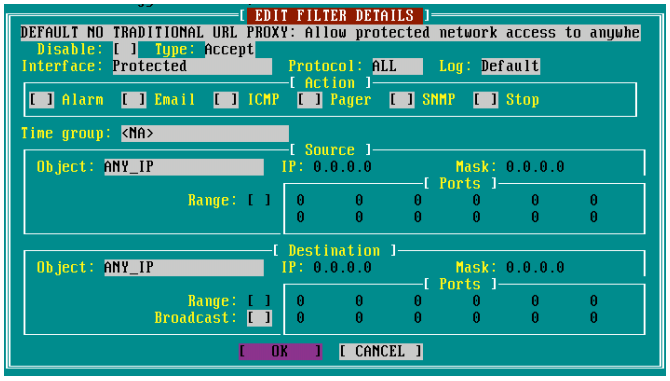
Outbound Filter List

When the Outbound... menu item is selected from the Filters submenu the Outbound Filter List screen is displayed. This scrolling list summarizes all of the defined outbound filters. To edit a filter simply move the cursor to the specific filter and press the <Return> key. A filter edit form will be displayed with the details about the selected filter. Make changes or additions to the filter and save it. Remember to save the entire filter set once you have made changes to the individual filters.

To delete a filter simply move the cursor to the filter in the scrolling list and press the <Delete> key. All changes are applied when the "Save" button or F10 key is pressed on the srcolling list screen.

Adding an Outbound Filter

Since order is important with all filters you should decide where a new filter should reside in the filter list. Move to the filter before your insertion point and press the <Insert> key, (inserts are always below the current filter). An empty filter definition form will be displayed. Define the filter and press either F10 or move the cursor to the "OK" button and press the <spacebar>.



Filter Cut and Paste

You can also rearrange the filters in the list using cut and paste. When pasting a filter definition it is always pasted before the current filter. The cut and paste keys are:

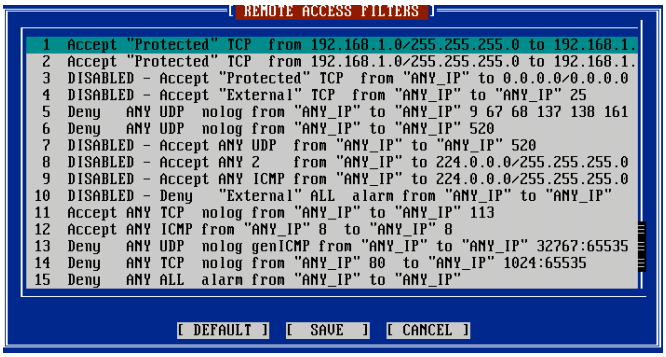
Copy - Cntl c
Paste - Cntl v
Cut - Cntl x

All cut and paste operations are isolated to the current scrolling list. Any data in the cut and paste buffer will be lost upon exiting the filter scrolling list.

Please reference the filter section in Chapter 2 Terms & Concepts for a discussion of filter definitions.

Remote Access

Remote Access Filters control inbound access primarily on Tunnels. Additionally, Remote Access Filters control inbound access to any network interface on the GNAT Box from any attached network. When the GNAT Box is initially configured, a set of default Remote Access Filters are generated dynamically but not saved. These filters can be used as is, modified, disabled or deleted to suit the local network security policy. A list of default filters are listed in Appendix E.



Remote Access filters are added, deleted and modified using the same techniques describe in the **Outbound Filters** section of this chapter.

Filter Preferences

The Filter Preferences configuration form. This form provides the administrator with the ability to define preferences for functional areas that are associated with filters.

Default Logging

Every filter has a log action associated with it, regardless of the filter type (Accept or Deny). This action can be 'Yes' to explicitly log the packet, 'No' to explicitly not log the packet or 'Default' to take the default action defined in the Logging section of the Filter Preferences. The default Filter Logging Preference is set to log all rejected packets for all protocols.

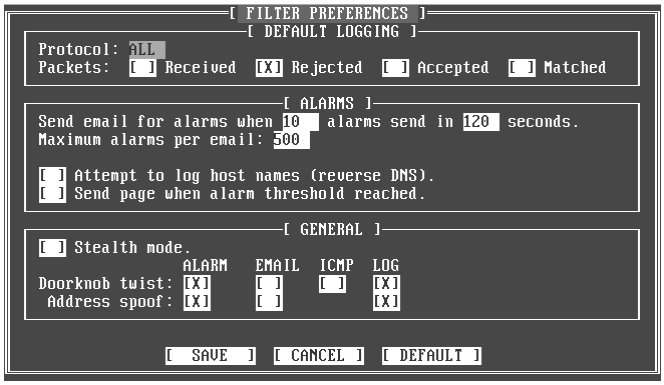
If you wish to change the Filter Preferences, follow this procedure:

1. Select the desired protocol to log from the Log Protocol choice list. The choices available are: ALL, TCP, UDP, ICMP or NONE.
2. Select the type of packets to log by clicking the checkbox next to the desired packet type. The available packet types are:

Received	Means any packet that is compared to the filter.
Rejected	Means any packet that is rejected by the filter.
Accepted	Means any packet that is accepted by the filter.
Matched	Means any packet that matches the filter criteria.

The packet type choices are not mutually exclusive. However, selecting multiple types may result in as many as four log records being generated for a single packet. This option can quickly generate an excessive amount of logging and

should be used with care.



Alarms

This dialog allows the administrator to set the parameters that are involved in alarm notifications. An alarm event occurs when a filter (Remote Access, Outbound or IP Pass Through) is matched and the alarm filter action is enabled. Each alarm event increments the alarm count by one. If the alarm threshold is reached within the specified time period, an email alarm notification will be sent to the designated email address defined on the Email Server tab. The email message will document all the alarm events that contributed to the alarm notification. Multiple email messages will be sent, if the number of alarm events exceed the maximum alarm count parameter defined in this section. Optionally, if the pager option is configured, a pager message can be generated when the alarm threshold is reached.

Send email for alarms when...

Configure the alarm threshold by entering values for the number of alarms and time period.

Maximum alarms per email

This parameter controls the maximum number of alarm messages that will be included in a single email message. A larger number will reduce the number of email messages at the expense of larger email messages. An alarm message is generally 200 bytes.

Attempt to log host names

If this checkbox is selected, the GNAT Box will attempt to resolve the hostname of the source IP address that generated the alarm. This feature will increase the

amount of processing required to deliver the alarm notification and increase the delivery time, due to the nature of DNS lookups.

Send page when alarm threshold reached
If your GNAT Box has been configured to support pager notification, this item if enabled will send a page when the alarm threshold is reached.

General
The General section contains miscellaneous configuration parameters.

Stealth Mode
If this option is selected the Remote Access default "No Stealth" filters will be set to “Disable” and the runtime system operates in the stealth mode. Enabling and disabling this option will change the system operation mode. However it will not change the Remote Access filters, unless you either press the “default” button or change them manually (via the Disable option). In the stealth mode, the GNAT Box will not respond to ICMP ping and traceroute request, UDP traceroute request and will not reply with an ICMP message when a packet arrives for a port where no service or tunnel exists.

Actions for doorknob twists
These options control how the GNAT Box will respond to "doorknob twists". A doorknob twist is when a connection is attempted to 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 GNAT Box has been mis-configured.

Generate alarm
Selecting this option will generate an alarm event if a doorknob twist occurs.

Send email
Selecting this option will immediately send an email message documenting the doorknob twist event. The email message will be sent to the address specified on the "Email Server" configuration section.

Log
Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.

ICMP
Selecting this option will generate an ICMP "service not available" message

to the source IP address of the attempted connection.

Actions for address spoofs

These options control how the GNAT Box will respond to an address spoof. An address spoof is when an IP packet arrives at a GNAT Box network interface and its return path is not back through the interface it arrived on. Address spoofs generally occur because of two situations:

1. Mis-configuration. Network(s), subnet(s), or host(s) are located or connected to the Protected/PSN network and have not been defined to the GNAT Box. The GNAT Box assumes all IP addresses that are not on the Protected network, or defined in the static route table, or are learned via RIP on the protected network, should only appear on the EXTernal side of the GNAT Box.

2. An intrusion attempt by altering the source IP address of a packet directed at a GNAT Box network interface.

Generate alarm

Selecting this option will generate an alarm event if an address spoof occurs.

Send email

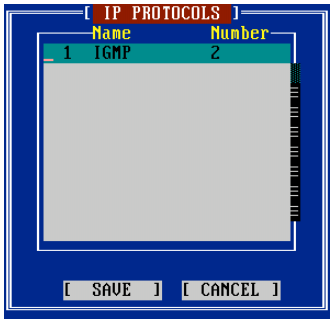
Selecting this option will immediately send an email message documenting the address spoof event. The email message will be sent to the address specified on the "Email Server" tab.

Log

Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.

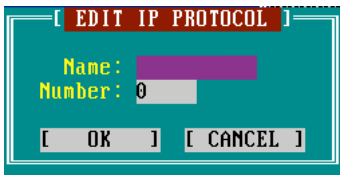
Protocols

The Protocols configuration dialog provides a means to define IP protocols other than TCP, UDP, and ICMP. This protocol definition list is available for use on any of the filter definition dialogs. In the current version of GNAT Box, the additional protocols may only be used with a Deny filter on Remote Access and Outbound filters, since the system currently can only process TCP, UDP, and ICMP IP packets in the NAT mode.



Any defined IP protocol however can be used with **IP Pass Through** filters. This means you can define IP protocols such as the IPSec ESP and AH protocols, then utilizing the IP Pass Through facility allow these packets to pass through the GNAT Box system.

The main purpose for the additional protocols in the NAT mode (Remote Access and Outbound filters) GNAT Box is to minimize extraneous protocol block messages in the log files. Since the default action of the GNAT Box is to deny that which is not explicitly allowed and the default filter logging action is to log all rejected packets, an unknown protocol that reaches the GNAT Box will be logged. If the unknown protocol is a routing protocols such as EGP, the log files could quickly grow to an enormous size. Therefore, it is often convenient to create a remote access filter that simply denies a protocol and explicitly does not log it. The protocol list is limited to 100 protocols.



How to Add a Protocol

1. In the scrolling protocol window press the <Insert> key to display an empty **Edit IP Protocol** window.
2. In the **Name** field enter the name of the protocol
3. In the **Number** field enter the IP protocol number.
4. Press F10 or move the cursor to the OK button and press <spacebar> to save the protocol definition.
5. On the protocol scrolling window cursor to the "Save" button and press the <spacebar> or F10 to save the protocol list definition.

Services

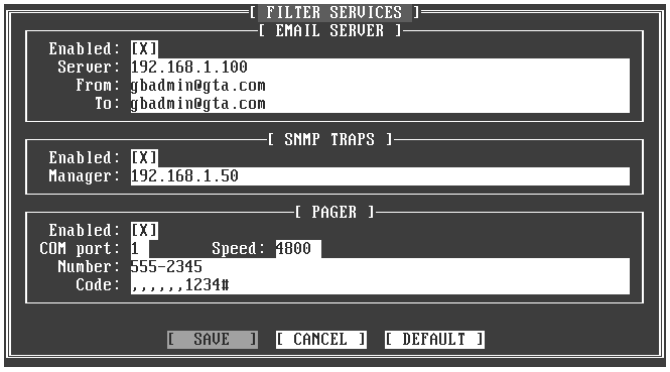
The Filter Services... menu item displays the Email Preferences configuration form. There are two distinct, but related sections on this form: Email Server and Email Proxy.

Email Server Section

This dialog allows the administrator to configure where the GNAT Box will send email notifications and alarms.

Email Server

If this item is enabled the GNAT Box will be able to send email and alarm notifications. If alarms and/or email notifications are set on a filter and the email server is not enabled, an error message will be written to the console and remote log file.



Server

Enter the hostname (if you have an internal DNS server) or IP address of the email server where alarms and email notification messages will be sent. Typically, the email server is a host on the Protected or PSN network, although this is not a requirement. The sever may be an external host. The email/alarm notifications can be sent to any valid email address, as long as the server is accessible.

Note: *The email server defined on this configuration dialog need not be the same server that is used with the email proxy.*

In order to use a hostname for the email server, you must have defined a

DNS server which is to be used for lookups on the GNAT Box system (this is done in the DNS form). If the hostname is an internal host (PSN or Protected networks), the DNS server must be an internal server which can resolve the name of the hidden host. If the DNS server referenced is an External server and the target mail server is an internal host, you will have to use the IP Address. If you are unsure about the hostname, use the IP address of the host.

From

This is the "from" email address that will appear in the email and alarm notifications. You can leave this field blank. However some email servers don't like to receive email with an empty "from" field. If you enter an email address in this field, it should be valid, otherwise if there are problems delivering the email the server will attempt to return the mail to the address in the "from" field (an email loop may ensue). The "From" address may be a fully qualified address, such as jdoe@gta.com or it can simply be the mailbox name on the specified email server, such as jdoe.

To

This is the email address that will receive the email and alarm notifications. The email address can be a fully qualified address, such as jdoe@gta.com or it can simply be the mailbox name on the specified email server, such as jdoe. If the email address is not for local delivery within your protected network, make sure that the specified email server will allow the email to be relayed.

SNMP Traps

Although the GNAT Box does not provide a SNMP facility, it does have the ability to send a SNMP trap to a SNMP management station as the result of a filter action. The trap sent is an enterprise specific generic trap.

Enable SNMP

Select this checkbox to enable the SNMP alarm facility. Upon selection the SNMP Manager IP field will allow data entry. If SNMP is not enabled, selecting SNMP filter actions on the filter definition screens will have no effect.

SNMP Manager Info

The SNMP Manager is the host that is running some kind of SNMP management tool or facility to receive SNMP trap messages. The GNAT Box will generate an enterprise specific generic SNMP trap, if SNMP is checked

as a filter action, on a filter definition and when the filter is matched.

Manager IP
The Manager IP is the IP address of the host running the SNMP management tool. This field uses the IP history list. The SNMP manager IP address may reside on any network, although the Protected network is the most common location.

Pager
The Pager dialog allows the administrator to configure the optional pager facility. To utilize the pager facility, a modem needs to be installed on one of the four available COM ports. If you are using an async modem or ISDN, you must configure an additional modem for pager support.

Enable Pager Support
Select this checkbox to enable the Pager alarm facility. If the Enable Pager Support field is not enabled, selecting Pager filter actions on the filter definition screens will have no effect.

Serial Port
This section provides a means to define which COM port and what DTE speed will be used to communicate with a modem for paging purposes.

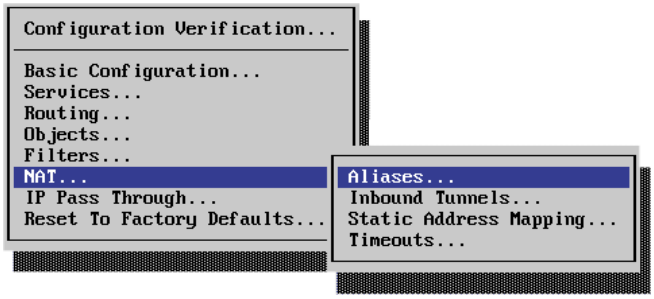
Phone number
Enter the telephone number for the numeric pager in this field along with any access codes if required.

Code
Enter the numeric message that should be sent to the pager. Typically, a greeting message is played upon connection to a pager service. Prior to sending the numeric message you may want to send a series of pauses. Most modems that utilize the Hayes "AT" command set, utilize a comma as a pause.

Note: *Most numeric paging services require a "#" to be entered at the end of the numeric message.*

NAT
The four menu items under this section of the menu are associated with network

address translation (NAT) facilities.

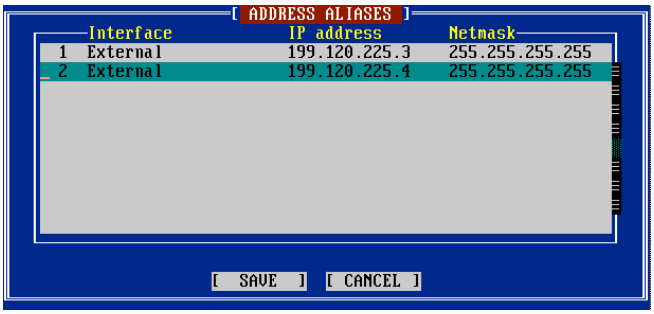


Aliases

The Aliases form is used to assign IP aliases to GNAT Box network interfaces. Aliases may be assigned to an External, a Protected or a Private Service network interface. All changes take effect after the save has been confirmed. The GNAT Box supports a total of 300 aliases.

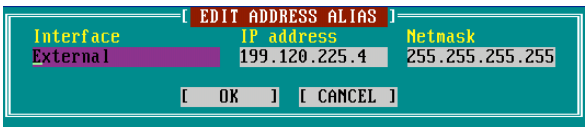
How to Create an Alias

1. In the scrolling Alias list press the <Insert> key to display an empty Alias Edit form.



2. Using the <spacebar> or F2 select the network interface you wish to assign an alias to.
3. Enter the alias IP address
4. Modify the netmask if required. The netmask should always be 255.255.255.255 if the alias is on the same subnet/network as a previous defined IP address assigned to the same network interface.
5. Move the cursor to the "OK" button and press the <spacebar> or F10 to save the ailas.
6. The save will then be acknowledged. Pressing the OK button will re-display the Alias form with two blank data entry slots at the end of the table.

7. After defining your aliases move the cursor to the “Save” button on the Alias scrolling list to commit the alias definitions.



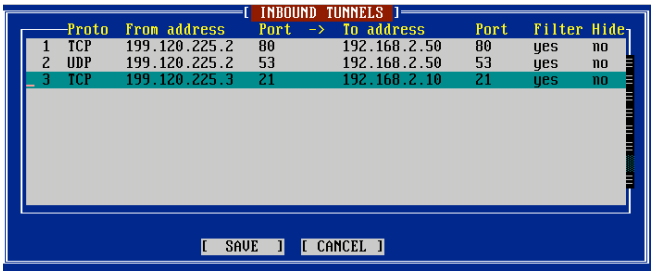
Note: *If you create an alias that resides on the same logical network as the primary IP address for the selected network interface, you must use a netmask of 255.255.255.255.*

To Delete an Alias

1. Move the cursor to the alias definition you wish to delete in the alias scrolling list.
2. Press the <Delete> key.

Tunnels

As defined in the Introduction section of this guide, a Tunnel is a GNAT Box facility that allows a host on an external network to initiate a TCP, UDP or ICMP session with a host on an otherwise inaccessible host for a specific service. The Inbound Tunnel form allows the user to define tunnels for both the External network interface and the Private Service network interface. A maximum of 300 tunnels may be defined.

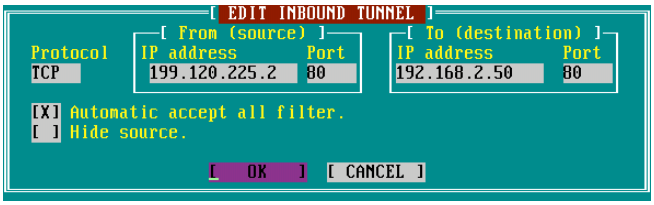


How to Define a Tunnel

1. In the scrolling Tunnel list press the <Insert> key to display an empty **Edit Inbound Tunnel** form.

2. In the Protocol field use the F2 key or the <spacebar> to select the protocol for the tunnel.

3. In the From section enter the IP address for the source of the tunnel and the port number.



4. In the To section enter the IP address of the target host and port number on the target host.

5. Move the cursor to the "OK" field and press the <spacebar> or F10.

Options

Automatic Accept All Filter

Enabling this option will create an automatic filter that will accept IP packets for the defined tunnel from any source IP address. For example this option would typically be used for a http tunnel to a public accessible web server located on a PSN network.

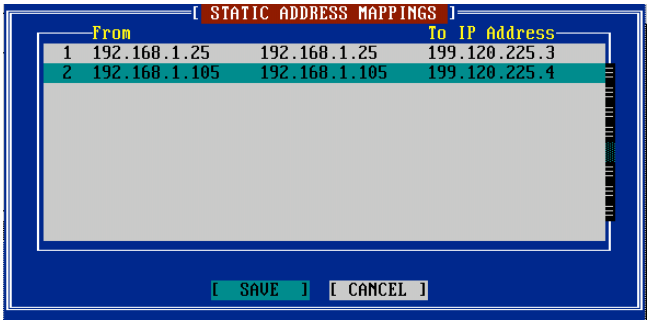
Hide Source

Enabling this option will cause the source IP address of packets received on the tunnel to be changed to the IP address assigned to the NIC where the packet exits from the GNAT Box system. Under normal conditions the source IP Address is preserved. This option is useful in situations where the GNAT Box system is used in an intranet situation.

6. Continue defining inbound tunnels. When you are finish move the cursor to the "Save" button on the alias scrolling list and press the <spacebar> or the F10 key.

Static Address Mapping

As mentioned earlier in this guide, Static Address Mapping is a GNAT Box facility that allows an internal IP address or subnet to be statically mapped to an external IP address during the network address translation process. By default, all IP addresses on a Protected and a Private Service networks are dynamically assigned to the primary IP address of the outbound network interface.



In certain situations where it is desirable to statically assign the IP address used in the network address translation. To use the Mapping facility, you must have assigned at least one IP alias to the desired outbound network interface (External or Private Service network interfaces).

Define a Static Address Map

Use the following procedure:

1. Select the Static Address Mapping... menu item.
2. Move the cursor to the scrolling list and press the <Insert> key to display an empty **Edit Static Address Mapping** form.

3. In the Object field select an Address Object or select <USE IP ADDRESS> from the choice list using either the <spacebar> or F2 key.

4. In the From IP Address field, key in the IP address of the host or subnet that should be mapped if an Address Object was not selected in the Object column otherwise leave this field empty.

5. If <USE IP ADDRESS> was selected in the Object column then key in a netmask that will be ANDed with the From IP Address to yield an IP address or subnet that will be mapped. Otherwise leave this field blank.

   For example, to map a single IP address use a netmask of 255.255.255.255. To map a class C network use 255.255.255.0 to map half of a class C use 255.255.255.128.

6. In the To IP Address field, key in the IP address to which the source IP address(s) will be mapped. Remember this needs to be an alias IP address.

7. Move the cursor to the "OK" button and press <spacebar> or press F10.

8. On the Static Address Mapping form move the cursor to the "Save" button and press <spacebar> or simply press F10 to save the Static Address Mapping set.

Delete a Static Address Map

1. Move the cursor the Static Address Map you wish to delete and press the <Delete> key.

2. On the Static Address Mapping form move the cursor to the "Save" button and press <spacebar> or simply press F10 to save the Static Address Mapping set.

Timeouts

Timeouts define when a connection is viewed as being excessively idle. What happens when a connection reaches its timeout value differs for each IP protocol. The reason for the difference has to do with how different protocols operate. Both ICMP and UDP are connectionless network services, while TCP is a connection-oriented network service. This means that generally speaking it is impossible to determine when ICMP and UDP connections are finished (ready to close). The TCP protocol has enough information embedded, so that GNAT Box can determine when a TCP connection is finished.

***Note**: You should not change the values on this preference dialog unless you know what you are doing. Setting the incorrect values can result in your GNAT Box system operating poorly or not at all.*

TCP Section

Timeouts

When UDP and TCP reach their respective timeouts the connection is marked as ready to close. TCP connections are a little tricky because TCP has two timeout values:

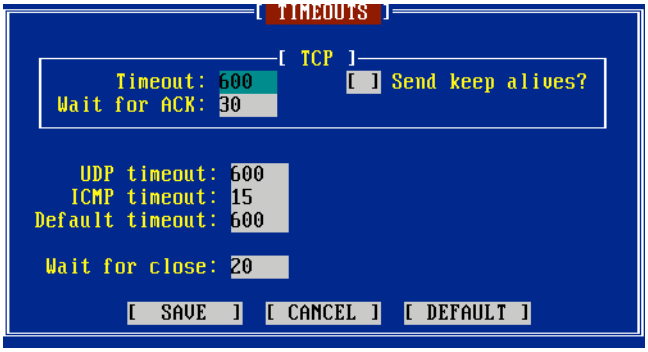
The first TCP timeout is for idleness on a successfully created connection. When the idleness timeout for TCP is reached two things can happen:

Send Keep Alives?

1. If "send keep alive" is disabled the connection is marked as ready to close.

2. If “send keep alive” is enabled, a TCP keep alive IP packet is constructed and sent to the client. The client will then send a keep alive IP packet to its server, if the connection is still valid. If the connection is invalid, the client will send a connection reset to its server. If the GNAT Box sees the keep alive message, it will set the connection’s idle time to zero. If a connection reset packet is seen, the connection is marked as ready to close. If no response is received from the GNAT Box’s keep alive message after five minutes, the connection will be marked as ready to close.

After a connection is marked as ready to close, the GNAT Box will wait five seconds before it actually closes the connection. This gives redundant IP packets a chance to clear the GNAT Box without causing false doorknob twist error messages.



Wait for Ack

The second TCP time-out is “Wait for ACK.” As part of the TCP connection creation process, the client and server exchange several IP packets. All packets sent from the server will have a bit indicating ACK (acknowledge) with the packet header. As part of its stateful packet inspection processing, the GNAT Box keeps track of the fact that it has seen this bit. If this bit is never seen it usually means that the remote server is down. If the “Wait for Ack” idle time is reached without an ACK from the server, the connection is marked as ready for close.

UDP Timeout

This field is the amount of time in seconds, when a UDP connection is considered to be timed out.

ICMP Timeout
This field is the amount of time in seconds, when and ICMP connection is considered to be timed out.

Default Timeout
The Default timeout is a catchall for any other supported protocol, besides TCP, UDP or ICMP. At this time, the only other protocol directly supported by the GNAT Box is GRE (used by PPTP).

Wait for Close
Default value is 10 seconds. If your site is experiencing a large number of spurious "Remote Access Filter" blocks from reply packets (typically from port 80 - http), you may want to increase this value, which will give packets from slow/ distant connection more time to return before the connection is closed down.

IP Pass Through
IP Pass Through is the GNAT Box term for "no NAT." The IP Pass Through data entry screens allow the user to define a host, subnet, or network that will not have NAT applied to packets from specified IP addresses.

Two items must be in place for an IP pass through to operate correctly:

1. The IP address must be defined on the Network/Host form.
2. An IP pass through filter(s) must be created to allow packets to flow from and/or to the IP pass through IP address.

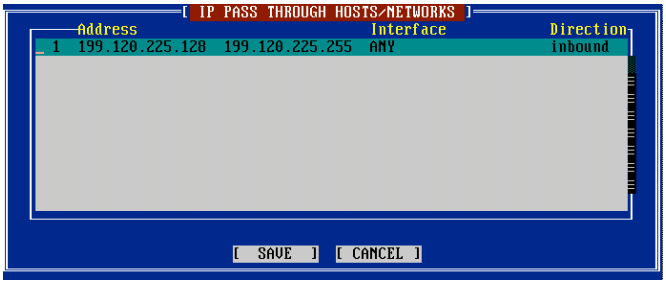
Note: *If an IP pass through address is configured to use the External network interface and the GNAT Box is connected to the Internet, the IP pass through address must be a*

valid registered address.

The IP Pass Through facility provides a great deal of flexibility, since an IP address(es) can be configured not to use NAT for specific interfaces. 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, yet packets from the same IP address which are destined for the Internet will have NAT applied.

Hosts/Networks

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



How to add an IP Pass Through Hosts/Network entry

1. In the scrolling list press the <Insert> key to display an empty **Edit IP Pass Through Host/Network** form.
2. In the Object field use F2 or <spacebar> to display the choice list and select either an Address Object or **<USE IP ADDRESS>.**

3. If you selected an Address Object in the Object column then leave the IP Address field empty otherwise enter a host IP address, subnet or network.

4. If you select an Address Object in the Object column then leave the Netmask field empty otherwise enter a netmask that will be ANDed with the IP Address field which will yield the desired results. Single IP addresses should use 255.255.255.255.

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

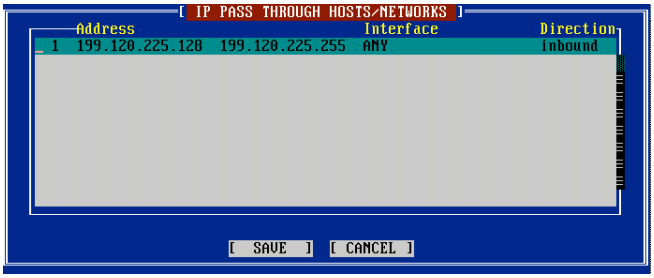
5. Use the **Interface** choice list to select which network interfaces will have no NAT applied to the specified IP packets, when they pass through the specific NIC.

6. If you wish unsolicited IP packets to be accepted for the specified IP pass through address(es), then select the **Inbound** checkbox. If you only wish to allow for the return of the IP pass through reply packets be allow to return then it is unnecessary for the Inbound option to be selected.

6. After you have finished creating your definitions, move the cursor to the "OK" button and press the <spacebar> or press F10.

7. On the IP Pass Through Hosts/Networks form move the cursor to the "Save" button and press <spacebar> or press F10 to save the set of definitions.

The IP Host/Networks list is limited to 100 entries.



Filters

I**P Pass Through Filters** control access to and from IP addresses that have been specified as IP pass through addresses. IP pass through filters, although similar to the other two filter types (Remote Access and Outbound), are a bit different since they control both inbound and outbound access to/from the designated IP Pass Through addresses. Since IP pass through addresses are not translated, the GNAT Box functions as a gateway for these addresses. Therefore the IP Pass Through Filters utilize IP Pass Through addresses in the filter definitions not GNAT Box NIC addresses.

If IP pass through host/networks are defined, pressing the "Default" button on the IP Pass Through filter screen will create a set of filters based on the IP pass through addresses defined. Since IP pass through host/networks can be defined in various combinations, the default filters will vary according to options selected.

These generated filters are quite general and should be modified to match your security requirements.

Typically, two filters are required for each different Host/Network IP pass through IP address: one for outbound access and the other for inbound access. The Remote Access and Outbound filters do not apply to IP Pass Through designated IP addresses.

This release supports 400 IP Pass Through filters.

Defining IP Pass Through Filters

IP Pass Through Filters are defined in the same manner as Remote Access or Outbound filters. The same rules about filter order also apply. The major difference is that since IP Pass Through addresses are not hidden, filtering rules always address the IP Pass Through host(s) and not any IP address assigned to the GNAT Box. The GNAT Box functions only as a passive gateway with regard to IP Pass Through addresses.

As mentioned in the previous section, one of the easiest methods of creating IP Pass Through Filters is to first configure any IP Pass Through hosts or networks using the Host/Network form. Then use the Default button on the IP Pass Through filter set form to generate a set of default filters based on the definitions created on the Host/Network form. The disadvantage of this method is that if filters have been previously created and customized, they will be replaced with the system generated default filters.

How to Create IP Pass Through Filters

To create a pair of IP Pass Through filters for a defined IP pass through host:

1. In the scrolling list of the IP Pass Through Filters form press the <Insert> key to display an empty **Edit Filter Details** form.
2. IP Pass Through addresses require two filters (inbound and outbound), with the outbound filter created first. Complete the filter definition in the same manner as an outbound filter, specifying the source IP address as that of the IP Pass Through address. Once you have the filter defined move to the “OK” button and press the <spacebar> or press F10.
3. Back on the scrolling list press the <Insert> key again to create another filter. This filter will handle the inbound connection. Define the filter as you would a Remote Access filter except the destination IP address will be the IP Pass Through address, not the IP address on the GNAT Box NIC. Save the filter.
4. After you have completed adding all IP Pass Through filters, move the cursor

to the Save button on the filter set to save the filters and apply them to the running system.

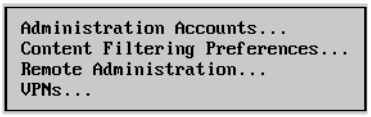
Reset to Factory Defaults

The Reset to Factory Defaults... menu item will reset all GNAT Box configuration parameters back to their original empty pre-install state. A pop up window is displayed which requests confirmation of the reset request.

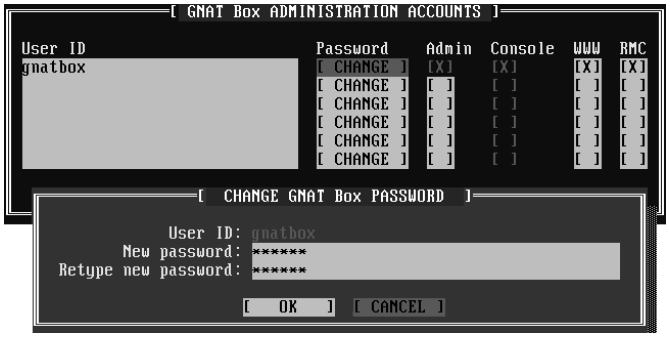
Attention: *Using the Factory Reset will permanently erase all configuration information from the system!*

Authorization Menu

The Authorization menu consists of those functional areas that address authorization for administration, remote management, inbound email, URL blocking and VPN configuration.



The Administration Accounts section provides a means to manage the administration accounts used to access the GNAT Box system. Up to five (5) additional administration accounts can be defined. Each additional account is assigned a unique User ID, password and access privileges.



The default administration account has a default user ID of "gnatbox". However, this may be changed using this interface. The primary administration account ("gnatbox") is the only account that can log in on the GNAT Box console. Except for this capability all other privileges can be assigned to additional accounts.

User ID

This is the administration account name which is used to log on to the GNAT Box system. It may be up to 39 characters long. Any characters that can be generated from the keyboard are valid, except leading and trailing spaces.

Password

The password may be up to 39 characters long. Any characters that can be generated from the keyboard are valid, except leading and trailing spaces.

Enable Options

Admin - If enabled the admin account has update authority.

Console - If enabled the admin account can login on the console.

WWW - If enabled the admin account can login via the web browser interface.

RMC - If enabled the admin account can login via the Win95/98/NT remote management console (GBAdmin).

How to Add an Account

1. Enter the User ID you wish to use for the new administration account.
2. Select the options that are to be enabled for the new account. By selecting Admin, the User ID will have the authority to make changes to the GNAT Box configuration; including adding and deleting User IDs and password.
3. Press the <space bar> on the Change button in the Password column to display the password dialog box.
4. Complete the password dialog window to create a password for the new account.
5. Save

How to Delete an Account

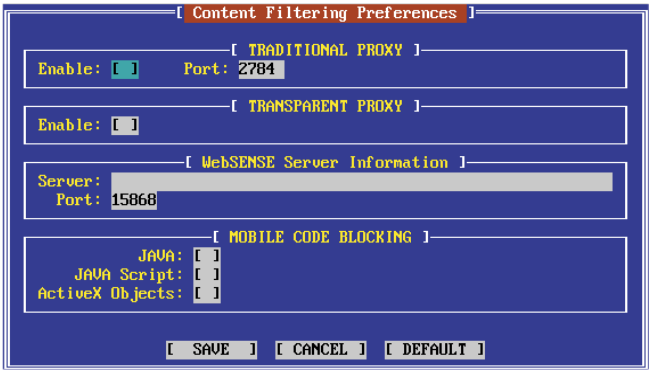
1. Select the row that contains the account you wish to delete.
2. Space out the User ID.
3. Save

Content Filtering Preferences

The URL Blocking configuration dialog provides a means to configure the GNAT Box's content filtering capabilities. The GNAT Box has a built-in JAVA blocking facility which blocks JAVA and JAVA Script on HTML connections operating on port 80/TCP and 8080/TCP. GNAT Box has integrated support for

the built-in CyberNOT content feature and the external server based Websense Internet content filtering system from Websense, Inc.

The major implementation difference between these two content filtering facilities is that the CyberNOT service runs on the GNAT Box system, while the Websense system runs on a separate Windows NT or Solaris computer system.



CyberNot

On the GB-Flash, GB-100 and GB-1000 products the CyberNOT content filtering feature is a built-in feature. To utilized this feature an annual license subscription must be purchased first before the facility can be enabled. Configuration of the CyberNOT facility can not be performed with the Console interface. The web or GBAdmin interfaces should be used to perform this function.

Websense

In order to use URL blocking, you must first have the Websense, Inc. Websense OpenServer setup and configured (available on the NT or Solaris) on your platform of choice. The Websense software does not run on the GNAT Box system directly, but rather on a server (often on the Protected network) which the GNAT Box will communicate with.

Once you have the OpenServer configured and operational, you need to determine how you would like to implement URL blocking on the GNAT Box. The GNAT Box provides two methods: Traditional Proxy method and Transparent Proxy method.

Traditional Proxy

This method requires all users located on the Protected network to configure their browsers for a proxy. All URL requests will be directed to the designated proxy.

How to configure GNAT Box for the Traditional Proxy

1. Enable. Make sure the Enabled Traditional Proxy is checked.

2. Set the Proxy Port. When the GNAT Box is operating without the Websense OpenServer feature enabled, it does not use a proxy mechanism. However, when the GNAT Box http proxy is used in conjunction with the Websense open server, it runs on TCP port 2784 by default. If the user wishes to run the http proxy on a different port, enter the value in the Port field at the top of the dialog box. This proxy port is the port number users should set their web browsers to for use with the GNAT Box/Websense configuration.

3. Set the Websense OpenServer address. In the Server field, under the Websense section, enter the IP address or host name of the Websense OpenServer. If you have configured the DNS section of your GNAT Box and your DNS server is internal, you can simply use the host name of the OpenServer. Otherwise, you must enter the IP address of the OpenServer.

4. Set the OpenServer port number. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the WebSense Port field.

Note: *Users should set the proxy IP address to that of the GNAT Boxes' Protected network interface IP address, (this is the same address users should have as their Gateway/default route).*

Transparent Proxy

This method is transparent to users located on the Protected network; no modification to a browser is required.

How to configure GNAT Box for the Transparent Proxy

1. Enable - Select the Enabled checkbox for the Transparent Proxy.

2. Set the Websense OpenServer address. In the Server field, under the Websense section, enter the IP address or host name of the Websense OpenServer. If you have configured the DNS section of your GNAT Box and your DNS server is internal, you can simply use the host name of the

OpenServer. Otherwise, you must enter the IP address of the OpenServer.

3. Set the OpenServer port number. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the Websense Port field.

Mobile Code Blocking

This section allows the administrator to selectively block possible malicious mobile code. When any of the items is enabled the GNAT Box system will block the specified type of mobile code which appears in the inbound HTML streams on TCP port 80 and 8080.

Remote Administration

The Remote Administration... menu item displays the Remote Administration dialog window, which provides a means to control how and if remote administration, via the Web Browser interface and the Remote Management Console (GBAdmin), of the GNAT Box will be provided. The default settings enable remote administration and the ability to apply updates, with the Web Browser interface being served on the standard TCP port 80 and the RMC interface on TCP port 77.

Remote Web Administration

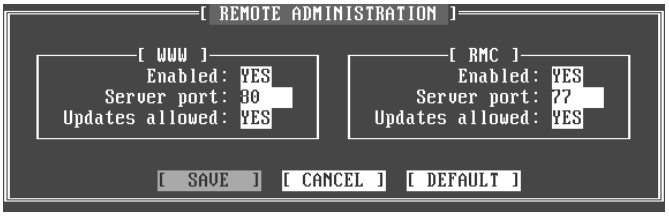
This section controls how and if access will be allowed via the web browser interface.

Enable Web Administration

Select "YES" to enable remote administration via the web browser interface.

Server Port

The default port the web browser interface is served on is port 80. If you wish to change this, enter the new port number and make sure to change the Remote Access filter associated with remote administration to match the port number. Although port 80 is the standard for http, it is suggested that an alternative port number (8000 or 8080 are good choices) is utilized. The reason for moving the web administration port is that a possible mis-configuration of the Remote Access filters could expose the remote web browser interface to unauthorized users.



How to perform a port number change

If you decide to change the port number for the web browser interface you should implement this change in the following order:

1. Find the Remote Access filter that controls access via the web browser interface and add the new port you wish to use to the destination port list. Do not remove port 80 yet. Save the filter and the filter set. It is generally best to use the web browser or GBAdmin interface to perform this task, otherwise you will have to use the Advanced Configuration interface from the console.

2. On the Remote Access configuration screen change the port number to the new port value. Save your changes.

3. Find the Remote Access filter that control access via the web browser interface and delete port 80 from the destination port list, leaving only the new port value you have chosen. Save the filter and the filter set.

Updates Allowed

Updates are allowed by default. If you wish to disallow remote updates via the web browser interface, deselect this checkbox.

Remote Management Console

The Remote Management Console established an encrypted network connection to the GNAT Box on port 77/TCP. By default the GNAT Box 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 the External and PSN networks.

Enable RMC

Select “YES” to enable access via the Remote Management Console (GBAdmin).

Server Port
The default port for RMC access is 77. If you wish to change this, enter the new port number and make sure you change the Remote Access filter associated with the RMC administration to match the new port number.

Updates allowed
Updates are allowed by default. If you wish to disallow remote updates via GBAdmin, deselect this checkbox.

VPN

The VPN menu item provides access on the console interface for the creation and management of GNAT Box VPNs. This section provides information about the mechanics of managing VPN definitions on the console interface (see Chapter 9 of this guide for a complete discussion of the VPN capabilities of the GNAT Box system).

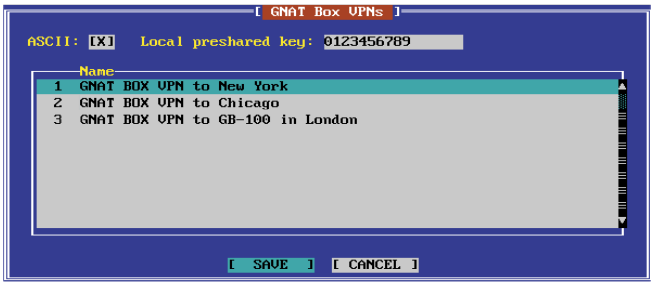
The supported VPN features vary depending on which platform the GNAT Box system is running on. All of the flash based products (GB-Flash, GB-100 and GB-1000) support both automated key exchange (IKE) and manual key exchange. The floppy disk based GNAT Box Pro only supports manual key exchange.

Selecting the VPN menu item will display a scrolling summary list of all defined VPN Security Associations. At the top of the display are data entry fields for the local pre-shared key. The pre-shared key information is only used by IKE. So if you are only using manual key exchange this information is ignored.

Local Pre-shared Key
The Local Pre-shared key is the key that is associated with the local gateway IP address. This key is sent to the remote VPN gateway during the phase I key exchange for IKE. You will need to provide this key and the IP address to the administrator of the remote VPN gateway. Likewise you will need to obtain the remote VPN's gateway IP address and pre-shared key to be used in your VPN definition.

If the ASCII selection box is checked then the information entered in the Local Pre-shared Key field is interperted as ASCII values. If the ASCII box is not selected the data is interperted as hexadecimal values.

To create a new VPN definition (manual or IKE), move the cursor to the scrolling list and press the <Insert> key. Delete a VPN definition by moving the selection cursor to the VPN definition to be deleted and press the <Delete> key. Edit a VPN definition by moving the cursor to a definition summary and press the <Return> key.



In order for all changes, deletions and additions to take effect move to the “Save” button and press the <Spacebar>. Leaving the VPN definition list without saving will result in the loss of all changes, additions and deletions. A maximum limit of 300 VPNs may be defined.

VPN Edit Form

The VPN Edit form is used to define and edit a GNAT Box VPN definition (or Security Association). As mentioned in the previous section the form is display by moving the cursor to the VPN definition summary and pressing the <Return> key or pressing the <Insert> key to create a new definition.

Disable

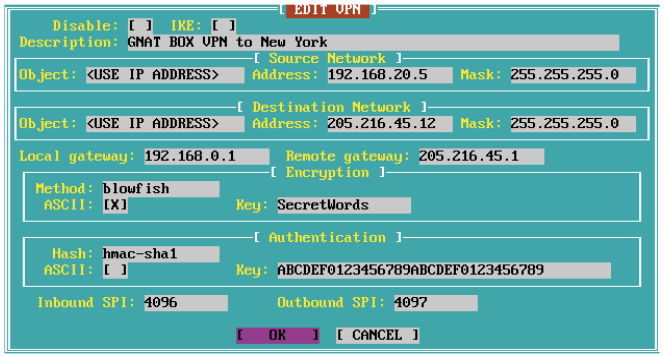
Like many GNAT Box facilities, with VPN definitions you have the ability to create a definition then use the Disable item to toggle the item between active and inactive status.

IKE

If you are a VPN that will use IKE for key exchange the select this check box. Otherwise for manual key exchange leave it empty.

Description

Use this field to write a brief description of the VPN definition.



Source Network

The Source Network defines the source network(s) that will be allowed to use this VPN definition. The source network can be defined using IP addresses or IP Address Objects. As will all Address Objects the object can be various combinations of IP addresses, from a single IP address, a group of IP address, a network or a group of networks. The source network should be a network located behind the firewall on either a protected or PSN network.

If you are not using IP Address Objects enter the network IP address of the remote network that resides behind the VPN gateway. In the case of a GNAT Box it would typically be the Protected network. Use the Mask field to define the type of network, (e.g. 255.255.255.0 for a class C network). The Source network doesn't have to be the entire remote network, only the network that is to be accessible via the VPN definition.

Destination Network

The Destination Network section operates the same as the Source Network section. The Destination network defines the remote network behind the remote VPN gateway. The remote network can be either a registered or unregistered network. The remote network MUST be logically a different network from the local source network.

Local Gateway

This is an IP address that is assigned to an External network interface on the local GNAT Box system. So this IP address can be the real External NIC IP address or any alias assigned to it. The encapsulated packets will appear at the remote gateway with this IP address as the source IP address. Hence

the local gateway IP address will should be used on the remote gateway when Remote Access filters are created to accept the VPN connection.

Remote Gateway
This is the IP address of the gateway to the remote network. If the remote network is behind a GNAT Box system then this IP address would be one that is assigned to the External network interface. This IP address will also play a role in determining the routing of the encapsulated packet.

Encryption
The encryption section requires differenet information depending upon which key exchange method has been selected.

Manual Key Exchange
If you choose to use an ESP transformation for your VPN you should complete this section. ESP provides confidentiality to your data, while AH only provides authentication and integrity. If you do not select an ESP transformation by selecting “None” then you must at least have the Authentication section completed which will define an AH transformation.

Method
Use the selection list to select the method that will be used for the ESP transformation. Selecting “None” will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128 and DES. The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Hexadecimal key
If this item is selected then the values entered in the “Key” field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

Key
This is the appropriate key for the select ESP transformation. The Blowfish, and CAST128 transformations use variable length keys, while DES uses a fixed length key.

Blowfish

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

CAST128

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

DES

64 bits	8 ASCII characters or 16 Hex chars

Authentication

If you are using Manual Key Exchange you have the option of defining three different VPN tunnel mode transformations: AH, ESP and ESP with authentication. If you would like to define an AH transformation then you should only complete the Authenication section and leave the Encryption section set to None. If you only want to use ESP then leave the Authentication section set to None. If you want to use ESP with authentication set both the Encryption and Authentication sections. Remember each transformation introduces additional computational requirements for the processing of the VPN.

Method

Use the selection list to select the method that will be used for the AH transformation. Selecting "None" will result in no AH transformation being applied to the packet. The available choices are: None, HMAC-MD5 and HMAC-SHA1.

Hexadecimal key

If this item is selected then the values entered in the "Key" field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

Key

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

Inbound SPI

The Inbound Security Parameter Index is used to uniquely identify a Security Association, (SA). The Inbound SPI will be the Outbound 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.

Outbound SPI

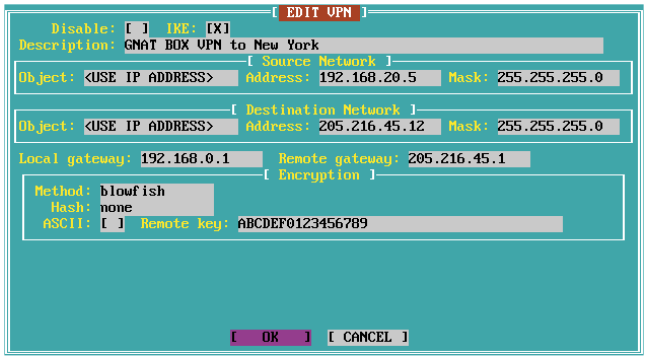
The Outbound Security Parameter Index is used to uniquely identify a Security Association, (SA). The Outbound SPI will be the Inbound SPI on the remote side of the VPN. The SPI should be unique for each SA, although the inbound and outbound SPI may have the same value.

Save

Move the cursor to the Save button and press the <spacebar> to save the VPN definition. The VPN definition is not fully committed until the entire VPN definition list has been saved. Once the list has been save the VPN definition is active. The VPN definition although active can not be used until a Remote Access filter is in place to accept the remote gateway's packets and IP Pass Through filters for access control on the VPN are defined.

