

H₂A

High Availability

Feature Guide

a *GNAT Box*
System Software Option



Global
Technology
Associates, Inc.

Copyright

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

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

Disclaimer

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

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

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

Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated.
H₂A High Availability is a trademark of Global Technology Associates, Incorporated.
RoBoX is a trademark of Global Technology Associates, Incorporated.
All other products are trademarks of their respective companies.

Version Information

GNAT Box System Software version 3.3.2

November 2002

Technical Support

GTA's direct customers in the USA should email GTA via the contact information listed below. Other customers should contact their local GTA authorized reseller.

Contact Information

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

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

Document Information

GNAT Box H₂A High Availability Feature Guide
with GNAT Box System Software Version 3.3.2

December 2002

Contents

1 INTRODUCTION	1
About H₂A	1
Inside GTA's High Availability Solution	1
Features	2
Requirements	2
Registration & Activation	2
Feature Activation Codes	2
Copy Protection	3
Installation Support	3
Documentation	4
Documentation Conventions	4
Additional Documentation	4
2 HA CONCEPTS	7
High Availability Modes	7
Init Mode	7
Standby (Slave) Mode	7
Master Mode	8
General Terms	8
Beacon	8
Broadcast Port and Multi-cast Address	8
HA Network Interface	9
Priority	9
VRID	9
Virtual Firewall	9
Virtual IP Addresses	10
Physical (Configuration) IP Addresses	10
Virtual (Master) MAC Address	10
3 INSTALLATION & CONFIGURATION	11
Quickstart	11
Overview	12
H ₂ A System Location	12
Set Up H ₂ A Firewalls	13
New System Examples	13
GB-1000 A (Highest Priority)	13
GB-1000 B (Lower Priority)	14
Set Up GB-1000 A	14
Set Up GB-1000 B	16
Configure GB-1000 A	17
Remote Access Filters	17
Local Gateway in VPN Objects	18

Test Firewall Configuration	18
Network Configuration	18
Configure GB-1000 B	19
Update the Standby/Slave	19
Test Fail-over	20
4 TROUBLESHOOTING	21
Q&A	21
APPENDIX	23
H₂A on Two Subnets	23
Configure the GB-1000 A	23
HA Configuration	24
Beacon IP Addresses	24
Static Address Mapping	25
Two Subnets Examples	25
GB-1000 A (