Automated Key Exchange (IKE)

Both the manual key exchange and IKE methods require the same type of gateway and network information in their definitions. The Encryption section differs between the two.



Method

Select an encryption method to be used for the VPN. Use the selection list to select the method that will be used for the encryption method. Selecting "None" will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128 and DES.

Note: Remeber that the variable length encryption methods (Blowfish and Cast128) are limited to 64 bits.

The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Hash
The hash algorithm is used for authentication. Select None, HMAC-MD5 or HMAC-SHA1. If None is selected for the Encryption method then either HMAC-MD5 or HMAC-SHA1 must be selected, (this indicates that an AH transform will be used). If an Encryption method other than None is selected and a hash algorithm other than None is selected then an ESP transform with authentication will be used.

Remote Key
Enter the remote VPN gateway's pre-shared key in this field. If the ASCII box is checked then the data in the pre-shared key field is assumed to be ASCII, otherwise it is assumed to be hexadecimal values.

Three Steps to VPN Activation.

1. Define a VPN Security Association.

2. Create a Remote Access filter(s) 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 first prior to defining any VPN filters, as the ESP and AH protocols may not be included in the list. Go to the protocol list and press the "Default" button to create a list that includes the ESP and AH protocols. Do not use the Default button if you have added protocols by hand. You can add the ESP (protocol 50) and AH (protocol 51) by hand.

3. Create IP Pass Through filters that allow inbound and outbound access on the defined VPN. Generally you will need two filters for each VPN definition, (one for inbound access and the other for outbound). If you have one or more VPN definitions, simply go to the IP Pass Through filter screen and

press the “Default” button and a set of filters will be created for your VPN definitions. Please note that the Inbound filters will be disabled and set to Deny. Please make modifications to these filters as required and enable them as per your local security policy. Please note that IP Pass Through filters for VPN definitions do NOT require that entries be created on the IP Pass Through Host/Network data section.

Please see Chapter 9: GNAT Box VPN for more information about the VPN facility.

Admin Menu

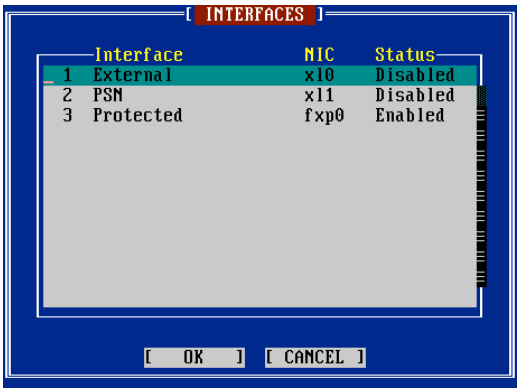
The Admin menu contains menu items which address operational and diagnostic functions on the GNAT Box system.

Halt

The Halt... menu item will halt the GNAT Box system. A pop up window is displayed which will request confirmation of the halt request.

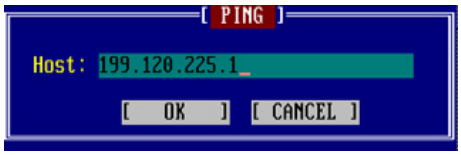
Interfaces

The Interfaces... menu item will display a popup window that shows the current status of each logical network interface. Each interface’s state can be either enabled or disabled by toggling the associated choice list with the **<space bar>.** When a network interface is disabled, it will neither accept nor transmit network packets. In the case where the External interface is a PPP connection, disabling the External interface will cause the PPP link to be forced down, and drop the RS-232 signal *carrier detect*.



Ping

The Ping... menu item provides a method to test network connectivity by sending ICMP ping packets. The popup window provides a data entry field for the target IP address or host name (if you have assigned a DNS server on the DNS configuration screen).



Reboot

The Reboot... menu item will reboot the GNAT Box system. A pop up window is displayed which will request confirmation of the reboot request.

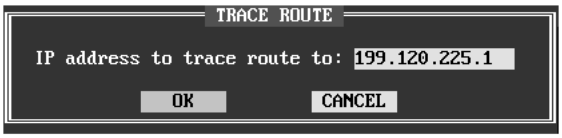
Note: *Some system boards will not respond properly to a warm reboot request; you must reset them manually.*

Set Date/Time

The Set Date/Time... menu item provides a means to set/adjust the system time and date.

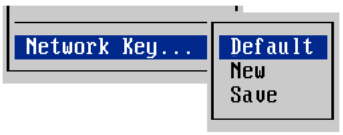
Traceroute

The Traceroute... menu item provides yet another method to test network connectivity. It traces the route an IP packet would follow to some Internet host by launching ICMP probe packets with a small TTL (time to live), then listens for an ICMP “time exceeded” reply from a gateway. When the trace is running, three probes are launched for each gateway with the output showing the TTL, address of the gateway, and round trip time of each probe.



Network Key

The Network Key... menu item provides access to functions that are involved in the generation and storage of the network encryption key. Changes made to the network key from the console interface will only affect the local GNAT Box system.



In order to use the Remote Management Console functionality of the GBAdmin program, the network encryption key on the remote GNAT Box system and the key stored in the configuration loaded by GBAdmin must match. A new key generated on the GNAT Box system can only be made available to GBAdmin by taking the floppy diskette to the remote workstation and reading the floppy diskette. The exception to this method is to set the encryption key to the default value, which can be done both on the GNAT Box system and in GBAdmin.

The Network Key submenu provides three functions for manipulating the network

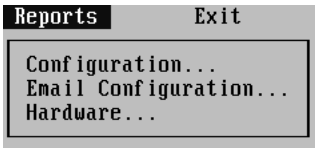
encryption key: create a default key, create a new key and save the key.

Default
The Default menu item sets the network encryption key to the default value. Since the default value is common to all GNAT Box systems, it is advised this option only be used to establish initial communications between GBAdmin and the local GNAT Box system. Once GBAdmin has established a communications link, a new key should be generated from GBAdmin and stored on both the GNAT Box system and in the GBAdmin configuration.

New
The New menu item generates a new random network encryption key. Since this function is performed locally on the GNAT Box system, the key will be unknown to any remote GBAdmin client. In order to use a new key generated on the GNAT Box system, the key must be saved and the floppy diskette must be taken to a remote workstation running GBAdmin to read the configuration (containing the key).

Save
The Save menu item will save the network encryption key for the current configuration. This can be either the default key value or a new random key generated by the New function.

Reports Menu
The Reports menu provides access to system configuration reporting facilities available on the console. These reports are mainly to diagnose problems, since they can only be displayed on the console and not printed or saved. The web browser and GBAdmin user interfaces provide access to the same reports. However facilities in those interfaces allow the reports to be saved or printed.



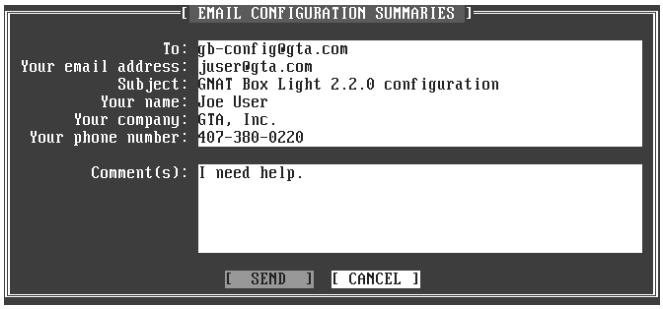
Configuration Report
The Configuration... menu item will generate the GNAT Box Software Configuration Summary report which is a comprehensive formatted report of the currently loaded configuration data. When the Configuration menu item is selected, data from each configuration section is read and formatted as text output.

Email Configuration

The Email Configuration... menu item is provided mainly for support purposes. However the administrator may find this feature useful for internal reporting and auditing. This facility will email the following as attachments:

- A software configuration report
- A hardware configuration report
- A verification report
- A copy of the current routing table
- A copy of the current ARP table
- A binary copy of the system configuration data in MIME encapsulated format.

A comments field is supplied, so the administrator can provide some additional information.



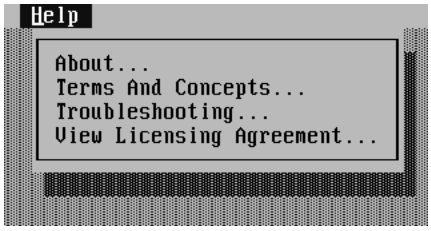
The data entry fields are populated from the Preferences section. Any fields may be overridden. This facility will use the designated mail server to deliver this email.

Hardware Report

The Hardware... menu item will generate a report of the hardware detected in a GNAT Box system at boot time. This report is useful in diagnosing possible hardware problems.

Help Menu

The Help menu contains various informational menu items.



About

Selecting the About... menu item will display the GNAT Box console splash screen. This display provides the version number of the GNAT Box software along with information for contacting GTA, Inc.

Terms & Concepts

The Terms and Concepts... menu item displays a brief document which addresses some of the basic GNAT Box Terms and Concepts.

Troubleshooting

This menu item displays a list of common problems and their solutions, along with methods for solving problems.

View Licensing Agreement

This menu item will display the GNAT Box license agreement.

Chapter 6: Web Browser User Interface

About the Web Browser Interface

The GNAT Box system can be remotely administered using a frames capable web browser such as Netscape Navigator, Microsoft Internet Explorer (3.0 or newer), or even the text based Lynx browser. This feature allows you to administer your GNAT Box system from a variety of different platforms such as Windows 95, Unix X-Windows or Macintosh.

Although the GNAT Box runtime system has a small footprint, it also contains a built-in web server. This built-in web server only serves web pages for the GNAT Box system user interface; it cannot be used for other purposes.

The Web Browser interface is not required for operation of the GNAT Box system, since administration can be performed using the console based user interface or GBAdmin remote administration client. The Web Browser interface, however, is often more convenient for most users.

The Web Browser interface can be disabled or set to a read-only mode where no updates are allowed. Configuration of remote administration is performed from the console via the Configuration menu Remote Administration item, or via the web interface Remote Administration menu item. Once the Web Browser interface has been disabled, you must use the console interface to re-enable it if desired.

By default, the GNAT Box web server operates at the standard http TCP port of 80. If you want to change the port the web server operates on, simply assign the port number on the Remote Administration screen, (make sure that you create a Remote Access filter to allow the new port number before changing the port number otherwise access will not be possible). This change will occur immediately.

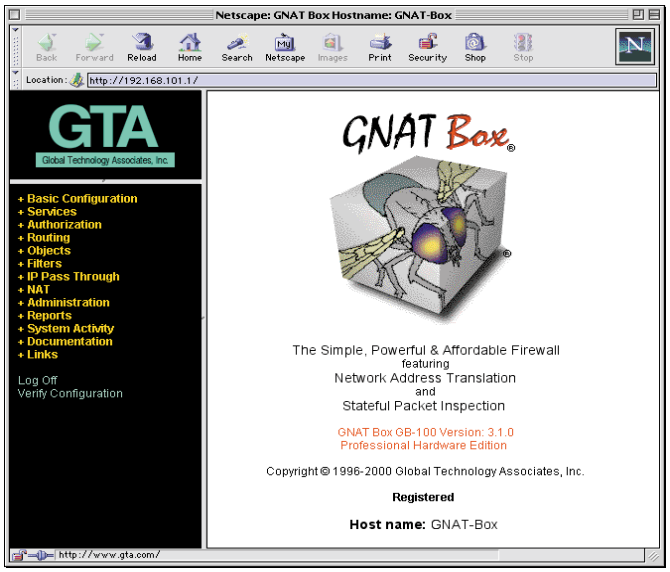
Web Browser Access

By default, access to the GNAT Box Web Browser interface is allowed to any host on the Protected network interface. You will need to modify the default Remote Access filter, which allows access to the Web Browser interface, if you wish to restrict this access.

Caution: *Be careful when opening up access. You do not want to allow arbitrary hosts to access your GNAT Box.*

To access the GNAT Box user interface web server

1. Start a frames capable web browser.
2. Enter the IP address or host name of the GNAT Box's Protected network interface as a URL in the Location: entry field (i.e. http://192.168.1.2/). If your workstation does not have an IP address on the same logical network as the Protected network interface on the GNAT Box system, you will need to adjust the Remote Access filter which controls access. You may need to add a new filter, if adjusting the netmask on the default Web Browser interface filter will not enable access from your workstation.



Web Browser Interface Characteristics

1. All changes made with the Web Browser interface are dynamic and will take effect immediately.
2. Caching is disabled since the configuration data is dynamic.
3. Some delay may be experienced when the server is reading or writing images to/from the floppy diskette.
4. Re-sizing your browser will re-display the main screen.
5. Password authorization is persistent for a session.
6. List oriented data entry forms always display two empty rows for inserting new records, if possible.
7. Blanking out data entry fields in a row of a list oriented form will cause the row to be deleted when the "submit" button is pressed.

8. **The default Admin User ID is initially “**gnatbox**”. The administrator may should change this value.**

Browser Layout

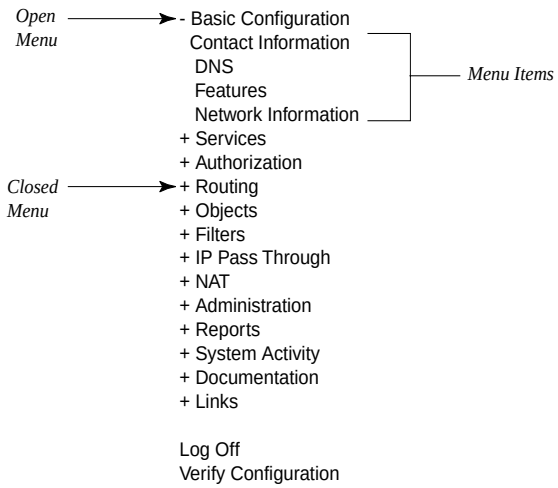
The Web Browser interface uses HTML frames to subdivide the browser’s display area into 3 separate areas:

1. **GTA Logo Hyperlink -** Clicking in this area will take you to GTA’s Home page.
2. **Menu -** Provides direct access to all command functions on the GNAT Box.
3. **Work/Display Area -** In this area, all system data is displayed and worked on.

The Menu

The menu consists of 13 main functional areas: **Basic Configuration**, **Authorization**, **Services, Routing**, **Objects, Filters**, **IP Pass Through**, **NAT**, **Administration**, **Reports**, **System Activity**, **Documentation** and **Links**. Located at the bottom of the menu are two special menu items: **Log Off** and **Verify Configuration**, which when selected with a mouse click will run verification tests on the current system configuration and produce a report with the results.

Each functional area menu item, when selected with a mouse click, will expand to reveal menu items related to the specific functional area. Clicking on the title item again, will collapse the revealed menu.



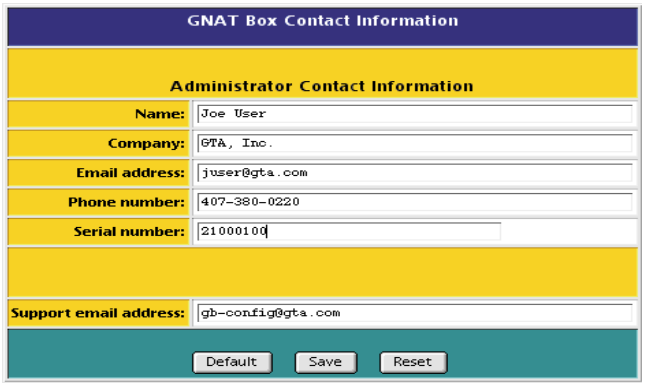
Basic Configuration

The Basic Configuration section consists of the functional areas that are typically required for basic operation and setup of the GNAT Box. Some areas in this section are optional and are not required for operation of the GNAT Box system. The Basic Configuration functional areas are accessed via the Basic Configuration menu item. Clicking on this menu item will toggle the display of the functional area menu items.

Contact Information

The **Contact Information** display provides data entry fields that store contact information and your GNAT Box serial number. This information is used by the "Email Configuration" facility and other reporting functions.

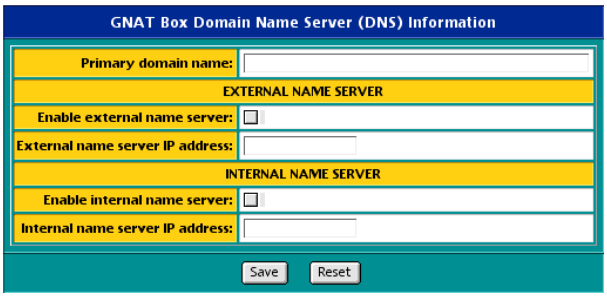
Name - Primary contact name.
Company - The name of your company or organization.
Email address - The email address of the primary contact.
Phone number - The telephone number of the primary contact.
Serial number - Your GNAT Box serial number. This can be found in several different locations: registration card, software box, and on the license certificate. It is important to have your serial number enter correctly since it is used in various validation functions.
Support email address - The email address of your support organization. If you have a support contract, your reseller should provide you with an email address for this field. By default this is "gb-config@gta.com".



DNS

The Domain Name Server configuration dialog provides the user with a means to specify the IP address of a DNS server that will be used to resolve host names to

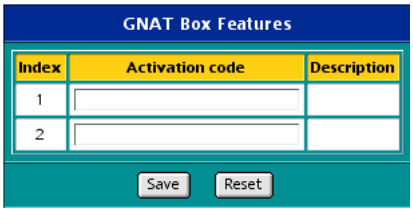
IP addresses. If an internal DNS server is not available, use the IP address of your external DNS server. The **Primary domain name** field is used to specify the DNS domain of the site. If multiple domains are used, simply select the primary DNS domain (i.e. gta.com).



Features

The Features form is where GNAT Box activation codes are entered to enable features on the GNAT Box system. The list displays the activation code and a description of the features.

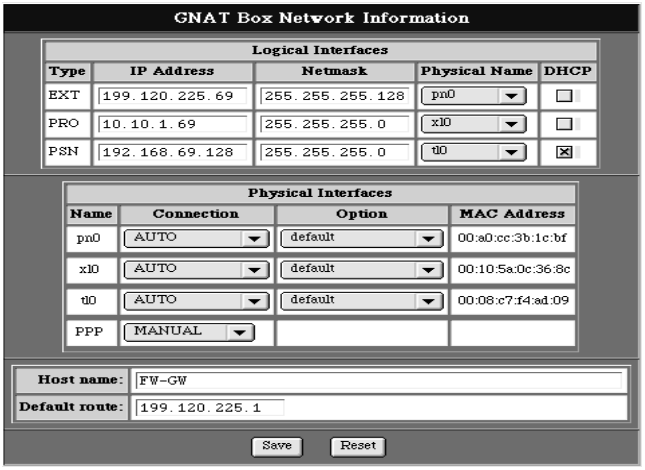
To add a feature enter the activation code you received for the specific feature on an empty row in the "Activation code" field then press the “save” button. If the feature description displayed after pressing the “save” button is displayed as a jumble of characters rather than the specified feature then either the activation code was enter incorrectly or the activation code is not correct for the current GNAT Box system.



Note: *In order for the activation code to function properly the system serial number must have been entered on the Preferences data entry form.*

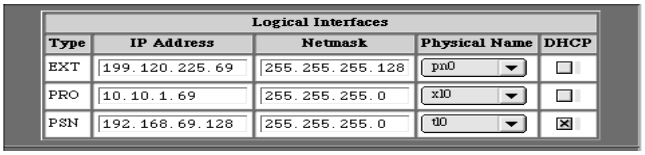
Network Information

The Network Information form allows you to assign IP addresses, netmasks, default route, network interface card options, and associate logical devices with physical devices installed in the system. All supported and detected network interfaces will be listed on the Network Information form.



Logical Interfaces

In the Logical Interfaces section, you assign an IP address, netmask, and a physical device name to each logical interface on your GNAT Box system. If you will not be using a PSN and have not installed a network card, simply leave the PSN data entry fields with their default values.



The **Logical Name** field allows the administrator to name each interface to suit local conventions. By default the Logical Name values are set to the traditional GNAT Box names of: Protected, External and PSN.

Type

The **Type** column lists the possible logical network interface types that are available on the GNAT Box system. There are three logical interfaces types available on a GNAT Box system:

External	External network interface.
Protected	Protected network interface.
PSN	Private Service network interface.

The minimum GNAT Box configuration requires that both an External and

Protected network interface be present and configured. Since the standard GNAT Box system allows only three network interfaces, the remaining network interface typically is assigned the PSN type, however this is not a requirement. It is therefore possible to have two External and one Protected interface or two Protected and one External.

Note: *The* ***GNAT Box Multi-interface option*** *allows a system to utilize up to 16 network interfaces of any supported type.*

IP Address

The IP address of the logical network interface. The IP address is entered in standard “dotted decimal” notation. An IP address must be entered for each active network interface. In the case of a PPP connection, leave this field blank.

Netmask

Each active network interface must have a netmask. The value of the netmask depends on the network the interface will be attached to. Some common netmasks are:

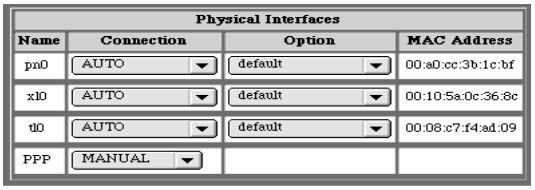
Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

NIC

This field is used to select the physical network Interface (NIC) which will be associated with the logical name. The NIC field is a choice list of the options available. The physical names are dependent on the type of network interface cards that are present in the system. A list of the network device names can be found in the hardware section of this manual. The display of “**???**” means no device assigned. The special case of the **PPP** device is only valid for use on the External network interface.

DHCP

The DHCP (Dynamic Host Configuration Protocol) field when checked, utilizes the DHCP protocol to obtain an IP address for the specified network interface. When the DHCP field is checked, the IP and netmask fields are protected from user input. The assigned DHCP IP address/netmask will be displayed in these protected fields, after assignment. DHCP may be used on all network interfaces. Users of cable modems typically require the use of DHCP on their External network interface.



Physical Interfaces			
Name	Connection	Option	MAC Address
pn0	AUTO	default	00:a0:cc:3b:1c:bf
xl0	AUTO	default	00:10:5a:0c:36:8c
tl0	AUTO	default	00:08:c7:f4:ad:09
PPP	MANUAL		

Network Interface Cards

In the Network Interface Cards section you can select the type of network connection and options for each physical device. The type of connection and options will vary depending on the type and capabilities of each device. Some devices have only a single network connection type and no options. Frequently, a family of network cards will be available in various connection configurations. Some connection types, however, may not be available on a given card although all connection types will appear in the choice list for that device. Common sense should be exercised in these situations (e.g. don't select BNC if your network card only has a UTP interface).

NIC

The NIC column lists the NIC device names of supported and configured network interfaces that have been detected by the GNAT Box system at boot time. A list of NIC device names and the associated NICs can be found in the hardware section of this manual.

Connection

AUTO

The card will auto select the active network connection.

MANUAL

The card will use the network connection configured by the vendor's configuration software or jumper selections.

UTP_10

The card will use the unshielded twisted pair interface at 10Mbps.

BNC_10

The card will use the BNC interface at 10Mbps.

AUI_10

The card will use the AUI interface at 10Mbps.

TX_100

The card will use the unshielded twisted pair interface at

100Mbps.

Default

The card will use the default option setting.

Option

Full Duplex - The card will operate in the full duplex mode.
Half Duplex - The card will operate in the half duplex mode.

MTU

The MTU field provides the administrator the with the ability to adjust the MTU value for each network interface. This is especially useful for a gigabit ethernet interface when jumbo packets are to be utilized. Do not adjust the MTU value unless you fully understand the impact of the adjustment. Incorrect values can cause poor or non performance of the system.

MAC Address

If the physical device is an ethernet card, its MAC address will be displayed in this section. The MAC address, which is usually printed on the circuit board, should be written down prior to installing the board in the target GNAT Box system. The MAC address display is useful in determining which physical card is assigned to a particular logical (EXT, PRO, PSN) interface.

Host Name

This name is used to tag log messages. Although it is not a DNS host name, you can use such a name if desired. For cable modem and xDSL sites you may be assigned a system name which should be placed in this field.

Default Route

The default route is generally the IP address of your router that connects your network to the Internet. The default route is the gateway where any non-local IP packets are sent.
It is important to remember that a default route must always be on the same logical network as one of your network interfaces. The only exception to this default route rule is for a GNAT Box PPP connection. In almost all installations the default route is an IP address on the External network.

Caution: *Since updates are immediate, it is possible that mis-configuring your GNAT Box may result in a system configuration which does not allow remote access.*

PPP

The PPP Configuration form should be used when PPP has been selected as the External network interface on the Network Information form. Basic PPP configuration can only be performed from the console interface. However, complete configuration control is available with the Web Browser interface.

Connections

Select the desired connection type from the pulldown choice list.

The available connection types are:

On-demand

This connection type will initiate and establish a PPP connection (if the link is down) with the remote site, whenever a packet arrives on the Protected or PSN interfaces and is destined for the External network. The PPP link will stay up as long as packets are received before the specified time-out period has expired.

On-enabled

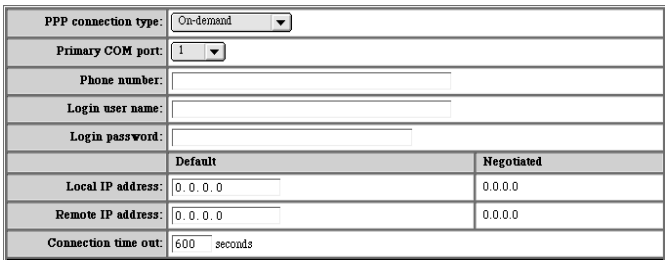
This type of connection requires the GNAT Box administrator to manually enable the External network interface, which will then initiate a PPP session and establish a link with the remote site. The External network interface may be enabled either from the Interfaces option under the Admin menu on the Console interface, or from the Interfaces menu item on the web browser admin interface. The PPP link will stay established until manually disabled by the GNAT Box administrator.

Dedicated

This type of connection means that a PPP link will be established when the GNAT Box system boots up. The PPP link will remain up until the GNAT Box administrator manually disables the interface, or the system is halted.

Primary COM Port

Select the COM port which will be used for the PPP interface. COM ports 1-4 are allowed. The COM port may be an internal modem card or a serial interface.



Phone Number

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

Login User Name & Password

Enter the user id used for remote PPP access. This is the user id issued by the remote site. The password is obscured in the data entry field. If the remote system uses CHAP or PAP, the Login User Name and Password fields are typically left empty.

Local & Remote IP Addresses

A PPP link uses two IP addresses: one is local and the other is remote. The GNAT Box PPP facility has the capability to negotiate the local and remote address dynamically, if the remote site supports dynamic address assignment (generally the default for most ISPs and remote sites). Dedicated IP addresses are supported for either. Pressing the Save button will commit the data on the Network Information screen to the floppy diskette and apply any changes immediately.

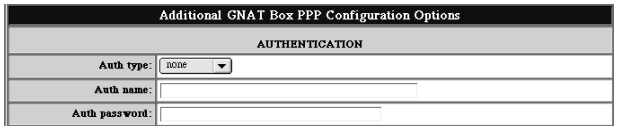
If your remote site uses dynamic address assignment, use the following configuration:

1. Leave the Local IP number set to 0.0.0.0; the default.
2. In the Remote IP number field enter an IP address that may be assigned dynamically. It is not important whether the specified IP number will actually be assigned, since this value will be negotiated. The PPP protocol, however, requires that an IP address be used that resides on the remote network. Very often a good choice for this number is the remote system’s router IP address or DNS server IP address.

If you have a dedicated Local and/or Remote IP address, enter the applicable dedicated addresses in the appropriate fields. If you have a dedicated Local IP address, but the Remote side is dynamic, use the technique described in Dynamic Address Assignment for the Remote IP address. If your Remote IP address is static, simply leave the Local IP number set to: 0.0.0.0.

Connection Timeout
Sets the number of seconds of inactivity that the PPP link should wait before taking down the connection. Setting the time out value to zero indicates that no time out should be used.

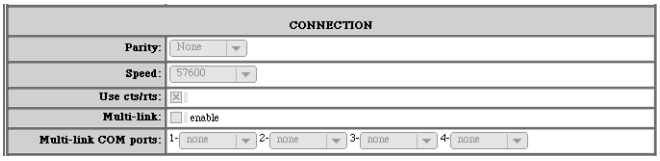
Authentication



Auth Type
Default value is: **None**. This option allows the authentication protocols of **PAP** and **CHAP** to be enabled.

When the Authentication Type is set to **None**, this field is ignored. Enter the authentication name or id for the selected authentication protocol in this field.

Connection



Parity
None, Odd or Even

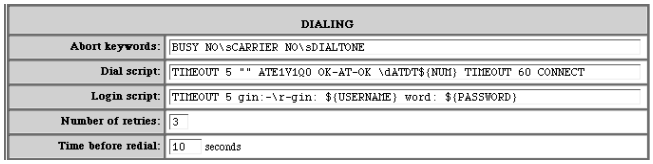
Modem Speed
DTE speed
1200, 2400, 9600, 19200, 38400, 57600, 76800, 115200

CTS/RTS

CTS/RTS handshaking is enabled by default.

Multi-Link

Select this checkbox if you will be using Multi-link PPP. Then select the COM ports that will be used in this configuration.



DIALING	
Abort keywords:	BUSY NO\sCARRIER NO\sDIALTONE
Dial script:	TIMEOUT 5 "" ATE1V1Q0 OK-AT-OK \dATDT${NUM} TIMEOUT 60 CONNECT
Login script:	TIMEOUT 5 gin:-\r-gin: ${USERNAME} word: ${PASSWORD}
Number of retries:	3
Time before redial:	10 seconds

Abort Keywords

Many modems will report the status of the call as a string. These strings may be **CONNECTED** or **NO CARRIER** or **BUSY**. It is often desirable to terminate the script should the modem fail to connect to the remote. The difficulty is that a script would not know exactly which modem string it may receive. On one attempt, it may receive **BUSY** while the next time it may receive **NO CARRIER**. These “abort” strings may be specified in the Abort keywords data entry field. The keywords should be entered with a space separating each word. For abort strings that have embedded spaces, use the escape character “\s” to represent the space.

Example: BUSY NO\sCARRIER ERROR

If the chat facility receives any of the Abort strings, the chat session will terminate.

Dial Script

The default dial script tends to work for most configurations. Make adjustments for your modem and local telephone configuration. The Dial script’s purpose is to instruct the modem to dial the remote ppp server. Initialization of the modem and any special configuration should be done in this script.

The default **Dial Script** is:

```
TIMEOUT 5 “” ATE1V1Q0 OK-AT-OK \dATDT${NUM} TIMEOUT 60 CONNECT
```

The script sets up a 5 second time-out, expects nothing, then sets the modem to echo mode and response codes returned. An expect string of "OK" should be returned. If not, an "AT" command is sent and an expect string of "OK" should be returned. Next, the script will delay 1/10th of a second then dial the telephone number using the telephone number token ${NUM} with tone dialing. The timeout is increased to 60 seconds and the expect string should be "CONNECT". If the script receives the expect string, the chat facility begins processing the Login Script. See the discussion about chat scripts for further information.

Login Script

The Login Script provides the script used to communicate with the remote PPP server login facility. The Login Script uses the same grammar and rules as the Dial Script. The tokens ${USERNAME} and ${PASSWORD} are provided for use in the Login script. The default GNAT Box Login script is listed below.

This login script is typical:

```
TIMEOUT 5 gin:-BREAK-gin: ${USERNAME} word: ${PASSWORD}
```

See Appendix A for more information about creating a Login Script.

Number of Retries

Default is 3. This is the number of attempts the system will make before giving up on the establishment of a connection. After failure, any new packets arriving for the external network will restart a new dialing attempt.

Time Before Redial

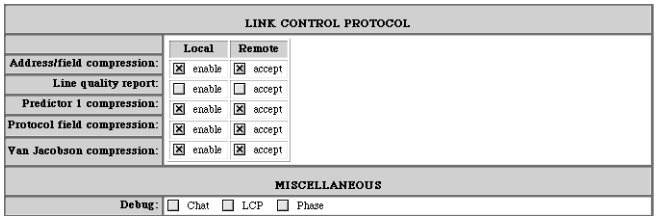
Default is 10 seconds. This is the amount of time to wait before retrying after a failure.

Link Control Protocol

This section allows for the specification of Link Control Protocol (LCP) options. In most cases the default settings work just fine, but for some remote access devices certain LCP values may need to be changed. There are two settings for each available LCP option: one for the local side and the other for the remote side of the connection. If the local side option is set to enable, the GNAT Box will request that the remote side use the selected LCP option. If enable is not set, no request will be made from the local side. If the remote side option of accept is set, then the local side will "accept" the option if offered by the remote side.

Available LCP Options

Address and Field Compression
Line Quality Report
Predictor 1 Compression
Protocol Field Compression
Van Jacobson Compression



If you are unsure which option to set, simply use the default values and enable the LCP debug option. When a PPP session is attempted, you can then monitor the LCP debug output on the primary console (ALT-F1). As the LCP conversation proceeds watch for which options are rejected and requested, and set your LCP options to match the request.

Debug

These options, when enabled, provide helpful information when a PPP configuration is initially created. There are three debug options:

Chat

Displays the dialing and login chat script conversations. This option is very helpful in defining and configuring chat scripts.

LCP

Displays the LCP conversation between the remote and local side of the PPP connection. Use this debug option to help select the appropriate LCP options.

Phase

Displays the network phase conversation. This debug output can be useful in determining the specification of both the Local and Remote IP addresses.

Chat Scripting

See Appendix A for a detailed discussion of chat scripting.

Services

The Services menu consists of those functions that provide services. These include the two built-in servers: DHCP Server and DNS Server, the Email Proxy and the Remote Logging facility. All of these services are optional, as they do not have to be operational in order for the GNAT Box system to function. However the use of a service such as the Email Proxy can add to the security of your GNAT Box system, (it is highly recommended that you run the Email Proxy).

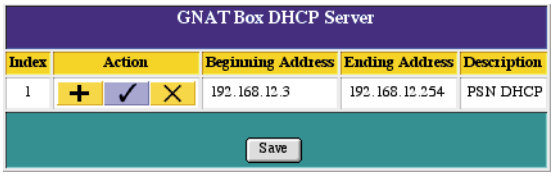
Servers
DHCP Server
DNS Server
Email Proxy
Remote Logging

Services Menu

DHCP Server

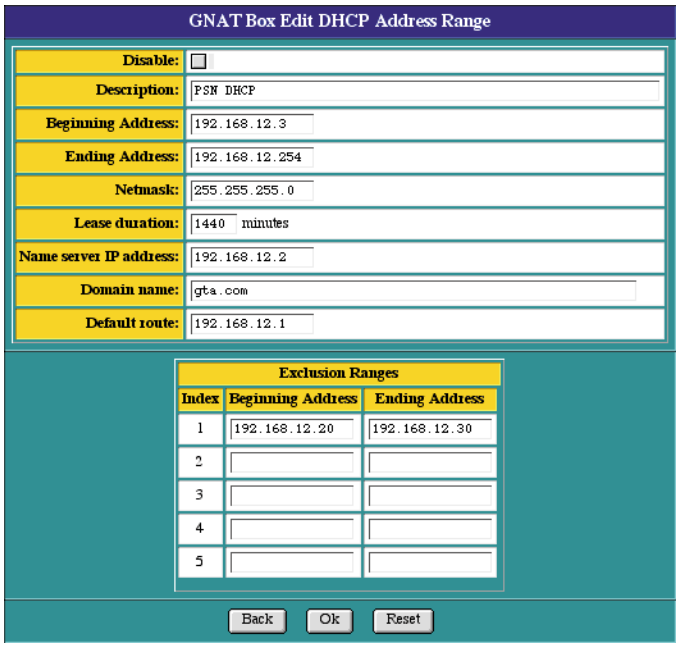
DHCP, Dynamic Host Configuration Protocol, automates the process of assigning IP addresses to host systems on locally attached networks. Additionally DNS server and default route can be provided by the DHCP server. The DHCP server manages a range of IP addresses (i.e. 10.10.10.4 - 10.10.10.254) which can be assigned to clients. The address ranges do not need to be contiguous. Non-contiguous ranges are defined using exclusion ranges. An exclusion range defines a range of IP addresses that should not be assigned from the pool of IP addresses.

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 always reassign the same IP address. The only time it will not reassign the same IP address, is when the number of clients exceeds the number of addresses in the pool and the previous IP address was assigned to a different host.



Selecting the DHCP Server from the menu will display a summary list of current DHCP address ranges. The DHCP server can serve clients located on any attached network interface (Protected, PSN or External). The DHCP server may

serve clients on any logically connected network, (e.g. a network interface is aliased on to multiple networks). The DHCP summary screen operates in the same manner as other GNAT Box system web browser list displays, ("+" to add an item, "x" to delete an item and check to edit an item). All additions, changes and deletions are not effective until the "Save" button is clicked. The DHCP server will start up when the "Save" button is clicked if any of the DHCP server address ranges are marked enabled and the server is enabled.



DHCP Address Range Setup Screen

This screen allows the administrator to define the begining and ending IP address of the address range. Up to 5 exclusion ranges can be defined. Each exclusion range defines an inclusive range of IP addresses that are to be excluded from the range defined by the begininng and ending IP address. The DNS server and default route that DHCP clients should use cal also be configured on the screen.

Disable

Select this box to disable the currently displayed DHCP address range.

Deselect it to enable the currently displayed address range.

Description
This is a brief description of the current DHCP address range.

Beginning Address
This is the first IP, of a block of IP's, that will be assigned.

Ending Address
This is the last IP, of a block of IP's, that iwll be assigned.

Netmask
This is the netmask to assign to DHCP clients.

Lease Duration
This is the maximum time that the DHCP address is valid for a requesting client to use. A client must negotiate to reuse the assigned address before the end of the least time or quit using the address.

Name Server IP Address
This is the IP address of a DNS server that will issued to the requesting client. This IP can be any valid DNS server. It can be that of a local DNS server (such as the built-in GNAT Box DNS server) or a server that is remote from the local area network, (e.g. located at an ISP).

Domain Name
This is a DNS domain name. It typically is that of the local network.

Default Route
The value is the IP address that the requesting clients will use for their default route, (gateway). For hosts located behind a GNAT Box system, (on Protected or PSN networks) this value will be the IP address of the GNAT Box NIC where the network is attached, (i.e. if the client is located on the Protected network then the Default route will be the Protected NICs' IP address).

Note: *If the DHCP service is for an External network then the default route would most likely be the Internet router's IP address.*

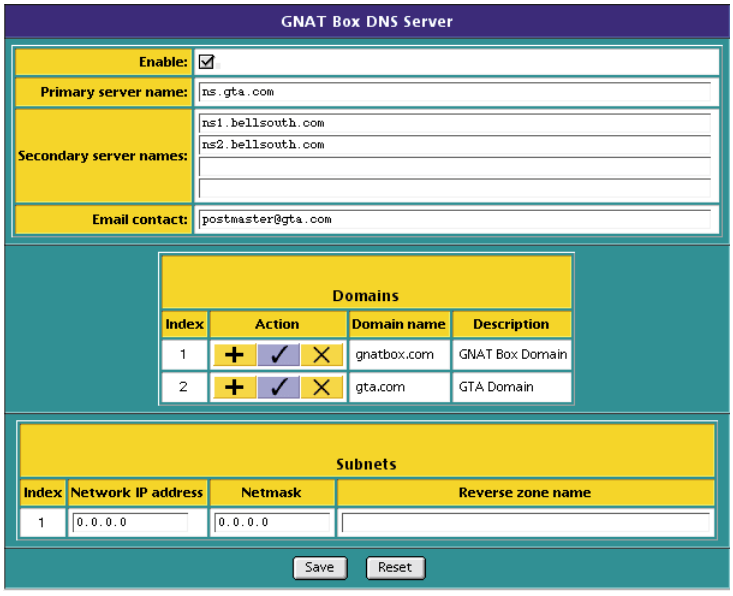
Exclusion Ranges

Define up to 5 inclusive ranges of addresses to exclude from being assigned. To exclude a single IP, enter the IP address to be excluded in both the beginning and ending address fields.

DNS Server

The GNAT Box DNS (Domain Name Server) server functions as a primary domain name server, (functionality as a secondary DNS server is not supported). Before configuring the DNS server you should have an understanding of how the domain name system functions on the Internet. A good reference book about DNS is: **DNS and Bind** 3rd edition by Paul Albitz & Cricket Liu, published by O'Reilly and Associates.

The configuration and operation of a DNS server can range from simple to complex. The built-in DNS server in the GNAT Box system provides a great deal of functionality and flexibity, however it can not be configured to support every possible configuration or option available in DNS. It however does address the needs of most GNAT Box system users. If your site requires DNS services that require complex configurations, or hosting secondary name services then the built-in DNS server will probably not meet your requirements. It is suggested that with such requirements your site would be better served by a DNS server hosted on a separte host.



Enable
If this checkbox is selected the the DNS server will start up/re-start when the "Save" buton is clicked. To halt and disable the DNS server de-select the checkbox and click "Save."

Primary Server Name
The hostname of your DNS server. This will be a host name assigned to your GNAT Box (if you are configuring a external DNS server then this will be the host name seen from the Internet side). The host name should be listed as a host in the domain defintion section.

Secondary Server name
These are the host names of DNS servers that will be acting as secondary servers for the domain. Up to four secondary name servers may be listed.

E-mail Contact
This field should contain the e-mail address of the primary contact for the domain. (i.e. administrator@gta.com).

Domains
This is a summary list of the domains that are configured for the built-in DNS server. They are listed from top to bottom in the order that they were entered, and they are color coded for easy active/disabled reference. If the background of the box is white, the current DNS entry is enabled, and if the background is grey, the configuration is disabled.

The domain summary list operates in the same manner as other summary lists on the the GNAT Box system. Click the "+" to add a new domain, click the "X" to delete a domain and click the check mark to edit a domain.

Subnets
For most domains this section is not required and can remain empty. However if your domain falls into the special case situation of having a subnet rather than a full network assigned to your domain you will need to use this section.

DNS subnets provide a way for splitting up a network into a series of contiguous same size address ranges. These are commonly used to help with performance and managability of large networks. The IP Address and Netmask fields are used to identify the subnet desired.

Network IP Address
This field should contain the network address of the subnet, (i.e. 199.120.225.128).

Netmask
Each subnet must have a netmask. The value of the netmask is dependent on the subnet they will be associated with. Some common netmasks are:

Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

Reverse Zone Name
Reverse Zone Name is the optional zone name used for reverse name address resolution (i.e addeess to name). The GNAT Box can automatically determine the zone name if the subnet uses a Class A, B or C netmask. Normally if needed, reverse zone names are assigned to you by your ISP. For the network 199.120.225.128 with netmask 255.255.255.128 the reverse zone name might be:
128/25.225.120.199.in-addr.arpa.

Domain Name Edit Form
This data entry form is displayed when you either add or edit an entry in the domain name summary list. This form is used to define host names and their associated IP addresses (A records) , aliases (CNAME records) mail exchangers (MX records) for the selected domain zone.

Disable
When this checkbox is selected the domain definition is disabled and the zone will not be served by the GNAT Box name server. You must click the “OK” button to affect this change. De-selecting the checkbox and clicking “OK” will make the zone available to be served by the GNAT Box name server.

Description
This field should contain a brief description of the domain for your reference.

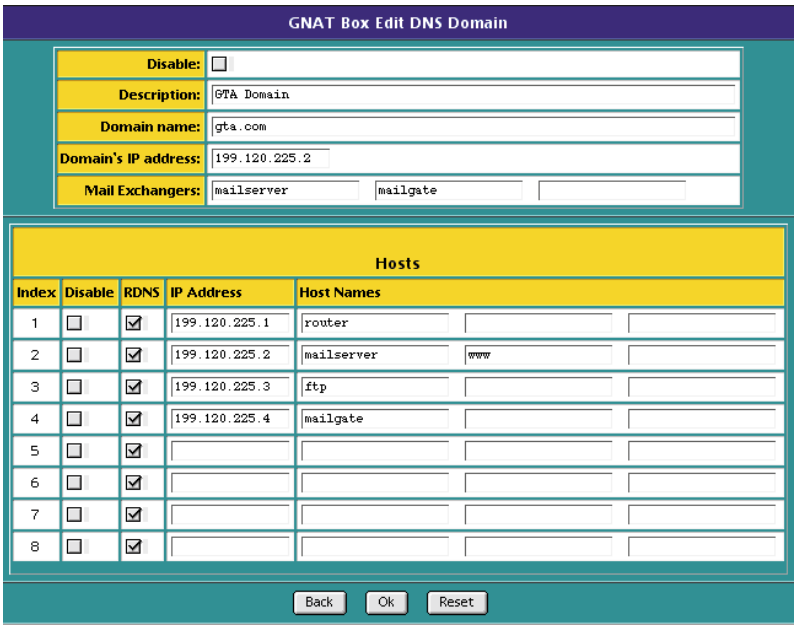
Domain name
This is the DNS domain name for the current zone defintion, (i.e. gnatbox.com).

Domain IP address

Often it is a good idea to have a host (A record) in your zone that has the same name as the zone. (i.e. gnatbox.com). This means that, for example, if you have a web server a visitor can simply use the zone name rather than the fully qualified host name for the the web server. Enter the IP address of a host that you would like to response to the zone name.

Mail Exchangers

When a remote system sends mail to this domain, it will query a DNS server to determine what IP addresses are designated to accept email for the zone. The Mail Exchanger fields define the mail server(s) for the domain. When there is more than one Mail Exhanger for the zone, they are graded in order of preference. The desired order of preference is specified by entering the most perferred server in the first field, followed by a second and third entry. Very often there is only one Mail Exchanger for a zone, so the second and third fields are not required. The first mail exchanger will receive a priority of 5, the second 10 and the third 15.



Hosts
The Hosts section is where host names and IP address associations are defined.
Disable
If this checkbox is selected the entry will not be included in the zone defintion.

RDNS
If this checkbox is selected then a reverse record will be created for this host in the zone's reverse database (IP address to host names). Typically this item should always be checked. A DNS server provides IP and hostname information which can be looked up either by the hostname (which will return the IP address) or by the IP address (which will return the hostname). The RDNS or Reverse Domain Name Service provides IP address to hostname information.

IP Address
This field contains the IP address for the host names defined in the row.

Host Names
These are the host names that are associated with the IP address defined for the row. The first hostname is the real host name (A record) with the additional host names in the row being aliases (CNAME records). Up to three hostnames can be entered in a single row. If additional names need to be associated with a single IP address, the IP address should be repeated in another row. All subsequent hostnames for that IP address will be considered aliases (CNAME records) including the first entry.

Email Proxy
The Email Proxy dialog is used to configure the GNAT Box Email Proxy. The Email Proxy is an SMTP (TCP/25) proxy which is used to proxy inbound email connections. The Email proxy will answer on any IP address assigned to the External NIC, unless there is a tunnel created on port 25/TCP which will then override the proxy startup on the IP address in question. The GNAT Box email proxy shields your internal email server from unauthorized access attempts through SMTP exploits. The GNAT Box email proxy also provides facilities to reduce and possibly eliminate unsolicited email (known as "SPAM").

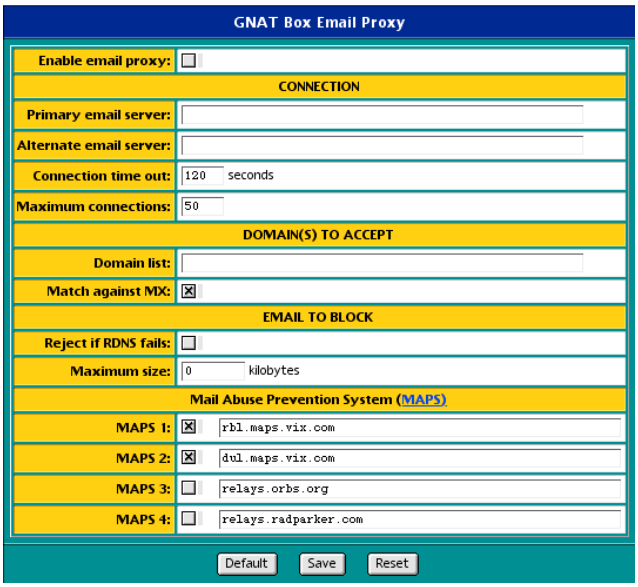
Enable Email Proxy
Select this checkbox to enable the email proxy. Deselect it to disable the email proxy.

Connection

This section is where the administrator enters data for parameters that are involved with the email proxy connection.

Primary Email Server

This field should contain the host name (if you are using an internal DNS server) or IP address of your email server. The primary email server must reside either on the PSN or the Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.



Secondary Email Server

This field should contain the host name (if you are using an internal DNS server) or IP address of a backup or secondary email server, if you have one. The secondary email server must reside either on the PSN or the Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.

Connection Timeout

The time value is the number of seconds to wait between each SMTP command exchange.

Maximum Connections
This parameter is the maximum number of simultaneous SMTP connections you wish to run on the GNAT Box. If additional connections are attempted once this maximum limit has been reached, the additional connections will be deferred, until a connection slot becomes available. Each simultaneous connection invokes a copy of the SMTP proxy program.

Domain(s) to Accept
The GNAT Box Email Proxy will only accept SMTP connections for specific domains. The domains are explicitly specified manually in the Domain list and/or rely on the DNS MX records that are assigned to the IP Address(es) on the External NIC of the GNAT Box.

Domain List
Enter your primary and any additional email domains which you wish to accept email. The domains should be separated by a whitespace (blank, tab), or a comma. This field may be used in conjunction with the MX (DNS Mail Exchanger Record) match option. This facility prevents your site from being used to relay email to other sites.

Match Against MX
If this item is enabled, the GNAT Box Email proxy will make a DNS MX record query to determine if the domain(s) assigned to the IP Address on which the proxy answered matches the domain in the “To:” portion of the email header. If there is no match, the email is rejected. This facility prevents your site from being used to relay email to other sites.

Email to Block
This section enables the administrator to impose additional controls over inbound SMTP connections.

Reject if RDNS Fails
If this item is enabled, the GNAT Box Email proxy will perform a reverse DNS lookup on the IP address of the remote host attempting to make the SMTP connection. A DNS lookup is then performed on the returned host name to see if it matches the IP address of the remote host. If these lookups fail or don’t match, the connection is refused. This facility imposes a stringent requirement on all hosts wishing to deliver email to an address in your domain. Although all hosts on the Internet should be correctly defined in DNS, many sites have improper or mis-configured DNS entries. If you

chose to enable this facility, legitimate hosts with incorrectly defined DNS entries will not be able to deliver email to your domain.

Note: *If a DNS server has not been defined in the DNS configuration section, this facility will not function correctly.*

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

Mail Abuse Prevention System - MAPS
The Mail Abuse Prevention System (MAPS) - Realtime Blackhole List (RBL) is a list that consists of hosts and domains that have been documented as transmitting and/or generating unsolicited email (SPAM).

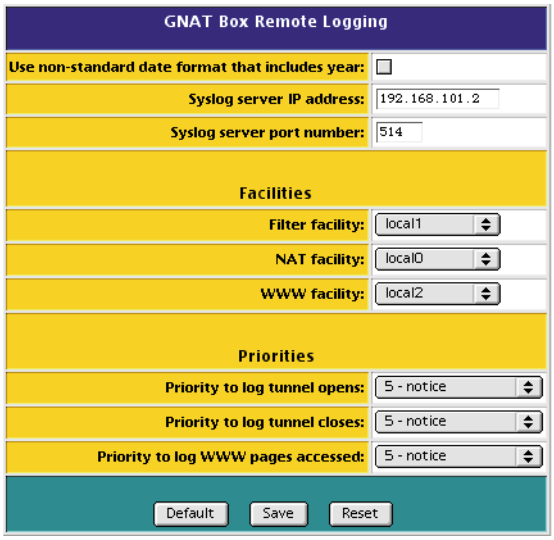
MAPS1, MAPS2, MAPS3, MAPS4
The four MAPS data entry fields provide the administrator to selectively enable specific MAPS servers to be utilized to block email from known SPAM sites (sites that send bulk unsolicited email). The administrator may replace the provided MAPS sites with other sites if desired.
Currently the primary site is: "rbl.maps.vix.com". More sites should soon be available at other locations around the world. Please check the RBL website: **http://www.maps.vix.com** for updated site information.

Remote Logging
The Remote Logging data entry form provides a means to configure how and where log information is sent. The GNAT Box system uses the syslog TCP/IP protocol for recording logs remotely. The syslog service is a standard Unix service, however, a server for use under Windows NT or Windows95/ 98 is provided with the GNAT Box installation.

If you wish to enable remote logging, simply enter the IP address of the host system that will receive the syslog data. Changing the IP address requires a system reboot, before the change becomes effective.

No changes will be saved unless you click on "Save" before exiting this menu.

Note: *Enabled log events are always displayed on the main system console (ALT-F1), regardless if you have remote logging enabled or not.*



Use non-standard date format that includes year
If this option is checked a non-standard date format will be used in the log in place of the standard syslog date/time format. The non-standard date/time log format provides 3rd party log clients and analysis programs a date/time stamp that is complete and easier to parse.

Standard syslog date/time format: **MMM dd hh:mm:ss**
MMM - three character month
dd - day
hh - hou
mm - minutes
ss - seconds
Example: Aug 20 19:21:28

Non-standard date/time format: **MM/DD/CCYY hh:mm:ss**
MM - 2 digit month
DD - 2 digit day
CC - 2 digit century
YY - 2 digit year
Example: 08/20/2000 19:21:52

Syslog server IP address
This is the location of the Syslog server that you wish to have your GNAT Box send the logs to. Leaveing this blank will disable Remote Logging.

Syslog Server Port number
This is the port number of the Syslog server that you wish to have your GNAT Box send the logs to. (by default Syslog runs on port 514).

Facility
Facilities will allow you to control what is or is not logged. The Filter, NAT, and WWW facilies are the three most general facilities that one would use, and you can control them by selecting the proper options under the drop down menus. If for any reason you wish not to log one of these facilities, just select none from the drop down menus, and it will be disabled.

Filter Facility
The **Filter facility** list contains all the standard Unix syslog facilities, some of which have no context for the GNAT Box. However, all of the facilities are available to use. The Filter Facility is the syslog stream which logs information associated with any filter that has logging enabled. Additionally, the default logging configuration is set to log any rejected packets to this log stream. Any attempts at unauthorized access will be logged to the Filter Facility log stream. This facility may be disabled by selecting "none" in the choice list.

NAT Facility
The **NAT facility** list is the same list used by the Filter Facility field. The NAT facility is the syslog stream which logs information associated with any network address translation. Network connections that will logged to the NAT facility are all outbound connections that have NAT applied and all inbound connections on GNAT Box Tunnels. Selecting "none" will disable the remote logging of NAT packets.

WWW Facility
The **WWW facility** list is the same list used by the Filter facility field. The WWW facility is the syslog stream that logs all URLs which are accessed through the GNAT Box system. Selecting "none" will disable the remote logging of URL information.

Tunnel Opens and Closes

Both of the **Priority to log tunnel** lists contain all the standard Unix syslog priorities, some of which have no context for the GNAT Box. However, all of the priorities are available to use. Whenever a network connection is initiated, an “open” log record will be generated. If you wish to log these “open”, then select a priority other than “**none**.” A “close” record will be generated when a network connection is terminated. In addition to the standard log information, “close” records contain the number of packets and bytes sent and received. To disable the generation of remote “close” log records, set the priority to “**none**.”

Priority to Log WWW Pages Accessed

The list contain all the standard Unix syslog priorities, some of which have no context for the GNAT Box. However, all of the priorities are available to use. Whenever a web page connection is initiated, a WWW log record will be generated with the URL accessed in the log message. If you wish to log these web accesses, then select a priority other than “**none**.” To disable the generation of remote WWW log records, set the priority to “**none**.”

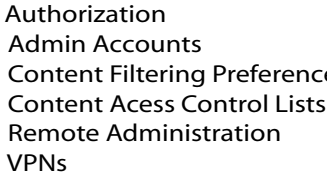
Other Log Data

All other log data is sent to the “daemon” facility. This data includes:

- Audit trails of all modifications made to the GNAT Box system.
- Remote administration access from either the web browser or GBAdmin.
- Console administration access.
- Startup messages.
- System warning and diagnostic messages.
- Proxy module messages.

Authorization

The Authorization menu consists of those functional areas that address authorization for administration, remote management, inbound email, and user web access.



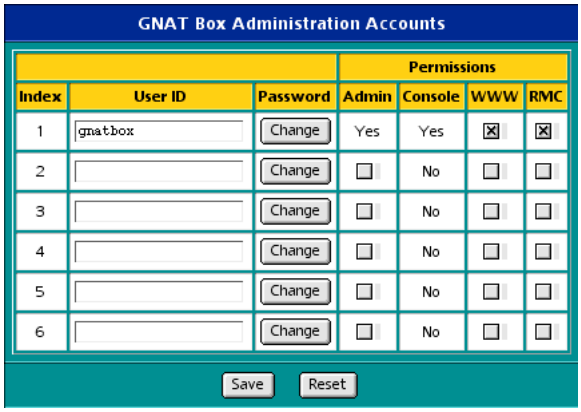
Authorization Menu

Admin Accounts

The Administration Accounts section provides a means to manage the administration accounts that are used to access the GNAT Box system. Up to five (5) additional administration accounts can be defined. Each additional account is assigned a unique User ID, password, and access privileges. The default administration account has a default user ID of "gnatbox", which may be changed using this interface. The primary administration account ("gnatbox") is the only account that can log in on the GNAT Box console. Except this capability, all other privileges can be assigned to other accounts.

User ID

This is the administration account name which is used to logon to the GNAT Box system. It may be up to 39 characters long. Any characters that can be generated from the keyboard are valid. Leading and trailing spaces, however, are not valid.



Password

The password may be up to 39 characters long. Any characters that can be generated from the keyboard are valid. However, leading and trailing spaces are not valid.

Admin

If enabled, the admin account has update authority.

Console

If enabled, the admin account can login on the console.

WWW

If enabled, the admin account can login via the web browser interface.

RMC

If enabled, the admin account can login via the Win95/98/NT remote management console (GBAdmin).

To Add an Account

1. In an empty row enter a User ID you wish to use for the new admin account.
2. Select the options that are to be enabled for the new account
3. Click the Change button in the Password column to display the password dialog box.
4. Complete the password dialog window to create a password for the new account.
5. Save.

To Delete an Account

1. Clear out the User ID field(s) you wish to delete.
2. Save.

Content Filtering

Content Filtering provides the administrator with the ability to control web site access based on the content of the web site. The GNAT Box system provides two methods for web site access control. The first facility is the CyberNOT list, which is a built-in content filtering facility running directly on the GNAT Box system. The second facility is the Websense content filtering system, which runs on a separate server.

CyberNOT List

The CyberNOT list is a built-in GNAT Box facility. In order to use this facility you are required to purchase an annual subscription. Once you purchase the subscription you will receive an activation code to enable the facility on your GNAT Box system.

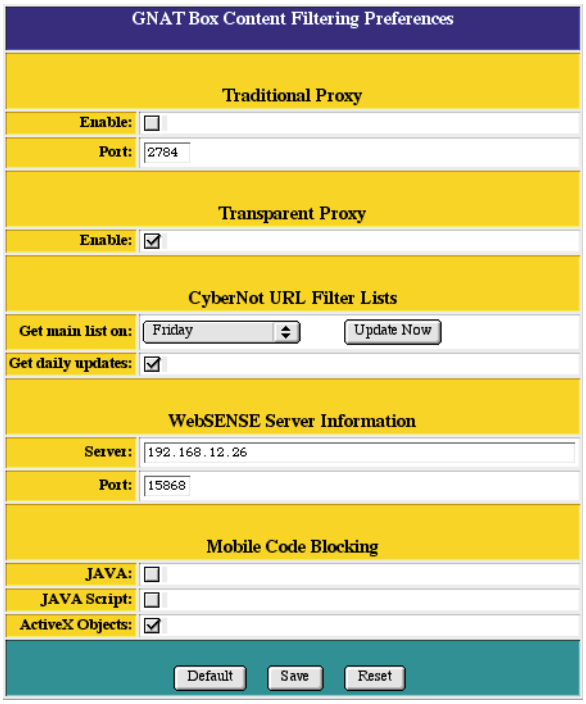
Websense

Websense is a content filtering system that runs on a remote server (NT or Solaris). A Websense license subscription must first be purchased and installed on a remote server before you can use it with GNAT Box. You

should install and configure your Websense server prior to setting any options for it on the GNAT Box system.

Content Filtering Preferences

Content Filtering Preferences form provides the administrator a means to specify the access control facility (if any) and which proxy mechanism to use with the access control facility. This form also allows the administrator to schedule when the CyberNOT list will be updated.



Traditional Proxy

This method requires all users located on the Protected network to configure their browsers for a proxy. All URL requests will be directed to the designated proxy.

1. **Enable.** Make sure the Enabled Traditional Proxy is checked.

2. **Set the Proxy Port.** When the GNAT Box is operating without a content filtering mechanism enabled, it does not use a proxy mechanism. However,

when the GNAT Box http proxy is used in conjunction with a content filtering facility (CyberNOT or Websense) it runs on TCP port 2784 by default. If the user wishes to run the http proxy on a different port, enter the value in the Port field at the top of the dialog box. This proxy port is the port number users should set their web browsers to for use with the GNAT Box content filtering configuration.

Websense

1. If you are using the Websense OpenServer enter the IP address in the Server field, under the Websense Server Information section.

2. If you are using the Websense Openserver set the port number used by the Websense server. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the WebSense Port field.

CyberNOT

No additional server configuration is required for the CyberNOT facility since it runs directly on the GNAT Box system.

Note: *Users should set the proxy IP address to that of the GNAT Boxes' Protected network interface IP address, (this is the same address users should have as their Gateway/default route).*

Transparent Proxy

This method is transparent to users located on the Protected network; no modification to a browser is required.

1. **Enable** - Select the Enabled checkbox for the Transparent Proxy.

Websense

1. If you are using the Websense OpenServer enter the IP address in the Server field, under the Websense Server Information section.

2. If you are using the Websense Openserver set the port number used by the Websense server. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the WebSense Port field.

CyberNOT
No additional server configuration is required for the CyberNOT facility since it runs directly on the GNAT Box system.

CyberNOT URL Filter List
Either manual or automatic updates for the CyberNOT URL Filter List may be done through this section. To manually update CyberNOT's URL Filter List simply click the "Update Now" button. Automatic updating takes place daily on the day specified from Sunday through Saturday.

Get main list on - Valid selections are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday, which will specify the day to perform automatic updates.

Get Daily Updates - To enable automatic updates of the CyberNOT URL Filter List make sure this checkbox is selected.

Update Now - Manually begin the update process of the CyberNOT URL Filter List. This facility only functions if you have installed an activation code for the CyberNOT subscription.

Note: Make sure you have defined a DNS server in the DNS section under Basic Configuration, as the system needs to lookup and access the CyberNOT List server.

WebSENSE Service Information
This section only needs to be completed if you are using the Websense server facility.
Server - Either the DNS Name or IP Address of the Websense server should be entered in this field to use the Websense URL filtering.

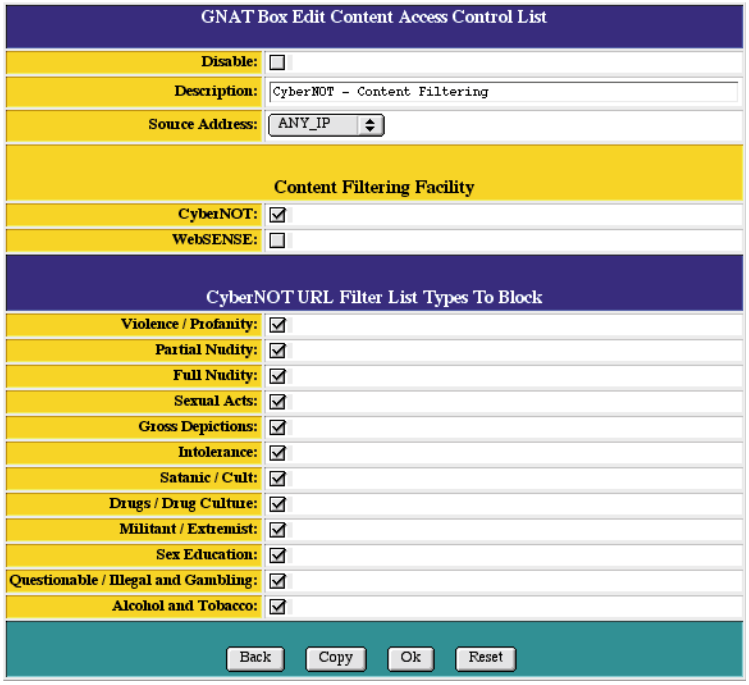
Port - The port the WebSENSE server listens to for URL filtering requests. The default this port is 15868.

Mobile Code Blocking
The GNAT Boxes' built-in facility to block mobile code (i.e. JAVA, JAVA Script, and ActiveX) may block any combinations of these three, which appear in the inbound HTML streams on TCP port 80, 8000, and 8080.

Content Access Control Lists

The Content Access Control Lists provides a means to specify how the selected web access control facility (CyberNOT or Websense) will be applied to web requests. The Content Access Control Lists consists of one or more definitions of groups of IP addresses and how the content filtering facility will be applied to them.

When the Content Access Control List menu item is selected a summary list of all access control lists will be displayed. Each row summarizes a specific access control list, with the source address group and description of the list displayed. This lists functions in the same manner as the filter lists with the up and down arrows providing insertion above and below, “X” to delete an entry and the check mark to edit an entry. The access control list is processed sequentially, so order is important. Any changes, deletetions or additions to the list will be applied only after the “Save” button is pressed.



Edit Content Access Control List

Disable
If this checkbox is selected then the access control list will be disabled and not used for access control filtering.

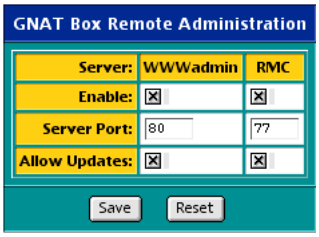
Description
This field should contain a description of the access control list.

Source Address
This entry must be a IP Address object. Only defined IP Address objects will be listed in the pull down. The IP Address object selected for this field will be used to match against web requests. If web request matches an element of the specified IP Address object then the specified content filtering facility will be used to process the packet.

Content Filtering Facility
CyberNOT - if this item is checked then the packet will be processed against the CyberNOT list.
WebSense - if this item is checked then the packet will be processed by the Websense server.

CyberNOT URL Filter Lists Types to Block
If CyberNOT was selected then the categories selected in this section will be used to filter the web request.

Remote Administration
The **Remote Administration** menu item displays the Remote Administration dialog window, which provides a means to control if and how remote administration, via the Web Browser interface and the Remote Management Console (GBAdmin), of the GNAT Box will be provided. The default settings enable remote administration and the ability to apply updates, with the Web Browser interface being served on the standard TCP port 80 and the RMC interface on TCP port 77.



WWW Admin

This section controls if and how access will be allowed via the web browser interface.

Enable

Select this checkbox to enable remote administration via the web browser interface.

Server Port

The default port the web browser interface is served on is port 80. If you wish to change this, enter the new port number and make sure to change the Remote Access filter associated with remote administration to match the port number. Although port 80 is the standard for http, it is suggested that an alternative port number (8000 or 8080 are good choices) is utilized. The reason for moving the web administration port is that possible mis-configuration of the Remote Access filters could expose the remote web browser interface to unauthorized users.

How to Change the Server Port

If you decide to change the port number for the web browser interface you should implement this change in the following order:

1. Find the Remote Access filter that controls access via the web browser interface and add the new port you wish to use to the destination port list. Do not remove port 80 yet. Save the filter and the filter set.

2. On the Remote Access configuration, screen change the port number to the new port value. Save your changes.

3. Find the Remote Access filter that allows access via the web browser interface and delete port 80 from the destination port list, leaving only the new port value you have chosen. Save the filter and the filter set.

Allow Updates
Updates are allowed by default. If you wish to disallow remote updates via the web browser interface, deselect this checkbox.

Remote Management Console
The Remote Management Console (RMC) establishes an encrypted network connection to the GNAT Box on port 77/TCP. By default, the GNAT Box 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 the External and PSN networks.

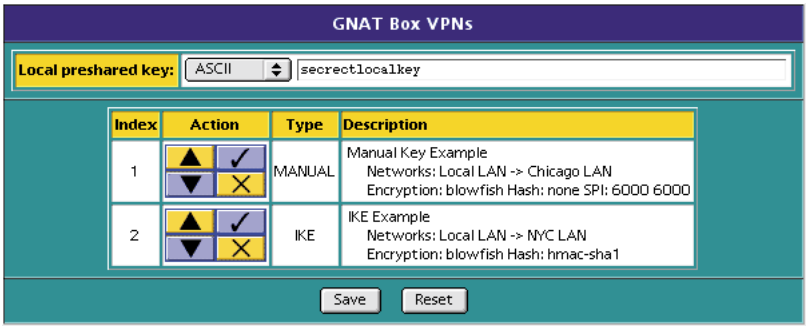
Enable
Select the checkbox to enable access via the Remote Management Console (GBAdmin).

Server Port
The default port for RMC access is 77. If you wish to change this, enter the new port number and make sure you change the Remote Access filter associated with the RMC administration to match the new port number. Follow the same procedure described previously with regard to the web browser interface.

Allow Updates
By default, updates are allowed. If you wish to disallow remote updates via GBAdmin deselect this checkbox.

VPNs
The VPNs menu item provides access on the web interface for the creation and management of GNAT Box VPNs. This section provides information about the mechanics of managing VPN definitions using the web interface (see Chapter 9 of this guide for a complete discussion of the VPN capabilities of the GNAT Box system).

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



Selecting the VPN menu item will display a scrolling summary list of all defined VPN Security Associations. At the top of the display are data entry fields for the local pre-shared key. The pre-shared key information is only used by IKE. So if you are only using manual key exchange this information is ignored.

Local Pre-shared Key

The Local Pre-shared key is the key that is associated with the local gateway IP address. This key is sent to the remote VPN gateway during the phase I key exchange for IKE. You will need to provide this key and the IP address to the administrator of the remote VPN gateway. Likewise you will need to obtain the remote VPN's gateway IP address and pre-shared key to be used in your VPN definition.

The pulldown selector determines how the pre-shared key data is interperted. If **ASCII** is selected then the information entered in the Local Pre-shared Key field is interperted as ASCII values. If the pulldown selector is set to **Hex** then the pre-shared key data is interperted as hexadecimal values.

To delete a VPN definition simply click on the X icon in the row of the VPN definition you wish to delete. To edit a VPN definition click on the Check icon to display the VPN defintion edit screen. To create a new VPN definition, click on either the Up arrow icon or the Down arrow icon to insert a new definition at the selected location in the list. A dialog box will then be displayed prompting you to use IKE. If you wish to create an IKE VPN definition simply click the "OK" button. If you wish to create an manual key exchange defintion uncheck the selector for IKE and then click "OK." No addition, deletion or changes will be applied until the "Save" button on the VPN definition scrolling list has been pressed. If you fail to save your modifications they will be lost once you exit the VPNs section.

VPN Edit Form

The VPN Edit form is used to define and edit a GNAT Box VPN definition (or Security Association). As mentioned in the previous section the form is display for editing by clicking the Check icon on the row of the VPN definition you wish to edit or by creating a new entry by clicking any of the Up/Down icons. Depending upon which key exchange method you selected a different VPN definition form will be displayed. Both forms are very similar except for the lower part that addresses authentication and encryption.

Disable

Like many GNAT Box facilities, with VPN definitions you have the ability to create a definition then use the Disable item to toggle the item between active and inactive status.

Description

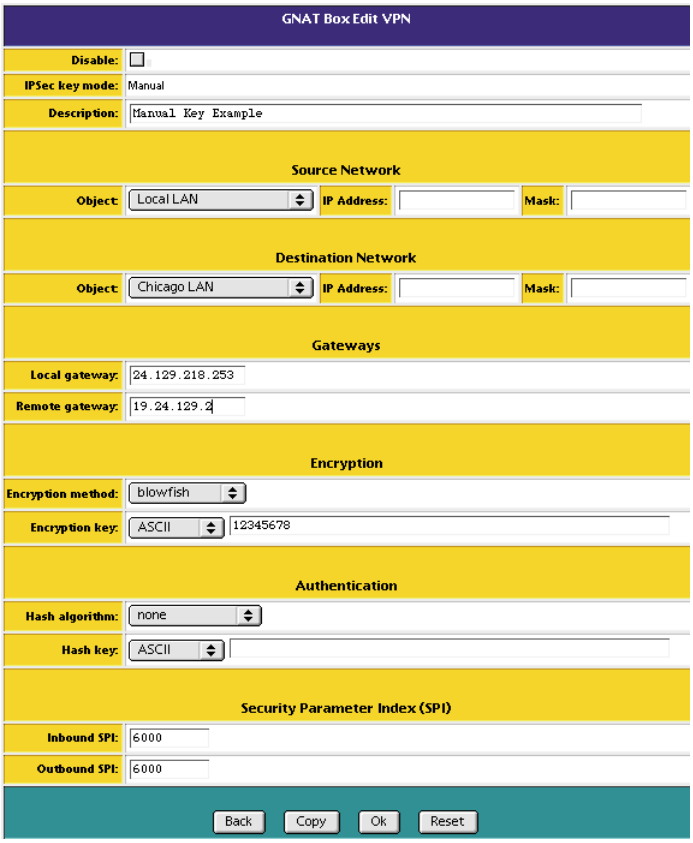
Use this field to write a brief description of the VPN definition.

Source Network

The source network can be specified using an IP Address Object or an IP address and netmask. If you have defined an IP Address Object for the source network (typically your protected network or some part of it), then select that object from the Object pulldown. However if you have not defined an IP Address Object for the source network enter the network IP address of the local network that resides behind the firewall (your protected network, PSN or a subnet of either). Use the Mask field to define the type of network, (e.g. 255.255.255.0 for a class C network). The source network doesn't have to be the entire local network, only the network that is to be accessible via the VPN definition.

Destination Network

The destination network can be specified using an IP Address Object or an IP address and netmask. If you have defined an IP Address Object for the destination network, then select that object from the Object pulldown. However if you have not defined an IP Address Object for the destination network enter the network IP address of the remote network that resides behind the remote firewall (if the remote firewall is a GNAT Box then typcially this will be the protected network, PSN or a subnet of either). Use the Mask field to define the type of network, (e.g. 255.255.255.0 for a class C network). The destination network doesn't have to be the entire remote network, only the network that is to be accessible via the VPN definition.



Local Gateway

This is an IP address that is assigned to an External network interface on the local GNAT Box system. So this IP address can be the real External NIC IP address or any alias assigned to it. The encapsulated packets will appear at the remote gateway with this IP address as the source IP address. Hence the local gateway IP address will should be used on the remote gateway when Remote Access filters are created to accept the VPN connection.

Remote Gateway

This is the IP address of the gateway to the remote network. If the remote network is behind a GNAT Box system then this IP address would be one that is assigned to the External network interface. This IP address will also

play a role in determining the routing of the encapsulated packet.

Manual Key Exchange

This section describes the fields on the Manual Key Exchange form a later section describes the fields on the IKE form.

Encryption

Encryption Method

Use the selection list to select the method that will be used for the ESP transformation. Selecting "None" will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128, and DES. The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Encryption Key

Select either ASCII or Hexadecimal key type. If this item is set to Hexadecimal then the values entered in the key field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F. Otherwise if ASCII is selected any of the ASCII characters may be used to define the key.

Key

This is the appropriate key for the select ESP transformation. The Blowfish, CAST128, RC5 and Simple transformations use variable length keys, while DES uses a fixed length key.

Blowfish

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

CAST128

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

DES

64 bits	8 ASCII characters or 16 Hex chars

Authentication

If you are using Manual Key Exchange you have the option of defining three different VPN tunnel mode transformations: AH, ESP and ESP with authenti-

cation. If you would like to define an AH transformation then you should only complete the Authenication section and leave the Encryption section set to None. If you only want to use ESP then leave the Authentication section set to None. If you want to use ESP with authentication set both the Encryption and Authentication sections. Remember each transformation introduces additional computational requirements for the processing of the VPN.

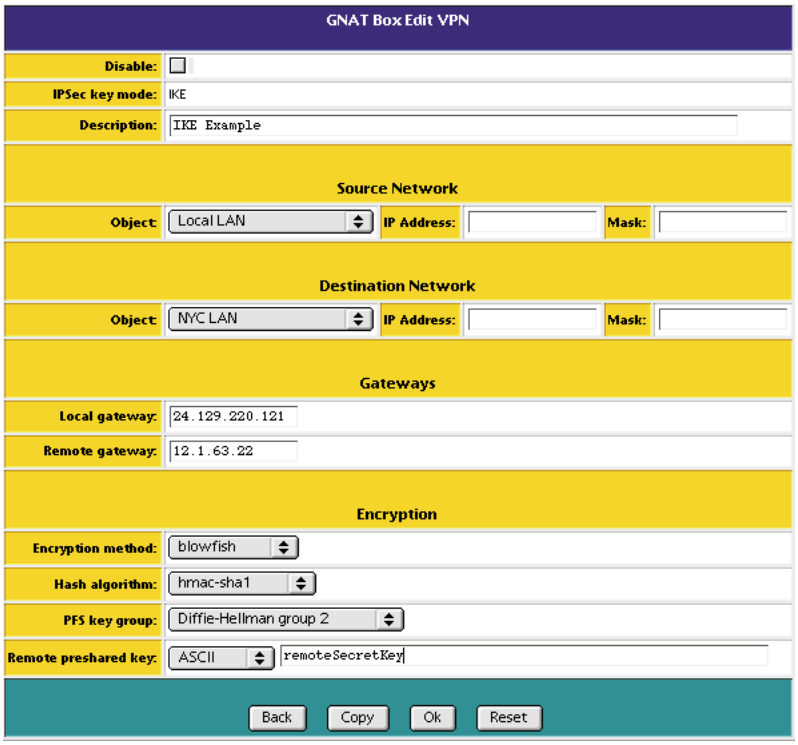
Hash Algorithm
Use the selection list to select the method that will be used for the authentication transformation. Selecting “None” will result in no AH transformation being applied to the packet. The available choices are: None, HMAC-MD5 and HMAC-SHA1.

Hask Key
Select either ASCII or Hexadecimal key type. If this item is set to Hexadecimal then the values entered in the “AH Key” field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F. Otherwise if ASCII is selected any of the ASCII characters may be used to define the key.

Key
This is the appropriate key for the selected hash algorithm transformation. The key length for the MD5 transformations is 128 bits, which is 16 ASCII characters or 32 hexadecimal characters. The key length for the SHA1 transformations is 160 bits or 20 ASCII characters or 40 hexadecimal characters.

Inbound SPI
The Inbound Security Parameter Index is used to uniquely identify a Security Association, (SA). The Inbound SPI will be the Outbound 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.

Outbound SPI
The Outbound Security Parameter Index is used to uniquely identify a Security Association, (SA). 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.



Automated Key Exchange (IKE)

Both the manual key exchange and IKE methods require the same type of gateway and network information in their definitions. The Encryption section differs between the two.

Encryption Method

Select an encryption method to be used for the VPN. Use the selection list to select the method that will be used for the encryption method. Selecting "None" will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128 and DES.

Note: *Remeber that the variable length encryption methods (Blowfish and Cast128) are limited to 64 bits.*

The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little

impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Hash Algorithm
The hash algorithm is used for authentication. Select None, HMAC-MD5 or HMAC-SHA1. If None is selected for the Encryption method then either HMAC-MD5 or HMAC-SHA1 must be selected, (this indicates that an AH transform will be used). If an Encryption method other than None is selected and a hash algorithm other than None is selected then an ESP transform with authentication will be used.

PFS Key Group
Select the Diffie-Hellman group that will be used for Perfect Forward Secrect (PFS) in phase II.

Remote Pre-shared Key
Enter the remote VPN gateway's pre-shared key in this field. If ASCII is selected then the data in the pre-shared key field will be interperted as ASCII values, otherwise if Hex is selected then the data will be interperted as hexadecimal values.

Back
Clicking this button will return to the VPN definition list.

Copy
Clicking this button will save a copy of the entire VPN defintion in a copy buffer. When editing subsequent VPN definitions a "Paste" button will appear at the bottom of the form as long as the copy buffer is loaded with data. This is a convient way to create multiple VPN definitions that have similar characteristics.

OK
Click the "OK" button to save the VPN definition. The VPN definition is not fully committed until the entire VPN definition list has been saved. Once the list has been save the VPN definition is active. The VPN definition although active can not be used until a Remote Access filter is in place to accept the remote gateway's packets and IP Pass Through filters for access control on the VPN are defined.

Reset
Clicking this button will reset the form to the state it existed in when the form was opened.

Three Steps to VPN Activation.

1. Define a VPN Security Association.
2. Create a Remote Access filter(s) 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 first prior to defining any VPN filters, as the ESP and AH protocols may not be included in the list. Go to the protocol list and press the "Default" button to create a list that includes the ESP and AH protocols. Do not use the Default button if you have added protocols by hand. You can add the ESP (protocol 50) and AH (protocol 51) by hand.

3. Create IP Pass Through filters that allow inbound and outbound access on the defined VPN. Generally you will need two filters for each VPN definition, (one for inbound access and the other for outbound). If you have one or more VPN definitions, simply go to the IP Pass Through filter screen and press the "Default" button and a set of filters will be created for your VPN definitions. Please note that the Inbound filters will be disabled and set to Deny. Please make modifications to these filters as required and enable them as per your local security policy. *Please note that IP Pass Through filters for VPN definitions do **NOT** require that entries be created on the IP Pass Through Host/Network data section.*

Please see Chapter 9: GNAT Box VPN for more information about the VPN facility.

Routing

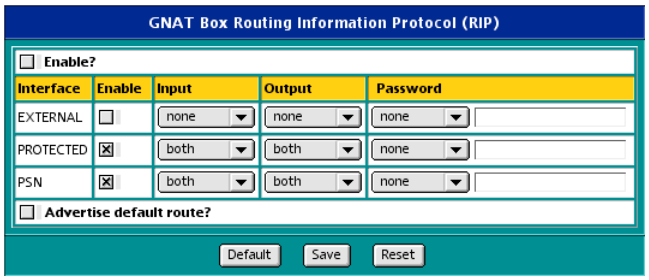
This section provides the administrator screens that address the routing facilities on the GNAT Box system. This menu section provides configuration dialogs for RIP and static routes.

- Routing
  RIP
  Static Routes

Rip Menu

RIP

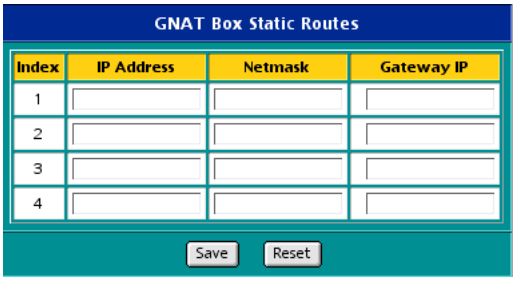
The Routing Information Protocol... menu item displays the Routing Information Protocol window, which provides a means to enable and configure the RIP protocol on a per network interface basis. The GNAT Box like any good firewall does not accept routing information from external sources to redirect packets through the firewall. However, if desired, the GNAT Box can enable the capability to receive as well as broadcast, routing information via individual interfaces.



Static Routes

The Routing menu item provides access to the Static Routes form. This form provides a means for the administrator and to define static routes on the GNAT Box system. Because the GNAT Box system is a firewall it does not normally listen to routing protocols such as RIP. Consequently it is sometimes necessary to define a static routes on the GNAT Box system.

Static routes are quite often used defined the routes to remote networks that are located somewhere beyond a local router on the PROtected network. These static routes override the default routing rules and explicitly define a routing path for a particular host or network.



Defining a Static Route

Use the following procedure to define a static route:

1. Click on the Routes menu item to display the Static Routes form.
2. Click in an empty Destination IP address field, or modify an existing field, and key in the IP address which will be the target of the route.
3. Click in the Destination Netmask field and key in the netmask.
4. Click in the Gateway field and key in the IP address which is the gateway to the destination IP address.
5. Click the Save button to apply your update.

The GNAT Box system supports 300 static routes.

- Objects
  Addresses

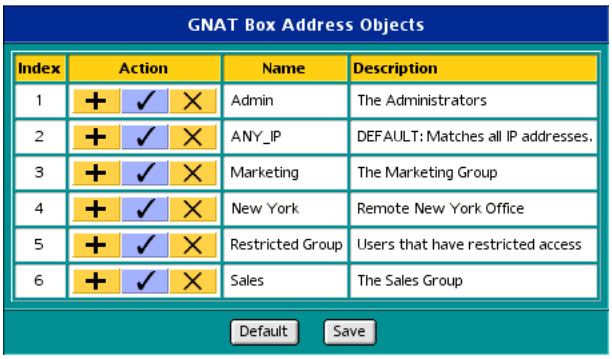
Objects Menu

Objects

The Objects section currently contains a single item: Addresses. Future releases of GNAT Box will add more object types to this menu section.

Addresses

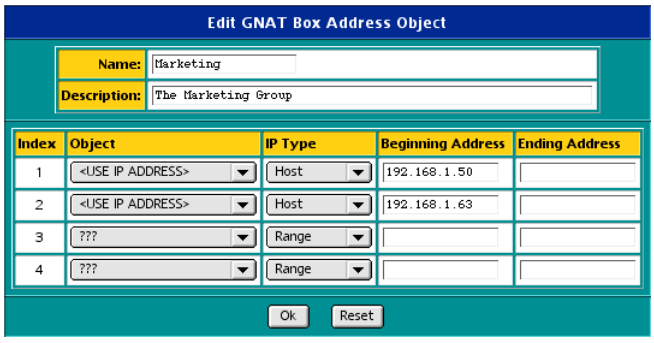
Clicking on the Addresses item will invoke the GNAT Box Address Object list. The list displays the name and description of all defined GNAT Box Address Objects. Use the icons in the Action column to add (plus), edit (check) and delete (X) an object.



A maximum of 300 Address Objects may be defined, with an Address Object having a maxium of 10 members. The members may be either a single IP address, a range of IP addresses, a subnet specified by an IP address and netmask, or a previous defined Address Object.

How to Add an Address Object

1. Click on an add icon in any row. This will display the Address Object Edit form.
2. Enter a name for the Address Object by which it will be referenced. The name must be unique.
3. Enter a description for the Address Object.



4. In an empty row click the pull down choice list in the Object column and choose an item that will be used to define a member of the Address Object. The member may be defined by either selecting a previously defined Address Object to inclued in the new Address Object definition or by selecting <USE IP ADDRESS> item to define the member by using IP Addresses.

If you choose to use another Address Object as a member of the current Address Object, then there is nothing else to do to define the member.

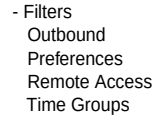
If you choose to define the new member with an IP Address select the type of definition from the pull down choice list in the IP Type column. Your choices are:

Host
Use a single IP address. Simply enter an IP address in the Beginning Address field. Leave the Ending Address field empty.

Range
Use a range of IP addresses. Enter the beginning IP address in the Beginning Address field and the last address in the Ending Address field.

Mask
Use an IP Address and a netmask to specify the desired IP addresses.

5. Repeat step 4 until all the empty rows have been used or until you have added all the members you desire. If you need to enter more members, simply press the "OK" button then click the Edit icon of the Address Object again and additional empty rows will be provided on the Edit Address Object form.



Filters Menu

Filters
Filters are best managed from the Web or GBAdmin Interfaces since they offer the most convenient methods for inserting, deleting, and editing filters. Both types of filters, **Remote Access Filters** and **Outbound Filters**, use the same mechanisms for filter management. Clicking on the specific filter type in the menu will display the corresponding filter set. The filter set is the group of all the filters for a specific filter type. It is important to remember that any changes to individual filters, including additions and deletions, will **not** be effective until the

filter set is saved. If you forget to save the filter set and leave the filter set display, your changes will be lost.

Note: *The order in which filters appear in the filter set is very important, since a filter set is processed sequentially.*

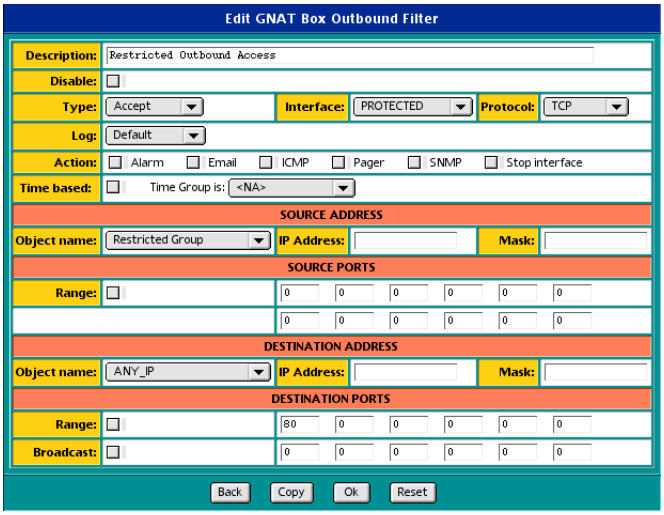
Filter Interface Operation

When the filter set is displayed, each filter in the set is listed with its index number, description, filter summary, and a set of four editing buttons. The four buttons provide a means to: insert a new filter above the current filter, insert a filter below the current filter, edit the filter, and delete the filter.

Filter Manipulation Buttons

Filter Definition

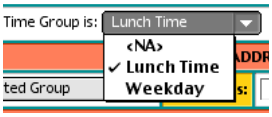
Clicking on the insert or edit buttons associated with a filter will display a filter definition form. The two insert buttons will display an empty form, while the edit button will display the definition of the associated filter.



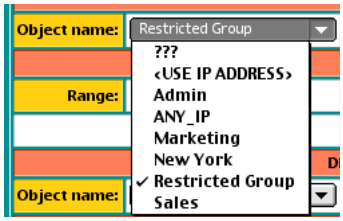
To define a filter, proceed as follows:

1. Click on the Description field and type in your description of the filter.

2. Select the filter action from the Action choice list. A filter action is either Accept or Deny.
3. Select the particular network interface you want this filter associated with, if any, from the dynamic interface choice list. Choices are **ANY** and all available interfaces defined on the **Network Information** Screen. If you choose **ANY** the filter will be applied to packets on all defined interfaces.
4. From the protocol choice list, define which IP protocol you wish the filter to use. Choices are ALL, TCP, UDP, ICMP, or any user defined protocol that has been defined on the protocol screen.
5. Select the logging action you desire from the Log choice list. The choices available are: D - default (defined by the Filters Parameters), N- No logging or Y- Yes, log the packet.
6. Select a filter Action (optional): Email, ICMP, Pager, SNMP, and Stop Interface. These filter actions are configured and enabled via the Preferences configuration dialog under the Basic Configuration section. If an action is enabled, and the filter is matched (accepted or denied), the filter action will be executed.
7. If you wish to apply a time based object to the filter click the **Time based** checkbox and select a time group from the Time Group choice list.



8. Complete the packet source filter criteria from the Source area.
   - Click the **Object name** choice list and select an *address object* or select **<USE IP ADDRESS>** to use an IP address in the adjecent IP Address field and key in the source IP address or network where the packet will be coming from. If an Address Object is selected both the IP Address field is left empty.



   - Next if you have choosen **<USE IP ADDRESS>** rather than an *address object* click the Netmask field and key in a netmask that will be ANDed with the IP address from the Source IP address field.
   - If you will be specifying a range of service ports, click the Range

checkbox. Enter the starting port in the first port data entry field and the ending port in the second port data entry field. If you will be specifying individual ports, simply key those values into the port data entry fields.

Note: *Typically, most TCP/IP applications use a dynamic port allocation scheme for the source port, thus filtering on a source port is generally not useful.*

9. Complete the packet destination filter criteria from the Destination area.
   - Click the **Object name** choice list and select an *address object* or select **<USE IP ADDRESS>** to use an IP address in the adjecent IP Address field and key in the destination IP address or network where the packet will be going to. If an Address Object is selected both the IP Address field is left empty.

   - Next if you have choosen **<USE IP ADDRESS>** rather than an *address object* click the Netmask field and key in a netmask that will be ANDed with the IP address from the **destination IP** Address field.
   - If you will be specifying a range of ports, click the Range checkbox. Enter the starting port in the first port data entry field and the ending port in the second port data entry field. If you will be specifying individual ports simply key those values into the port data entry fields.

10. Click the OK button to confirm your filter definition and add it to the filter set.

Note: *Remember that the filter set needs to be saved before your new filter or modified filter will be effective on your GNAT Box system.*

Filter Editing Tips

Below are some tips for working with filters on the web browser interface.

Copy and Paste

Copy and paste can be quite helpful if you are defining multiple filters which are similar in some ways. To copy a filter definition into the copy/paste buffer, simply click on the Edit button of the filter you wish to copy. Once it is displayed, click the Copy button to copy it. Next click the Back button to return to the filter set display. Click one of the insert buttons at the location where you would like to insert the filter definition in the copy/paste buffer. An empty filter definition will be displayed with the Paste button active. Click the Paste button and the data will be pasted into the empty filter definition form.

Default Button

The Default button that appears on the filter set display panel will generate a default filter set based on the current system configuration. This set will take into account the IP address and netmask of all the defined network interfaces. The new filter set will also create one filter for each defined Tunnel, in the case of Remote Access Filters. The Default button will completely replace any existing filters, and any changes you have made will be lost. However, the changes will not be applied until you save the new filter set.

Combining Filters

It is often useful to combine multiple filters into one filter, when the filters share similar filtering criteria. This case most often occurs when all the filter parameters are the same except for the destination port. Combining filters also makes the filtering process more efficient, by reducing the number of filters in the filter set. Common filters that might be combined are for SMTP, FTP, and HTTP, since these are all TCP based protocols and are quite often served from the same host system.

Filter Disable

The filter disable feature is quite handy when you are experimenting with various filter configurations. The GNAT Box default filter set utilizes this feature. All possible default filters are created, but only those which should be operational, based on configuration parameters, are enabled. If a feature needs to be enabled later, it's simply done by changing the configuration and enabling/ disabling filters.

Checking Current Filters

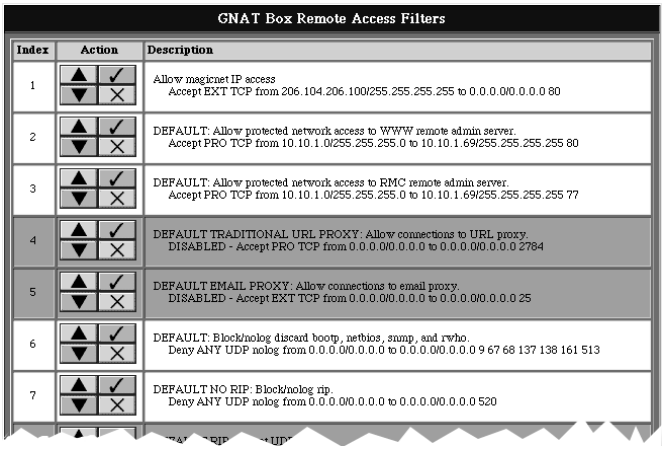
If you are unsure which filters are currently in effect on your GNAT Box system click the Configuration Report item in the menu. This will generate a report of all the current system settings, including a listing of the current filters.

Remote Access Filters

Remote Access Filters control inbound access primarily on Tunnels. Additionally, Remote Access Filters control inbound access to any network interface on the GNAT Box from any attached network. When the GNAT Box is initially configured, a set of default Remote Access Filters are generated dynamically but not saved. These filters can be used as is, modified, disabled or deleted to suit the local network security policy. A list of default filters are listed in Appendix E.

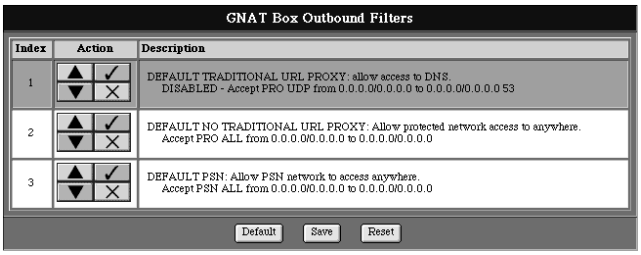
Filter Summary Display

Clicking the Remote Access link in the Filters menu will display the Remote Access filter summary list.



Generally it is best to select and configure the GNAT Box system preferences and inbound Tunnels first. Next access the Remote Access filter set and click the **Default** button. The system will generate a set of Remote Access filters for the selected configuration. The generated filters can then be adjusted if desired.

This release supports 400 Remote Access Filters. The Terms & Concepts section describes the Remote Access filters in detail.



Outbound Filters

Outbound Filters control access to the External network (typically the Internet) and to the PSN (if one exists). As mentioned previously, the implicit filter rule is "**that which is not expressly permitted is denied.**" It applies to outbound packets as well as inbound packets. When the GNAT Box is initially configured, a default Outbound Filter will be created dynamically, but not saved. The default filter allows all IP addresses on the Protected network to access any IP address

and any service external to the Protected network. If a PSN network interface exists, a similar default Outbound Filter will be created that allows all access to the External network (typically the Internet). These filters can be modified or deleted to suit the local network security policy for external network access. An example of the default Outbound filters can be found in Appendix E.

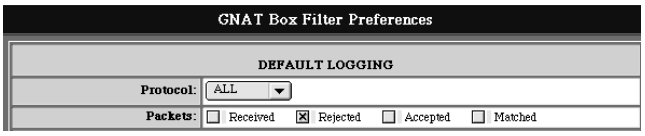
This release supports 400 Outbound Filters.

Filter Preferences

The Filter Preferences item displays the Filter Preferences configuration form. This form enables the administrator to define preferences for functional areas that are associated with filters.

Default Logging

Every filter has a log action associated with it, regardless of the filter type (Accept or Deny). This action can be 'Yes' to explicitly log the packet, 'No' to explicitly not log the packet, or 'Default' to take the default action defined in the Logging section of the Filter Preferences. The default Filter Logging Preference is set to log all rejected packets for all protocols.



If you wish to change the Filter Preferences, follow this procedure:

1. Select the desired protocol to log from the Log Protocol choice list. The choices available are: ALL, TCP, UDP, ICMP or NONE.
2. Select the type of packets to log, by clicking the checkbox next to the desired packet type. The available packet types are:

   Received

   Means any packet that is compared to the filter.

   Rejected

   Means any packet that is rejected by the filter.

   Accepted

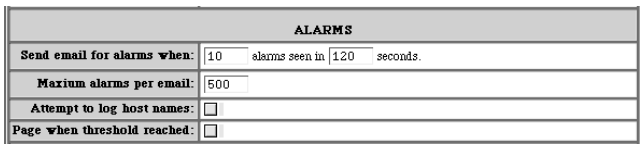
   Means any packet that is accepted by the filter.

   Matched

   Means any packet that matches the filter criteria.

The packet type choices are not mutually exclusive. However, selecting multiple

types may result in as many as four log records being generated for a single packet. This option can quickly generate an excessive amount of logging and thus should be used with care.



Alarms

This dialog allows the administrator to set the parameters that are involved in alarm notifications. An alarm event occurs when a filter (Remote Access, Outbound or IP Pass Through) is matched and the alarm filter action is enabled. Each alarm event increments the alarm count by one. If the alarm threshold is reached within the specified time period, an email alarm notification will be sent to the designated email address defined on the Email Server screen. The email message will document all the alarm events that contributed to the alarm notification. Multiple email messages will be sent, if the number of alarm events exceed the maximum alarm count parameter defined in this section. If the pager option is configured, a pager message can be generated when the alarm threshold is reached.

Send Email for Alarms When...

Configure the alarm threshold by entering values for the number of alarms and time period.

Maximum Alarms per Email

This parameter controls the maximum number of alarm messages that will be included in a single email message. A larger number will reduce the number of email messages at the expense of larger email messages. An alarm message is generally 200 bytes.

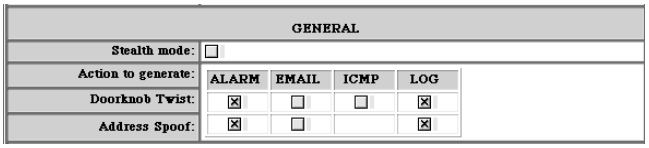
Attempt to Log Host Names

If this checkbox is selected the GNAT Box will attempt to resolve the hostname of the source IP address that generated the alarm. This feature will increase the amount of processing time required to deliver the alarm notification, due to the nature of DNS lookups.

Page When Threshold Reached

If your GNAT Box has been configured to support pager notifications, this item if

enabled will send a page when the alarm threshold is reached.



General

The General section contains miscellaneous configuration parameters.

Stealth Mode

If this option is selected, the Remote Access default "No Stealth" filters will be set to "Disable" and the runtime system operates in the stealth mode. Enabling and disabling this option will change the system operation mode. However, it will not change the Remote Access filters, unless you either press the "default" button or change them manually (via the Disable option). In the stealth mode, the GNAT Box will not respond to ICMP ping and traceroute request, UDP traceroute request, and will not reply with an ICMP message when a packet arrives for a port where no service or tunnel exists.

Action to Generate for Doorknob Twist

These options control how the GNAT Box will respond to "doorknob twists". A doorknob twist occurs when a connection is attempted to 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 GNAT Box has been mis-configured.

Alarm

Selecting this option will generate an alarm event if a doorknob twist occurs.

Email

Selecting this option will immediately send an email message documenting the doorknob twist event. The email message will be sent to the address specified on the "Email Server" configuration section.

Log

Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.

ICMP

Selecting this option will generate an ICMP "service not available" message

to the source IP address of the attempted connection.

Address Spoof

These options control how the GNAT Box will respond to an address spoof. An address spoof occurs when an IP packet arrives at a GNAT Box network interface and its return path is not back through the interface it arrived on. Address spoofs generally occur because of two different situations:

1. Mis-configuration. Network(s), subnet(s), or host(s) are located on or connected to the Protected/PSN network and have not been defined to the GNAT Box. The GNAT Box assumes all IP addresses that are not on the Protected network, or defined in the static route table, or are learned via RIP on the protected network, should only appear on the EXTernal side of the GNAT Box.

2. An intrusion attempt by altering the source IP address of a packet directed at a GNAT Box network interface.

Alarm

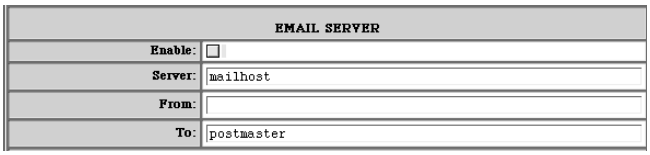
Selecting this option will generate an alarm event if an address spoof occurs.

Email

Selecting this option will immediately send an email message documenting the address spoof event. The email message will be sent to the address specified on the “Email Server” tab.

Log

Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.



Email Server

This dialog allows the administrator to configure where the GNAT Box will send email notifications and alarms.

Enable
If this item is enabled, the GNAT Box will be able to send email and alarm notifications. If alarms and/or email notifications are set on a filter and the email server is not enabled an error message will be written to the console and remote log file.

Server
Enter the hostname (DNS hostname, if an internal DNS server is used) or IP address of the email server where alarms and email notification messages will be sent. Although the email server typically is a host on the Protected or PSN network, it isn't a requirement and the server may be on any accessible network. The email/alarm notifications can be sent to any valid email address, as long as the server is accessible.

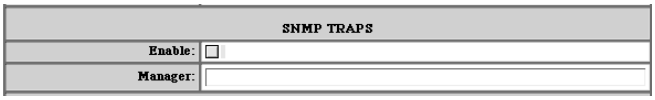
Note: *The email server defined on this configuration dialog need not be the same server that is used with the email proxy.*

In order to use a hostname for the email server, you must have defined a DNS server which is to be used for lookups on the GNAT Box system (this is done in the DNS form). If the hostname is an internal host (PSN or Protected networks), then the DNS server must be an internal server which can resolve the name of the hidden host. If the DNS server referenced is an External server and the target mail server is an internal host, you will have to use the IP Address.
If you are unsure about the hostname, use the IP address of the host.

From
This is the "from" email address that will appear in the email and alarm notifications. Although you can leave this field blank, some email servers don't like to receive email with an empty "from" field. An email address entered in this field should be valid, otherwise if there are problems delivering the email the server will attempt to return the mail to the address in the "from" field (an email loop may ensue). The "From" address may be a fully qualified address, such as jdoe@gta.com, or it can simply be the mailbox name on the specified email server, such as jdoe.

To
This is the email address that will receive the email and alarm notifications. The email address can be either a fully qualified address, such as jdoe@gta.com or it can simply be the mailbox name on the specified email server, such as jdoe. If

the email address is not for local delivery within your protected network, make sure that the specified email server will allow the email to be relayed.



SNMP Traps

Although the GNAT Box does not provide SNMP management, it does have the ability to send a SNMP trap to a SNMP management station as the result of a filter action. The SNMP trap sent is an enterprise specific generic trap.

In order to utilize this SNMP trap facility, SNMP management software must be running on an accessible host.

Enable

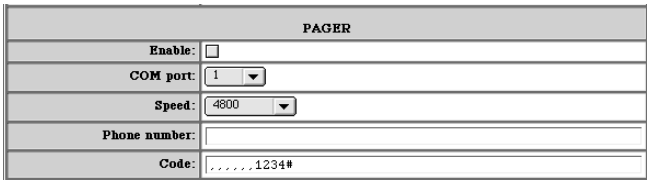
Select this checkbox to enable the SNMP alarm facility. Upon selection, the SNMP Manager IP field will allow data entry. If SNMP is not enabled, selecting SNMP filter actions on the filter definition screens has no effect.

Manager

The Manager IP is the IP address of the host running the SNMP management tool. This field uses the IP history list. The SNMP manager IP address may reside on any network although the Protected network is the most common location.

Pager

The Pager dialog allows the administrator to configure the optional pager facility. To utilize the pager facility, a modem needs to be installed on one of the four available COM ports. If you are using an async modem or ISDN, you must configure an additional modem for pager support.



Enable

Select this checkbox to enable the Pager alarm facility. If the Enable Pager Support field is not enabled, selecting Pager filter actions on the filter definition

screens has no effect.

COM Port
This section provides a means to define which COM port will be used for the pager.

Speed
This parameter is the DTE speed that will be used to communicate with a modem for paging purposes.

Phone Number
Enter the telephone number for the numeric pager in this field along with any access codes if required.

Code
Enter the numeric message that should be sent to the pager. Because a greeting message is typically played upon connection to a pager service, you may want to send a series of pauses prior to sending the numeric message.

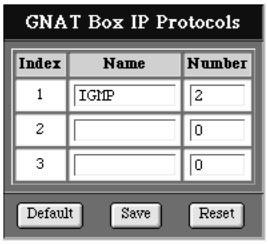
Note: *Most numeric paging services require a "#" to be entered at the end of the numeric message.*

Protocols
The Protocols configuration dialog provides a means to define IP protocols other than TCP, UDP, and ICMP. This protocol definition list is available for use on any of the filter definition dialogs. In the current version of GNAT Box, the additional protocols may only be used with a Deny filter on Remote Access and Outbound filters, since the system currently can only process TCP, UDP, and ICMP IP packets in the NAT mode.

Any defined IP protocol however can be used with **IP Pass Through** filters. This means you can define IP protocols such as the IPSec ESP and AH protocols, then utilizing the IP Pass Through facility allow these packets to pass through the GNAT Box system.

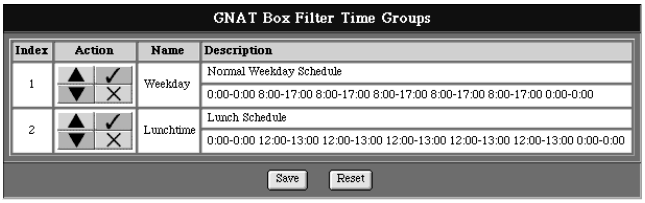
The main purpose for the additional protocols in the NAT mode (Remote Access and Outbound filters) GNAT Box is to minimize extraneous protocol block messages in the log files. Since the default action of the GNAT Box is to deny that which is not explicitly allowed and the default filter logging action is to log all rejected packets, an unknown protocol that reaches the GNAT Box will be logged. If the unknown protocol is a routing protocols such as EGP, the log files

could quickly grow to an enormous size. Therefore, it is often convenient to create a remote access filter that simply denies a protocol and explicitly does not log it. The protocol list is limited to 100 protocols.

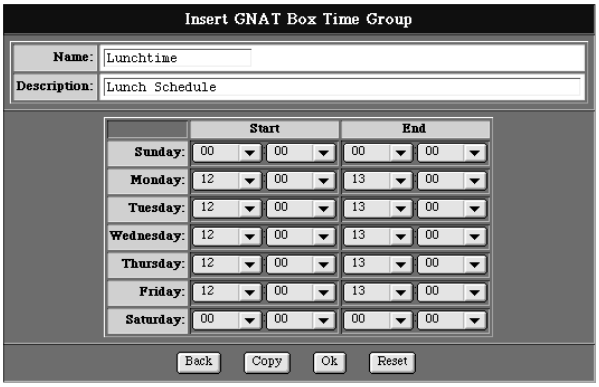


Time Groups

Time Groups are user defined time schedules that can be associated with any type of filter. Time Groups provide the firewall administrator with the ability to control access (both inbound or outbound) based on the time of day and day of the week. A filter that has an associated Time Group will only be in effect during the defined time period. The time granularity is based on 10 minute increments. Time Groups can provide a great deal of flexibility, especially when multiple filters are involved. This release supports 100 Time Groups.



The Time Group list operates similar to the filter group screens. The editing buttons have the same functions as described in the filter section. Like the filter group screens, it is important to save the entire Time Group list after any modification, additions, or deletions.



1. Click on either of the insert icons (above or below) to create a new empty Time Group form, or click the edit icon (check) to edit an existing Time Group.
2. In the **Name** field enter a name that will appear in the Time Group popup list on the filter definition screen.
3. Enter text that describes the Time Group in the **Description** field.
4. Using the pull down lists, select a **Start** and **End** time for each day you wish the Time Group to be in effect. Days with a **Start** and **End** time of 00:00 define an inactive day.
5. When you have finished with your definition, click the **OK** button to save the Time Group.
6. When you have finished editing the Time Group list, click the Save button at the bottom of the list screen to save the entire set. The Time Group list will now be available from any of the filter definition form screens.

Note: *The Copy button can be used to copy an entire definition which can be pasted it into a new definition.*

- IP Pass Through
  Hosts/Networks
  Filters

IP Pass Through Menu

IP Pass Through

IP Pass Through is the GNAT Box term for "no NAT." The IP Pass Through data entry screens allow the user to define a host, subnet, or network that will not have NAT applied to packets from specified IP addresses.

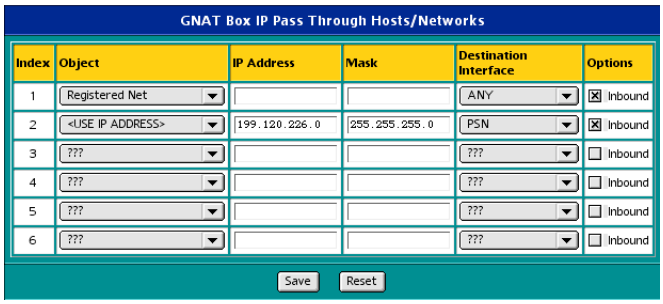
Two items must be in place for an IP pass through to operate correctly:

1. The IP address must be defined on the Network/Host form.
2. An IP pass through filter(s) must be created to allow packets to flow from and/or to the IP pass through IP address.

Note: *If an IP pass through address is configured to use the External network interface and the GNAT Box is connected to the Internet, the IP pass through address must be a valid registered address.*

The IP Pass Through facility provides a great deal of flexibility, since an IP address(es) can be configured not to use NAT for specific interfaces. 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, yet packets from the same IP address which are destined for the Internet will have NAT applied.

IP Pass Through Host/Networks



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

1. Select an empty row or edit an existing row.
2. In the Object column use the choice list to select either an Address Object or **<USE IP ADDRESS>.**
3. If you selected an Address Object in the Object column then leave the IP Address field empty otherwise enter a host IP address, subnet or network.
4. If you select an Address Object in the Object column then leave the Netmask field empty otherwise enter a netmask that will be ANDed with the IP Address field which will yield the desired results. Single IP addresses should use 255.255.255.255.

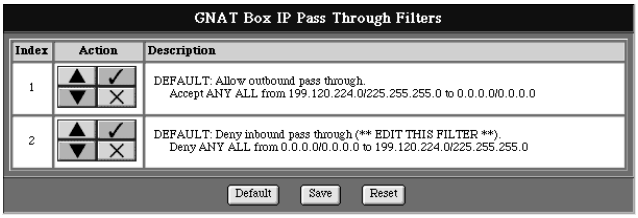
Note: *The netmask has no relation to the network netmask. It is strictly a means to specify a single IP address or a group of contiguous IP addresses.*

5. Use the **Interface** pull down to select which network interfaces will have no NAT applied to the specified IP packets, when they pass through the specific NIC.
6. If you wish unsolicited IP packets to be accepted for the specified IP pass through address(es), then select the **Inbound** checkbox. If you only wish to allow for the return of the IP pass through reply packets be allow to return then it is unnecessary for the Inbound option to be selected.
6. After you have finished creating your definitions, click the Save button to save the IP Pass Through Host/Network definitions.

The IP Host/Networks list is limited to 100 entries.

IP Pass Through Filters

IP Pass Through Filters control access to and from IP addresses that have been specified as IP pass through addresses. IP pass through filters, although similar to the other two filter types (Remote Access and Outbound), are a bit different since they control both inbound and outbound access to/from the designated IP Pass Through addresses. Since IP pass through addresses are not translated, the GNAT Box functions as a gateway for these addresses. Therefore the IP Pass Through Filters utilize IP Pass Through addresses in the filter definitions not GNAT Box NIC addresses.



If IP pass through host/networks are defined, pressing the "Default" button on the IP Pass Through filter screen will create a set of filters based on the IP pass through addresses defined. Since IP pass through host/networks can be defined in various combinations, the default filters will vary according to options selected. These generated filters are quite general and should be modified to match your security requirements.

Typically, two filters are required for each different Host/Network IP pass through IP address: one for outbound access and the other for inbound access. The

Remote Access and Outbound filters do not apply to IP Pass Through designated IP addresses.

This release supports 400 IP Pass Through filters.

Defining IP Pass Through Filters

IP Pass Through Filters are defined in the same manner as Remote Access or Outbound filters. The same rules about filter order also apply. The major difference is that since IP Pass Through addresses are not hidden, filtering rules always address the IP Pass Through host(s) and not any IP address assigned to the GNAT Box. The GNAT Box functions only as a passive gateway with regard to IP Pass Through addresses.

As mentioned in the previous section, one of the easiest methods of creating IP Pass Through Filters is to first configure any IP Pass Through hosts or networks using the Host/Network form. Then use the Default button on the IP Pass Through filter set form to generate a set of default filters based on the definitions created on the Host/Network form. The disadvantage of this method is that if filters have been previously created and customized, they will be replaced with the system generated default filters.

How to Create IP Pass Through Filters

To create a pair of IP Pass Through filters for a defined IP pass through host:

1. Click one of the insert icons (above or below) on an existing filter to create an empty filter definition, or edit an existing filter.
2. IP Pass Through addresses require two filters (inbound and outbound), with the outbound filter created first. Complete the filter definition in the same manner as an outbound filter, specifying the source IP address as that of the IP Pass Through address. Once you have the filter defined click the save button.
3. Click the insert icon again to create another filter. This filter will handle the inbound connection. Define the filter as you would a Remote Access filter except the destination IP address will be the IP Pass Through address, not the IP address on the GNAT Box NIC. Save the filter.
4. After you have completed adding all IP Pass Through filters, click the Save button on the filter set to save the filters and apply them to the running system.

- NAT
  Aliases
  Inbound Tunnels
  Static Address Mappings
  Timeouts

NAT Menu

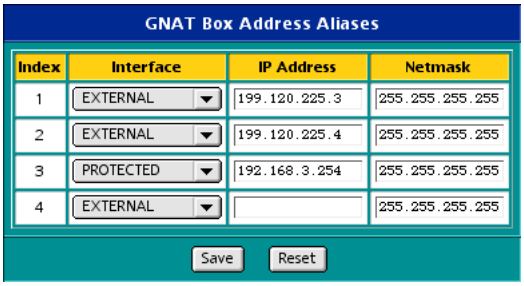
NAT

The four menu items under this section of the menu are associated with network address translation (NAT) facilities.

Aliases

The Aliases form is used to assign IP aliases to GNAT Box network interfaces. Aliases may be assigned to the External, Protected or Private Service network interfaces. All changes take effect after the save has been confirmed.

The GNAT Box supports a total of 300 aliases.



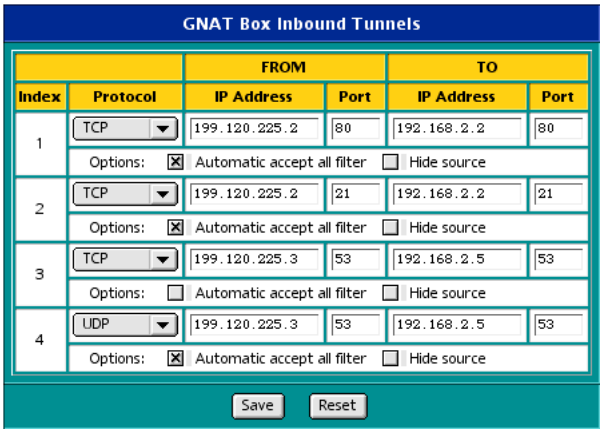
How to Create an Alias

1. Select the desired network interface to be aliased from the choice list.
2. Enter the alias IP address.
3. Modify the netmask if required.
4. Press the "**Save**" button.
5. The save will then be acknowledged. Pressing the OK button will re-display the Alias form with two blank data entry slots at the end of the table.

Note: *If you create an alias that resides on the same logical network as the primary IP address for the selected network interface, you must use a netmask of 255.255.255.255.*

To Delete an Alias

1. Simply blank out the IP Address field and press Save.



Tunnels

As defined in the Introduction section of this guide, a Tunnel is a GNAT Box facility that allows a host on an external network to initiate a TCP, UDP or ICMP session with a host on an otherwise inaccessible host for a specific service. The Inbound Tunnel form allows the user to define tunnels for both the External network interface and the Private Service network interface.

Tunnels are **never** used on a Protected network interface, because tunnels are associated only with inbound connections. Tunnels can only be created for these inbound connections:

1. From an External network interface to a host on a Private Service network.
2. From an External network interface to a host on a Protected network.
3. From a Private Service network interface to a host on a Protected network.

Tunnel Characteristics

1. A tunnel will not be usable unless an appropriate Remote Access Filter has been defined to allow access to the tunnel. As mentioned in the earlier Remote Access Filter discussion, the default button on the Remote Access Filter set screen will generate default filters for all defined tunnels. The filters generated by this method are broad in scope, and may require modification to meet your specific security policy.
2. Tunnels are defined by a source IP address/port pair and a destination IP address/port pair.

3. Only the source side of a tunnel is visible. Since GNAT Box tunnels are a form of network address translation, a user on the source network side will

never see the ultimate destination of the tunnel. For all practical purposes, the tunnel appears to be a service operating on a server with the tunnel's source IP address.

4. 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 you could define a tunnel with a source port of 99 and a destination port of 23.

5. A tunnel with a source and destination port of zero, means tunnel all ports for the specified protocol. You can completely expose a host by creating a zero tunnel with the protocol type set to ALL.

Please note, exposing a host in this manner is extremely dangerous and not recommended.

6. If a tunnel originates from an alias IP address, you may need to add a "mapping" to map the destination host to the alias IP address. This is necessary, so that secondary connections will appear to originate from the same address as the Tunnel.

7. A maximum of 300 tunnels may be defined.

How to Define a Tunnel

To define a tunnel, use the following procedure:

1. Click on the Inbound Tunnels menu item to display the data entry form.

2. Select an empty row or choose an existing tunnel definition to modify.

3. Select the protocol type form the Protocol choice list. The choices available are TCP, UDP, ICMP, or ALL.

4. In the From IP Address field, key in the IP address of the source side of the tunnel. This address may be the real IP address or an alias assigned to the network interface. Remember, only the External and Private Service network interfaces may be used.

5. In the From Port field, enter the port value which users will access. A list of services and their port numbers is listed in an appendix of this guide.

6. In the To IP Address field, key in the IP address of the target host. The host may reside on either the Private Service network or the Protected network (including subnets routed behind either network).

7. In the To Port field, enter the port value which will be the destination of the tunnel. This is the port value of the service being offered on the target host.

8. You may wish to enable one or both of the tunnel options.

   Automatic Accept All Filter
   Enabling this option will create an automatic filter that will accept IP packets for the defined tunnel from any source IP address. For example this option would typically be used for a http tunnel to a public accessible web server located on a PSN network.

   Hide Source
   Enabling this option will cause the source IP address of packets received on the tunnel to be changed to the IP address assigned to the NIC where the packet exits from the GNAT Box system. Under normal condiditions the source IP Address is preserved. This option is useful in situations where the GNAT Box system is used in an intranet situation.

9. Click the Save button to apply your tunnel definition, it will be effective immediately. You may add and/or modify any or all tunnels on the form and apply them with a single save.

10. Select the Remote Access Filter menu item and create or modify a filter to allow access to your new tunnel.

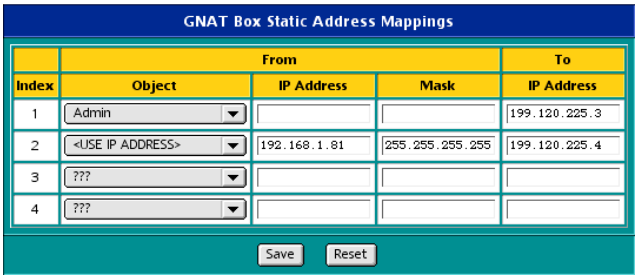
Static Address Mapping
As mentioned earlier in this guide, Static Address Mapping is a GNAT Box facility that allows an internal IP address or subnet to be statically mapped to an external IP address during the network address translation process. By default, all IP addresses on a Protected and a Private Service networks are dynamically assigned to the primary IP address of the outbound network interface.

In certain situations where it is desirable to statically assign the IP address used in the network address translation. To use the Mapping facility, you must have assigned at least one IP alias to the desired outbound network interface (External

or Private Service network interfaces).

Static Address Mapping is Allowed

1. From a host or subnet on a Protected network to an IP alias assigned to a Private Service network interface.
2. From a host or subnet on a Protected network to an IP alias assigned to an External network interface.
3. From a host or subnet on a Private Service network to an IP alias assigned to an External network interface.



Static Address Mapping Rules

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.
4. 300 Outbound Maps may be defined.
5. Any changes or additions are applied immediately.

Define a Static Address Map

Use the following procedure:

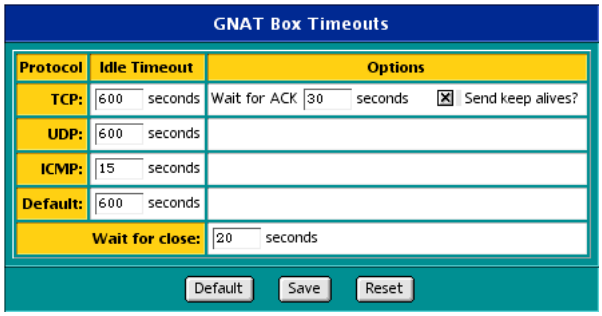
1. Click the Outbound Mapping menu item to display the data entry form.
2. Select an empty row or an existing definition.
3. In the Object column select an Address Object or select <USE IP ADDRESS> from the choice list.
4. In the From IP Address field, key in the IP address of the host or subnet that should be mapped if an Address Object was not selected in the Object column otherwise leave this field empty.
5. If <USE IP ADDRESS> was slected in the Object column then key in a netmask that will be ANDed with the From IP Address to yield an IP address or subnet that will be mapped. Otherwise leave this field blank.
   For example, to map a single IP address use a netmask of 255.255.255.255. To map a class C network use 255.255.255.0 to map half of a class C use

255.255.255.128.

6. In the To IP Address field, key in the IP address to which the source IP address(s) will be mapped. Remember this needs to be an alias IP address.
6. Click the Save button to apply your Address Map.

Timeouts

Timeouts define when a connection is viewed as being excessively idle. What happens when a connection reaches its timeout value differs for each IP protocol. The reason for the difference has to do with how different protocols operate. Both ICMP and UDP are connectionless network services, while TCP is a connection-oriented network service. This means that generally speaking it is impossible to determine when ICMP and UDP connections are finished (ready to close). The TCP protocol has enough information embedded, so that GNAT Box can determine when a TCP connection is finished.



***Note**: You should not change the values on this preference dialog unless you know what you are doing. Setting the incorrect values can result in your GNAT Box system operating poorly or not at all.*

When UDP and TCP reach their respective timeouts the connection is marked as ready to close. TCP connections are a little tricky because TCP has two timeout values:

Wait for Ack

The first TCP time-out is “Wait for ACK.” As part of the TCP connection creation process, the client and server exchange several IP packets. All packets sent from the server will have a bit indicating ACK (acknowledge) with the packet header. As part of its stateful packet inspection processing, the GNAT Box keeps track of the fact that it has seen this bit. If this bit is never seen it usually means that the remote server is down. If the “Wait for Ack” idle time is reached without an ACK

from the server, the connection is marked as ready for close.

Send Keep Alives?

The second TCP timeout is for idleness on a successfully created connection. When the idleness timeout for TCP is reached two things can happen:

1. If "send keep alive" is disabled the connection is marked as ready to close.

2. If "send keep alive" is enabled, a TCP keep alive IP packet is constructed and sent to the client. The client will then send a keep alive IP packet to its server, if the connection is still valid. If the connection is invalid, the client will send a connection reset to its server. If the GNAT Box sees the keep alive message, it will set the connection's idle time to zero. If a connection reset packet is seen, the connection is marked as ready to close. If no response is received from the GNAT Box's keep alive message after five minutes, the connection will be marked as ready to close.

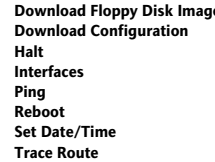
After a connection is marked as ready to close, the GNAT Box will wait five seconds before it actually closes the connection. This gives redundant IP packets a chance to clear the GNAT Box without causing false doorknob twist error messages.

Default Timeout

The Default timeout is a catch-all for any other supported protocol, besides TCP, UDP or ICMP. At this time, the only other protocol directly supported by the GNAT Box is GRE (used by PPTP).

Wait for Close

Default value is 10 seconds. If your site is experiencing a large number of spurious "Remote Access Filter" blocks from reply packets (typically from port 80 - http), you may want to increase this value, which will give packets from slow/ distant connection more time to return before the connection is closed down.



Administration Menu

Administration

The items that appear under the Administration section of the menu are functions associated with operational and administrative aspects of the GNAT Box system. The administrator should exercise care with the Halt facility, especially if not geographically near the GNAT Box system. The only way to restart the system after a halt is from the console or power/reset switch. It should also be noted that a Halt or Reboot will never send a reply to the local web browser, since the network connection will have been terminated. Included in this section are two useful tools (ping and traceroute) that can be quite helpful in testing and diagnosing connectivity problems.

Downlaod Floppy Disk Image

This menu item will only be available if you are connected to a GNAT Box Pro system, since the flash memory based systems (GB-100, GB-Flash and GB-1000) do use floppy diskettes. This item will initiate a file transfer of the entire GNAT Box floppy diskette image. If the web browser is running on a system with GBAdmin installed (Win95/98/NT), the user can either save the image file or choose to launch GBAdmin with the data.

Download Configuration

This item provides the same functionality as the previous Download Floppy Image, except only the configuration data will be transmitted.

Halt

The Halt menu item provides a means to halt the GNAT Box system. A form will be displayed requesting confirmation of the halt request. Click on Submit to initiate a system halt. Since this action will terminate your network connection to the GNAT Box 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 GNAT Box system must be restarted either from the console interface or by performing a power cycle or hardware reset.

Interfaces

The Interfaces menu item accesses a form which displays the current state of the

network interfaces. The form also provides the user with the ability to control the state of the network interfaces. A network interface is either Enabled, meaning up and ready to send/receive packets or Disabled, meaning down and not accepting or sending packets.

If you are using PPP for your External network device, changing the state of the External network interface has differing effects depending on the type of PPP connection you have selected. Please review the PPP section of this guide, for a discussion of this subject.

How to use the Interfaces Facility

Use the following procedure to change the state of an interface:

1. Click the Interfaces menu item to display the Interfaces form.
2. Change the network interface state from the Status choice list to the desired network interface.
3. Click the Save button to apply your change. The state change will be effective immediately.

Ping

The ping menu item provides a means to test network connectivity by using the ping ICMP protocol. Clicking this menu item will display the Ping form. This form allows the user to generate ping packets from the GNAT Box to a specified IP address. Since the target IP address can be on any network, the Ping facility is very useful in validating your network connectivity for all network interfaces.

How to use the Ping Facility

To use the ping facility follow this procedure:

1. Click the Ping menu item to display the ping form.
2. Click in the IP address or fully qualified host name field (if DNS has been enabled) and key in the IP address to ping. The IP address should be entered in the standard network “dot” notation.
3. Click the Submit button to start the ping process. The ping process will attempt to send five ping ICMP packets to the target IP address. When the process is complete, press the <return> key to exit the ping output display screen and return to the ping form.

Reboot

The Reboot menu item will signal your GNAT Box system to restart. A form will be displayed asking you to confirm the reboot request. Clicking on OK will initiate a system reboot. Since this action will terminate your network connection to the GNAT Box web server, your web browser will never receive a reply. Your connection will eventually time-out or you can opt to press the stop button on your browser.

Note: *Some computer systems have been known to not respond properly to the reboot request. In this case the system must be manually reset.*

Set Date/Time

The Set Date/Time form provides a means to set and adjust the date and time values used on the GNAT Box system. The current, local time should be used when setting the time. The date should be entered in the form month/day/year (mm/dd/yyyy). All changes are effective immediately.

Traceroute

The Traceroute form provides yet another method to test network connectivity. It traces the route an IP packet would follow to some Internet host by launching UPD probe packets with a small TTL (time to live) and then listening 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 Traceroute form will accept either a fully qualified host name (if DNS has been enabled on the GNAT Box), or

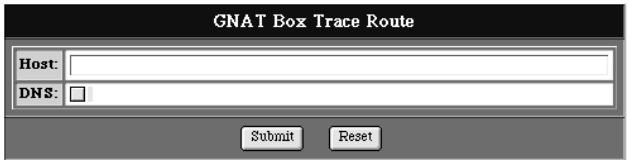
an IP address entered in standard "dot" notation.

Upload Configuration

This item will allow you to upload a previously saved GNAT Box runtime system configuration file. Selecting the item will display a data entry screen that allows you to enter the configuration file name to upload. You can also use the "Browse" button to find the file on your local workstation. Pressing submit will upload the configuration file to the GNAT Box system.

Upload Runtime

This item is only available on flash based systems (GB-Flash, GB-100 and GB-1000). This function allows the administrator to update the GNAT Box runtime system on the remote firewall system. Selecting this item will display a data entry field where you can specify the runtime system file, (files with the ".rtm" extension are runtime system files). You may also use the "Browse" button to find the file on your local workstation. Once you have selected the file to upload press the "Submit" button to upload it to the remote system. The file will be validated on the remote system. If the file is corrupted or an incorrect runtime for the target system the update will be aborted. If the update is successful the new runtime system will be installed and the system will be rebooted automatically. Your browser will most likely timeout waiting for a response, which will never be sent. Refresh your browser about a minute later to reconnect to the rebooted system.



Reports

The reports section consists of various reports that provide information about the system hardware and software configurations. Additionally, one menu item will generate the system reports and email them to a designated support address. These reports are quite helpful in diagnosing and troubleshooting problems. Examples of the reports can be found in Appendix G.

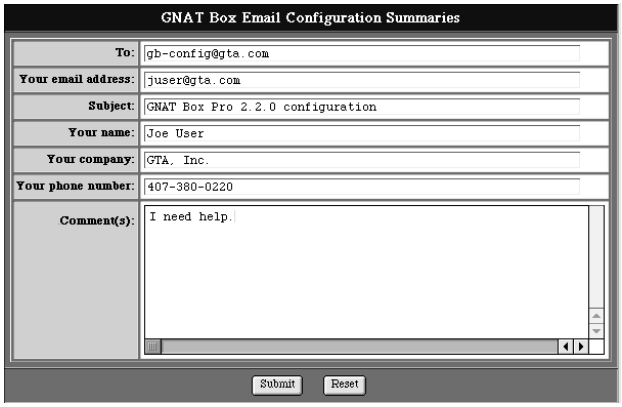
Configuration

The Configuration menu item is an excellent diagnostic tool, since it reports the current configuration state of the GNAT Box system. The report displays

information about all configuration parameters. If you need to contact technical support about a GNAT Box issue, please make sure to generate a current configuration report, which will be requested by the support staff.

Hardware

The Hardware menu item generates a report of the hardware detected in your system at boot time. This report is useful in diagnosing possible hardware problems. If you suspect a hardware problem, you should generate and review this report. If you need to contact technical support about a suspected hardware problem, you must have this report readily available.



Email Configuration

The Email Configuration... menu item is provided mainly for support purposes. However, the administrator may find this feature useful for internal reporting and auditing as well. This facility will email the following as attachments:

- A software configuration report
- A hardware configuration report
- A verification report
- A copy of the current routing table
- A copy of the current ARP table
- A binary copy of the system configuration data in MIME encapsulated format.

A comments field is supplied so the administrator can provide some additional information.

System Activity
Active ARP Table
Active Connections
Active Filters
Active Routes
Current Statistics
DHCP Leases
View Log Messages

System Activity

The System Activity menu lets the administrator access reporting facilities that provide information about the system activity of an operational GNAT Box system. Clicking on any of the menu items will generate a snapshot report of the selected facility, unless the "refresh rate" option on the report display is changed from its default of zero.

Active ARP Table

The Active ARP Table report will create and display a report listing the current ARP (Address Resolution Protocol) table used by the GNAT Box system. The report displays the IP address to MAC address translations and "Time to Live" for each entry.

Each ARP table entry is retained for 20 minutes. The ARP table is scanned every 5 minutes to check for expired entries. Once an entry is expired, the GNAT Box will not try to re-ARP the address for 20 seconds.

Active Connections

The Active Connection menu item is used to display all currently active connections, both inbound and outbound, on the GNAT Box. By default, the displayed report is static and represents only a snapshot of the connection activity at one point in time. To refresh the display and observe changes in the connection activity, simply click on the Active Connections menu item again. If you wish to have the report updated on a periodic basis click on the "Refresh Rate" link on the report display and adjust the interval to your liking, (a value of zero means no update). Simply click in the display frame to select the report and choose the desired function (save, print, email) from the menu of your browser application.

The Active Connections report displays:

- Connection Direction
- Protocol
- Source IP Address/Source Port
- NAT IP Address/NAT Port
- Destination IP Address/Destination Port
- Idle Time
- Packets Received
- Packets Sent
- Bytes Received
- Bytes Sent

Active Filters

The Active Filters report will create and display a report that lists all filters with the number of hits on each filter. Inactive Time based filters are displayed with an '*' next to the filter entry. By default the report is a static snapshot. However, the display can be updated on a periodic basis by adjusting the refresh rate.

The Active FIlters Report displays the following information for each filter type.

- Filter Number
- Filter Hits
- Filter Type
- Logical Interface
- Physical Interface
- Protocol
- Filter Actions
- From IP Address/From Netmask
- From Ports
- Destination IP Address/To Netmask
- Destination Ports

Active Routes

The Active Routes report will create and display a report that shows the active routing table used by the GNAT Box system. The report displays the destination, netmask, gateway and flags. Possible flag values are:

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

This report can be helpful in diagnosing and troubleshooting routing problems.

Current Statistics

The Current Statistics menu item provides access to the GNAT Box system statistics display. Statistics are displayed for both connections and packets of the TCP, UDP, and ICMP protocols. The current date, time, and "uptime" are printed at the top of the form. The report displays the following information:

- The current and average (60 seconds) number of connections by protocol for both inbound and outbound traffic
- The total packets sent and received by protocol for both inbound and outbound traffic
- The bandwidth utilization by protocol for both inbound and outbound traffic.
- A summary line that displays the totals for each column in the report.
- A summary line of the total of packets sent and received since the system has been booted
- A summary line of the peak bandwidth utilization
- The CPU state, which displays % user process, % system process, % interrupt, and % idle.

View Log Messages

The most recent log messages are displayed when this report item is selected. These log messages are the most recent logged, not log data from

the remote logging system. The locally logged messages are stored in a fixed size circular buffer. When the circular buffer is filled it will begin writing over older data. On GB-Light, GB-Demo, GB-Pro and GB-100 there are 512 record entries in the buffer. In GB-1000 and GB-Flash up to 1024 entries are stored in the buffer.
Warning messages are displayed in red.

Documentation

The Documentation section provides menu items that display text documents of an informational nature about the GNAT Box system.

License

Displays the GNAT Box license agreement.

Terms & Concepts

Displays a document that explains GNAT Box terms and concepts.

Troubleshooting

Displays helpful information to aid in troubleshooting problems.

Version

The version menu item displays the splash screen image. The GNAT Box software version and system name appear at the bottom of the splash screen display.

Links

The Links section provides web hyperlinks to online web pages.

MAPS - Mail Abuse Prevention System
Content Filtering - Information about the CyberNOT list
Email to GTA - Email GTA feedback
GNAT Box Home - GNAT Box website
Upgrade Information - Dynamic information about updates

Log Off

The Log Off selection will flush the persistent data that is associated with the current Admin User ID used to access the GNAT Box system thus activating the display of an “Authorization Error”. Clicking “OK” will display a Username and Password dialog box, indicating that you are no longer logged on to the remote GNAT Box system.

Verify Configuration

The Verify Configuration menu item will run a system configuration verification

check of your GNAT Box system. The check will verify the following functional areas: IP addressing, Netmasks, Interface assignment, filters, tunnels, PPP, and outbound maps. After you have configured your GNAT Box, please run the Configuration Verification check to ensure that you have a valid configuration. Make it a habit to run the check each time after you make any changes to your system. See Appendix F for an example Verification Report.

Chapter 7: GBAdmin Interface

About GBAdmin

GBAdmin is a Windows 95/98/NT/Win2000 program that is both an off-line configuration utility and an on-line remote management client. In the off-line mode GBAdmin provides a means to:

- Format floppy diskettes
- Create GNAT Box runtime diskettes
- Read/write GNAT Box runtime diskettes
- Read/write GNAT Box image data to any accessible storage device
- Merge configuration data with the runtime OS
- Make backups
- Create/modify GNAT Box configuration data
- Create system configuration reports
- Upload/download system configurations
- Upload runtime system updates

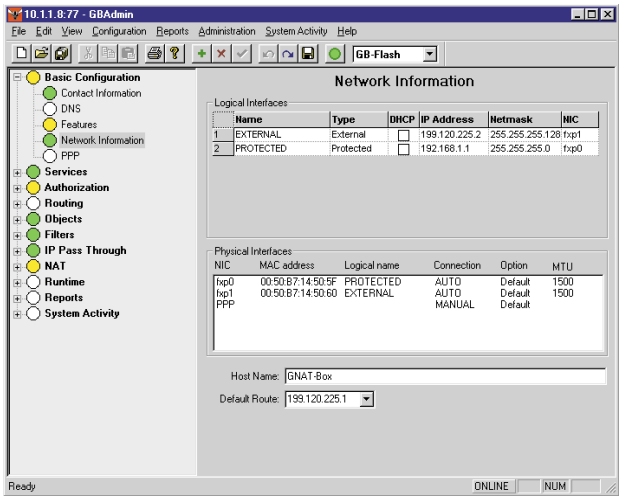
Furthermore, once GBAdmin has established a network connection to a running GNAT Box, it operates as a remote management console (RMC). In RMC mode any modifications or additions to the configuration can be immediately applied to the running remote GNAT Box system. The on-line component of GBAdmin includes the following features which are enabled when a network connection is established with a running GNAT Box system:

- All data transfers are encrypted
- Additions and modifications can be applied on a per functional section basis
- Management of encryption keys
- Generate system activity reports
- Perform system operational tasks (reboot, halt, etc.)
- Run network utilities on the remote system
- Upload/download system configurations

Requirements

- Windows 95, Window98, Windows NT 4 or Windows 2000.
- Microsoft Internet Explorer 3.x or higher installed.
- 32 Mb RAM

GBAdmin Layout

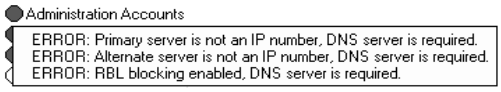


Scrolling Main Menu

The scrolling main menu located on the left side is the main access point to the configuration areas. The scrolling menu is divided into nine functional areas: 1) Basic Configuration, 2) Services, 3) Authorization 4) Routing, 5) Filters, 6) IP Pass Through, 7) NAT, and 8) Runtime 9) Reports and 10) System Activity. Each section consists of menu items and their associated status indicators. The menu items, when selected with a right mouse click, display the selected configuration dialog in the right side panel. Clicking on a section label will display help information for the specific section.

Status Indicators

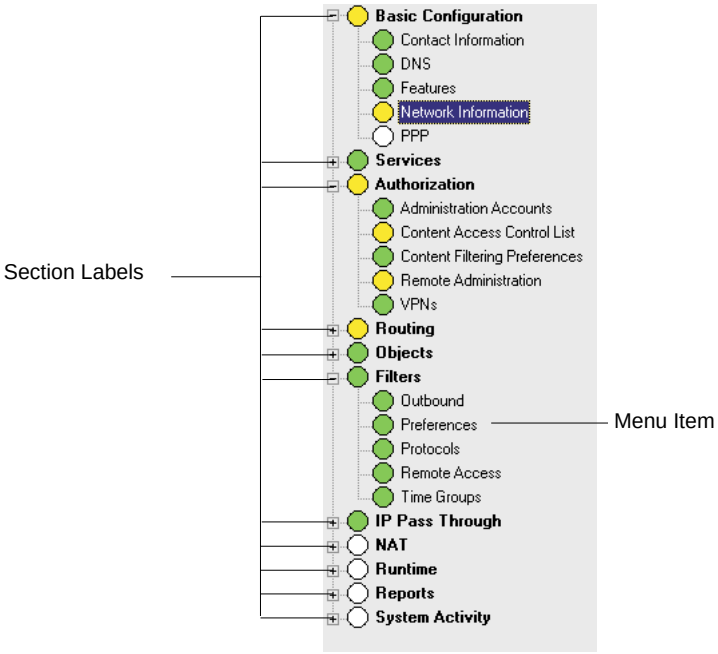
The status indicator associated with a menu item displays the status of the configuration section. The status indicators provide a quick visual indication of the status of the currently loaded configuration. Since a validation check is performed anytime data is added, deleted or modified, the state of the status indicator will changed to reflect the current state of the configuration. Error and warning messages are displayed when the mouse is moved over the status indicator.



Status Indicators Example

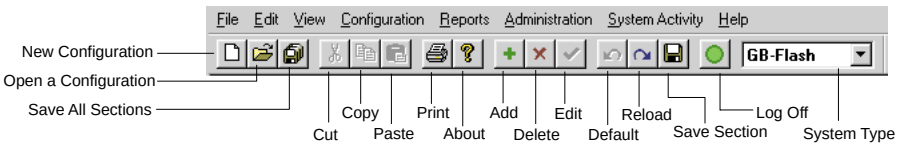
Status	Description
Empty	Section contains no data
Green	Section contains valid data
Yellow	Section contains data with warnings
Red	Section contains data with errors

Note: *Some validation is only performed when a configuration section is exited. Often status indicators will not change until the current menu item is deselected.*



Toolbar

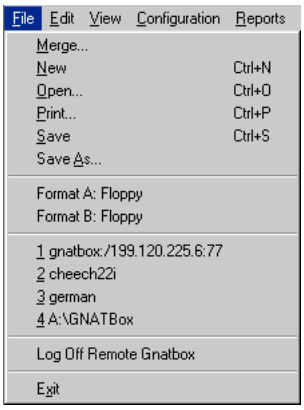
The menu bar contains pull down menus and the tool bar items. Some items are only applicable for particular configuration sections and will not be selectable when unavailable.



The Toolbar provides quick access to certain system functions common to many Windows applications. Additional items on the Tool Bar are specific to GBAdmin. Not all toolbar icons are always enabled. If a particular function does not apply to the current functional section, the icon will be 'dimmed' and the color will be removed.

File Menu

The File menu presents items which involve input/output functions such as, opening and saving data to files, formatting floppy diskettes, and creating a new empty configuration. The lower portion of the menu (above the Exit menu item) lists the most recent files that have been accessed. This file list provides quick access to the most recently used files.



Merge

This menu item provides a means to merge (and replace), either a GNAT Box runtime OS image or configuration data, with the currently loaded data. This feature is useful for performing OS runtime upgrades.

New

Creates a new empty configuration. If a configuration is currently loaded, you will be prompted to save it. If you choose not to save the current configuration all data will be lost.

Open

This menu item will open and load data into the application. Selecting the Open menu item will display the Open dialog window. This dialog window provides the user with a variety of open options. Data can be loaded from

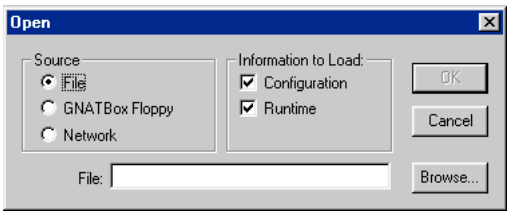
three different sources:

1. A file on any accessible direct access storage device.
2. A GNAT Box floppy diskette.
3. A network connection to a running GNAT Box system.

GBAdmin can open three different types of GNAT Box image files:

1. Runtime diskette image, which consisting of the runtime system and the configuration data.
2. Configuration data only.
3. Runtime system only.

Use the check boxes in the "**Information to Load**" section of the dialog window to select the desired image type to load.



How to Open a File or GNAT Box Diskette

Any of the three different types of images can be currently loaded from two different sources: a GNAT Box floppy diskette, or a file residing on any accessible storage medium (hard disks, network disks, floppy disks, etc.). Select the source type from the "Source" section of the dialog.

To load an image file into GBAdmin:

1. Select the image source.
2. Select the image to load.
3. Key in the complete path of the target (if a file) in the File text box, or use the Browse button to browse for the image.
4. Once the file has been selected or keyed in the File text box, press the "OK" button to load the image.

Note: *Image files are written with a ".flp" extension by default and the browse feature is configured to display only .flp files. GBAdmin will read any file regardless of name or extension, if it is stored in the correct format. If you wish to browse for a file without the .flp extension, simply select "All files(*.*) in the browse dialog window.*

How to Open a Network Connection

GBAdmin can connect to a running GNAT Box system and load the configuration data into the application's workspace.

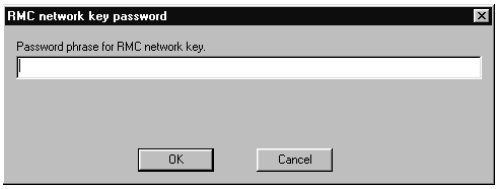
1. Enter the IP address of the remote GNAT Box system. The IP address is typically one assigned to the PROtected network interface. However, if the appropriate Remote Access Filters are in place, a network connection from GBAdmin may be established to any IP address assigned to any GNAT Box network interface (EXT, PRO, PSN). By default, GBAdmin communicates with a remote GNAT Box system on port 77 using the TCP protocol. This port may be changed to suite local requirements (make sure you modify the port number in the Remote Access filter that addresses GBAdmin remote access). If a different port is utilized then it must be specified along with the IP address at the network prompt in the Open dialog box.

   The following format is used to specify an alternative port: `xxx.xxx.xxx.xxx:port_number`, where xxx.xxx.xxx.xxx is the IP address of the remote GNAT Box system.

   Example: Use port 88

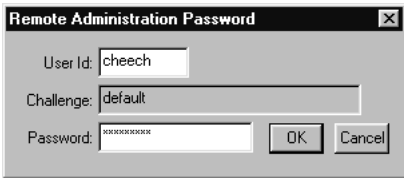
   ```
   192.168.1.2:88
   ```

2. When you save an encryption key, the key itself is encrypted when stored on the local workstation. If an encryption key has been saved for the remote GNAT Box, you will be prompted for the pass phrase which was used to encrypt the key. If you have not saved a key, you will not be prompted.



3. After a connection is established to the remote GNAT Box system, the Remote Administration Password dialog box will be displayed prompting you for a User Id and Password.

Note: *Although there is a data entry field for the Challenge portion of a challenge/ response onetime password mechanism, this facility is currently not enabled.*



4. Once a valid User Id and Password have been accepted, the data from the remote system will be loaded into the workspace of the GBAdmin program. The data may then be: modified and applied to the running GNAT Box, saved locally to a file, or to a floppy diskette.

Print

This menu item will print a configuration report for the currently loaded configuration.

Save

This menu item will save the currently loaded data to the same source from which it was loaded. If the data was created using the “New” menu option, this menu selection will operate as if the “Save As...” item was selected.

Save As

This menu item will save the currently loaded data to a specified target. Selecting the Save As... menu item will display the Save dialog window. This dialog window provides the user with a variety of save options. These options are identical to the options available in the Open dialog window discussed in the previous section.

There is no requirement to save all the currently loaded data. It is possible, therefore to save only the configuration data, even if the runtime OS data is also loaded or visa versa. This feature makes it convenient for the user to save multiple configuration files since they are quite small as opposed to a complete runtime image file which includes the OS. The Save As... menu item also allows the user to experiment with different configurations, by modifying an existing configuration and saving it under a different file name.

This facility also provides a convenient means to make a backup of a runtime GNAT Box diskette.

How to make a backup runtime diskette

1. Use the "Open..." menu item to load the GNAT Box runtime diskette.
2. Use "Save As..." to save the entire image to a local file.

Or

1. Use the "Open..." menu item to load the GNAT Box runtime diskette.
2. Remove the diskette and insert a new diskette.
3. Format the diskette.
4. Use "Save As.." to write the image to the new diskette.

The Save As... menu item can also be used to backup a remote running GNAT Box system.

How to backup a remote system

1. Open a connection to the remote system.
2. Use the "Save As..." menu item.
3. Select the destination to save the data (GNAT Box floppy diskette or local file).

Format A: Floppy

Format B: Floppy

These items invoke the system format function and provide the user with a means to format a floppy diskette in either drive A or drive B.

Recent Files

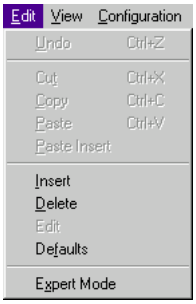
At the bottom of the File menu is a list of the last four files or remote systems accessed. Clicking on any of the entries in this list will perform an open with the file name/IP address as the parameter.

Log Off Remote GNAT Box

If a network connection is established, this menu item will be active, otherwise it will be dimmed. Clicking on this menu item when active will terminate an existing network connection. The network icon in the toolbar performs the same function.

Exit

Selecting this menu item will terminate the GBAdmin program.



Edit Menu

The Edit menu is similar to the Edit menu found in most Windows applications, with a few additional items. These following nine items correspond to the same items found on the toolbar:

Undo - undoes the last cut/paste operation.

Cut - cuts the currently selected object to the clipboard.

Copy - copies the currently selected object to the clipboard.

Paste - pastes the currently selected object from the clipboard to the current insertion point.

Paste Insert - creates a new row to paste the contents of the clipboard into the row object.

Insert - Inserts a row in a table.

Delete - Deletes a row in a table

Edit - Edit the currently selected object.

Defaults - Generates the default values for a configuration sections

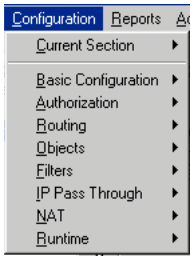
Expert Mode - Toggles the expert mode off or on. When expert mode is enabled, the “Port Number Helper” dialog is not displayed when the user clicks in the ports field of a filter definition.

View Menu

This menu provides access to menu items that control the display of the Toolbar and the Status Bar.

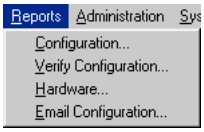
Configuration Menu

This menu duplicates access to the functional configuration areas found in the **Main Scrolling** menu. Selecting an item in any functional area will display the data entry dialog for the selected area.



Reports Menu

The Reports menu provides access to three reports that deal with the system hardware and software configuration. Additionally, there is a menu item that will email system configuration information to a designated support email address.

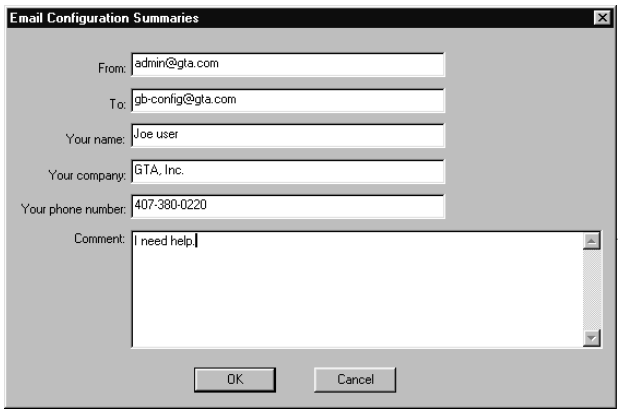


Verify Configuration

The Verify Configuration menu item will run a system configuration verification check of your GNAT Box system. The check will verify the following functional areas: IP addressing, Netmasks, Interface assignment, filters, tunnels, PPP, and outbound maps. After you have configured your GNAT Box please run the Configuration Verification check to ensure that you have a valid configuration. Make it a habit to run the check each time after you make any changes to your system. See Appendix F for an example Verification Report.

Hardware

The Hardware menu item generates a report of the hardware detected in your system at boot time. This report is useful in diagnosing possible hardware problems. If you suspect a hardware problem, you should generate this report and review the hardware the system has detected. If you need to contact technical support about a suspected hardware problem, you must have this report readily available. This report can only be generated when an network connection has been established with a remote GNAT Box system.



Email Configuration

The **Email Configuration** menu item is provided mainly for support purposes. However, the administrator may find this feature useful for internal reporting and auditing. This facility will email the following as attachments:

- A software configuration report
- A hardware configuration report
- A verification report
- A copy of the current routing table
- A copy of the current ARP table
- A binary copy of the system configuration data in MIME encapsulated format.

A comments field is supplied, so that the administrator can provide additional information. This feature is only enabled when a network connection is established with a remote GNAT Box system.

Administration Menu

The items in this menu are only active when GBAdmin has established a network connection to a remote GNAT Box system. The exception is the Network key sub-menu which is always active.

Halt... - Halts the remote GNAT Box system.

Interfaces... - Displays a dialog which allows any network interface on the remote GNAT Box to be enable or disabled.

Ping... - Provides a dialog which will execute the network ping connectivity test. The ping is executed from the remote GNAT Box system, not from the local workstation.

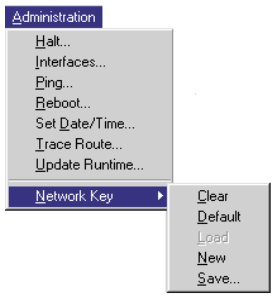
Reboot... - Reboots the remote GNAT Box system.

Set Date/Time... - Provides a means to set the date and time of the remote GNAT Box system.

Trace Route... - Executes a network trace route to a designated IP address or host name. The trace route is executed from the remote GNAT Box system. This implementation of trace route uses the ICMP protocol rather than UDP.

Update Runtime - This menu item provides a means to upload and install a GNAT Box runtime system image to a remote GNAT Box system. This feature is only available for flash based systems (GB-Flash, GB-100 and GB-1000). When this item is selected a standard file dialog box is displayed which will allow you to browse your local workstation for GNAT Box runtime files (these files have a file extension of ".rtm"). Once the file is selected press the "Open" button to upload the runtime file. A dialog box will then be displayed to confirm that you want to update the runtime on the remote GNAT Box system. Selecting "Yes" will upload the image. The remote GNAT Box system will validate the runtime file and if valid it will be installed

on the system. The system will then reboot and GBAdmin will be disconnected.



Network Key

Clear - Clears the network encryption key from memory.

Default - Sets the network encryption key to the default value.

Load - Loads the network encryption key from the local workstation.

New - Generates a new network encryption key.

Save - Saves the network encryption key for the current configuration. The key can be saved both locally and on the remote system. When saving a key, you will be prompted for a pass-phrase that will be used to encrypt the key so it can be securely stored on your local hard disk. You will be prompted for this pass-phrase when you initially attempt an on-line connection with the remote GNAT Box. Each encrypted key is associated with the configuration data for a particular remote GNAT Box system.

System Activity Menu

This menu is only active when a network connection is established with a remote GNAT Box system. This menu provides access to the System Activity reports. These
reports may also be accessed from the Main Scrolling menu. The menu items are:

Active ARP Table - Generates a report which displays the active ARP table of the remote GNAT Box system.

Active Connections - Generates a snapshot report of the current active connections on the remote GNAT Box system.

Active Filters - Generates a snapshot report of the active filter table list.

Active Routes - Generates a report which displays the active routing table of the remote GNAT Box system.

Current Statistics - Generates a report of the current statistics of the remote GNAT Box system.

Help Menu
This menu item displays a version and release information dialog box. On-line help information is accessed by clicking on the section labels in the **Main Scrolling menu**.

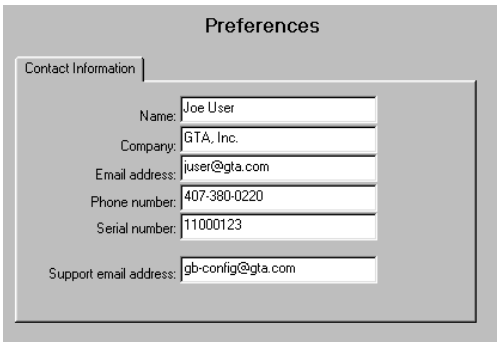
Scrolling Configuration Menu
The GBAdmin application closely matches the web browser interface. Nearly all configuration sections and rules applicable to the web browser interface also apply to GBAdmin.

A primary difference between the web browser interface and GBAdmin is that all changes made in GBAdmin are applied immediately to the data currently in memory. Data is not permanently committed to the source target (floppy diskette, file, or remote GNAT Box) until:

- A configuration file save is performed, saving the entire configuration.
- A section save is performed, where the current configuration section is written to the source target.

Basic Configuration
The Basic Configuration section consists of functional areas that address the basic setup and configuration of a GNAT Box system. Some facilities in this section need not be configured for operation of the GNAT Box system.

Contact Information
The Preferences configuration dialog provides data entry fields that store information about the GNAT Box installation, including serial number and contact information. This information is used by the "Email Configuration" facility and other reporting functions.



Name
Primary contact name.

Company
The name of your company or organization.

Email address
The email address of the primary contact.

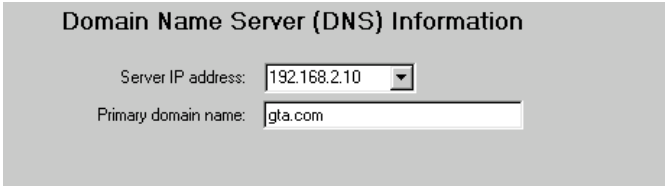
Phone number
The phone number of the primary contact.

Serial number
Your GNAT Box serial number, which can be found in several different locations: registration card, software box, and on the license certificate.

Support email address
The email address of your support organization. If you have a support contract, your reseller should provide you with an email address for this field.

DNS

Selecting the DNS menu item displays the Domain Name Server configuration dialog. Enter the IP address of a DNS server in the **Server IP address** field which the GNAT Box system will use for domain name resolution. GBAdmin maintains a global history of IP addresses that have been used in the application. You may also use the pull down to select a previously entered IP address. If you have an internal DNS server then use that IP address for your DNS name resolution, otherwise your external DNS server (which may be at your ISP), should be used.



Enter your primary domain name into **Primary domain name** field (e.g. "gnatbox.com").

Network Information

Nearly all other configuration sections depend on the data entered on the Network Information dialog. It is best to complete this dialog prior to entering data in any other configuration section. Please note that entries for some fields in the Network Information dialog depned on the hardware installed in the target GNAT Box system. The fields in the Physical Interfaces section are for display purposes only and will only contain data if configuration is loaded from a GNAT Box configuration source that was actually booted in a GNAT Box system.

Once the configuration is booted, any supported devices present are detected by the GNAT Box system. If devices previously selected in the Device Type field do not match the actual devices present, the GNAT Box system will detect this situation. The console user interface's Network Information screen will be displayed, so that the correct device assignments can be made and the system can continue booting.

One of the purposes of the Network Information dialog is to associate a physical interface with a logical interface. This makes changes very convenient since throughout the GNAT Box configuration all references are to the logical interface and not the physical interface.

Logical Interfaces

In the Logical Interfaces section, you assign an IP address, netmask, and a physical device name to each logical interface on your GNAT Box system. If you will not be using a PSN and have not installed a network card, simply leave the PSN data entry fields with their default values.

Name

The **Logical Name** field allows the administrator to name each interface to suit local conventions. By default the Logical Name values are set to the traditional GNAT Box names of: Protected, External and PSN.

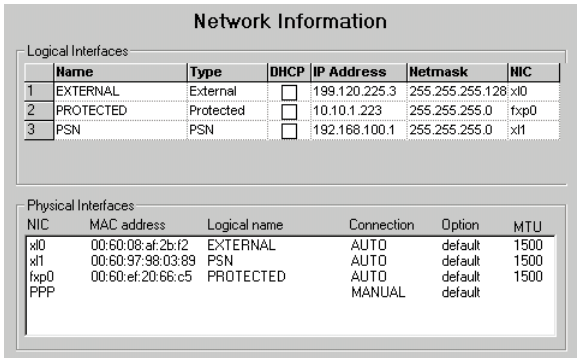
Type

The **Type** column lists the possible logical network interface types that are available on the GNAT Box system. There are three logical interfaces types available on a GNAT Box system:

External	External network interface.
Protected	Protected network interface.
PSN	Private Service network interface.

The minimum GNAT Box configuration requires that both an External and Protected network interface be present and configured. Since the standard GNAT Box system allows only three network interfaces, the remaining network interface typically is assigned the PSN type, however this is not a requirement. It is therefore possible to have two External and one Protected interface or two Protected and one External.

Note: *The* ***GNAT Box Multi-interface option*** *allows a system to utilize up to 16 network interfaces of any supported type.*



DHCP

The DHCP (Dynamic Host Configuration Protocol) field, when checked, utilizes the DHCP protocol to obtain an IP address for the specified network interface. When the DHCP field is checked, the IP and netmask fields are protected from user input. The assigned DHCP IP address/netmask will be displayed in these protected fields after assignment. DHCP may be used on all network interfaces. Users of cable modems typically require the use of DHCP on their External network interface.

IP Address
This is the IP address of the logical network interface. The IP address is entered in standard "dotted decimal" notation. An IP address must be entered for each active network interface, except for a PPP connection. This field will not allow data entry, since address assignment is handled on the PPP configuration dialog.

Netmask
Each active network interface must have a netmask. The value of the netmask is depends on the network the interface will be attached to. Some common netmasks are:

Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

NIC
This field is used to select the physical network device which will be associated with the logical name. The device type field is a choice list of all possible devices that can be present on a GNAT Box system. If you aren't sure of the type of network card installed in your target GNAT Box system, simply pick any of the network interfaces available. However, you are configuring a PPP setup, however you must select PPP.

Since the actual devices will be displayed on the runtime system, it is simply a matter of assigning the correct physical interface to the logical interface via the console user interface (a task performed only once).

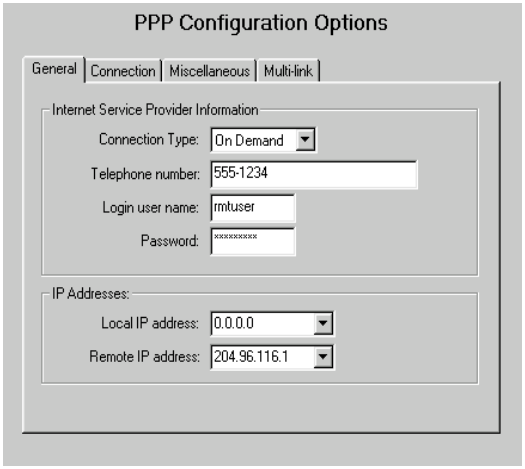
Physcial Interfaces
This section is always protected in the GBAdmin application. If you load a configuration that has been booted and run on a GNAT Box system, this section should contain information about the physical interfaces present in that system. Otherwise this section will be empty.

This name is used to tag log messages. It is not a DNS host name, although you can use such a name if desired.

The default route is generally the IP address of your router that connects your network to the Internet. The default route is the gateway where any non-local IP packets are sent.

It is important to remember that a default route must always be on the same logical network as the External network interface. The only exception being in the case of a GNAT Box PPP connection.

The PPP configuration dialog only needs to be completed, if you are performing a PPP configuration and have selected PPP as the device type for the External network interface in the Network Information dialog.



Select the desired connection type from the pull down choice list. The available connection types are:

On-demand - This connection type will initiate and establish a PPP connection (if the link is down) with the remote site, whenever a packet arrives on the Protected or PSN interfaces and is destined for the External network. The PPP link will stay up as long as packets are received before the specified time-out period has expired.

On-enabled - This type of connection requires the GNAT Box administrator to manually enable the External network interface, which will then initiate a PPP session and establish a link with the remote site. The External network interface may be enabled either from the Interfaces option under the Admin menu on the Console interface, or from the Interfaces menu item on the web browser admin interface. The PPP link will stay established until manually disabled by the GNAT Box administrator.

Dedicated - This type of connection means that a PPP link will be established when the GNAT Box system boots up. The PPP link will remain up until the GNAT Box administrator manually disables the interface or the system is halted.

Telephone Number

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

Login user Name and Password

Enter the user id used for remote PPP access. This is the user id issued by the remote site. The password is obscured in the data entry field. If the remote system uses CHAP or PAP you will have to configure those parameters either from the Advance Options section of the Console interface, or use the Web Browser interface once your GNAT Box system has booted up.

Local and Remote IP Numbers

A PPP link uses two IP addresses: one is local and the other is remote. The GNAT Box PPP facility has the capability to negotiate the local and remote address dynamically, if the remote site supports dynamic address assignment (generally the default for most ISPs and remote sites). Dedicated IP addresses are supported for either.

Dynamic Address Assignment

If your remote site uses dynamic address assignment (this is the most common case), then use the following configuration:

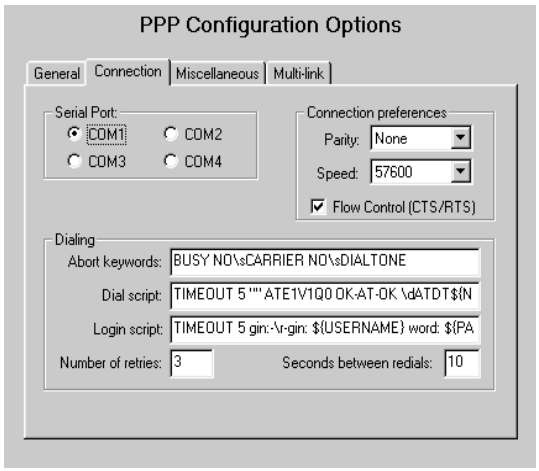
1. Leave the Local IP address set to 0.0.0.0; the default.
2. In the Remote IP address field, enter an IP address that may be assigned dynamically. It is not important that the specified IP number will actually be assigned, since this value will be negotiated. The PPP protocol, however, requires that an IP address be used that resides on the remote network. Very often a good choice for this number is the remote system's router IP address or DNS server IP address.

Static Address Assignment

If you have a dedicated Local and/or Remote IP address, enter the appli-

cable addresses in the appropriate fields. If you have a dedicated Local IP address, but the Remote side is dynamic, use the technique described in Dynamic Address Assignment for the Remote IP address. If your Remote IP address is static, simply leave the Local IP number set to: 0.0.0.0.

Connection Dialog



Serial Port

Select the COM port which will be used for the PPP interface. Only COM ports 1-4 are allowed. The COM port may be an internal modem card or a serial interface.

Connection preferences

Parity None, Odd or Even

Modem Speed DTE speed

1200, 2400, 9600, 19200, 38400, 57600, 76800, 115200

CTS/RTS

CTS/RTS handshaking is enabled by default. Uncheck this option if you wish to disable this feature.

Dialing

Abort Keywords

Many modems will report the status of the call as a string. These strings may be **CONNECTED** or **NO CARRIER** or **BUSY**. It is often desirable to terminate the script should the modem fail to connect to the remote. The difficulty is that a script would not know exactly which modem string it may receive. On one attempt, it may receive **BUSY** while the next time it may receive **NO CARRIER**. These "abort" strings may be specified in the Abort keywords data entry field. The keywords should be entered with a space separating each word. For abort strings that have embedded spaces use the escape character "\s" to represent the space.

Example:

```
BUSY NO\sCARRIER ERROR
```

If the chat facility receives any of the abort strings, the chat session will terminate.

Dial Script

The default dial script tends to work for most configurations. Make adjustments for your modem and local telephone configuration. The purpose of the dial script is to instruct the modem to dial the remote PPP server. Initialization of the modem and any special configuration should be done in this script.

The default **Dial Script** is:

```
TIMEOUT 5 "" ATE1V1Q0 OK-AT-OK \dATDT${NUM} TIMEOUT 60 CONNECT
```

The script sets up a 5 second time, expects nothing, then sets the modem to echo mode and response codes returned. An expect string of "OK" should be returned, if not, an "AT" command is sent and an expect string of "OK" should be returned. Next the script will delay 1/10th of a second, then dial the telephone number using the telephone number token ${NUM} with tone dialing. The timeout is increased to 60 seconds and the expect string should be "CONNECT." If the script receives the expect string, the chat facility begins processing the Login Script. See the discussion about chat scripts in Appendix A for further information.

Login Script

The **Login Script** provides the script used to communicate with the remote PPP server login facility. The Login Script uses the same grammar and rules

as the Dial Script. The tokens ${USERNAME} and ${PASSWORD} are provided for use in the Login script. The default GNAT Box Login script is listed below.

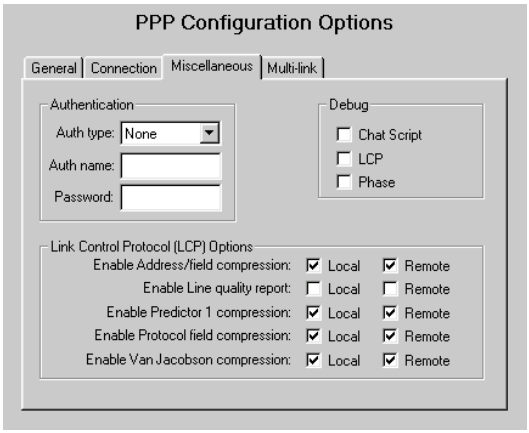
This login script is typical:

```
TIMEOUT 5 gin:-BREAK-gin: ${USERNAME} word: ${PASSWORD}
```

See the discussion about chat scripting in appendix A for more information about creating a login script.

Number of Retries
Default is 3. This is the number of attempts the system will make before giving up on establishing a connection. After failure, any new packets arriving for the external network will restart a new dialing attempt.

Time Before Retry
Default is 10 seconds. This is the amount of time to wait before retrying after a failure.



Authentication
This configuration dialog deals with PPP protocol options.

Auth Type - Default value is: **None**. This option allows the authentication protocols of PAP and CHAP to be enabled.

Auth Name - When the Authentication Type is set to none, this field is ignored. Enter the authentication name or id for the selected authentication protocol in this field.

Password - When the Authentication Type is set to none, this field is ignored. Enter the authentication password for the selected authentication protocol in this field.

Debug
These options, when enabled, provide helpful information when a PPP configuration is initially created. There are three debug options:

Chat - Display the dialing and login chat script conversations. This option is very helpful in defining and configuring chat scripts.

LCP - Displays the LCP conversation between the remote and local side of the PPP connection. Use this debug option to help select the appropriate LCP options.

Phase - Displays the network phase conversation. This debug output can be useful in determining the specification of both the Local and Remote IP addresses.

Link Control Protocol Options
This section allows for the specification of Link Control Protocol (LCP) options. In most cases the default settings work just fine, but for some remote access devices certain LCP values may need to be changed. There are two settings for each available LCP option; one for the local side and the other for the remote side of the connection. If the local side option is set to enable, the GNAT Box will request that the remote side use the selected LCP option. If enable is not set, no request will be made from the local side. If the remote side option of accept is set, the local side will "accept" the option if offered by the remote side.

The available LCP options are:
Address and Field Compression
Line Quality Report
Predictor 1 Compression
Protocol Field Compression
Van Jacobson Compression

If you are unsure of which option to set, simply use the default values and enable the LCP debug option. When the configuration is run on the target GNAT Box system and a PPP session is attempted, you can monitor the LCP debug output on the primary console (ALT-F1). As the LCP conversation proceeds watch for which options are rejected and requested, and set your LCP options to match the request.

Multi-Link

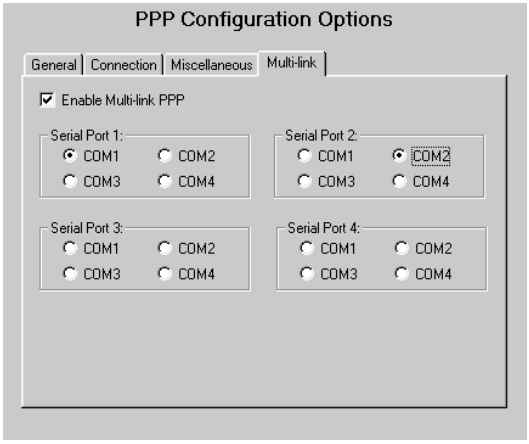
This configuration dialog deals with the Multi-link PPP protocol options.

Enable Multi-Link PPP

This checkbox should be selected, if you will be using multi-link PPP.

Serial Ports

Select the COM port that will be used for each modem in the multi-link PPP configuration. Make sure that a different COM port is selected for each modem. All other parameters concerning the serial interfaces are set on the Connection tab dialog.



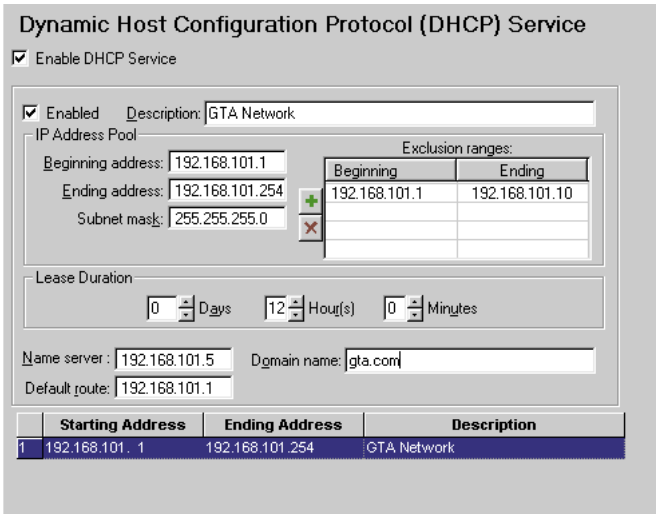
Services

The Services menu consists of those functions that provide services. These include the two built-in servers: DHCP Server and DNS Server, the Email Proxy and the Remote Logging facility. All of these services are optional, as they do not

have to be operational in order for the GNAT Box system to function. However the use of a service such as the Email Proxy can add to the security of your GNAT Box system, (it is highly recommended that you run the Email Proxy).

DHCP Server

DHCP, Dynamic Host Configuration Protocol, automates the process of assigning IP addresses to host systems on locally attached networks. Additionally DNS server and default route can be provided by the DHCP server. The DHCP server manages a range of IP addresses (i.e. 10.10.10.4 - 10.10.10.254) which can be assigned to clients. The address ranges do not need to be contiguous. Non-contiguous ranges are defined using exclusion ranges. An exclusion range defines a range of IP addresses that should not be assigned from the pool of IP addresses.



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 always reassign the same IP address. The only time it will not reassign the same IP address, is when the number of clients exceeds the number of addresses in the pool and the previous IP address was assigned to a different host.

Selecting the DHCP option from the Services menu will display the DHCP server configuration form. This form has a detail display area at the top and a summary list of defined DHCP IP address Pools at the bottom. To add a DHCP IP address

pool click the “+” icon on the toolbar and an empty row will be added to the summary list. When the row is selected its detailed data will be displayed in the upper date entry section of the form. To delete an IP Address Pool, select the row and click “X” in the toolbar. All changes will not be applied until either the section is saved or then entire configuration is saved. If a network connection is established and the section is saved those changes will be immediately applied to the remote GNAT Box system.

Enable DHCP Service
If this checkbox is select the DHCP server will be started when the GNAT Box system boots or restarted if the section is saved. To disable the DHCP server deselect the checkbox.

Enable
Select this checkbox to enable the currently displayed DHCP IP Address Pool. Deselect it to disable the currently displayed IP Address Pool.

Description
Enter a description of the currently displayed DHCP IP Address Pool.

IP Address Pool Section
This section allows the administrator to define the begining and ending IP address of the address range. Up to 5 exclusion ranges can be defined. Each exclusion range defines an inclusive range of IP addresses that are to be excluded from the range defined by the begininng and ending IP address. The DNS server and default route that DHCP clients should use cal also be configured on the screen.

Beginning Address
This is the first IP, of a block of IP’s, that will be assigned.

Ending Address
This is the last IP, of a block of IP’s, that iwll be assigned.

Netmask
This is the netmask to assign to DHCP clients.

Exclusion Ranges
Define up to 5 inclusive ranges of addresses to exclude from being assigned. To exclude a single IP, enter the IP address to be excluded in both

the beginning and ending address fields. Click the "+" icon to the left of the Exclusion Range table to add an exclusion range. Select the row and click the "X" to delete a range.

Lease Duration
This is the maximum time that the DHCP address is valid for a requesting client to use. A client must negotiate to reuse the assigned address before the end of the least time or quit using the address.

Name Server IP Address
This is the IP address of a DNS server that will issued to the requesting client. This IP can be any valid DNS server. It can be that of a local DNS server (such as the built-in GNAT Box DNS server) or a server that is remote from the local area network, (e.g. located at an ISP).

Domain Name
This is a DNS domain name. It typically is that of the local network.

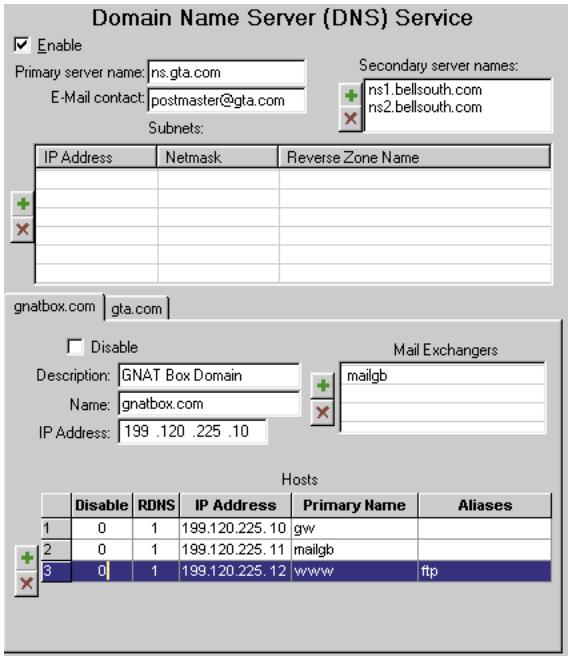
Default Route
The value is the IP address that the requesting clients will use for their default route, (gateway). For hosts located behind a GNAT Box system, (on Protected or PSN networks) this value will be the IP address of the GNAT Box NIC where the network is attached, (i.e. if the client is located on the Protected network then the Default route will be the Protected NICs' IP address).

Note: *If the DHCP service is for an External network then the default route would most likely be the Internet router's IP address.*

DNS Server
The GNAT Box DNS (Domain Name Server) server functions as a primary domain name server, (functionality as a secondary DNS server is not supported). Before configuring the DNS server you should have an understanding of how the domain name system functions on the Internet. A good reference book about DNS is: **DNS and Bind** 3rd edition by Paul Albitz & Cricket Liu, published by O'Reilly and Associates.

The configuration and operation of a DNS server can range from simple to complex. The built-in DNS server in the GNAT Box system provides a great deal of functionality and flexibity, however it can not be configured to support every

possible configuration or option available in DNS. It however does address the needs of most GNAT Box system users. If your site requires DNS services that require complex configurations, or hosting secondary name services then the built-in DNS server will probably not meet your requirements. It is suggested that with such requirements your site would be better served by a DNS server hosted on a separte host.



When the DNS Server item is selected from the menu the DNS Service form is displayed. This form is divided into two sections with the top of the form containing general data entry fields specific to the DNS server. While the bottom part of the form contains information about the DNS zones that will be served by the DNS server. The DNS server must first be enable before data entry can take place.

To add a zone click the “+” icon on the toolbar. To delete a zone, select its tab from the defined zone in the lower part of the form and click “X” from the toolbar. All changes will be applied with the section is saved. If you have an online connection to a remote GNAT Box system and save the section all changes will be applied immediately.

Enable
If this checkbox is selected the the DNS server will start up/re-start when the section is saved. To halt and disable the DNS server de-select the checkbox and save the section. If you are online connected to a remote GNAT Box system these changes will be applied immediately once you save the section.

Primary Server Name
The hostname of your DNS server. This will be a host name assigned to your GNAT Box (if you are configuring a external DNS server then this will be the host name seen from the Internet side). The host name should be listed as a host in the domain defintion section.

Secondary Server name
These are the host names of DNS servers that will be acting as secondary servers for the domain. Up to four secondary name servers may be listed.

E-mail Contact
This field should contain the e-mail address of the primary contact for the domain. (i.e. administrator@gta.com).

Subnets
For most domains this section is not required and can remain empty. However if your domain falls into the special case situation of having a subnet rather than a full network assigned to your domain you will need to use this section.

DNS subnets provide a way for splitting up a network into a series of contiguous same size address ranges. These are commonly used to help with performance and managability of large networks. The IP Address and Netmask fields are used to identify the subnet desired.

To add a Subnet click the "+" icon to the left of the Subnet table. To delete a Subnet, select the row and click the "X" icon to the left of the table.

IP Address
This field should contain the network address of the subnet, (i.e. 199.120.225.128).

Netmask
Each subnet must have a netmask. The value of the netmask is dependent on the subnet they will be associated with. Some common netmasks are:

Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

Reverse Zone Name
Reverse Zone Name is the optional zone name used for reverse name address resolution (i.e addeess to name). The GNAT Box can automatically determine the zone name if the subnet uses a Class A, B or C netmask. Normally if needed, reverse zone names are assigned to you by your ISP. For the network 199.120.225.128 with netmask 255.255.255.128 the reverse zone name might be: 128/25.225.120.199.in-addr.arpa.

Domain Name Edit Form
This data entry form is displayed when you either add or edit an entry in the domain name summary list. This form is used to define host names and their associated IP addresses (A records) , aliases (CNAME records) mail exchangers (MX records) for the selected domain zone.

Disable
When this checkbox is selected the domain definition is disabled and the zone will not be served by the GNAT Box name server. You must save the section to make this select effective if online. De-selecting the checkbox and saving the section will make the zone available to be served by the GNAT Box name server.

Description
This field should contain a brief description of the domain for your reference.

Domain name
This is the DNS domain name for the current zone defintion, (i.e. gnatbox.com).

Domain IP address
Often it is a good idea to have a host (A record) in your zone that has the same name as the zone. (i.e. gnatbox.com). This means that, for example, if you have a web server a visitor can simply use the zone name rather than the fully qualified host name for the the web server. Enter the IP address of a host that you would like to response to the zone name.

Mail Exchangers
When a remote system sends mail to this domain, it will query a DNS server to determine what IP addresses are designated to accept email for the zone. The Mail Exchanger fields define the mail server(s) for the domain. When there is more than one Mail Exhanger for the zone, they are graded in order of preference. The desired order of preference is specified by entering the most perferred server in the first field, followed by a second and third entry. Very often there is only one Mail Exchanger for a zone, so the second and third fields are not required. The first mail exchanger will receive a priority of 5, the second 10 and the third 15.

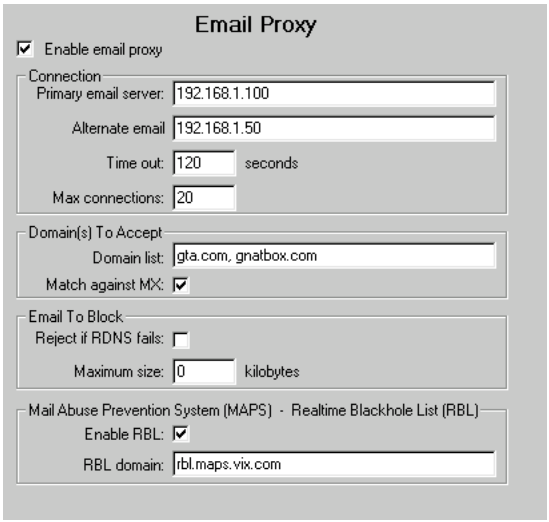
Email Proxy
The Email Proxy dialog is used to configure the GNAT Box Email Proxy. The Email Proxy is a SMTP (TCP/25) proxy which is used to proxy inbound email connections. The Email proxy will answer on any IP address assigned to the External NIC, unless a tunnel is created on port 25/TCP which will then override the proxy startup on the IP address in question. The GNAT Box email proxy shields your internal email server from unauthorized access attempts through SMTP exploits. Additionally, the GNAT Box email proxy provides facilities to reduce and possibly eliminate unsolicited email (known as "SPAM").

Enable Email Proxy
To enable the email proxy this checkbox must be selected. To disable the email proxy deselect this item.

Connection
In this section is where the administrator enters data for parameters that are involved with the email proxy connection.

Primary email server

This field should contain the host name (if an internal DNS server has been configured on your GNAT Box system) or IP address of your email server. The primary email server must reside either on the PSN or Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.



This field should contain the host name (if an internal DNS server has been configured on your GNAT Box system) or IP address of a backup or secondary email server, if you have one. The secondary email server must reside either on the PSN or Protected network. Defining an email server that does not reside behind the GNAT Box system will render the Email Proxy unusable.

Connection Timeout

The time value is the number of seconds to wait between each SMTP command exchange.

Maximum Connections

This parameter is the maximum number of simultaneous SMTP connections you wish to run on the GNAT Box. If additional connections are attempted once this maximum limit has been reached, the additional connections will be deferred, until a connection slot becomes available. Each simultaneous connection invokes a copy of the SMTP proxy program.

Domain(s) to Accept
The GNAT Box Email Proxy will only accept SMTP connections for specific domains. The domains are either explicitly specified manually in the Domain list and/or rely on the DNS MX records that are assigned to the IP Address(es) on the EXTernal NIC of the GNAT Box.

Domain List
Enter your primary and any additional email domains which you wish to accept email. The domains should be separated by a whitespace (blank, tab), or comma. This field may be used in conjunction with the MX (DNS Mail Exchanger Record) match option. This facility prevents your site from being used to relay email to other sites.

Match against MX
If this item is enabled, the GNAT Box Email proxy will make a DNS MX record query to determine if the domain(s) assigned to the IP Address on which the proxy answered matches the domain in the "To:" portion of the email header. If there is no match, the email is rejected. This facility prevents your site from being used to relay email to other sites.

Email to Block
This section allows the administrator the ability to impose additional controls over inbound SMTP connections.

Reject if RDNS fails
If this item is enabled the GNAT Box Email proxy will perform a reverse DNS lookup on the IP address of the remote host attempting to make the SMTP connection. A DNS lookup is then performed on the returned host name to see if it matches the IP address of the remote host. If these lookups fail or don't match, the connection is refused. This facility imposes a stringent requirement on all hosts wishing to deliver email to an address in your domain. Although all hosts on the Internet should be correctly defined in DNS, many sites have improper or mis-configured DNS entries. If you chose to enable this facility, legitimate hosts which are not properly defined in DNS will not be able to deliver email to your domain.

Note: If a DNS server has not been defined in the DNS configuration section, this facility will not function correctly.

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

Mail Abuse Prevention System
The Mail Abuse Prevention System (MAPS) - Realtime Blackhole List (RBL) is a list of hosts and domains that have been documented as transmitting and/or generating unsolicited email (SPAM).

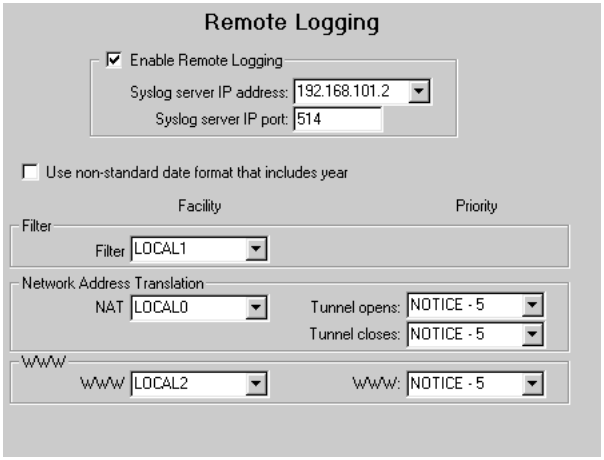
MAPS1, MAPS2, MAPS3, MAPS4
The four MAPS data entry fields provide the administrator to selectively enable specific MAPS servers to be utilized to block email from known SPAM sites (sites that send bulk unsolicited email). The administrator may replace the provided MAPS sites with other sites if desired.

Currently the primary site is: “rbl.maps.vix.com”. More sites should soon be available at other locations around the world. Please check the RBL website: **http://www.maps.vix.com** for updated site information.

Remote Logging
The Remote Logging data entry form provides a means to configure how and where log information is sent. The GNAT Box system uses the syslog TCP/IP protocol for recording logs remotely. The syslog service is a standard Unix service. However, a server for use under Windows NT, Windows95/98 or Windows2000 is provided with the GNAT Box installation.

If you wish to enable remote logging, simply enter the IP address of the host system that will receive the syslog data. Changing the IP address requires a system reboot, before the change becomes effective.

Note: *Enabled log events are always displayed on the main console (ALT-F1), regardless if you have remote logging enabled or not.*



Use non-standard date format that includes year
If this option is checked a non-standard date format will be used in the log in place of the standard syslog date/time format. The non-standard date/time log format provides 3rd party log clients and analysis programs a date/time stamp that is complete and easier to parse.

Standard syslog date/time format: **MMM dd hh:mm:ss**
MMM - three character month
dd - day
hh - hou
mm - minutes
ss - seconds
Example: Aug 20 19:21:28

Non-standard date/time format: **MM/DD/CCYY hh:mm:ss**
MM - 2 digit month
DD - 2 digit day
CC - 2 digit century
YY - 2 digit year
Example: 08/20/2000 19:21:52

Filter Facility
The **Filter facility** list contains all the standard Unix syslog facilities, some of which have no context for the GNAT Box. However, all of the facilities are available for use. The Filter Facility is the syslog stream which logs informa-

tion associated with any filter that has logging enabled. Additionally, the default logging configuration is set to log any rejected packets to this log stream. Any attempts at unauthorized access will be logged to the Filter Facility log stream. This facility may be disabled by selecting “none” in the choice list.

NAT Facility

The **NAT facility** list is the same list used by the Filter Facility field. The NAT facility is the syslog stream which logs information associated with any network address translation, which essentially means “outbound packets.” Selecting “none” will disable the remote logging of NAT packets.

WWW Facility

The **WWW facility** list is the same list used by the Filter facility field. The WWW facility is the syslog stream which logs all URLs accessed through the GNAT Box system. Selecting “none” will disable the remote logging of URL information.

Tunnel Opens and Closes

Both of the **Priority to log tunnel** lists contain all the standard Unix syslog priorities, some of which have no context for the GNAT Box. However all of the priorities are available for use. Whenever a network connection is initiated, an “open”, log record will be generated. If you wish to log these “open” then select a priority other than “**none**.” A “close” record will be generated when a network connection is terminated. In addition to the standard log information, “close” records contain the number of packets and bytes sent and received. To disable the generation of remote “close” log records, set the priority to “**none**.”

Other Log Data

All other log data is sent to the “daemon” facility. This data includes:

- Audit trails of all modifications made to the GNAT Box system.
- Remote administration access from either the web browser or GBAdmin.
- Console administration access.
- Startup messages.
- System warning and diagnostic messages.

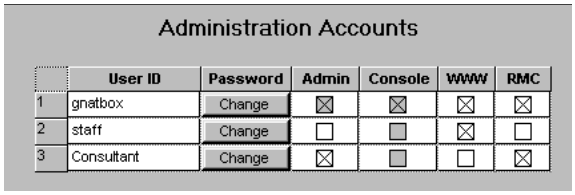
Authorization Menu

The Authorization menu consists of those functional areas that address authorization for administration, content filtering, remote administration and VPNs.

Admin Accounts

The Administration Accounts section provides a means to manage the administration accounts that are used to access the GNAT Box system. Up to five (5) additional administration accounts can be defined. Each additional account is assigned a unique User ID, password and access privileges. The default administration account has a default user ID of "gnatbox". However, this may be changed using this interface. The primary administration account ("gnatbox") is the only account that can login on the GNAT Box console. All other privileges can be assigned to new accounts other than this capability.

User ID - This is the administration account name which is used to login on to the GNAT Box system. It may be up to 39 characters long. Any characters that can be generated from the keyboard are valid, except leading and trailing spaces.



Password - The password may be up to 39 characters long. Any characters that can be generated from the keyboard are valid. However leading and trailing spaces are not valid.

Admin - If enabled the admin account has update authority.

Console - If enabled the admin account can login on the console.

WWW - If enabled the admin account can login via the web browser interface.

RMC - If enabled the admin account can login via the Win95/98/NT remote management console (GBAdmin).

To Add an Account

1. Click the “add” icon from the toolbar to create a new row in the table.
2. Enter the User ID (up to 32 characters)
3. Select the options that are to be enabled for the new account.
4. Click the Change button in the Password column to display the password dialog box.
5. Complete the password dialog window to create a password for the new account.
6. Update the section if on-line.

To Delete an Account

1. Select the row of the account to be deleted, then click the “delete” icon from the toolbar.
2. Update the section if on-line.

Content Filtering

Content Filtering provides the administrator with the ability to control web site access based on the content of the web site. The GNAT Box system provides two methods for web site access control. The first facility is the CyberNOT list, which is a built-in content filtering facility running directly on the GNAT Box system. The second facility is the Websense content filtering system, which runs on a separate server.

CyberNOT List

The CyberNOT list is a built-in GNAT Box facility. In order to use this facility you are required to purchase an annual subscription. Once you purchase the subscription you will receive an activation code to enable the facility on your GNAT Box system.

Websense

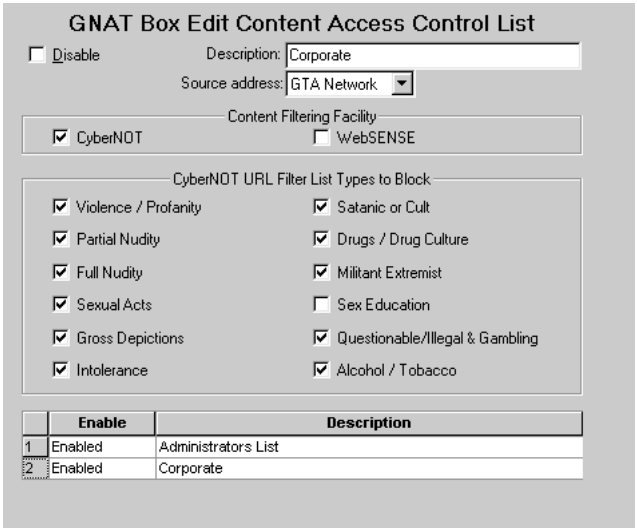
Websense is a content filtering system that runs on a remote server (NT or Solaris). A Websense license subscription must first be purchased and installed on a remote server before you can use it with GNAT Box. You should install and configure your Websense server prior to setting any options for it on the GNAT Box system.

Content Access Control Lists

The Content Access Control Lists provides a means to specify how the selected web access control facility (CyberNOT or Websense) will be applied to web requests. The Content Access Control Lists consists of one or more definitions of

groups of IP addresses and how the content filtering facility will be applied to them.

When the Content Access Control List menu item is selected the Content Access Control List form will be displayed. The upper part of the form displays detail about the selected Access Control List. The lower part of the form is a summary list of each defined Access Control List. To add an Access Control List click on the "+" icon on the toolbar. To delete a list, select the row that contains the list and click the "X" on the toolbar. The access control list is processed sequentially, so order is important. Any changes, deletetions or additions to the list will be applied only after the section is saved.



Disable

If this checkbox is selected then the access control list will be disabled and not used for access control filtering.

Description

This field should contain a description of the access control list.

Source Address

This entry must be a IP Address object. Only defined IP Address objects will be listed in the pull down. The IP Address object selected for this field will be used to match against web requests. If web request

matches an element of the specified IP Address object then the specified content filtering facility will be used to process the packet.

Content Filtering Facility

CyberNOT - if this item is checked then the packet will be processed against the CyberNOT list.

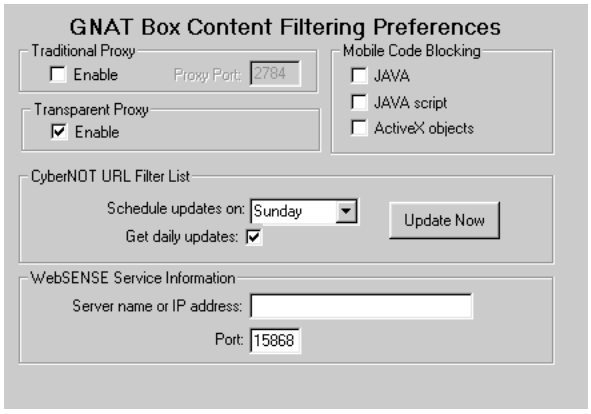
WebSense - if this item is checked then the packet will be processed by the Websense server.

CyberNOT URL Filter Lists Types to Block

If CyberNOT was selected then the categories selected in this section will be used to filter the web request.

Content Filtering Preferences

Content Filtering Preferences form provides the administrator a means to specify the access control facility (if any) and which proxy mechanism to use with the access control facility. This form also allows the administrator to schedule when the CyberNOT list will be updated.



Traditional Proxy

This method requires all users located on the Protected network to configure their browsers for a proxy. All URL requests will be directed to the designated proxy.

1. **Enable.** Make sure the Enabled Traditional Proxy is checked.

2. **Set the Proxy Port.** When the GNAT Box is operating without a content filtering mechanism enabled, it does not use a proxy mechanism. However,

when the GNAT Box http proxy is used in conjunction with a content filtering facility (CyberNOT or Websense) it runs on TCP port 2784 by default. If the user wishes to run the http proxy on a different port, enter the value in the Port field at the top of the dialog box. This proxy port is the port number users should set their web browsers to for use with the GNAT Box content filtering configuration.

Websense

1. If you are using the Websense OpenServer enter the IP address in the Server field, under the Websense Server Information section.

2. If you are using the Websense Openserver set the port number used by the Websense server. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the WebSense Port field.

CyberNOT

No additional server configuration is required for the CyberNOT facility since it runs directly on the GNAT Box system.

Note: *Users should set the proxy IP address to that of the GNAT Boxes' Protected network interface IP address, (this is the same address users should have as their Gateway/default route).*

Transparent Proxy

This method is transparent to users located on the Protected network; no modification to a browser is required.

1. **Enable** - Select the Enabled checkbox for the Transparent Proxy.
   Websense
   1. If you are using the Websense OpenServer enter the IP address in the Server field, under the Websense Server Information section.

   2. If you are using the Websense Openserver set the port number used by the Websense server. The default port used by the OpenServer is 15868. If you have configured your OpenServer to use a different port, enter that value in the WebSense Port field.

   CyberNOT

   No additional server configuration is required for the CyberNOT facility

since it runs directly on the GNAT Box system.

CyberNOT URL Filter List
Either manual or automatic updates for the CyberNOT URL Filter List may be done through this section. To manually update CyberNOT's URL Filter List simply click the "Update Now" button. Automatic updating takes place daily on the day specified from Sunday through Saturday.

Get main list on - Valid selections are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday, which will specify the day to perform automatic updates.

Get Daily Updates - To enable automatic updates of the CyberNOT URL Filter List make sure this checkbox is selected.

Update Now - Manually begin the update process of the CyberNOT URL Filter List. This facility only functions if you have installed an activation code for the CyberNOT subscription.

Note: *Make sure you have defined a DNS server in the DNS section under Basic Configuration, as the system needs to lookup and access the CyberNOT List server.*

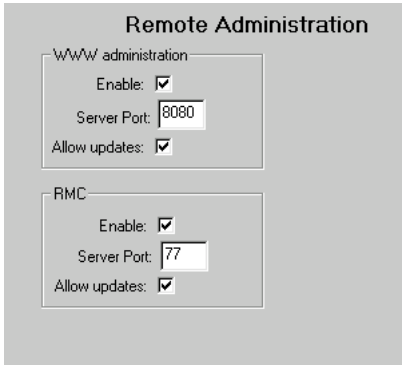
WebSENSE Service Information
This section only needs to be completed if you are using the Websense server facility.
Server - Either the DNS Name or IP Address of the Websense server should be entered in this field to use the Websense URL filtering.

Port - The port the WebSENSE server listens to for URL filtering requests. The default this port is 15868.

Mobile Code Blocking
The GNAT Boxes' built-in facility to block mobile code (i.e. JAVA, JAVA Script, and ActiveX) may block any combinations of these three, which appear in the inbound HTML streams on TCP port 80, 8000, and 8080.

Remote Administration
The **Remote Administration** menu item displays the Remote Administration dialog window, which provides a means to control if and how remote administration, via the Web Browser interface and the Remote Management Console

(GBAdmin), of the GNAT Box will be provided. The default settings enable remote administration and the ability to apply updates, with the Web Browser interface being served on the standard TCP port 80 and the RMC interface on TCP port 77.



WWW Admin

This section controls if and how access will be allowed via the web browser interface.

Enable

Select this checkbox to enable remote administration via the web browser interface.

Server Port

The default port the web browser interface is served on is port 80. If you wish to change this, enter the new port number and make sure to change the Remote Access filter associated with remote administration to match the port number. Although port 80 is the standard for http, it is suggested that an alternative port number (8000 or 8080 are good choices) is utilized. The reason for moving the web administration port is that a possible mis-configuration of the Remote Access filters could expose the remote web browser interface to unauthorized users.

How to Change the Server Port

If you decide to change the port number for the web browser interface, you should implement this change in the following order:

1. On the Remote Access configuration screen change the port number to the new port value. Save your changes.

2. Find the Remote Access filter that control access via the web browser interface and delete port 80 from the destination port list, leaving only the new port value you have chosen. Save the section.

Allow Updates
By default, updates are allowed. If you wish to disallow remote updates via the web browser interface, deselect this checkbox.

Remote Management Console (RMC)
The Remote Management Console establish an encrypted network connection to the GNAT Box on port 77/TCP. By default, the GNAT Box 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 the External and PSN networks.

Enable
Select the checkbox to enable access via the Remote Management Console.

Server Port
The default, port for RMC access is 77. If you wish to change this enter the new port number and make sure you change the Remote Access filter associated with the RMC administration to match the new port number. Follow the same procedure described previously with regards to the web browser interface.

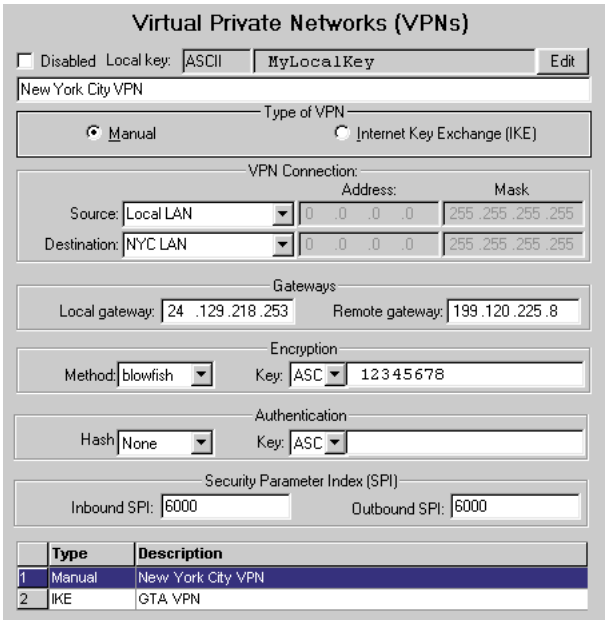
Allow Updates
By default updates are allowed. If you wish to disallow remote updates via GBAdmin, then deselect this checkbox.

VPNs
The VPNs menu item provides access on the web interface for the creation and management of GNAT Box VPNs. This section provides information about the mechanics of managing VPN definitions using the web interface (see Chapter 9 of this guide for a complete discussion of the VPN capabilities of the GNAT Box system).

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

Selecting the VPN menu item will display the VPN definition form. This consists of a scrolling summary list of all defined VPN Security Associations at the bottom of the form and a VPN definition editing section at the top. To create a new VPN definition, click on Add icon "+" on the toolbar to insert a new definition at the selected location in the list. To delete a VPN definition select the row which contains the VPN definition and simply click on the Delete icon "X" on the toolbar. To edit a VPN definition click on row to display the VPN definition in the edit section of the screen.

All changes will not be permanently applied until either the VPN section is saved (when on-line) or the entire configuration is saved, via the File menu Save or Save as... menu items.



Example of a Manual Key VPN Definition

VPN Edit Section

The VPN Edit section is used to define and edit a GNAT Box VPN definition (or Security Association).

Disable

Like many GNAT Box facilities, with VPN definitions you have the ability to create a definition then use the Disable item to toggle the item between

active and inactive status.

Local Key

The Local Pres-hared Key is only used by the IKE key method, so if you will be only using manual key exchange this value will be ignored. The Local Pre-shared key is the key that is associated with the local gateway IP address. This key is sent to the remote VPN gateway during the phase I key exchange for IKE. You will need to provide this key and the IP address to the administrator of the remote VPN gateway. Likewise you will need to obtain the remote VPN's gateway IP address and pre-shared key to be used in your VPN definition.

The pulldown selector determines how the pre-shared key data is interperted. If **ASCII** is selected then the information entered in the Local Pre-shared Key field is interperted as ASCII values. If the pulldown selector is set to **Hex** then the pre-shared key data is interperted as hexadecimal values.

To edit these fields click the Edit button to the right of the field. Please be aware that the Local Pre-shared Key is used by all IKE definitions, so changing it will affect all IKE VPNs.

Description

Use this field to write a brief description of the VPN definition.

Type of VPN

Select the type of key exchange method you want to use for this VPN defintion. Either manual key exchange or automated key exchange (IKE).

VPN Connection

Source Network

The source network can be specified using an IP Address Object or an IP address and netmask. If you have defined an IP Address Object for the source network (typically your protected network or some part of it), then select that object from the Object pulldown. However if you have not defined an IP Address Object for the source network enter the network IP address of the local network that resides behind the firewall (your protected network, PSN or a subnet of either). Use the Mask field to define the type of network, (e.g. 255.255.255.0 for a class C network). The source network doesn't have to be the entire local network, only the network that is to be accessible

via the VPN definition.

Destination Network

The destination network can be specified using an IP Address Object or an IP address and netmask. If you have defined an IP Address Object for the destination network, then select that object from the Object pulldown. However if you have not defined an IP Address Object for the destination network enter the network IP address of the remote network that resides behind the remote firewall (if the remote firewall is a GNAT Box then typcially this will be the protected network, PSN or a subnet of either). Use the Mask field to define the type of network, (e.g. 255.255.255.0 for a class C network). The destination network doesn't have to be the entire remote network, only the network that is to be accessible via the VPN definition.

Gateways

Local Gateway

This is an IP address that is assigned to an External network interface on the local GNAT Box system. So this IP address can be the real External NIC IP address or any alias assigned to it. The encapsulated packets will appear at the remote gateway with this IP address as the source IP address. Hence the local gateway IP address will should be used on the remote gateway when Remote Access filters are created to accept the VPN connection.

Remote Gateway

This is the IP address of the gateway to the remote network. If the remote network is behind a GNAT Box system then this IP address would be one that is assigned to the External network interface. This IP address will also play a role in determining the routing of the encapsulated packet.

Encryption and Authentication

The next sections of the form require different information depending upon which key exchange method you select. First the Manual Key method will be described followed by the IKE method.

Manual Key Exchange

This section describes the fields on the Manual Key Exchange form a later section describes the fields on the IKE form.

Encryption

Encryption Method

Use the selection list to select the method that will be used for the ESP

transformation. Selecting “None” will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128, and DES. The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Encryption Key

Select either ASCII or Hexadecimal key type. If this item is set to Hexadecimal then the values entered in the key field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F. Otherwise if ASCII is selected any of the ASCII characters may be used to define the key.

Key

This is the appropriate key for the select ESP transformation. The Blowfish and CAST128 transformations use variable length keys, while DES uses a fixed length key.

Blowfish

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

CAST128

40-64 bits	5-8 ASCII chars or 10-16 Hex chars

DES

64 bits	8 ASCII characters or 16 Hex chars

Authentication

If you are using Manual Key Exchange you have the option of defining three different VPN tunnel mode transformations: AH, ESP and ESP with authentication. If you would like to define an AH transformation then you should only complete the Authenication section and leave the Encryption section set to None. If you only want to use ESP then leave the Authentication section set to None. If you want to use ESP with authentication set both the Encryption and Authentication sections. Remember each transformation introduces additional computational requirements for the processing of the VPN.

Hash Algorithm

Use the selection list to select the method that will be used for the authentication transformation. Selecting “None” will result in no AH

transformation being applied to the packet. The available choices are: None, HMAC-MD5 and HMAC-SHA1.

Hask Key
Select either ASCII or Hexadecimal key type. If this item is set to Hexadecimal then the values entered in the "AH Key" field should be only hexadecimal characters. The valid hexadecimal characters are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F. Otherwise if ASCII is selected any of the ASCII characters may be used to define the key.

Key
This is the appropriate key for the selected hash algorithm transformation. The key length for the MD5 transformations is 128 bits, which is 16 ASCII characters or 32 hexadecimal characters. The key length for the SHA1 transformations is 160 bits or 20 ASCII characters or 40 hexadecimal characters.

Inbound SPI
The Inbound Security Parameter Index is used to uniquely identify a Security Association, (SA). The Inbound SPI will be the Outbound 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.

Outbound SPI
The Outbound Security Parameter Index is used to uniquely identify a Security Association, (SA). 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.

Automated Key Exchange (IKE)
Both the manual key exchange and IKE methods require the same type of gateway and network information in their definitions. The Encryption section differs between the two.

Encryption Method
Select an encryption method to be used for the VPN. Use the selection list to select the method that will be used for the encryption method. Selecting "None" will result in no ESP transformation being applied to the packet. The available choices are: None, Null, Blowfish, CAST128 and DES.

Note: *Remeber that the variable length encryption methods (Blowfish and Cast128) are limited to 64 bits.*

The Null transformation method is a special case where no encryption is performed, so that only IP encapsulation occurs. The Null method has little impact on performance and is useful when unsupported application protocols are desired to be used in the NAT mode between two GNAT Box systems, (i.e. Microsoft Netmeeting).

Hash Algorithm
The hash algorithm is used for authentication. Select None, HMAC-MD5 or HMAC-SHA1. If None is selected for the Encryption method then either HMAC-MD5 or HMAC-SHA1 must be selected, (this indicates that an AH transform will be used). If an Encryption method other than None is selected and a hash algorithm other than None is selected then an ESP transform with authentication will be used.

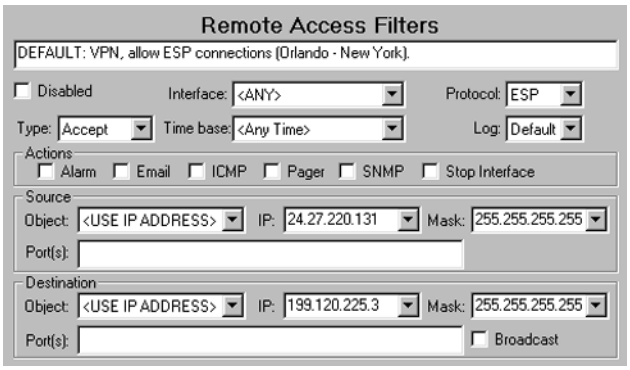
PFS Key Group
Select the Diffie-Hellman group that will be used for Perfect Forward Secrect (PFS) in phase II.

Remote Pre-shared Key
Enter the remote VPN gateway's pre-shared key in this field. If ASCII is selected then the data in the pre-shared key field will be interperted as ASCII values, otherwise if Hex is selected then the data will be interperted as hexadecimal values.

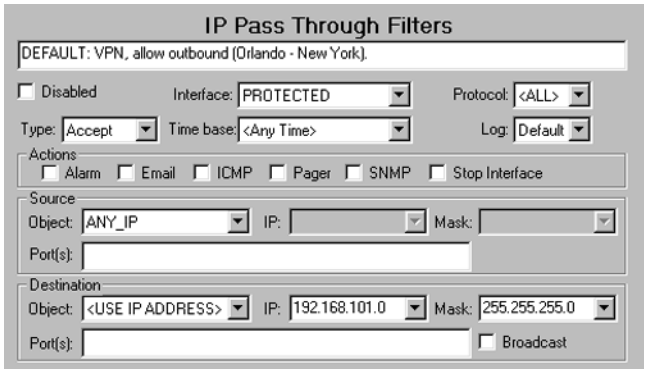
Three Steps to VPN Activation.

1. Define a VPN Security Association.

2. Create a Remote Access filter(s) 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 first prior to defining any VPN filters, as the ESP and AH protocols may not be included in the list. Go to the protocol list and press the "Default" button to create a list that includes the ESP and AH protocols. Do not use the Default button if you have added protocols by hand. You can add the ESP (protocol 50) and AH (protocol 51) by hand.



3. Create IP Pass Through filters that allow inbound and outbound access on the defined VPN. Generally you will need two filters for each VPN definition, (one for inbound access and the other for outbound). If you have one or more VPN definitions, simply go to the IP Pass Through filter screen and press the "Default" button and a set of filters will be created for your VPN definitions. Please note that the Inbound filters will be disabled and set to Deny. Please make modifications to these filters as required and enable them as per your local security policy. *Please note that IP Pass Through filters for VPN definitions do* ***NOT*** *require that entries be created on the IP Pass Through Host/Network data section.*



Please see Chapter 9: GNAT Box VPN for more information about the VPN facility.

Routing

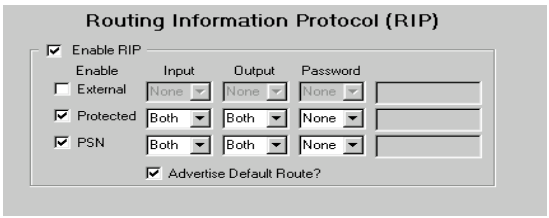
This section provides the administrator screens that address the routing facilities on the GNAT Box system. This menu section provides configuration dialogs for

RIP and static routes.

RIP

The Routing Information Protocol... menu item displays the Routing Information Protocol dialog which provides a means to enable and configure the RIP protocol on a per network interface basis. The GNAT Box, like any good firewall, does not accept routing information from external sources to redirect packets through the firewall. However, the GNAT Box can receive as well as broadcast routing information via an individual interface if the RIP facility is enabled. The GNAT Box RIP facility supports both version 1 and version 2 of the RIP protocol.

Note: *Most GNAT Box network configurations do not require the use of RIP. If your network doesn't require RIP, don't enable this facility.*



Enable RIP

Selecting this checkbox will enable the RIP facility. If connected to a remote GNAT Box, the RIP facility will not begin operation until a section update is applied.

Interface

This column lists all configured network interfaces that are available to run the RIP protocol.

Enable

Selecting these checkboxes will enable RIP on the specified network interface. Each interface may be independently configured to accept and/or export RIP information.

Input/Output

These two columns control how RIP is implemented on the selected network interface. The Input column determines which, if any, version of RIP will be accepted. The Output column determines which, if any, version of RIP will be exported.

The pulldown choice list offers:

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

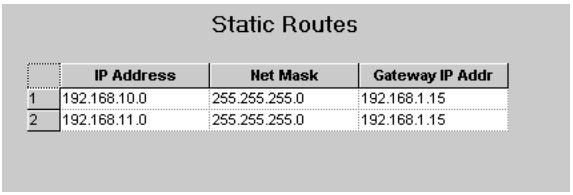
The Password field is used in conjunction with RIP protocol version 2. The pulldown choice list offers a choice of password encoding schemes. If a password encoding scheme is selected, a data entry field is enabled to accept a password.

Advertise Default Route?

This checkbox, if enabled, will advertise the default route on the Protected and PSN networks (if RIP is enabled on those interfaces).

Static Routes

This dialog allows the user to define static routes on the GNAT Box system. Since the GNAT Box system is a firewall, it does not, by default, listen to routing protocols such as RIP; therefore it is sometimes necessary to define a static route for the GNAT Box system.



Defining a Static Route

Use the following procedure to define a static route:

1. Click on the Routes menu item to display the Static Routes form.
2. Click the plus icon in the toolbar or modify an existing field. In the IP address which will be the target of the route.
3. Click in the Destination Netmask field and key in the netmask.
4. Click in the Gateway field and key in the IP address which is the gateway to the destination IP address.

The GNAT Box system supports 300 static routes.

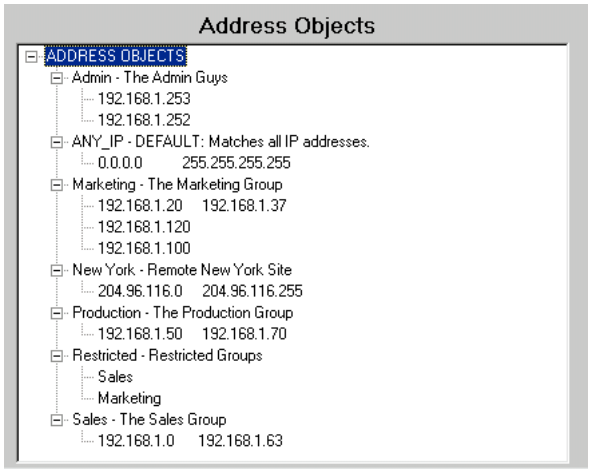
Objects

The Objects section currently contains a single item: Addresses. Future releases of GNAT Box will add more object types to this menu section.

Addresses

Clicking on the Addresses item will invoke the GNAT Box Address Object list. The list displays the name and description of all defined GNAT Box Address Objects. Use the icons in the Action column to add (plus), edit (check) and delete (X) an object.

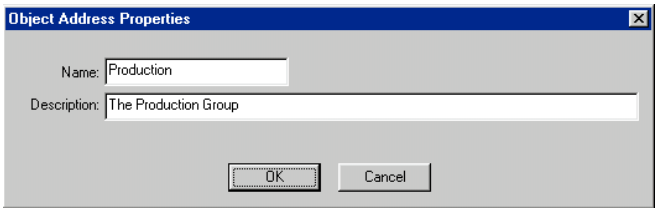
A maximum of 300 Address Objects may be defined, with an Address Object having a maxium of 10 members. The members may be either a single IP address, a range of IP addresses, a subnet specified by an IP address and netmask, or a previous defined Address Object.



How to Add an Address Object

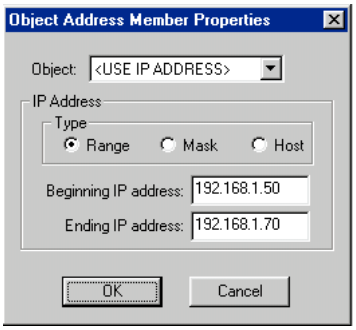
1. Click on the **ADDRESS OBJECTS** item to select it, then click the add icon on the toolbar (plus icon). This will create a new object called "**new object**".

2. Double click on the new object to display the Object Address Properties dialog. Enter a name for the object in the Name field and a description of the object in the Description field. Then click the "OK" button.



3. To add members to the object, select the object name, then click the add icon (plus icon) on the toolbar. A new member object will be created and appear as:
"0.0.0.0 0.0.0.0".

4. Double click on the new member object to display the **Object Address Member Properties** dialog.



5. In the Object field click the pull down choice list and choose an item that will be used to define a member of the Address Object. The member may be defined by either selecting a previously defined Address Object to include in the new Address Object definition or by selecting <USE IP ADDRESS> item to define the member by using IP Addresses.

   If you choose to use another Address Object as a member of the current Address Object, then there is nothing else to do to define the member.

   If you choose to define the new member with an IP Address select the type of definition from the pull down choice list in the IP Type column. Your choices are:

   Host
   Use a single IP address. Simply enter an IP address in the Beginning

Address field. Leave the Ending Address field empty.

Range
Use a range of IP addresses. Enter the beginning IPaddress in the Beginning Address field and the last address in the Ending Address field.

Mask
Use an IP Address and a netmask to specify the desired IP addresses.

6. Repeat steps 3-5 until you have added all the members you desire.

Filters
Filters, as discussed in the Terms and Concepts section of this guide, control access to and through the GNAT Box system. All filter configuration dialogs (Outbound, Remote Access, and IP Pass Through) in GBAdmin have the same layout and operation. So this discussion of the dialogs layout and operation applies to all filter types.

Filter Dialog Layout
At the bottom of the filter dialog, a summary table is displayed with a single line description of each defined filter. If no filters have been defined, this area will be empty except for the table labels. The filter summary table has the same user interface features as all tables used in GBAdmin. These features are discussed at the beginning of this chapter.
The upper portion of the dialog displays the detailed filter information that can be modified. To display a filter, simply click on the row of the desired filter.

Filter Description - The detailed filter information begins with the filter description text box. This description is for your reference. Use it to describe the particular filter. Any filters generated by the system will have their descriptions predicated with a label tag. These tags include:

DEFAULT - The standard GNAT Box default filters that were generated by the system.

Traditional URL PROXY - A filter that is generated for use with the optional URL blocking software.

EMAIL PROXY - A filter that is generated for use with the GNAT Box

Email proxy.

RIP - A filter generated by the GNAT Box system for RIP support.

NO RIP - A filter that is generated for use when RIP is disabled.

STEALTH - A filter that is generated for use when the stealth mode is enabled.

Disable - If this checkbox is selected, the filter is disabled and will have no effect on the GNAT Box filtering operations.

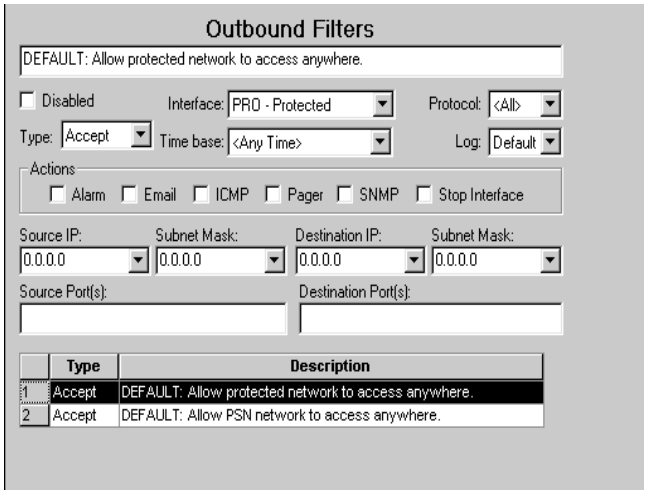
Filter Type - Accept or Deny.

Interface - A popup list of all defined network interfaces and the **<ANY>** item which will match any interface.

Protocol - TCP, UDP, ICMP, ALL, or any defined protocol via the protocol configuration dialog.

Time base - Any defined time group via the time group configuration dialog. If empty, the filter is always in effect.

Log - Yes, No, and Default. Where default is the value defined in the **Filter Preferences** configuration dialog.



Actions - Alarm, Email, ICMP, Pager, SNMP, and Stop Interface. These filter actions are configured and enabled via the Filter Preferences configuration dialog. If an action is enabled, and the filter is matched (accepted or denied) the filter action will be executed.

Source Section

Object - This is a choice list of objects that will be used to match against the source IP address of the packet. If you wish to use an IP Address select the item **USE_IP_ADDRESS** and the IP and Mask fields in the Source section will be enabled.

IP - This is the source IP Address or network address of the IP packet.

Netmask - The netmask that will be logically ANDed with the Source IP. The result will be compared to the Source IP address of the packet being analyzed.

Ports - The source port(s). Typically left empty as this value is usually random. If the Expert Mode is not enabled, a Port Description Dialog helper will be displayed if this field is entered.

Destination Section

Object - This is a choice list of objects that will be used to match against the

destination IP address of the packet. If you wish to use an IP Address select the item **USE_IP_ADDRESS** and the IP and Mask fields in the Destination section will be enabled.

IP - The IP address or network address destination of the IP packet.

Netmask - The netmask that will be logically ANDed with the Destination IP. The result will be compared to the Destination IP address of the packet being analyzed.

Ports - The destination port(s), also known as service(s) of the IP packet. If the Expert Mode is not enabled, entering this field will cause the Ports Description Dialog helper to be displayed. The helper dialog provides a sorted list of services and their associated port numbers. This field may contain a single port, multiple ports separated by commas, or a range (two ports separated by a dash).

Outbound Filters

Outbound Filters control access to the External network (typically the Internet) and to the PSN (if one exists). As mentioned previously, the implicit filter rule "**that which is not expressly permitted is denied**" applies to outbound packets as well as inbound packets. If the Network Information dialog has been completed, you can click the Default icon in the toolbar to create a set of default Outbound filters. The default filter allows all IP addresses on the Protected network to access any IP address and any service external to the Protected network. If a PSN network interface exists, a similar default Outbound Filter will be created that allows all access to the External network (typically the Internet). These filters can be modified or deleted to suit the local network security policy for external network access. An example of the default Outbound filters can be found in Appendix E.

This release supports 400 Outbound Filters.

Preferences

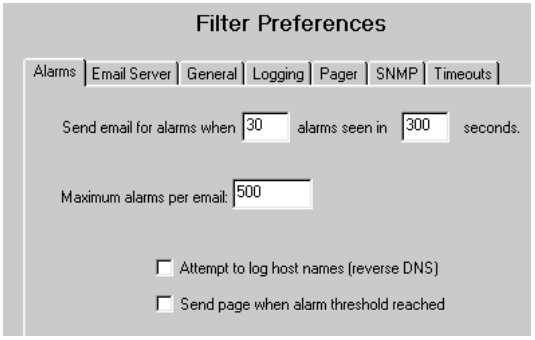
The Filter Preferences item displays the Filter Preferences configuration form. This form allows the administrator the to define preferences for functional areas associated with filters.

Alarms

This dialog allows the administrator to set the parameters that are involved

in alarm notifications. An alarm event occurs when a filter (Remote Access, Outbound, or IP Pass Through) is matched and the alarm filter action is enabled. Each alarm event increments the alarm count by one. If the alarm threshold is reached within the specified time period, an email alarm notification will be sent to the designated email address defined on the Email Server screen. The email message will document all the alarm events that contributed to the alarm notification. Multiple email messages will be sent, if the number of alarm events exceed the maximum alarm count parameter defined in this section. If the pager option is configured, a pager message can be generated when the alarm threshold is reached.

Send email for alarms when...
Configure the alarm threshold by entering values for the number of alarms and time period.



Maximum alarms per email
This parameter controls the maximum number of alarm messages that will be included in a single email message. A larger number will reduce the number of email messages at the expense of larger email messages. An alarm message is generally 200 bytes.

Attempt to log host names
If this checkbox is selected, the GNAT Box will attempt to resolve the hostname of the source IP address that generated the alarm. This feature will increase the amount of time required to process and deliver the alarm, due to the nature of DNS lookups.

Page when threshold reached
If your GNAT Box has been configured to support pager notifications, this

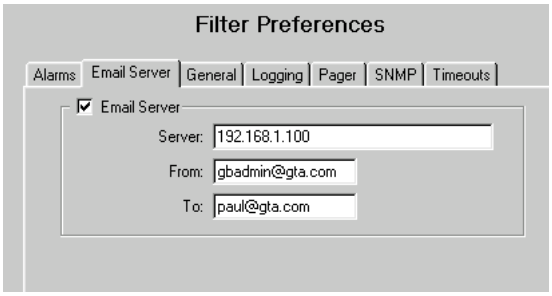
item, if enabled, will send a page when the alarm threshold is reached.

Email Server

This dialog allows the administrator to configure where the GNAT Box will send email notifications and alarms.

Enable Email Server

If this item is enabled, the GNAT Box will be able to send email and alarm notifications. If alarms and/or email notifications are set on a filter and the email server is not enabled, an error message will be written to the console and remote log file.



Server

Enter the hostname (DNS hostname) or IP address of the email server where alarms and email notification messages will be sent. Although the email server typically is a host on the Protected or PSN network this is not a requirement and the sever may be an external host. The email/alarm notifications can be sent to any valid email address, as long as the server is accessible.

Note: *The email server defined on this configuration dialog need not be the same server that is used with the email proxy.*

In order to use a hostname for the email server, you must have defined a DNS server which is to be used for lookups on the GNAT Box system (this is done in the DNS form). If the hostname is an internal host (PSN or PROtected networks), the DNS server must be an internal server which can resolve the name of the hidden host. If the DNS server referenced is an External server and the target mail server is an internal, host you will have to use the IP Address. If you are unsure about the hostname use the IP address of the host.

From

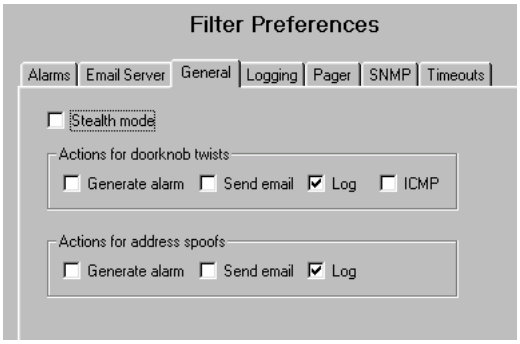
This is the “from” email address that will appear in the email and alarm notifications. Although you can leave this field blank, some email servers don’t like to receive email with an empty “from” field. An email address in this field it should be valid; otherwise, if there are problems delivering the email the server will attempt to return the mail to the address in the “from” field (an email loop may ensue). The “From” address may be a fully qualified address, such as jdoe@gta.com or it can simply be the mailbox name on the specified email server, such as jdoe.

To

This is the email address that will receive the email and alarm notifications. The email address can be a fully qualified address, such as jdoe@gta.com or it can simply be the mailbox name on the specified email server, such as jdoe. If the email address is not for local delivery within your protected network, make sure that the specified email server will allow the email to be relayed.

General

The General section contains miscellaneous configuration parameters.



Stealth Mode

If this option is selected, the Remote Access default “No Stealth” filters will be set to “Disable” and the runtime system operates in the stealth mode. Enabling and disabling this option will change the system operation mode. However, it will not change the Remote Access filters, unless you either press the “default” button or change them manually (via the Disable option). In the stealth mode, the GNAT Box will not respond to ICMP ping and traceroute request, UDP traceroute request and will not reply with an ICMP message when a packet arrives for a port where no service or tunnel exists.

Actions to generate for doorknob twist
These options control how the GNAT Box will respond to "doorknob twists". A doorknob twist occurs when a connection is attempted to 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 GNAT Box has been mis-configured.

Alarm - Selecting this option will generate an alarm event, if a doorknob twist occurs.

Email - Selecting this option will immediately send an email message documenting the doorknob twist event. The email message will be sent to the address specified on the "Email Server" configuration section.

Log - Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.

ICMP - Selecting this option will generate an ICMP "service not available" message and sent to the source IP address of the attempted connection.

Actions for Address Spoofs
These options control how the GNAT Box will respond to an address spoof. An address spoof occurs when an IP packet arrives at a GNAT Box network interface and its return path is not back through the interface it arrived on. Address spoofs generally occur because of two different situations:

1. Mis-configuration. Network(s), subnet(s), or host(s) are located or connected to the Protected/PSN network and have not been defined to the GNAT Box. The GNAT Box assumes all IP addresses that are not on the Protected network, or defined in the static route table, or are learned via RIP on the protected network, should only appear on the EXTernal side of the GNAT Box.

2. An intrusion attempt by altering the source IP address of a packet directed at a GNAT Box network interface.

   Alarm **- Selecting this option will generate an alarm event if an address spoof occurs.**

   Email **- Selecting this option will immediately send an email**

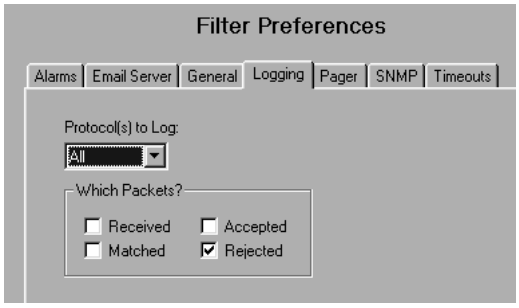
message documenting the address spoof event. The email message will be sent to the address specified on the "Email Server" tab.

Log **- Selecting this option will generate a log entry, which will appear on the console and be sent to the remote log host.**

Logging

Every filter has a log action associated with it, regardless of the filer type (Accept or Deny). This action can be 'Yes' to explicitly log the packet, 'No' to explicitly not log the packet, or 'Default' to take the default action defined in the Logging section of the Filter Preferences. The default Filter Logging Preference is set to log all rejected packets for all protocols.

If you wish to change the Filter Preferences, follow this procedure:



1. Select the desired protocol to log from the Log Protocol choice list. The choices available are: ALL, TCP, UDP, ICMP or NONE.
2. Select the type of packets to log, by clicking the checkbox next to the desired packet type. The available packet types are:

   Received
   Means any packet that is compared to the filter.
   Rejected
   Means any packet that is rejected by the filter.
   Accepted
   Means any packet that is accepted by the filter.
   Matched
   Means any packet that matches the filter criteria.

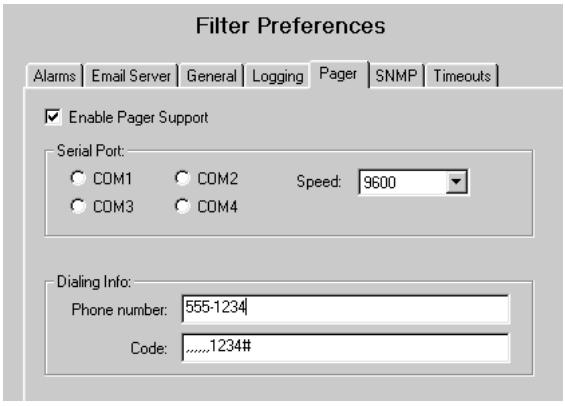
Pager

The packet type choices are not mutually exclusive. However, selecting multiple types may result in as many as four log records being generated for a single packet. This option can quickly generate an excessive amount of logging and should be used with care.

Enable Pager Support

To use the pager facility, you must connect a modem to one of the available serial ports on your GNAT Box system or use an internal modem card. The modem can be a rather simple model, since it is only used for dialing and sending DTMF tones, not data.

Select this checkbox to enable the Pager alarm facility. If the Enable Pager Support field is not enabled selecting Pager filter actions on the filter definition screen has no effect.



Serial Port

This section provides the choice of COM ports 1 through 4. Select the COM port to which the modem used for paging is attached or assigned.
Speed - Set the Speed to the speed at which the GNAT Box will communicate with the modem (known as the DTE speed).

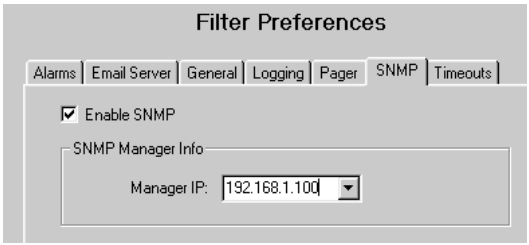
Dialing Info

Phone number - The telephone number for the target numeric pager. You should enter all numbers and dialing codes that are required to make a call.

Code - The Code is the numeric values that will be displayed on the pager. This code may be any valid numbers, or symbols, that your numeric pager

may use. The commas represent pauses and are typically required while the pager announcement message is played. Most pagers have the message terminated by a # symbol. Please consult your pager service for specifics of your pager.

SNMP



Enable SNMP

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

SNMP Manager

The SNMP Manager is the host that is running some kind of SNMP management tool or facility to receive SNMP trap messages. The GNAT Box will generate an enterprize specific generic trap, if SNMP is checked as a filter action, on a filter definition, when the filter is matched.

Manager IP

The Manager IP is the IP address of the host running the SNMP management tool. This field uses the IP history list. The SNMP manager IP address may reside on any network, although the Protected network is the most common location.

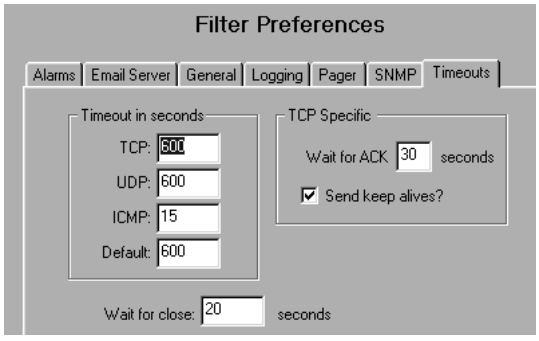
Timeouts

Timeouts define when a connection is viewed as being excessively idle. What happens when a connection reaches its timeout value differs for each IP protocol. The reason for the difference has to do with how different protocol operate. Both ICMP and UDP are connectionless network services, while TCP is a connection-oriented network service. This means that in the general case it is impossible to determine when ICMP and UDP connections are finished (ready to close). The TCP protocol has enough information embedded, so that GNAT Box can determine when a TCP connection is finished.

When UDP and TCP reach their respective timeouts, the connection is marked as ready to close. TCP connections are a little tricky, because TCP has two timeout values:

Wait for ACK

The first TCP time-out is "Wait for ACK." As part of the TCP connection creation process, the client and server exchange several IP packets. All packets sent from the server will have a bit indicating ACK (acknowledge) with the packet header. As part of its stateful packet inspection processing, the GNAT Box keeps track of the fact that it has seen this bit. If this bit is never seen it usually means that the remote server is down. If the "Wait for Ack" idle time is reached without an ACK from the server, the connection is marked as ready for close.



Send keep alives?

The second TCP timeout is for idleness on a successfully created connection. When the idleness timeout for TCP is reached two things can happen:

1. If "send keep alive" is disabled the connection is marked as ready to close.

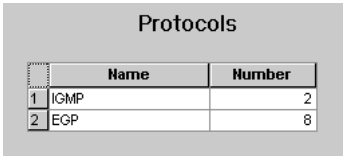
2. If "send keep alive" is enabled, a TCP keep alive IP packet is constructed and sent to the client. The client will then send a keep alive IP packet to its server, if the connection is still valid. If the connection is invalid the client will send a connection reset to its server. If the GNAT Box sees the keep alive message, it will set the connection's idle time to zero. If a connection reset packet is seen, the connection is marked as ready to close. If no response is seen to the GNAT Box's keep alive message after five minutes, the connection will be marked as ready to close.

Default Timeout

After a connection is marked as ready to close, the GNAT Box will wait five seconds before it actually closes the connection. This gives redundant IP packets a chance to clear the GNAT Box without causing false doorknob twist error messages.

The Default timeout is a catch-all for any other supported protocol, besides TCP, UDP or ICMP. At this time, the only other protocol directly supported by the GNAT Box is GRE (used by PPTP).

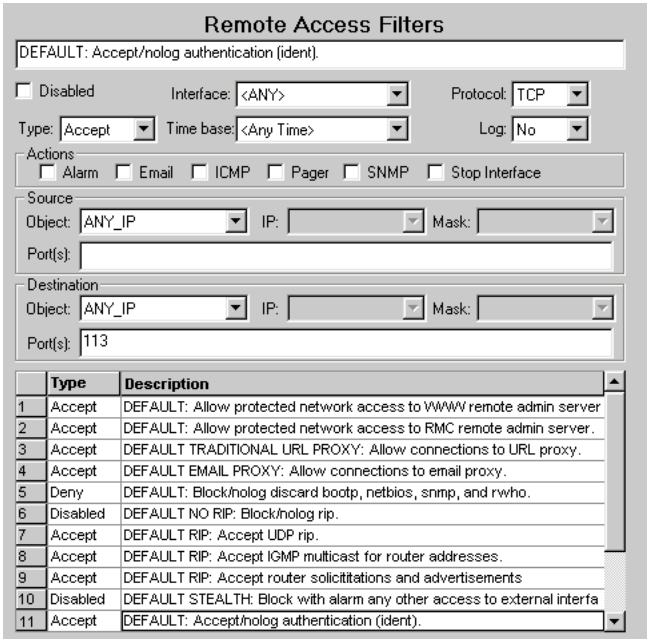
Wait for close
Default value is 10 seconds. If your site is experiencing a large number of spurious “Remote Access Filter” blocks from reply packets (typically from port 80 - http), you may want to increase this value, which will give packets from slow/distant connections more time to return before the connection is closed down.



Protocols
The Protocols configuration dialog provides a means to define IP protocols other than TCP, UDP, and ICMP. This protocol definition list is available for use on the filter definition dialogs. In the current version of GNAT Box, the additional protocols may only be used with a Deny filter, since the system can only process TCP, UDP, and ICMP IP packets. The main purpose for the additional protocols in the current version of GNAT Box is to minimize extraneous protocol block messages in the log files. Since the default action of the GNAT Box is to deny that which is not explicitly allowed and the default filter logging action is to log all rejected packets, an unknown protocol that reaches the GNAT Box will be logged. If the unknown protocol is a routing protocol such as EGP, the log files could quickly grow to an enormous size. Therefore, it is often convenient to create a remote access filter that simply denies a protocol and explicitly does not log it.

Remote Access Filters
Remote Access Filters control inbound access primarily on Tunnels. Additionally, Remote Access Filters control inbound access to any network interface on the GNAT Box from any attached network. If the Network Information dialog has

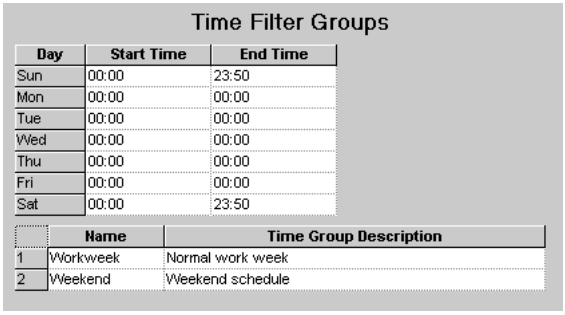
been completed, the **Default** icon on the toolbar can be clicked to generate the default Remote Access filters. These filters can be used as is, modified, or deleted to suit the local network security policy. A list of default filters are listed in Appendix E.



Generally, it is best to select and configure the GNAT Box system preferences and inbound Tunnels first. Next access the Remote Access filter set and click the **Default** icon and will generate a set of Remote Access filters for the selected configuration. The generated filters can then be adjusted if desired. This release supports 400 Remote Access Filters. The Terms & Concepts section describes the Remote Access filters in detail.

Time Groups

Time Groups are user defined time schedules that can be associated with any type of filter. Time Groups provide the firewall administrator the ability to control access (both inbound or outbound) based on the time of day and day of the week. A filter that has an associated Time Group will only be in effect during the defined time period. The time granularity is based on 10 minute increments. Time Groups can provide a great deal of flexibility, especially when multiple filters are involved. This release supports 100 Time Groups.



The Time Group list operates similar to the filter group screens. The editing buttons have the same functions as described in the filter section.

Creating a Time Group

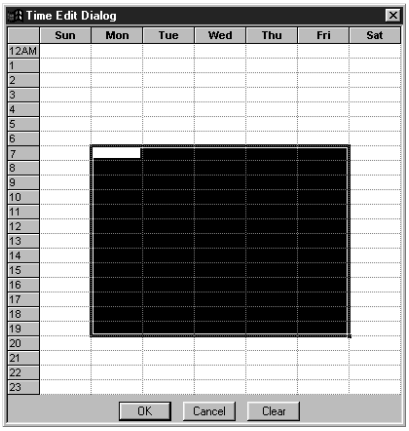
1. Click on the add icon in the toolbar to create a new, empty Time Group entry.

2. In the **Name** field, enter a name that will appear in the Time Group popup list on the filter definition screen.
3. Enter text that describes the Time Group in the **Description** field.

4. Double click the row to display the Time Edit dialog, or choose to edit the time schedule directly.

5. In the Time Edit dialog, select the desired time schedule by clicking and dragging the mouse. To select noncontiguous sections use “control click.”

6. Once you are satisfied with your selection, click the OK button. Your schedule will be saved and displayed on the primary dialog screen. You may edit the time values in the table, if you wish.



IP Pass Through

IP Pass Through is the GNAT Box term for "no NAT." The IP Pass Through data entry screens allow the user to define a host, subnet or network that will not have NAT applied to packets from specified IP addresses.

Two items must be in place for an IP pass through to operate correctly:

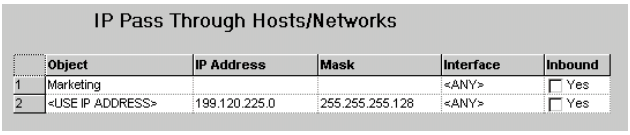
1. The IP address must be defined on the Network/Host form.
2. An IP pass through filter(s) must be created to allow packets to flow from and/or to the IP pass through IP address.

Note: *If an IP pass through address is configured to use the External network interface and the GNAT Box is connected to the Internet, the IP pass through address must be a valid registered address*.

The IP Pass Through facility provides a great deal of flexibility, since an IP address(es) can be configured not to use NAT for specific interfaces. 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 destined for the Internet can have NAT applied.

Hosts/Networks

The IP Hosts/Networks definition form is used to specify the IP address, subnet, or network that will not have NAT applied to packets to or from those addresses.



How to Add an IP Pass Through Host/Network

1. Click the “Add” icon in the toolbar to add an empty row in the Network/ Host table.
2. In the **IP Address** field, enter a host IP address (for a single host), subnet, or network (for multiple hosts).
3. In the **Netmask** field, enter a netmask that will be ANDed with the IP Address field which will yield the desired results. Single IP addresses should use 255.255.255.255.

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

4. Use the **Interface** pulldown to select which network interfaces will have no NAT applied to the specified IP packets, when they pass out through the specific NIC.
5. If you wish unsolicited IP packets to be accepted for the specified IP pass through address(es), select the **Inbound** checkbox. If you wish to allow only the IP pass through reply packets be allow to return then it is unnecessary to select the **Inbound** option.

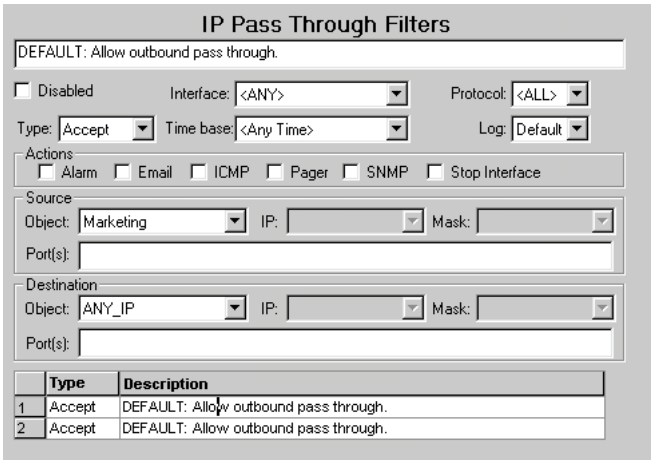
The IP Hosts/Networks list is limited to 100 entries.

IP Pass Through Filters

IP Pass Through Filters control access to and from IP addresses that have been specified as IP pass through addresses. IP pass through filters, although similar to the other two filter types (Remote Access and Outbound), are different, because they control both inbound and outbound access to/from the designated IP Pass Through addresses. Since IP pass through addresses are not translated, the GNAT Box functions as a gateway for these addresses. The IP Pass Through Filters utilize IP Pass Through addresses in the filter definitions not GNAT Box NIC addresses.

If IP pass through host/networks are defined, pressing the “Default” icon on the

toolbar will create a set of filters based on the IP pass through addresses defined on the Hosts/Networks screen. Since IP pass through hosts/networks can be defined in a variety of different combinations, the default filters will vary according to options selected. These generated filters are quite general and should be modified to match your security requirements.



Typically, two filters are required for each different Hosts/Network IP pass through IP address; one for outbound access and the other for inbound access. The Remote Access and Outbound filters do not apply to IP Pass Through designated IP addresses.
This release supports 400 IP Pass Through filters.

IP Pass Through Filters are defined in the same manner as Remote Access or Outbound filters. The same rules concerning filter order also apply. The major difference is that since IP Pass Through addresses are not hidden, filtering rules always address the IP Pass Through host(s) and not the IP addresses assigned to the GNAT Box. The GNAT Box functions only as a passive gateway with regard to IP Pass Through addresses.

As mentioned in the previous section, one of the easiest methods to create IP Pass Through Filters is to first configure any IP Pass Through hosts or networks using the Host/Network form. Next, use the Default button on the IP Pass Through filter set form to generate a set of default filters based on the definitions created on the Host/Network form. The disadvantage of this method is that if filters have been previously created and customized, they will be replaced with

the system generated default filters.

Creating IP Pass Through Filters

To create a pair of IP Pass Through filters for a defined IP pass through host, do the following:

1. Click the “Add” icon on the toolbar to create an empty filter definition, or edit an existing filter.
2. Since IP Pass Through address must have two filters (inbound and outbound), first create the outbound filter. Complete the filter definition in the same manner as an outbound filter, specifying the source IP address as that of the IP Pass Through address. Once you have the filter defined, click the save button.
3. Click the add icon again to create another filter. To handle the inbound connection. Define the filter as you would a Remote Access filter except that the destination IP address will be the IP Pass Through address, not the IP address on the GNAT Box NIC. Save the filter.
4. Once you have completed adding all IP Pass Through filters, click the Save button on the filter set to save the filters and apply them to the running system.

NAT

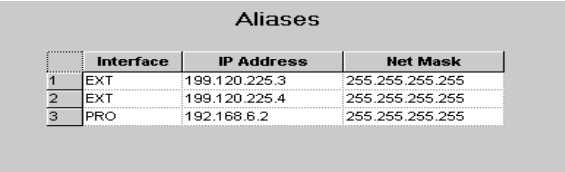
The NAT section contains configuration areas that are involved with network address translation.

Aliases

An IP Alias is the GNAT Box facility that allows a network interface to have multiple IP addresses. An IP alias may be assigned to any network interface (PRO, PSN or EXT). This facility is useful on the External network interface, if multiple targets on the PSN or Protected network are required for the same service (port) via the Tunnel facility (e.g. multiple webservers). This release supports 300 aliases.

All IP aliases used on the External network interface must be registered or legitimate IP addresses, if attached to the Internet. An IP alias need not be from the same network as the real IP address; this feature is useful since the GNAT Box will route packets between all networks it is attached to logically.

This screen uses the same table mechanism used throughout the GBAdmin program.



How to Add an Alias

1. Click the "add" icon or choose Add from the Edit menu. A new row will be inserted. From the popup list select the Logical Network Interface (EXT, PRO, or PSN) to which the alias will be assigned.
2. Enter an IP address, or select an IP address from the popup history list and modify it.
3. Select a netmask for the IP alias. If the alias is on the same network as ANY IP address assigned to the selected logical network interface (EXT, PRO or PSN), the netmask must be 255.255.255.255. If the alias is on a different network, you may assign an appropriate netmask as suitable to your site.
4. If GBAdmin is connected on-line to a remote GNAT Box, make sure to click the "section update" icon in the toolbar to apply the new aliases to the remote system.

How to Delete an Alias

1. Click on a row number to select the entire row, then click on the delete button on the tool bar or choose delete from the Edit menu.
2. If GBAdmin is connected on-line to a remote GNAT Box, make sure to click the "section update" icon in the toolbar to apply the deletion to the remote system.

How to Edit an Alias

1. Click on the desired element and make changes. The functions copy, cut, and paste operate on both individual items and rows.
2. If GBAdmin is connected on-line to a remote GNAT Box make sure to click the "section update" icon in the toolbar to apply the changes to the remote system.

Inbound Tunnels

As mentioned in the Introduction section of this guide, a Tunnel is a GNAT Box facility that allows a host on an external network to be able to initiate a TCP, UDP, or ICMP session with a host on an otherwise inaccessible host for a specific

service. The Inbound Tunnel form allows the user to define tunnels for both External network and Private Service network interfaces.

Tunnels are **not** used on a Protected network interface, since tunnels are associated only with inbound connections. Tunnels can only be created for these inbound connections:

1. From the External network interface to a host on the Private service network.
2. From the External network interface to a host on the Protected network.
3. From the Private Service network interface to a host on the Protected network.

Tunnel Characteristics

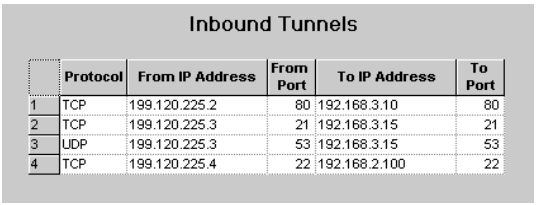
1. A tunnel will not be usable, unless an appropriate **Remote Access Filter** has been defined to allow access to the tunnel. As mentioned in the earlier Remote Access Filter discussion, the default button on the Remote Access Filter set screen will generate default filters for all defined tunnels. The filters generated by this method are broad in scope and may require modification to meet your specific security policy.
2. Tunnels are defined by a source IP address/port pair and a destination IP address/port pair.
3. Only the source side of a tunnel is visible. Since GNAT Box tunnels are a form of network address translation, a user on the source network side will never see the ultimate destination of the tunnel. For all practical purposes, the tunnel appears to be a service operating on a server with the tunnel's source IP address.
4. The source and destination port of the tunnel definition need not be the same. This means that 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 you could define a tunnel with a source port of 99 and a destination port of 23.
5. 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.

   Please note, exposing a host in this manner is very dangerous and not recommend, especially for a host on the Protected network.

6. If a tunnel is from an alias IP address, you may need to add a

"mapping." This mapping would map the destination host to the alias IP address. This is necessary, so that secondary connections will appear to originate from the same address as the Tunnel.

7. A maximum of 300 tunnels may be defined.



	Protocol	From IP Address	From Port	To IP Address	To Port
1	TCP	199.120.225.2	80	192.168.3.10	80
2	TCP	199.120.225.3	21	192.168.3.15	21
3	UDP	199.120.225.3	53	192.168.3.15	53
4	TCP	199.120.225.4	22	192.168.2.100	22

How to Add a Tunnel

1. Click on the Inbound Tunnels menu item to display the data entry form.

2. Click the "add" icon on the toolbar to add a new row.

3. Select the protocol type form the Protocol choice list. The choices available are TCP, UDP, ICMP, or ALL.

4. In the From IP Address field, key in the IP address of the source side of the tunnel. This address may be the real IP address or an alias assigned to the network interface. Remember, only the External and Private Service network interfaces may be used.

5. In the From Port field, enter the port value which users will access. A list of services and their port numbers is listed in an appendix of this guide.

6. In the To IP Address field, key in the IP address of the target host. The host may reside on either the Private Service network or the Protected network (including subnets routed behind either network).

7. In the To Port field, enter the port value which will be the destination of the tunnel. This is the port value of the service being offered on the target host.

8. If GBAdmin is connected on-line to a remote GNAT Box, make sure to click the "section update" icon in the toolbar to apply the additions to the remote system.

9. Select the Remote Access Filter menu item and create or modify a filter to allow access to your new tunnel.

How to Delete a Tunnel

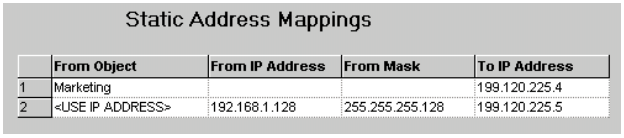
1. Select the row(s) you wish to delete.

2. Click the “delete” icon on the toolbar to remove the selected rows.

3. If GBAdmin is connected on-line to a remote GNAT Box, make sure to click the “section update” icon in the toolbar to apply the deletions to the remote system.

Static Address Mapping

As mentioned earlier in this guide, **Outbound Mapping** is a GNAT Box facility that allows an internal IP address or subnet to be statically mapped to an external IP address during the network address translation process. By default, all IP addresses on the Protected and Private Service networks are dynamically assigned to the primary IP address of the outbound network interface.


Static Address Mappings

	From Object	From IP Address	From Mask	To IP Address
1	Marketing			199.120.225.4
2	<USE IP ADDRESS>	192.168.1.128	255.255.255.128	199.120.225.5

In certain situations where it is desirable to statically assign the IP address used in the network address translation. To use the Mapping facility you must have assigned at least one IP alias to the desired outbound network interface (External or Private Service network interfaces). Mapping is allowed:

Allowed Mapping

1. From a host or subnet on the Protected network to an IP alias assigned to the Private Service network interface.

2. From a host or subnet on the Protected network to an IP alias assigned to the External network interface.

3. From a host or subnet on the Private Service network to an IP alias assigned to the External network 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.

4. 100 Outbound Maps may be defined.

Static Address Mapping Characteristics

1. Click the Outbound Mapping menu item to display the dialog.

2. Click the Add icon in the toolbar to create an empty row or select Insert from the Edit menu.

3. In the From IP Address field, key in the IP address of the host or subnet that should be mapped.

4. In the From Netmask field, key in a netmask that will be ANDed with the From IP Address to yield an IP address or subnet that will be mapped. For example: to map a single IP address use a netmask of 255.255.255.255, to map a class C network use 255.255.255.0, or to map half of a class C use 255.255.255.128.

5. In the To IP Address field, key in the IP address to which the source IP address(s) will be mapped. This must be an alias IP address.

6. If GBAdmin is connected on-line to a remote GNAT Box, make sure to click the "section update" icon in the toolbar to apply the additions to the remote system.

Runtime

The GNAT Box floppy diskette contains two distinct pieces of data: the **runtime operating system,** and the GNAT Box **configuration data**. GBAdmin is designed to manage and manipulate both of these distinct parts of the GNAT Box system. Although GBAdmin has detailed control over the configuration data, it can only manipulate the runtime operating system as a monolithic data entity.

Version

The **Runtime** section lets the administrator determine if the runtime system is loaded into GBAdmin's application memory. Click the

Version menu item will display version information about the currently loaded runtime operating system.

With regards to the runtime operating system, GBAdmin can perform the following tasks:

1. Load only the runtime operating system into its memory from a file.

2. Load only the runtime operating system into its memory from a GNAT Box floppy diskette.

3. Load the runtime operating system as part of a GNAT Box floppy diskette image from a GNAT Box floppy diskette.

4. Load the runtime operating system as part of a GNAT Box floppy diskette image from a file.

5. Write only the runtime operating system to a GNAT Box floppy diskette.

6. Write only the runtime operating system to a file.

7. Write the runtime operating system as part of a GNAT Box floppy diskette image to a file.

8. Write the runtime operating system as part of a GNAT Box floppy diskette image to a GNAT Box floppy diskette.

***Note**: It is **not** possible to update the runtime operating system to a remote GNAT Box using the network facility. All runtime updates must be performed directly to a floppy diskette.*

Reports

The Reports section functions essentially the same as the Reports Menu found on the menu bar. The Reports section provides access to three reports that deal with the system hardware and software configuration.

Verification

The **Verification** item will run a system configuration verification check of your GNAT Box system. The check will verify the following functional areas: IP

addressing, Netmasks, Interface assignment, filters, tunnels, PPP, and outbound maps. After you have configured your GNAT Box, please run a configuration verification check to ensure that you have a valid configuration. Make it a habit to run the check each time after you make any changes to your system. See Appendix F for an example Verification Report.

Configuration

The **Configuration** item is an excellent diagnostic tool, since it reports the current configuration state of the GNAT Box system. The report displays information about all configuration parameters. If you need to contact technical support about a GNAT Box issue, be sure to generate a current configuration report, which will be requested by the support staff.

Note: *If the configuration was loaded from a GNAT Box runtime diskette that had previously been booted up, ethernet MAC address information will be displayed. Otherwise these values will appear as "???" signifying an unknown value.*

Hardware

The **Hardware** item generates a report of the hardware detected in your system at boot time. The report is useful in diagnosing possible hardware problems. If you suspect a hardware problem, you should generate this report and review the hardware the system has detected. If you need to contact technical support about a suspected hardware problem, please have this report readily available when calling.

This report is only available when a network connection has been established with a remote GNAT Box system.

System Activity

This section is only active when a network connection is established with a remote GNAT Box system. This section provides direct access to the System Activity reports. The activity reports are only snapshots of the system activity and have no continuous update facility as found on the web interface. To refresh a report simply click the desired activity report item to generate an update.

These same reports may also be accessed from the System Activity menu on the menubar. The menu items are:

Active ARP Table

The **Active ARP Table** report will create and display a report that lists the current

ARP (Address Resolution Protocol) table used by the GNAT Box system. The report displays the IP address to MAC address translations and “Time to Live” for each entry.

ARP table entries are kept for 20 minutes. The ARP table is scanned every 5 minutes to check for expired entries. Once an entry is expired, the GNAT Box will not try to re-ARP the address for 20 seconds.

Active Connections

The **Active Connections** item is used to display a report of active connections, both inbound and outbound currently active on the GNAT Box. By default, the display is a static snapshot of activity. In order to observe a change in the active connection display, simply click on the Active Connections menu item again to refresh the display. If you wish to have the report updated on a periodic basis, click on the “Refresh Rate” link on the report display and adjust the interval to your liking (a value of zero means no update). The displayed report can be saved, emailed or printed by simply clicking in the displayed frame to select it, and then choosing the desired function from the menu of your browser application.

The Active Connections report displays:

- Connection Direction
- Protocol
- Source IP Address/Source Port
- NAT IP Address/NAT Port
- Destination IP Address/Destination Port
- Idle Time
- Packets Received
- Packets Sent
- Bytes Received
- Bytes Sent

Active Filters

The **Active Filters** report will create and display a report that lists all filters with the number of hits on each filter. Inactive Time based filters are displayed with an asterisk ‘*’ next to the filter entry. The report is a static snapshot. However, the display can be updated on a periodic basis by adjusting the refresh rate. The Active Filters Report displays the following information for each filter type:

Filter Number
Filter Hits
Filter Type
Logical Interface
Physical Interface
Protocol
Filter Actions
From IP Address/From Netmask
From Ports
Destination IP Address/To Netmask
Destination Ports

Active Routes

The Active Routes report will create and display a report that shows the active routing table used by the GNAT Box system. The report displays the destination, netmask, gateway, and flags. Possible flag values are:

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

This report can be helpful in diagnosing and troubleshooting routing problems.

Current Statistics

The **Current Statistics** item provides access to the GNAT Box system statistics display. Statistics are displayed for both connections and packets of the TCP, UDP, and ICMP protocols. The current date, time, and "uptime" are printed at the top of the form. The report displays the following information:

- The current and average (60 seconds) number of connections by protocol for both inbound and outbound traffic

- The total packets sent and received by protocol for both inbound and outbound traffic
- The bandwidth utilization by protocol for both inbound and outbound traffic.
- A summary line that displays the totals for each column in the report.
- A summary line of the total of packets sent and received since the system has been booted
- A summary line of the peak bandwidth utilization
- The CPU state, which displays % user process, % system process, % interrupt, and % idle.

Chapter 8: Troubleshooting

We recommend the following guidelines as a starting point, when trouble shooting network problems:

1. Start with the simplest case of locally attached hosts.
2. Use IP numbers, not names. Your real problem could be DNS.
3. Work with one network segment at a time.
4. Verify your system configuration with the Configuration Verification feature. The verification check is the best method of insuring that your system is configured correctly. All errors and warnings listed should be corrected.
5. Your first tests should be connectivity tests. Ping and traceroute are very useful tools for testing connectivity.

1. Network cabling connected to wrong network interface.

It is easy to confuse network interface cards, especially if they are all from the same manufacturer. Determining which network interface card is assigned to a particular device physical name can be confusing. A few useful guidelines are:

- Most network cards have their MAC address printed on a label attached to the card. Record the MAC address and location of each network card installed in your system. If you are performing a new install, the Setup Wizard will display the MAC address and physical name for each card installed in the system. Simply refer to your list and select the desired card. In a running GNAT Box system the MAC addresses/ Physical names are listed on the Network Information screen and in the software summary report.

If you didn't record the MAC addresses of your cards prior to installation, you can try the following:

- PCI based cards are typically assigned a physical name in the order that they appear in the PCI bus.

- ISA based cards are often assigned based on the card's MAC address, which is usually printed on the card. The lowest MAC address is typically assigned to the first device, and so on.

- 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 (label the card). Connect the next network cable and perform the test again with the two remaining network interface cards.

2. **Unsupported network cards.**
   Make sure that the network cards installed in your GNAT Box system are all supported devices. 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. If you can not access the system with the web browser, watch the console at boot time to identify the network device in question. Pressing the <Scroll Lock> key will allow you to use the up and down cursor keys, the page up, and page down keys to scroll about two screens worth of data. Make sure you toggle <Scroll Lock> off when you are finished.

3. **Wrong network connection type selected.**
   If your network card has multiple connection interface types (e.g. BNC, AUI, and UTP), check the Network Information screen to ensure the desired connection type is selected.

4. **Improper IP address assignment.**
   All network interfaces on the GNAT Box system must be on different logical networks.

5. **Improper default route assignment on the GNAT Box system.**
   The default route must always be on the same logical network as the network interface of the host (this is true for all hosts, not just the GNAT Box). In the case of the GNAT Box, the default route must be an IP address on the network which is attached to the External network interface.

6. **Improper or no default route assigned to hosts on the Protected or Private Service networks.**
   All hosts protected by the GNAT Box must use the IP address of the GNAT Box'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.

7. **Failure to define a Remote Access filter for a Tunnel.**

All Tunnels require a Remote Access filter which allows access to the Tunnel. A Tunnel that has no Remote Access filter, or an improperly configured filter assigned to it, will generate a “blocked packet” message on the console and remote log file.

8. **Cannot access the Web Browser interface from the Protected network.**
   The default Remote Access filter set is generated from the network configuration parameters entered on the Network Information data entry form. It is possible that the GNAT Box’s Protected network interface is on a different logical network from the remote host. Check the Remote Access filter for the Web Browser interface; it may need to be adjusted.

9. **Not all hosts behind GNAT Box can reach the Internet.**
   This is almost always a routing problem. Are the hosts that can’t reach the Internet on a different network segment (subnet)? Have you added a static route to the GNAT Box to tell it which router is used to reach the problem network? Have you set the router’s default route to be the GNAT Box? Have you set the default route for hosts on the problem network to be the router? When debugging routing problems, “traceroute” can be very useful.

10. **GNAT Box will not boot up.**
    There can be many reasons, but here are a few common problems:

    - **Bad floppy diskette.** This is usually indicated when you see a message such as: H:01 S:55 T:23 repeatedly displayed on the console at boot time.

    - **Corrupted floppy disk image.** Often in this situation the system will load the initial bootstrapper, but further along in the boot process the system will freeze.

    - **Unsupported hardware conflict.** Your runtime GNAT Box system should only contain the required components. Additional cards and devices can often cause problems and steal interrupts.

    - **Wrong hardware**. The GNAT Box only runs on a 386, 486, or Pentium CPU or compatibles. The system will not run directly on a 286, Mac, SPARC, SGI, or unsupported hardware. The system requires a minium of 8Mb of RAM to run.

11. **Can't read the diskette image in my Windows/DOS/Mac/Unix system.** The GNAT Box runtime/boot diskette is not directly readable: it has its own file system and format. Use the supplied utilities to read and write GNAT Box floppy diskettes.

12. **Can't access a Tunnel that I have created.** A few key points to remember about Tunnels:
    - You cannot access a Tunnel from the Protected network, since you can access the target 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.
    - Ensure your Tunnel is active. Run the Configuration Report command to verify that both your Tunnel and Remote Access filter(s) are active.

Check the console or your remote log file 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, the service in question running on the specified port. From the target host try to ping the remote host.

13. **My GNAT Box system booted up in "Demo" mode.** The GNAT Box system uses a hardware key block copy protection device. If this device is not present and installed properly on your hardware, the GNAT Box software will enter the demonstration mode at boot time. Check to see if your keyblock has come loose or fallen off your parallel port. Check your system BIOS to ensure that your parallel port is enabled.

14. **My GNAT Box halted.** Most likely your system was operating in the demo

mode and the time-out expired. Initially, the GNAT Box system will run for 180 minutes and then halt. Rebooting the system will decreases the amount of runtime by 30 minutes until no time remains. See item 13.

15. **My MS Exchange server located on the PSN can't find the PDC on the PROtected network.** 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 IP address on the PSN NIC where you will create a tunnel for access.

    2. Create three tunnels from the PSN's NIC 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.

```
    GNAT Box
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
192.168.2.100/255.255.255.255
192.168.2.1/255.255.255.255 137 138

2. Allow Exchange Server to access via NetBIOS TCP
Accept TCP PSN
192.168.2.100/255.255.255.255
192.168.2.1/255.255.255.255 139
```

Windows NT

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

16. **I enabled a GNAT Box feature (email, email proxy, RIP, etc.), but it doesn't work.** Most likely the correct filters are not installed/enabled for the selected features.
    The initial configuration of the GNAT Box 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 particular feature simply activate the feature, supply the required data, if needed, then enable or disable the appropriate Remote Access filter(s).

RIP

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

Stealth Mode

1. Enable the stealth mode and save the section.
2. Enable the "DEFAULT STEALTH" Remote Access filter.
3. Save the Remote Access filter set.

EMAIL Proxy

1. Enable the email (Authorization -> 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.

URL Blocking with WebSENSE

1. Enable either the Traditional or Transparent Proxy modes.
2. Set the IP address of the WebSENSE server.
3. Save the URL Blocking section.
4. If you are using the Traditional proxy, enable the “DEFAULT TRADITION URL PROXY” Remote Access filter.
5. Save the Remote Access filter set.
6. If you are using the Traditional proxy, enable the “DEFAULT TRADITIONAL URL PROXY” Outbound filter.
7. Save the outbound filter set.

17. **I get errors when GBAdmin starts up and/or online help information is not displayed.** GBAdmin requires Micosoft Internet Explorer 3.x or later installed on your workstation. Components from Internet Explorer are used to display the online help information.

Chapter 9: GNAT Box VPN

VPN Overview

The GNAT Box system includes a Virtual Private Networking (VPN) facility as a standard system feature. The VPN is based on the Internet Engineer Task Force (IETF) IP Security (IPSec) standard. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. It provides for transmitting blocks from sources to destinations, which are identified by fixed length addresses. The protocol is specifically limited in scope to provide the functions necessary to deliver a datagram from source to destination, and there are no mechanisms for other services commonly found in host-to-host protocols.

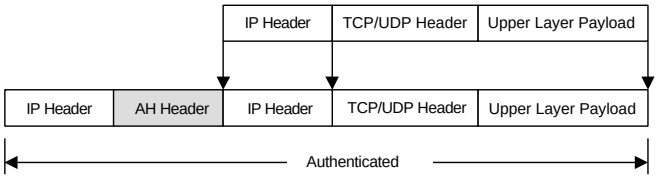
A critical issue concerning the current implementation of the Internet Protocol (IPv4) is that of security. In its growth, the Internet started attracting not only academic circles and research labs, but also banking, commerce, and business sites. It is a growing market area, which is yet to be exploited to its full potential. The lack of security is a rather crippling factor. IPv4 does not provide measures which would assure that the data being received by the end station has not been altered during the transmission, or that it actually came from the claimed source. Because of this, bank transactions can be altered, credit card numbers can be stolen, false data can be fed to companies, and so on.

In an effort to overcome the lack of security in IPv4 and utilize the public Internet as a secure communications network the IETF developed the IPSec standard for Virtual Private Networking. IPSec focuses on the security that can be provided by the IP-layer of the network. It does not concern itself with application level security. The security requirements are divided into two distinct parts: Authentication/Integrity and Confidentiality. These are independent of each other and can be used separately or together according to user needs.

Authentication & Integrity

Authentication guarantees that the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender. Integrity means that we are sure the transmitted data has arrived at destination without undetected alternation. The Authentication Header (AH) is a mechanism for providing strong integrity and authentication for IP datagrams. The security is provided by adding authentication information (to the IP datagram), which is calculated using all of the fields in the IP datagram (including not only the IP

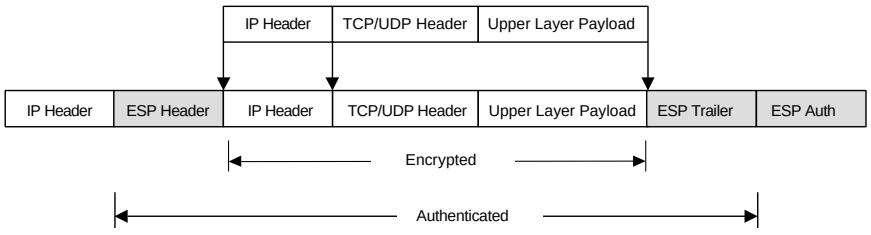
header but also the other headers and the user data). This does not change in transit. Authentication might actually be sufficient for some users who do not require confidentiality. The argument for not using more security measure for some types of packets is the processing costs associated with computation of authentication data by the participating end systems. The authentication data is carried in its own payload; hence the systems that are not participating in the authentication may ignore it. Below are some examples of the IP header structures with and without the AH:



Confidentiality

Confidentiality is the property of communicating such that the intended recipients know what was being sent, but unintended parties cannot determine it. A mechanism commonly used for providing confidentiality is called encryption. IPSec provides confidentiality services through Encapsulating Security Payload (ESP). ESP can also provide data origin authentication, connectionless integrity, and anti-reply service (a form of partial sequence integrity). Confidentiality can be selected independent of all other services. There are two modes for providing confidentiality using ESP. One is transport mode, and the other is tunnel mode. Tunnel mode encapsulates an entire IP datagram within the ESP header. Transport mode, encapsulates the transport layer frame inside ESP (the term 'transport mode' should not be misconstrued as restricting its use to TCP and UDP). The GNAT Box system only supports the tunnel mode.

Below are some examples how the typical IPv4 packets might look before and after applying ESP - tunnel mode:



Terms

Authentication Header (AH) - The AH information is inserted between the IP header and the payload. An AH is used to ensure the integrity of the whole IP packet, including both the payload and the IP header. It does not provide data encryption.

Encapsulating Security Payload (ESP) - An ESP only protects the contents of the payload, not any associated header. Therefore it is possible to change any field in the IP packet carrying an ESP without causing a security violation. The contents of the ESP header are unknown to anyone not possessing information about the transformation and SA needed to recover the protected data.

Hexadecimal Characters - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Internet Key Exchange (IKE) - IKE is the key exchange protocol used for exchanging cryptographic keys for dynamically establishing security associations between two VPN peers.

Lifetime - Value that specifies how long the IKE SA exists. The lifetime specifies a length of time and a specific amount of data. When either value is reached, the SA is terminated and the VPN peers will establish a new key. The software determines this value during each phase. Each phase has a separate lifetime.

Manual Key Exchange – Manual key exchange is a means for exchanging cryptographic keys between VPN peers. Each side must manually enter both the remote and local shared key to initiate the VPN tunnel. The keys do not change.

Null Tunnel Mode - In the Null Tunnel mode no encryption or authentication is used. This mode is useful when only IP encapsulation is desired, such as to utilize unsupported protocols in the NAT mode between two GNAT Box protected networks. To configure the VPN for the Null Tunnel mode, set AH to none and ESP to Null.

PFS Keygroup - Perfect Forward Secrecy (PFS) Key determines how a new key is generated. Using PFS ensures that a key used to protect a transmission, in whichever phase, cannot be used to generate any additional keys. In addition, the keying material for that key cannot be used to generate any new keys. Any one of the three PFS algorithms below may be used below to generate keys. [NOTE: Both sides of the VPN must use the same PFS algorithm to work correctly.]

1. Diffie-Hellman Group 1
2. Diffie-Hellman Group 2
3. Diffie-Hellman Group 5

Phase I - In IKE, a phase one exchange establishes a security association. This phase negotiates the terms of the VPN, authenticates the validity of the VPN peer, and sets the parameters of the VPN connection.

Phase II - In IKE, a phase two exchange establishes security associations for other protocols. This phase provides source authentication, integrity, and confidentiality to all messages.

Preshared Encryption Keys - Only available when using the IKE VPN setup. The Preshared Encryption Key is used to initiate communication with the other side of the VPN. Hence, the Remote Key would be the Local Key of the VPN's other side. [Both side's Local Keys together are the Preshared Encryption Keys.] The Local and Remote Keys should be unique to their respective firewalls.

NOTE: *The Local Key will remain the same for all IKE VPNs on a specific firewall.*

SA - Security Association - Identified by a unique triple of IP Address, SPI (numeric ID) and security protocol (e.g. ESP, AH). Specifies the parameters for communication with the specified host.

SPI - Security Parameter Index - Used to uniquely identify which SA should be applied to a packet. The SPI values should be unique for each SA. The inbound and outbound value may be the same for a given SA. Should be a value greater than 4096.

Implementation

The GNAT Box VPN is based on the IPSec standard using the tunnel mode. The tunnel mode seamlessly and securely establishes connections between networks without requiring any additional software to being installed on host machines. The GNAT Box performs the role of a security gateway by encrypting and routing packets to a remote network.

Before an IP packet is secured by IPSec, a Security Association (SA) must be in place. A Security Association may be created manually or dynamically. The GNAT Box offers both implementations with its manual keying facility and Internet Key Exchange (IKE) facility for dynamic key exchange.

NOTE: *IKE is only available on GB-100, GB-Flash and GB-1000.*

Manual Key Exchange

This method of establishing a VPN tunnel requires the manual exchange of keys between VPN peers. Once this manual exchange has been made, the keys will not change unless the tunnel is recreated.

IKE

Internet Key Exchange (IKE) is a method of dynamically creating a Security Association (SA). Initially, VPN peers must exchange Preshared keys. Using both keys, the IKE will dynamically establish a unique key for the peers using the SA. IKE will renegotiate SAs periodically based on the lifetime values established between the VPN peers.

NOTE: *When contacted by an initiator, the GNAT Box VPN will set itself to the Phase I lifetime values specified by the initiator.*

IKE can be broken down into two phases. Each phase performs a unique function that authenticates and validates VPN connections. The specific functions of each phase are covered below:

Phase I

This phase of the IKE connection establishes the initial SA and is used to authenticate subsequent Phase II exchanges. The GNAT Box IPSec VPN automatically supports a wide variety Phase I proposals. The supported proposals are listed below. Note: all variable length encryption algorithms (blowfish and Cast128) are limited to 64 bits.

Blowfish, sha1, Diffie-Hellman Group 5
Blowfish, md5, Diffie-Hellman Group 5
Cast128, sha1, Diffie-Hellman Group 5
Cast128, md5, Diffie-Hellman Group 5
Blowfish, sha1, Diffie-Hellman Group 2
Blowfish, md5, Diffie-Hellman Group 2
Cast128, sha1, Diffie-Hellman Group 2
Cast128, md5, Diffie-Hellman Group 2
Blowfish, sha1, Diffie-Hellman Group 1
Blowfish, md5, Diffie-Hellman Group 1
Cast128, sha1, Diffie-Hellman Group 1

Cast128, md5, Diffie-Hellman Group 1
DES, sha1, Diffie-Hellman Group 5
DES, md5, Diffie-Hellman Group 5
DES, sha1, Diffie-Hellman Group 2
DES, md5, Diffie-Hellman Group 2
DES, sha1, Diffie-Hellman Group 1
DES, md5, Diffie-Hellman Group 1

Phase II

Once Phase I has been authenticated and the SA has been established between the VPN peers, the Phase II exchange negotiates the encryption proposal used to encrypt the VPN data. The Phase II proposal specification is user configurable. Parameters that can be configured are:

PFS Key Group - Diffie-Hellman Group 1, Diffie-Hellman Group 2 or Diffie-Hellman Group 5.

Hash Algorithm - None, HMAC-MD5, HMAC-SHA1 or All. All is means that either HMAC-MD5 or HMAC-SHA1 are accepted.

Encryption Method - Null, Blowfish, Cast128, DES or Strong. Strong means that any of the following encryption methods will be accepted: Blowfish, Cast128, or DES.

Default Phase II lifetime: 8 hours or 100 MB

NOTE: *Phase I and Phase II have separate lifetimes.*

Access Control

A VPN can provide the secure transportation of data between two networks over an untrusted public network. However it has no control over who can send/ receive information and what data is sent/received between the two networks. A VPN can be a cost effective productive facility or it can also be a clear channel for unauthorized access from a remote network. The GNAT Box VPN facility addresses this issue with access control on the VPN tunnel. The GNAT Box VPN not only provides secure encrypted transportation of data between two networks, it also provides facilities to control access on the encrypted tunnel. The GNAT Box implicit rule, "that which is not explicitly allowed is denied", also applies to VPN connections. VPN access control is provided at three points:

1. At the Protected Network interface through the use of IP Pass Through filters to control the outbound access on the VPN tunnel.

2. At the External Network Interface through the use of Remote Access filters. This access control point allows or disallows the acceptance of an IPSec packet from a remote network.

3. At the External Network Interface through the use of IP Pass Through filters to control the inbound access on the VPN tunnel.

All the standard GNAT Box filter facilities may be used to define access policies on the VPN tunnel for both inbound and outbound access. These facilities are:

- Source IP Address or Network Address Object
- Destination IP Address or Network Address Object
- Source Port
- Destination Port
- Protocol
- T ime of Day/Day of Week
- Network Interface

Hash Algorithms

Hash Algorithms define the authentication method used in various aspects of the GNAT Box VPN. Each key exchange method uses the hash algorithm differently.

Manual Key Exchange

In the Manual Key exchange method, the hash algorithm defines the Authentication Header (AH) transformation when used without an ESP specification. When both hash algorithm and ESP specifications are defined then the hash algorithm specifies the authentication portion of the ESP packet. When creating a Manual Key VPN, a key must be specified using the Key field to the right of the Hash dropbox.

IKE Method

When using the IKE method the hash algorithm is used to define the authentication method with the associated ESP encryption method. If no encryption method is selected then the hash algorithm defines the AH method.

Supported Hash Algorithm

None - This selection indicates that AH will not be used in the Manual Key Mode

or no authentication with the IKE Mode. If None is selected for the authentication algorithm then ESP must have a value or be Null.

HMAC-MD5 - Requires 128 bit key.
NOTE: *When using Manual Key Exchange, the length of the key MUST be 16 characters in ASCII or 32 characters in HEX.*

HMAC-SHA1 - Requires 160 bit key.
NOTE: *When using Manual Key Exchange, the length of the key MUST be 20 characters in ASCII or 40 characters in HEX.*

All - Will accept either HMAC-SHA1 or HMAC-MD5, (negotiated). Only available with IKE method.

Encryption Methods
The Encryption Method defines the encryption used in the Encapsulated Security Payload (ESP) transformation. When using the Manual Key exchange method, a key must be specified using the Key field to the right of the Method dropbox.
Supported Encryption Methods

None - This selection indicates that no encryption will be used, (ie. no ESP transformation). If None is selected for ESP then an authentication method must be selected which is used to define the AH transformation.

Null -No key and no encryption, only IP encapsulation. This method does not provide any encryption however it will encapsulate any IP packet. This is useful when application protocols that are not supported by the GNAT Box system are desired to be used between two sites, (e.g. MS Netmeeting).

Blowfish - When using Manual Key exchange method, the length must be between 40 and 64 bits (ASCII between 5-8 chars, Hex is between 10-16 hexadecimal numbers.

Cast 128 - When using Manual Key VPN, the key length must be between 40 and 64 bits (ASCII between 5-8 chars, Hex is between 10-16 hexadecimal numbers).

DES - When using Manual Key VPN, the key length must be 64 bits (ASCII 8 characters, Hex is 16 hexadecimal numbers).

Strong - Only available when using IKE. Automatically negotiates an encryption technique with the other side of the VPN. When both sides have Strong Encryption implemented, the firewall will cycle through Blowfish, CAST, and DES.

Key Type

This choice list value indicates in which format the key will be specified. Either ASCII or HEX (Hexidecimal). If HEX is used only the valid hexadecimal values may be used.

Limits

The GNAT Box VPN facility allows for up to 300 security associations (SA) to be defined. The number of functional concurrent VPN tunnels is a function of how the tunnels are used, the encryption algorithm and the power of the CPU.

Operation

Since the GNAT Box VPN operates in the IPSec tunnel mode network address translation is **not** applied to the IP packets in the tunnel. This means that system configurations that use unregistered IP addresses on the Protected network (the default case for GNAT Box) will have IP packets transmitted with the unregistered IP address information in the source portion of the IP packet. The major impact of this is that the two physical networks joined by the VPN must be on logically different networks, (e.g. 192.168.1.0/24 <--> 192.168.1.0/24 is not allowed).

All the following configurations are valid with the GNAT Box VPN:
Unregistered Network - Unregistered Network
Unregistered Network - Registered Network
Registered Network - Registered Network

When an unregistered network to registered network VPN configuration is defined care should be taken on the registered network side of the connection to insure that packets to the unregistered network are routed back correctly, (if two GNAT Box systems are used this is performed automatically)

Since the VPN tunnel completely encapsulates the IP packet any IP protocol may be sent through the tunnel, (i.e. AppleTalk, IPX/SPX, etc). The tunnel mode also allows the use of application protocols, which are not normally supported in the NAT mode, such as Microsoft Net meeting.

Packet Flow

The follow is a description of the packet flow for the GNAT Box VPN. This description assumes that two GNAT Box systems are used on both sides of the VPN in order to illustrate both the inbound and outbound aspects of the packet flow.

Outbound

1. When a packet arrives on a protected network interface of the GNAT Box system the VPN Security Associations (SA) are checked to determine if destination is a VPN network? If the destination is not a remote VPN network then normal processing of the IP packet is performed.

2. If the destination is a remote VPN network then the IP Pass Through Filters rules are applied to the packet. If the packet is not accepted by a rule it is rejected.

3. If the packet is accepted by an IP Pass Through Filter rule then the VPN transformation defined in the VPN definition (SA) is applied to the packet.

Inbound

The VPN packet arrives at the External network interface of the remote GNAT Box system. The packet will be either an AH or ESP IP protocol packet.

1. When the VPN packet arrives at the External network interface of the GNAT Box system, Remote Access Filters are applied to the packet. A filter must be in place to accept a packet with either the AH or ESP protocol defined. If no Remote Access filter accepts the packet it is rejected.

2. If a Remote Access filter accepts the VPN packet, the SA table is searched to find a match. If a match is found the appropriate transformation is applied to the packet to decode it.

3. Once the packet has been successfully decrypted IP Pass Through filters are applied to the packet to determine if the packet will be accepted. If no filter match is made the packet is discarded. Otherwise the packet is routed to the target IP address.

Configuration

In order to use the GNAT Box VPN three functional areas must be configured. These are:

1. VPN Definition.

A Security Association (SA) must be in place and configured. The SA must exist on both sides of the VPN with the remote side having a SA that is the mirror image of the local side.

Note: *During VPN definition, once IKE or Manual has been selected it is not possible to change from IKE to manual or vice versa. In order to change, a new VPN must be created.*

2. Remote Access Filter.

Manual Key Exchange - The GNAT Box system requires at least one Remote Access filter that will accept a ESP VPN connection (IP protocol 50) from the remote side of the VPN gateway. A single Remote Access Filter may be used for multiple VPN connections, as it may be configured in a very open and generic manner. However it is best to create a Remote Access filter that is specific for the defined VPN, since this method provides the tightest security.

IKE- When using IKE, two Remote Access filters are needed. One for the ESP Tunnel (IP protocol 50) and the other is to allow access for the IKE on UDP/500.

3. IP Pass Through Filters. At a minimum an IP Pass Through filter that allows outbound access on the defined VPN is required. This filter should be created to meet the local security policy. It can be as simple as to allow any host on the local network outbound access to any remote host for any protocol at any time. Or it can be as narrow as to limit a specific local host outbound access to a specific remote host for a give protocol at a specific time. Generally an inbound IP Pass Through filter is created that allows the remote side of the VPN access to the local protected network. This filter does not have to be symmetrical to the outbound IP Pass through filter, but rather should be created to meet the local security policy. Although typically a single inbound and outbound IP Pass Through filter are created for a VPN definition, multiple filters may be required to provide an access policy that meets the local security policy.

Manual Key Exchange Example

This section provides an example of how a GNAT Box VPN is configured between two networks protected by GNAT Box systems using the manual key exchange method.

Network A

```
       Protected Network: 192.168.1.0/255.255.255.0
    GNAT Box External IP: 199.120.225.2
   GNAT Box Protected IP: 192.168.1.1
             Mail Server: 192.168.1.100
 Developer's Workstation: 192.168.1.225
             Sales Group: 192.168.1.20 - 192.168.1.30
```

Network B

```
       Protected Network: 172.16.0.0/255.255.0.0
    GNAT Box External IP: 204.96.116.15
   GNAT Box Protected IP: 172.16.1.1
         Database Server: 172.16.1.50
             R&D Network: 172.16.2.0
```

VPN Definition

Network A

```
        Key Exchange: Manual
         Description: VPN to Network B
Destination Network: 172.16.0.0/255.255.0.0
       Local Gateway: 199.120.225.2
      Remote Gateway: 204.96.116.15
                  AH: None
                 ESP: Blowfish Key: 87654321
         SPI Inbound: 5000
        SPI Outbound: 5001
```

Network B

```
         Description: VPN to Network A
 Destination Network: 192.168.1.0/255.255.255.0
       Local Gateway: 204.96.116.15
      Remote Gateway: 199.120.225.2
                  AH: None
                 ESP: Blowfish Key: 87654321
         SPI Inbound: 5001
        SPI Outbound: 5000
```

Remote Access Filters

Network A

```
1. Allow ESP connections from Network B
    Accept External ESP
      Source: 204.96.116.15/255.255.255.255
      Destination: 199.120.225.2/255.255.255.255
```

Network B

```
1. Allow ESP connections from Network A
    Accept External ESP
      Source: 199.120.225.2/255.255.255.255
      Destination: 204.96.116.15/255.255.255.255
```

IP Pass Through Filters

Network A

```
1. Allow only developer's workstation to access any host on
   the remote R&D network
    Accept Protected ALL
      Source: 192.168.1.225/255.255.255.255
      Destination: 172.16.2.0/255.255.255.0

2. Allow the sales group to access the database server on
   the remote network with web browser only.
    Accept Protected TCP
      Source: Object Sales Group
      Destination: 172.16.1.50/255.255.255.255 80

3. Allow anyone on the remote network to access the local
   mailserver with POP3 and SMTP
    Accept External TCP
      Source: 172.16.0.0/255.255.0.0
      Destination: 192.168.1.100/255.255.255.255 25, 110
```

Network B

```
1. Allow remote network A full access to any host.
    Accept External ALL
      Source: 192.168.1.0/255.255.255.0
      Destination: 172.16.0.0/255.255.0.0
```

```
2. Allow all users access to remote network A mailserver
    Accept Protected TCP
      Source: 172.16.0.0/255.255.0.0
      Destination: 192.168.1.100/255.255.255.255 25, 110
```

IKE Example Configuration

This section provides an example of how a GNAT Box VPN is configured between two networks protected by GNAT Box systems using the IKE method.

Network A:

```
           Protected Network: 192.168.1.0/255.255.255.0
 GNAT Box External Interface: 199.120.225.2
GNAT Box Protected Interface: 192.168.1.1
```

Network B:

```
           Protected Network: 172.16.0.0/255.255.0.0
 GNAT Box External Interface: 204.96.116.15
GNAT Box Protected Interface: 172.16.1.1
```

VPN Definition Network A:

```
Local pre-shared key: 987654321
```

Note: *The Local pre-shared key is the same for all IKE VPN's on a specific Firewall.*

```
   Description: Network A IKE VPN
   Key exchange: IKE
  Local Network: 192.168.1.0/255.255.255.0
 Remote Network: 172.16.0.0 255.255.0.0
  Local Gateway: 199.120.225.2
       Remote Gateway: 204.96.116.15
           Encryption: Blowfish
                 Hash: none
        PFS key group: Diffie-Hellman Group 2
Remote pre-shared key: 123456789
```

VPN Definition Network B:

```
Local pre-shared key: 123456789
```

```
         Description: Network B IKE VPN
        Key exchange: IKE
        Local Network: 172.16.0.0/255.255.0.0
      Remote Network: 192.168.1.0/255.255.255.0
        Local Gateway: 204.96.116.15
      Remote Gateway: 199.120.225.2
          Encryption: Blowfish
                Hash: none
       PFS key group: Diffie-Hellman Group 2
Remote pre-shared key:  987654321
```

Default Remote Access Filters for IKE:
Remote Access Filters for Network A

```
1 #DEFAULT: VPN: Allow ESP connections From Network B.
  Accept ANY 50
     Source 204.96.116.15/255.255.255.255
       Destination: 199.120.225.2/255.255.255.255

2 #DEFAULT: VPN: Allow access to IKE From Network B.
  Accept ANY UDP
     Source 204.96.116.15/255.255.255.255 500
        Destination: 199.120.225.2/255.255.255.255 500
```

Remote Access Filters for Network B

```
1 #DEFAULT: VPN: Allow ESP connections From Network A.
  Accept ANY 50
     Source 199.120.225.2/255.255.255.255
       Destination: 204.96.116.15/255.255.255.255

2 #DEFAULT: VPN: Allow access to IKE From Network A.
  Accept ANY UDP
     Source 199.120.225.2/255.255.255.255 500
        Destination: 204.96.116.15/255.255.255.255 500
```

IP Pass Through Filters for network A:

```
1. Description: VPN, inbound from Network B (Network A).
```

```
Accept "EXTERNAL" ALL
Source:  172.16.0.0/255.255.0.0
Destination: 192.168.1.0/255.255.255.0

2. Description VPN, allow outbound from network A to B
(Network A).
Accept "PROTECTED" ALL
Source: 192.168.1.0/255.255.255.0
Destination: 172.16.0.0/255.255.0.0

IP Pass Through Filters for network B:

1. Description: VPN, inbound from Network A (Network B).
Accept "EXTERNAL" ALL
Source:  192.168.1.0/255.255.255.0
Destination: 172.16.0.0/255.255.0.0

2. Description: VPN, allow outbound to Network B to A (Net-
work B).
Accept "PROTECTED" ALL
Source: 172.16.0.0/255.255.0.0
Destination: 192.168.1.0/255.255.255.0
```

Appendix A: PPP Chat Scripting

Both the Dial Script and the Login Script follow the same chat script grammar and rules. A chat script consists of one or more "expect-send" pairs of strings, separated by spaces with an optional "subexpect-subsend" string pair or separated by a dash as in the following example:

```
ogin:-BREAK-ogin: ${USERNAME}  ssword: ${PASSWORD}
```

This line indicates that the chat facility should expect the string "ogin:". If it fails to receive a login prompt within the time interval allotted, it is to send a break sequence to the remote and then expect the string "ogin:". If the first "ogin:" is received the break sequence is not generated.

Once it receives the login prompt, the chat facility will send the string stored in the ${USERNAME} token and then expect the prompt "ssword:". When it receives the prompt for the password, it will send the password stored in the ${PASSWORD} token.

A carriage return is normally sent following the reply string. It is not expected in the "expect" string, unless it is specifically requested by using the \r character sequence.

The expect sequence should contain only what is needed to identify the string. It is generally not acceptable to look for time strings, network identification strings, or other variable pieces of data as an expect string. To help correct for characters which may be corrupted during the initial sequence, look for the string "ogin:" rather than "login:". It is possible that the leading "l" character may be received in error and you may never find the string, even though it was sent by the system. For this reason, scripts look for "ogin:" rather than "login:", and "ssword:" rather than "password:".

A very simple script might look like this:

```
ogin:  ppp  ssword:  hello2u2
```

In other words, expect ....ogin:, send ppp, expect ...ssword:, send hello2u2.

In actual practice, simple scripts are rare. At the vary least, you should include sub-expect sequences in case the original string is not received. For example, consider the following script:

```
ogin:--ogin: ppp ssword: hello2u2
```

This would be a better script than the simple one used earlier. It looks for the same login: prompt. However, if one was not received, a single return sequence is sent and it will look for login: again. Should line noise obscure the first login prompt, sending the empty line will usually generate a second login prompt.

GNAT Box PPP Tokens

Three tokens are provided for use in chat scripting. The tokens are:

${USERNAME}

This token has its value assigned from the Login Name data entry field. The token value is usually the PPP login id assigned by the remote site.

${PASSWORD}

This token has its value assigned from the Login Password data entry field. Since the password data entry field obscures the password, this token makes it convenient to insert the password into the chat script without revealing the actual password value.

${NUM}

This token has its value assigned from the Phone Number data entry field. The phone number may contain dialing directives for the modem, in addition to the actual telephone number. For example:

```
9,555-1653
```

This telephone number entry will cause the modem to first dial a '9', then pause before dialing the remaining digits.

Note: *Most modems that use the Hayes AT dialing command set will ignore the '-' character.*

PPP Keywords

TIMEOUT

The initial timeout value is the value in seconds assigned from the "Wait Time" data entry field, in seconds. This may be changed using the TIMEOUT keyword and parameter. To change the timeout value for the next expect string, the following example may be used:

```
TIMEOUT 10 ogin: ${USERNAME} TIMEOUT 5 assword: ${PASSWORD}
```

This will change the timeout to 10 seconds before it expects the login: prompt. The timeout is then changed to 5 seconds before it looks for the password prompt. The timeout, once changed, remains in effect until it is changed again.

Sending EOT

The special reply string of EOT indicates that the chat program should send an EOT character to the remote. This is normally the End-of-file character sequence. A return character is not sent following the EOT. The EOT sequence may be embedded into the send string using the sequence ^D.

Generating Break

The special reply string of BREAK will cause a break condition to be sent. The break is a special signal on the transmitter. The normal processing on the receiver is to change the transmission rate. It may be used to cycle through the available transmission rates on the remote until you are able to receive a valid login prompt. The break sequence may be embedded into the send string using the \K sequence.

Escape Sequences

The expect and reply strings may contain escape sequences. All of the sequences are legal in the reply string, many are legal in the expect. Those which are not valid in the expect sequence are so indicated.

"" Expects or sends a null string. If you send a null string then it will still send the return character. This sequence may either be a pair of apostrophe or quote characters.

\b Represents a backspace character.

\c Suppresses the newline at the end of the reply string. This is the only

method to send a string without a trailing return character. It must be at the end of the send string. For example, the sequence hello\c will simply send the characters h, e, l, l, o.

\d Delay for one second (not valid in expect string).

\K Insert a BREAK (not valid in expect string).

\n Send a newline or linefeed character.

\N Send a null character. The same sequence may be represented by \0 (not valid in expect string).

\p Pause for a fraction of a second. The delay is 1/10th of a second.

\q Suppress writing the string to the string, "??????" is written to the log in its place (not valid in expect string).

\r Send or expect a carriage return.

\s Represents a space character in the string. This may be used when it is not desirable to quote the strings which contain spaces. The sequence 'HI TIM' and HI\sTIM are the same.

\t Send or expect a tab character.

**** Send or expect a backslash character.

\ddd Collapse the octal digits (ddd) into a single ASCII character and send that character (some characters are not valid in expect string).

^C Substitute the sequence with the control character represented by C.

For example, the character DC1 (17) is shown as ^Q (some characters are not valid in expect string).

Appendix B: Ports and Services

Common Services

The table below list some common services ports used by TCP/IP. The complete list of services is far too large to list in this guide. For a complete list of ports and services see the services file provided on the GNAT Box CDROM (services.pdf).

Service	Port	Protocol	Comments
Echo	7	TCP	
FTP	21	TCP	Control channel
SSH	22	TCP	
Telnet	23	TCP	
SMTP	25	TCP	
DNS	53	UDP	
Finger	79	TCP	
HTTP	80	TCP	
POP3	110	TCP	
Auth	113	TCP	
Sqlserv	118	TCP	
Netbios-ns	137	UDP	Name Service
Netbios-dgm	138	UDP	Datagram Service
Netbios-ssn	139	TCP	Session Service
SNMP	161	TCP	
SNMP Trap	162	UDP	
Archie Reply	191	TCP	
Syslog	514	UDP	
Printer	515	TCP	
PPTP	1723	TCP	PPTP control channel
Citrix	1494	TCP	
PCAnywhere	5631	TCP/UDP	
PCAnywhere	5632	TCP/UDP	
Lotus Notes	1352	TCP	

Audio/Video Protocols

The GNAT Box system supports many streaming audio/video protocols transparently. If you wish to block your internal users access to these services, simply create an Outbound filter that denies access to one or more of these services. Conversely you can simply create Outbound filters that allow desired services and allow the default rule to block all other services.

Service	Port	Protocol	Comment
AudioLink v0.5	2961	TCP	
AudioLink v0.7	9971	TCP	
CU-SeeMe	7648	UDP	
Real Audio	7070	TCP	Same for RealVideo
RTSP	554	TCP	QuickTime 4.0 streaming
StreamWorks1	1558	UDP	
StreamWorks2	1559	UDP	
StreamWorks3	1568	UDP	
StreamWorks4	1658	UDP	
VDOLive	7000	TCP	
Vosaic	1235	TCP	
VXtreme	12468	TCP	

Notes

1. Due to the design of the CU-SeeMe protocol only one user at a time can use a given IP address. To allow concurrent use of this protocol, an IP alias needs to be assigned to the External network interface for each additional user. The Static Mapping facility must then be used to statically map the alias IP addresses to the user's workstation IP address.

Appendix C: Examples

These examples are based upon the network illustrated from the Terms and Concepts section of this guide. The basic GNAT Box configuration for the example network is listed below.

```
Interface     IP Address      Netmask         Device
EXT           199.120.225.2   255.255.255.0   de0
PRO           192.168.1.2     255.255.255.0   de1
PSN           192.168.3.2     255.255.255.0   de2

GNAT Box Default Route: 199.120.225.1

Static Routes
192.168.2.0   255.255.255.0   192.168.1.254

IP Aliases
EXT 199.120.225.3 255.255.255.255

Remote GB     204.92.100.2
Web Server    192.168.3.20
FTP Server    192.168.3.20
DNS Server    192.168.3.20   (External server)
DNS Server    192.168.1.50   (Internal server)
Email Server  192.168.3.50   (NT Server)
Proxy Server  192.168.1.50
Log Server    192.168.1.50   (Remote logging host)
Remote Host   204.96.116.2   (Remote host on the Internet)
PDC           192.168.1.50

Hosts Configurations
Hosts on the 192.168.1.0 network
Default route: 192.168.1.2
          DNS: 192.168.1.50
  POP3 Server: 192.168.3.50
  SMTP Server: 192.168.3.50

Hosts on the 192.168.2.0 network
Default route: 192.168.2.2
          DNS: 192.168.1.50
  POP3 Server: 192.168.3.50
  SMTP Server: 192.168.3.50

Hosts on the 192.168.3.0 network
Default route: 192.168.3.2
          DNS: 192.168.3.20
  POP3 Server: 192.168.3.50
  SMTP Server: 192.168.3.50
```

Example 1

Allow public access to web, ftp, email and DNS servers on the PSN.

1. Create GNAT Box tunnels for the services on the PSN.

```
TCP 199.120.225.2  21  192.168.3.20 21
TCP 199.120.225.2  25  192.168.3.50 25
UDP 199.120.225.2  53  192.168.3.20 53
TCP 199.120.225.2  80  192.168.3.20 80
```

2. Create a Remote Access filters that allows access to the tunnels.
   Save the filter set.

```
Allow remote network access to ftp, SMTP, WWW
Accept EXT TCP
from 0.0.0.0/0.0.0.0
  to 199.120.225.2/255.255.255.255 21, 25, 80

Allow remote network access to DNS
Accept EXT UDP
from 0.0.0.0/0.0.0.0
  to 199.120.225.2/255.255.255.255 53
```

Example 2

Allow public access to a second web server running on the NT server.

1. Create a GNAT Box tunnel for the new web server on the PSN. We need to use the alias IP address of 199.120.225.3 because there is already a web server running on 199.120.225.2.

```
TCP 199.120.225.3  80  192.168.3.50 80
```

2. Create a Remote Access filter that allows access to the new tunnel. Save the filter set.

```
Allow remote network access to ftp, SMTP, WWW
Accept EXT TCP
from 0.0.0.0/0.0.0.0
  to 199.120.225.3/255.255.255.255 80
```

Example 3

Allow inbound access via Microsoft's PPTP to an NT server.

1. Create a GNAT Box tunnel to the NT server.

```
TCP 199.120.225.2  1723   192.168.3.50 1723
```

2. Create a Remote Access filter that allows access to the tunnel. Save the filter set.

```
Allow remote network access to NT server via PPTP
Accept EXT TCP log
from 199.120.226.2/255.255.255.0
  to 199.120.225.2/255.255.255.0 1723
```

3. Create a static route entry for the virtual network (192.168.10.0), to allow routing of TCP/IP traffic. This entry is only required if TCP/IP will be an encapsulated protocol used in the PPTP VPN.

```
192.168.10.0   255.255.255.0  192.168.3.50
```

Note: *Since the GNAT Box has builtin support for PPTP's transport protocol (GRE, IP protocol 47), only the TCP control port needs to be tunneled.*

Example 4

Require internal users to use cacheing/screening server for Internet web access.

1. Create Outbound filters. Save the filter set.

```
Allow web proxy server access to the Internet.
Accept PRO TCP log
from 192.168.1.50/255.255.255.255
  to 0.0.0.0/0.0.0.0 80

Disallow direct Internet web access to internal users.
Deny PRO TCP log
from 192.168.0.0/255.255.0.0
  to 0.0.0.0/0.0.0.0 80
```

Note: *The default Outbound filter can be left in place if other services are allowed. The new filters should be inserted before the default filter. Also note no tunnels are required for outbound access.*

Example 5

Allow a single remote host on the Internet access to the GNAT Box Web Browser Remote Admin Interface.

Note: *In this configuration remote administration will be moved to port 8080 since port 80 will be tunneled to a web server located on the Private Service network.*

1. Configure remote web browser administration to operate on port 8080.

If you use GBAdmin interface then select Remote Administration and set the parameters and perform a save.

2. In Remote Access filters change the filter that allows remote administration via the web browser, so the destination port reflects the new port number. Remove the old port number.

Note: *If you choose to use the web browser to make these changes you must first add the new port to the Remote Access filter, but don't delete the original port 80 at this time. Make the changes on the Remote Administration screen, then make the final changes to the Remote Access filter. Make sure after the change you add the port number to your URL, in your browser, such as: http://192.168.1.254:8080*

```
            WWW: Yes
Updates Allowed: Yes
    Server port: 8080
```

3. Change the default Remote Access filter which allows access to the Web Browser Remote Admin Interface, to allow access on port 8080 from port 80.

```
DEFAULT: Allow protected network access to remote admin
        server (WWW)
Accept PRO TCP
from 192.168.1.0/255.255.255.0
  to 192.168.1.2/255.255.255.255 8080
```

4. Create a Remote Access filter to allow a single remote host on the Internet access to the GNAT Box Web Browser Remote Admin Interface. After adding the new filter, save the filter set.

```
Allow a remote host access the Remote Web Admin Interface
Accept EXT TCP log
from 204.96.116.2/255.255.255.255
  to 199.120.225.2/255.255.255.255 8080
```

Note: *This configuration is not recommended since all data is sent in the clear. For remote access from the external network use the RMC interface as it encrypts all data.*

Example 6

Allow the Remote Management Console (GBAdmin) to access the GNAT Box from the external network.

1. Add a Remote Access Filter to accept packets for the RMC from the

EXT network interface.

```
Allow remote hosts to access the RMC Interface
Accept EXT TCP log
from 0.0.0.0/0.0.0.0
  to 199.120.225.2/255.255.255.255 77
```

2. Make sure that you generate a new encryption key and are not using the default key.

Example 7

Allow a MS Exchange server to access a PDC on the PROtected network, so authentication can be performed on client connections.

1. Create an LMHOSTS file and insert an entry for the PDC. This entry will use the PDC's NetBIOS name, the NetBIOS domain name and the IP address (or an alias) on the PSN NIC where you will create a tunnel for access.

   ```
   192.168.3.2    PDCserver    #PRE #DOM:gtanet
   ```

2. Create two tunnels from the PSN's NIC to the PDC for NetBIOS services.
   UDP 138 - NetBIOS datagrams
   TCP 139 - NetBIOS data transfer

   ```
   UDP  192.168.3.2  138   192.168.1.50  138
   TCP  192.168.3.2  139   192.168.1.50  139
   ```

3. Create two Remote Access filters that allow the MS Exchange server on the PSN to access the two tunnels you created in step 2.

   ```
   1. Allow Exchange Server to access the PDC via NetBIOS UDP
   Accept UDP PSN
   192.168.3.50/255.255.255.255
   192.168.3.2/255.255.255.255 138

   2. Allow Exchange Server to access the PDC via NetBIOS TCP
   Accept TCP PSN
   192.168.3.50/255.255.255.255
   192.168.3.2/255.255.255.255 139
   ```

4. Reboot the Exchange server.

Example 8

Setup a VPN between two GNAT Box networks (New York and Chicago). Hosts on the New York network are allowed to access any host on the Chicago network. Hosts on the Chicago network are only allowed to access a mail server (192.168.1.205) on the New York network with SMTP and POP3 protocols.

1. Define the VPN on each gateway

```
VPN New York - Chicago
Remote Gateway: 204.92.100.2
Local Gateway: 199.120.225.2
Remote Network: 192.168.100.0/255.255.255.0
AH Mode: None
ESP Mode: Blowfish
Key type: ASCII
Key: ABCDEFGH
SPI In: 5000  SPI Out: 5001
```

New York

```
VPN Chicago - New York
Remote Gateway: 199.120.225.2
Local Gateway: 204.92.100.2
Remote Network: 192.168.1.0/255.255.255.0
AH Mode: None
ESP Mode: Blowfish
Key type: ASCII
Key: ABCDEFGH
SPI In: 5001  SPI Out: 5000
```

Chicago

2. Create a remote access filter on each system.

```
1. Allow Chicago access with IPSec ESP protocol
Accept ESP EXT
204.92.100.2/255.255.255.255
199.120.225.2/255.255.255.255
```

New York

```
1. Allow New York access with IPSec ESP protocol
Accept ESP EXT
199.120.225.2/255.255.255.255
204.92.100.2/255.255.255.255
```

Chicago

3. Create the IP Pass Through filters to allow access on the tunnel.

New York

```
 1 Inbound VPN, for Chicago
  Accept "EXTERNAL" TCP
     from 192.168.100.0/255.255.255.0
       to 192.168.1.205/255.255.255.255 25 110

2 VPN, allow outbound for New York
  Accept "PROTECTED" ALL
     from "ANY_IP"
       to 192.168.1.0/255.255.255.0
```

Chicago

```
 1 Inbound VPN, for New York
  Accept "EXTERNAL" ALL
     from 192.168.1.0/255.255.255.0
       to "ANY_IP"

2 VPN, allow outbound for Chicago
  Accept "PROTECTED" ALL
     from "ANY_IP"
       to 192.168.100.0/255.255.255.0
```

Appendix D: Default Settings

Default Security Policy

The implicit security rule for GNAT Box is "**that which is not expressly permitted is denied**." If all filters (Remote Access, Outbound and IP Pass Through) were removed no packets would flow inbound or outbound. The GNAT Box system can generate a default configuration, based on the following security policy:

Remote Access

1. All inbound access from the External network is denied.
2. All access from the External network to the GNAT Box is not allowed.
3. Access to the Web browser interface is allowed only from IP addresses on the protected network.
4. Access from the Private Service network to the GNAT Box is not allowed.
5. Access from the Private Service network to the Protected network is not allowed.
6. Access to the Console interface requires a user ID and password (if one was assigned durning the initial configuration).
7. Access to the web browser interface requires a user ID and password (if one was assigned durning the initial configuration).

Outbound Access

1. All outbound access from the Protected network is allowed.
2. All outbound access from the PSN network is allowed.

```
OUTBOUND Filters
     1 #DEFAULT TRADITIONAL URL PROXY: allow access to DNS.
       DISABLED - Accept PRO UDP
          from 0.0.0.0/0.0.0.0
            to 0.0.0.0/0.0.0.0 53

     2 #DEFAULT NO TRADITIONAL URL PROXY: Allow protected network access
       to anywhere.
       Accept PRO ALL
          from 0.0.0.0/0.0.0.0
            to 0.0.0.0/0.0.0.0

     3 #DEFAULT PSN: Allow PSN network to access anywhere.
       Accept PSN ALL
          from 0.0.0.0/0.0.0.0
            to 0.0.0.0/0.0.0.0

Remote Access Filters
     1 #DEFAULT: Allow protected network access to WWW remote admin server.
       Accept PRO TCP
          from 10.10.1.0/255.255.255.0
            to 10.10.1.69/255.255.255.255 80
```

```
 2 #DEFAULT: Allow protected network access to RMC remote admin server.
   Accept PRO TCP
      from 10.10.1.0/255.255.255.0
        to 10.10.1.69/255.255.255.255 77

 3 #DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy.
   DISABLED - Accept PRO TCP
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 2784

 4 #DEFAULT EMAIL PROXY: Allow connections to email proxy.
   DISABLED - Accept EXT TCP
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 25

 5 #DEFAULT: Block/nolog discard bootp, netbios, snmp, and rwho.
   Deny   ANY UDP  nolog
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 9 67 68 137 138 161 513

 6 #DEFAULT NO RIP: Block/nolog rip.
   Deny   ANY UDP  nolog
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 520

 7 #DEFAULT RIP: Accept UDP rip.
   DISABLED - Accept ANY UDP
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 520

 8 #DEFAULT RIP: Accept IGMP multicast for router addresses.
   DISABLED - Accept ANY 2
      from 0.0.0.0/0.0.0.0
        to 224.0.0.0/255.255.255.0

 9 #DEFAULT RIP: Accept router solicititations and advertisements
   DISABLED - Accept ANY ICMP
      from 0.0.0.0/0.0.0.0
        to 224.0.0.0/255.255.255.0 9 10

10 #DEFAULT STEALTH: Block with alarm any other access to external
   interface.
   DISABLED - Deny   EXT ALL  alarm
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0

11 #DEFAULT: Accept/nolog authentication (ident).
   Accept ANY TCP  nolog
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 113

12 #DEFAULT: Allow pings and ICMP traceroutes to GNAT Box.
   Accept ANY ICMP
      from 0.0.0.0/0.0.0.0 8
        to 0.0.0.0/0.0.0.0 8

13 #DEFAULT: Allow UDP traceroutes to GNAT Box.
   Deny   ANY UDP  nolog genICMP
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0 32767:65535

14 #DEFAULT: Block with alarm any other access to all interfaces.
   Deny   ANY ALL  alarm
      from 0.0.0.0/0.0.0.0
        to 0.0.0.0/0.0.0.0
```

Appendix E: Sample Reports

Sample Reports

Active ARP Table

```
              GNAT Box Active ARP Table

  IP Address       MAC Address        Time To Live
  ---------------  -----------------  ------------
  10.10.1.67       incomplete
  10.10.1.68       incomplete
  10.10.1.200      00:60:97:60:11:23  00:08:00
  10.10.1.201      00:a0:24:3d:6a:8b  00:16:02
  199.120.225.1    00:00:a5:d8:38:00  00:05:58
  -------------------------------------------------
```

Active Routes

```
          GNAT Box Active Routes

  Destination      Netmask          Gateway           Flags
  0.0.0.0          0.0.0.0          199.120.225.1     UGSc
  10.10.1.0        255.255.255.0    le0               UC
  192.168.5.0      255.255.255.0    le2               UC
  192.168.30.0     255.255.255.0    10.10.1.67        UGSc
  199.120.225.0    255.255.255.128  le1               UC
  199.120.225.6    255.255.255.255  le1               UC
  199.120.225.7    255.255.255.255  le1               UC
  199.120.225.8    255.255.255.255  le1               UC
```

Active Filters

```
GNAT Box Active Filters

OUTBOUND
    1    43172  Accept PRO (le0) ALL  from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0
    2        0  Accept PSN (le2) ALL  from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0

REMOTE ACCESS
    1      215  Accept EXT (le1) TCP  from 206.104.206.100/255.255.255.255 to 199.120.225.5/255.255.255.255 80
    2        0  Deny   ANY TCP  email pager snmp from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0 26
    3        0  Accept ANY ICMP from 0.0.0.0/0.0.0.0 to 199.120.225.6/255.255.255.255
    4        0  Deny   EXT (le1) UDP  log from 0.0.0.0/0.0.0.0 to 199.120.225.5/255.255.255.255 6112
    5        0  Accept ANY TCP  from 0.0.0.0/0.0.0.0 to 199.120.225.6/255.255.255.255 21
    6        0  Accept EXT (le1) TCP  from 0.0.0.0/0.0.0.0 to 199.120.225.6/255.255.255.255 22
    7        2  Accept PRO (le0) TCP  from 10.10.1.0/255.255.255.0 to 10.10.1.222/255.255.255.255 80
    8        0  Accept EXT (le1) TCP  from 0.0.0.0/0.0.0.0 to 199.120.225.6/255.255.255.255 25
    9        1  Deny   PRO (le0) ALL  bcast nolog from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0
   10        0  Deny   ANY UDP  nolog from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0 9 67 68 137 138 161 513
   11        0  Deny   ANY UDP  nolog from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0 520
   12        0  Accept ANY UDP  from 0.0.0.0/0.0.0.0 53  to 0.0.0.0/0.0.0.0
   13        0  Accept ANY TCP  log from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0 113
   14        0  Accept ANY ICMP from 0.0.0.0/0.0.0.0 8  to 0.0.0.0/0.0.0.0 8
   15        0  Deny   ANY UDP  nolog genICMP from 0.0.0.0/0.0.0.0 to 0.0.0.0/0.0.0.0 32767:65535
   16        0  Accept PRO (le0) TCP  from 0.0.0.0/0.0.0.0 25  to 0.0.0.0/0.0.0.0 flags 16
   17        0  Accept ANY ICMP from 0.0.0.0/0.0.0.0 0  to 0.0.0.0/0.0.0.0 0
   18        0  Accept ANY ICMP from 0.0.0.0/0.0.0.0 3 4 11  to 0.0.0.0/0.0.0.0 3 4 11

IP PASS THROUGH
   none installed

* Indicates inactive time based filter.
```

GNAT Box Active Connections

GNAT Box Active Connections

						PACKETS		BYTES	
	PROTOCOL	SOURCE	NAT	DESTINATION	IDLE	RECEIVED	SENT	RECEIVED	SENT
-->	TCP	10.10.1.63/1333	199.120.225.5/39014	198.3.98.160/80	00:00:00	14	13	16832	876
-->	TCP	10.10.1.63/1334	199.120.225.5/39015	198.3.98.160/80	00:00:00	4	4	270	633
-->	TCP	10.10.1.63/1336	199.120.225.5/39017	198.3.98.160/80	00:00:01	0	1	0	48
-->	TCP	10.10.1.63/1335	199.120.225.5/39016	198.3.98.160/80	00:00:01	0	1	0	48
-->	TCP	10.10.1.201/1022	199.120.225.6/969	204.96.116.177/22	00:03:44	877	1066	98939	68087

GNAT Box Verification Report

GNAT Box GB-100 Version: 3.0.3 Sun Jan 12 14:18:40 2000

BASIC CONFIGURATION
Verify DNS.
Verify feature codes.
Verify network information.
Verify preferences.
Verify remote logging.

AUTHORIZATION
Verify administration accounts.
Verify email proxy.
Verify remote administration.
WARNING: WWW administration interface is running on port 80.
Verify URL blocking.
Verify VPN.

ROUTING
Verify RIP.
Verify static routes.

OBJECT

```
 Verify addresses.

FILTERS
 Verify outbound filters.
 Verify filter preferences.
 Verify protocols.
 Verify remote access filters.
 Verify time groups.

IP PASS THROUGH
 Verify IP pass through hosts/networks.

 Verify IP pass Through filters.

NAT
 Verify aliases.
 Verify inbound tunnels.
 Verify static address mappings.


                    Copyright © 1996-2000 Global Technology Associates, Inc.
```

Hardware Summary Report

```
                GNAT Box Version: 3.0.3                  Sun Jan 12 17:16:05 2000

GNAT Box: Kernel #303 bugmaster@gnatbox.com:GB100
Timecounter "i8254"  frequency 1193182 Hz
Timecounter "TSC"  frequency 133637377 Hz
CPU: Pentium/P54C (133.64-MHz 586-class CPU)
  Origin = "GenuineIntel"  Id = 0x52c  Stepping=12
  Features=0x1bf<FPU,VME,DE,PSE,TSC,MSR,MCE,CX8>
real memory  = 33554432 (32768K bytes)
avail memory = 30347264 (29636K bytes)
Probing for devices on PCI bus 0:
oltr: oltr_pci_probe
```

```
chip0: <VIA 82C597 (Apollo VP3) system controller> rev 0x04 on pci0.0.0
oltr: oltr_pci_probe
chip1: <VIA 82C598MVP (Apollo MVP3) PCI-PCI bridge> rev 0x00 on pci0.1.0
oltr: oltr_pci_probe
chip2: <VIA 82C586 PCI-ISA bridge> rev 0x47 on pci0.7.0
oltr: oltr_pci_probe
oltr: oltr_pci_probe
chip3: <VIA 82C586B ACPI interface> rev 0x10 on pci0.7.3
xl0: <3Com 3c905-TX Fast Etherlink XL> rev 0x00 int a irq 12 on pci0.9.0
xl0: Ethernet address: 00:60:08:af:2b:f2
xl0: autoneg complete, link status good (half-duplex, 10Mbps)
xl1: <3Com 3c905-TX Fast Etherlink XL> rev 0x00 int a irq 10 on pci0.11.0
xl1: Ethernet address: 00:60:97:98:03:89
xl1: autoneg complete, link status good (full-duplex, 100Mbps)
fxp0: <Intel EtherExpress Pro 10/100B Ethernet> rev 0x05 int a irq 11 on pci0.13.0
fxp0: Ethernet address 00:60:ef:20:66:c5
Probing for devices on PCI bus 1:
vga0: <S3 model 8a10 graphics accelerator> rev 0x06 int a irq 15 on pci1.0.0
Probing for devices on the ISA bus:
sc0 on isa
sc0: VGA color <3 virtual consoles, flags=0x0>
atkbdc0 at 0x60-0x6f on motherboard
atkbd0 irq 1 on isa
sio0 at 0x3f8-0x3ff irq 4 flags 0x10 on isa
sio0: type 16550A
sio1 at 0x2f8-0x2ff irq 3 on isa
sio1: type 16550A
sio2: configured irq 5 not in bitmap of probed irqs 0
sio2 not found at 0x3e8
sio3: configured irq 9 not in bitmap of probed irqs 0
sio3 not found at 0x2e8
fdc0 at 0x3f0-0x3f7 irq 6 drq 2 on isa
fdc0: FIFO enabled, 8 bytes threshold
fd0: 1.44MB 3.5in
ppc0 at 0x378 irq 7 on isa
ppc0: Generic chipset (EPP/NIBBLE) in COMPATIBLE mode
vga0 at 0x3b0-0x3df maddr 0xa0000 msize 131072 on isa
npx0 on motherboard
npx0: INT 16 interface
Intel Pentium detected, installing workaround for F00F bug
```

Software Summary Report

```
   GNAT Box Pro Version: 3.0.3                    Sat Mar 11 17:11:46 2000


BASIC CONFIGURATION
  DNS
    External name server: 199.120.225.2
    Internal name server: 10.10.1.7
                  Domain: gta.com

  FEATURES

  NETWORK INFORMATION
    LOGICAL INTERFACES
     Name                 Type        IP Address       Netmask          NIC
     -------------------  ---------   ---------------  ---------------  -----
     EXTERNAL             EXTERNAL    199.120.225.76   255.255.255.128  xl0
     PROTECTED            PROTECTED   10.10.1.76       255.0.0.0        xl1

    NETWORK INTERFACE CARDS
     NIC    MAC Address        MTU    State  Options
     -----  -----------------  -----  -----  -------
     xl0    00:60:08:af:2b:9a  1500   up
     xl1    00:10:5a:0c:35:03  1500   up
     PPP                       1500   down   MANUAL

    Default route (gateway): 199.120.225.1
                   Hostname: GNAT-Box

  PREFERENCES
    CONTACT INFORMATION
              Name: Joe User
```

```
          Company: GTA, Inc.
     Email Address: joe@gta.com
      Phone number: 407-380-0220
     Serial number: 111111111
     Support email: gb-config@gta.com

    KEYBOARD LAYOUT
     United States ISO-8859-1

    SCREEN SAVER
     Timeout: 0 seconds

  REMOTE LOGGING
    Logging System Messages to Server: 10.10.1.65.

    Filter facility: local0
       NAT facility: local0
       WWW facility: local2
      Open priority: notice
     Close priority: notice
       WWW priority: notice

AUTHORIZATION
  ADMINISTRATION ACCOUNTS
    Index  User             Permissions
    -----  ---------------  -------------------------
    1      gnatbox          admin console www remote

  EMAIL PROXY
                Enabled: yes
          Primary server: 10.10.1.7
       Alternate server:
              Time out: 120 seconds
```

```
  Maximum connections: 50
              Domain: gta.com
              Use MX: yes
         Verify RDNS: no
        Maximum size: 0 kilobytes
              MAPS 1: enabled rbl.maps.vix.com
              MAPS 2: enabled dul.maps.vix.com
              MAPS 3: enabled relays.orbs.org
              MAPS 4: enabled relays.mail-abuse.org

REMOTE ADMINISTRATION
  WWW  Server: enabled
      Updates: enabled
         Port: 8080

  RMC  Server: enabled
      Updates: enabled
         Port: 77

URL BLOCKING
  disabled

MOBILE CODE BLOCKING
          JAVA blocking: disabled
  JAVA script blocking: disabled
      ActiveX blocking: disabled

VPNs
   1 # VPN One
     Destination: 192.168.11.0/255.255.255.0
        Gateways: 199.120.225.76->199.120.225.80
              AH: hmac-md5
             ESP: des
             SPI: 7800 7800
```

```
     2 #PSN VPN
       Destination: 192.168.12.0/255.255.255.0
          Gateways: 199.120.225.76->199.120.225.80
                AH: hmac-md5
               ESP: null
               SPI: 4097 4096

ROUTING
  RIP
    disabled

  STATIC ROUTES
    Index  IP Address      Netmask           Gateway
    -----  --------------- ---------------   ---------------

OBJECTS
  ADDRESSES
    1      ANY_IP - DEFAULT: Matches all IP addresses.
              Index  Beginning        Ending
              -----  --------------   ---------------
              1      0.0.0.0          255.255.255.255


FILTERS
  OUTBOUND
     1 #DEFAULT TRADITIONAL URL PROXY: allow access to DNS.
       DISABLED - Accept "PROTECTED" UDP
          from "ANY_IP"
            to "ANY_IP" 53

     2 #DEFAULT NO TRADITIONAL URL PROXY: Allow protected network access to anywhere.
       Accept "PROTECTED" ALL
```

```
        from "ANY_IP"
          to "ANY_IP"

REMOTE ACCESS
   1 #DEFAULT: VPN, allow ESP connections (Test VPN).
     Accept "EXTERNAL" 50
        from 199.120.225.80/255.255.255.255
          to 199.120.225.76/255.255.255.255

   2 #DEFAULT: Allow protected network access to WWW remote admin server.
     Accept "PROTECTED" TCP
        from 10.0.0.0/255.0.0.0
          to 10.10.1.76/255.255.255.255 8080

   3 #DEFAULT: Allow protected network access to RMC remote admin server.
     Accept "PROTECTED" TCP
        from 10.0.0.0/255.0.0.0
          to 10.10.1.76/255.255.255.255 77

   4 #DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy.
     DISABLED - Accept "PROTECTED" TCP
        from "ANY_IP"
          to 0.0.0.0/0.0.0.0 2784

   5 #DEFAULT EMAIL PROXY: Allow connections to email proxy.
     Accept "EXTERNAL" TCP
        from "ANY_IP"
          to "ANY_IP" 25

   6 #DEFAULT: Block/nolog discard bootp, netbios, snmp, and rwho.
     Deny   ANY UDP  nolog
        from "ANY_IP"
          to "ANY_IP" 9 67 68 137 138 161 513
```

```
 7 #DEFAULT NO RIP: Block/nolog rip.
   Deny   ANY UDP  nolog
      from "ANY_IP"
        to "ANY_IP" 520

 8 #DEFAULT RIP: Accept UDP rip.
   DISABLED - Accept ANY UDP
      from "ANY_IP"
        to "ANY_IP" 520

 9 #DEFAULT RIP: Accept IGMP multicast for router addresses.
   DISABLED - Accept ANY 2
      from "ANY_IP"
        to 224.0.0.0/255.255.255.0

10 #DEFAULT RIP: Accept router solicititations and advertisements
   DISABLED - Accept ANY ICMP
      from "ANY_IP"
        to 224.0.0.0/255.255.255.0 9 10

11 #DEFAULT STEALTH: Block with alarm any other access to external interface.
   DISABLED - Deny   "EXTERNAL" ALL  alarm
      from "ANY_IP"
        to "ANY_IP"

12 #DEFAULT: Accept/nolog authentication (ident).
   Accept ANY TCP  nolog
      from "ANY_IP"
        to "ANY_IP" 113

13 #DEFAULT: Allow pings and ICMP traceroutes to GNAT Box.
   Accept ANY ICMP
```

```
        from "ANY_IP" 8
          to "ANY_IP" 8

  14 #DEFAULT: Allow UDP traceroutes to GNAT Box.
     Deny   ANY UDP  nolog genICMP
        from "ANY_IP"
          to "ANY_IP" 32767:65535

  15 #DEFAULT: Block/nolog stale WWW accesses.
     Deny   ANY TCP  nolog
        from "ANY_IP" 80
          to "ANY_IP" 1024:65535

  16 #DEFAULT: Block with alarm any other access to all interfaces.
     Deny   ANY ALL  alarm
        from "ANY_IP"
          to "ANY_IP"

TIME GROUPS
  None

PROTOCOLS
  Index  Name         Number
  -----  ----------  ------
  1      IGMP        2
  2      ESP         50
  3      AH          51

PREFERENCES
  DEFAULT LOGGING
      Log ALL packets rejected.
```

```
    ALARMS
        Send email for alarms when 2 seen within 60 seconds.
        Send a maximum of 500 alarms per email.
        Do not attempt to log host names using reverse DNS.

    GENERAL
                    Stealth mode: disabled
        Doorknob twists generate: alarm logMessage
         Address spoofs generate: alarm logMessage

    EMAIL SERVER
           disabled

    SNMP TRAPS
           disabled

    PAGER
           disabled

IP PASS THROUGH
  HOSTS/NETWORKS
    Index  Object or Address Range            Interface            Options
    -----  --------------------------------  ------------------   ---------

  FILTERS
     1 #DEFAULT: VPN, deny inbound (Test VPN).
       Accept "EXTERNAL" ALL
          from 192.168.11.0/255.255.255.0
            to "ANY_IP"

     2 #DEFAULT: VPN, allow outbound (Test VPN).
       Accept "PROTECTED" ALL
          from "ANY_IP"
```

```
            to 192.168.11.0/255.255.255.0

NAT
  ALIASES
    Index  Interface             IP Address      Netmask
    -----  -------------------  --------------- ---------------
    1      EXTERNAL             199.120.225.77  255.255.255.255

  INBOUND TUNNELS
    Index  Protocol  From IP Address  Port   To IP Address    Port   Options
    -----  --------  ---------------  -----  ---------------  -----  -----------
    1      TCP       0.0.0.0          80     10.10.1.65       80     filter
    2      TCP       199.120.225.76   21     10.10.1.65       21     filter

  STATIC ADDRESS MAPPINGS
    Index  From - Object or Address Range    To IP Address
    -----  --------------------------------  ---------------
    1      10.10.1.65       10.10.1.65       199.120.225.77

  TIMEOUTS
                       ICMP: 15 seconds
            TCP wait for ACK: 30 seconds
                        TCP: 600 seconds
    TCP keep alive enabled: yes
                        UDP: 600 seconds
            Wait after close: 20 seconds
```

Appendix F: Remote Logging

The GNAT Box system uses the Unix syslog facility for sending logging data to a remote host. The facility and priority values assigned to the log records are assigned from the Remote Logging configuration screen on any of the user interfaces. Log messages that don't fall into the user configurable categories (NAT, Filters, or WWW) are assigned to the "Daemon" facility and a priority of "Notice."

Log Message Format

```
Time_stamp system_name type_tag: Message
```

IP Address Message Format

Messages that include the IP Address/Port information use the following format to display this information.

```
[source_IP/sourc_port]->[destination_IP/destination_port]
```

Example: `[10.10.1.63/1224]->[198.3.98.160/80]`

In the case of a log message that includes NAT, an additional IP Address/Port set of data, documenting the translation is included.

```
[source_IP/sourc_port]->[NAT_IP/NAT_port]->[destination_IP/destination_port]
```

Example: `[192.168.1.19/1189]->[209.19.69.15/27322]->[209.19.69.2/80]`

Date/Timestamp Format

Standard syslog date/time format: **MMM dd hh:mm:ss**

MMM - three character month

dd - day

hh - hour

mm - minutes

ss - seconds
Example: Aug 20 19:21:28

Non-standard date/time format: **MM/DD/CCYY hh:mm:ss**
MM - 2 digit month
DD - 2 digit day
CC - 2 digit century
YY - 2 digit year
hh - hour
mm - minutes
ss - seconds
Example: 08/20/2000 19:21:52

Time: *hh:mm:ss, where hh is hours, mm is minutes and ss is seconds.*

Duration Format
Contains the duration of the connection.
Format: dur=*hh:mm:ss,* where hh is hours, mm is minutes and ss is seconds.
Example: `dur=00:00:48`

Packets Format
Contains the number of packets sent and received.
Format: pkts=*packets_sent:packets_received.*
Example: `pkts=25:23`

Bytes Format

Contains the number of bytes sent and received.

Format: bytes=*bytes_sent***:***bytes_received*

Example: `bytes=1412:29305`

Log Types

All log types begin with, *Date Timestamp firewall_IP*, the remainder of the log message depends on the log type.

WWW

This log record contains information about web (http) connections.

Format: **`WWW:`** `[IP info]` **`GET`** *`complete_url`*

Example:

`WWW: [10.10.1.58/1043]->[199.172.144.25/80] GET http://199.172.144.25/index.html`

NAT

Can be either an Open or Close connection record. The packet can be either:

1. Outbound from the PSN or Protected networks, in which case the message will include the intermediate network address translation IP/port.
2. Inbound on a tunnel.

Format: **`NAT:`** `Close tunnel TCP [IP info NAT Format] duration pkts bytes`

Example:

```
NAT: Close tunnel TCP [192.168.100.3/80]<-[19.120.25.3/80]<-[29.63.2.23/43720] dur=00:00:41 pkts=8:9
bytes=846:655.
```

FILTER

The filter type log records are generated when a packet matches a filter and the log option on the filter indicates a log record should be generated. Filter records include the Protocol, network interface, source/destination IP/port, any IP flags, and a message indicating the nature of the action.

Format: **`FILTER: Remote access filter blocks:`** *`Protocol NIC`* `[IP info]` *`length_of_packet`*

Note: *For TCP packets the TCP flags (in hex) are appended to the end of the messages in the form f=nnn*

Example:

```
FILTER: Remote access filter blocks: UDP de0 [192.168.100.2/53]->[192.168.100.1/12153] l=159.
```

alarm

These log messages are generated by the GNAT Box alarm mechanism. The messages can be administrative (a configuration change) or notification of an alarm action (email, pager or snmp trap generated).

Format: **alarm**: Message

Examples:

```
alarm: WARNING: email not enabled.
alarm: Alarms successfully queued.
alarm: Server ready. Email not enabled.
Aug 20 21:32:29 gbgw alarm: Send email for alarms when 10 seen within 120 seconds.
Aug 20 21:32:29 gbgw alarm: Send a maximum of 500 packets per email.
Aug 20 21:32:29 gbgw alarm: Do not attempt to log host names using reverse DNS.
Aug 20 21:33:53 gbgw alarm: WARNING: email not enabled.
```

console

Log messages with the console tag are generated when any changes are made to the GNAT Box configuration from the local console. The messages will detail the configuration changes.

Format: console: Message

Examples:

```
console: Successful administration login.
console: Disabling DNS.
console: Setting internal DNS server to 10.10.1.7.
console: Setting external DNS server to 199.120.225.2.
console: Primary DNS domain is gta.com.
console: Idle timeout reached, performing auto logoff.
```

WWW Admin

The WWWADMIN log tag is the header to any and all changes made through the web interface. This tag is attached to all connections, saves, errors, modifications, etc.

Format: WWWADMIN: Message

Examples:

```
WWWadmin: Remote administration access by host 10.10.1.63.
WWWadmin: Update of "IP Pass Through Filters" by 10.10.1.65.
WWWadmin: Update of "Outbound Filters" by 10.10.1.16
WWWadmin: Password verification failure from host 10.10.1.16
```

RMC

The Remote Management Console (RMC) log tag is the header to any and all changes made through the GBAdmin. This tag is attached to all connections, saves, errors, modifications, etc.

Format: RMC: Message

Examples:

```
RMC: Administration login successful from host 10.10.1.16
```

```
RMC: "EXTERNAL" interface (de2) address 199.120.225.80/255.255.255.128 removed.
RMC: "PROTECTED" interface (fxp0) address 10.10.1.80/255.255.255.0 removed.
RMC: "pROTECTED 2" interface (de0) address 10.10.10.80/255.255.255.0 removed.
RMC: "PSN" interface (de1) address 192.168.200.80/255.255.255.0 removed.
RMC: User information updated by 10.10.1.16
RMC: Close connection from 10.10.1.16
```

DHCPD

The DHCP Server will send all actions to the log file. Any client or server request, denies, or renews will be delta with through one of the the DHCP action types as described below.

Format: **`DHCPD:`** `action_type IP_Address MAC_Address Interface`

Action_types:

DHCPINFORM

DHCPRELEASE - A DHCP client has released the connection or has exceeded the specified lease duration.

DHCPDISCOVER - The initial Request from a client that it needs information from the DHCP server.

This is only seen if a host is not trying to renew a previous IP address.

DHCPOFFER - The DHCP server offers an IP after the initial client request has been made.

DHCPREQUEST - A client has requested a re-connection to the DHCP server.

DHCPACK - The server has accepted the DHCP request and has assigned a DHCP lease to the client.

DHCPNAK - The server has denied the client a DHCP lease.

Examples

```
dhcpd: DHCPINFORM from 10.10.10.3
dhcpd: DHCPRELEASE of 10.10.10.3 from 00:c0:f0:14:4e:01 via de1 (found)
dhcpd: DHCPDISCOVER from 00:c0:f0:14:4e:01 via de1
dhcpd: DHCPOFFER on 10.10.10.3 to 00:c0:f0:14:4e:01 via de1
dhcpd: DHCPREQUEST for 10.10.10.3 from 00:c0:f0:14:4e:01 via de1
dhcpd: DHCPACK on 10.10.10.3 to 00:c0:f0:14:4e:01 via de1
dhcpd: DHCPNAK on 10.10.1.239 to 00:c0:f0:14:4e:01 via de1
```

Proxy:

The Traditional or Transparent Proxy used with content filtering will log all web access. It will send basic log messages, accepts, and blocking (with Websense or CyberNOT enabled) to the log file and identify all authorized and unauthorized access.

Formats:

Message Type – proxy: <Message>

Accept/Block Type – proxy: [Accept/Block] GET [FROM_IP/PORT] -> [TO_IP/PORT] WEB_SITE

Examples:

```
proxy: Connecting to WebSENSE server "10.10.1.65/15868".
proxy: Disabling blocking of ActiveX Objects
proxy: Block GET [10.10.1.32/1835]->[206.251.29.10/80] http://www.xxx.com/
proxy: Accept GET [10.10.1.32/1836]->[207.46.176.121/80] http://www.gnatbox.com
```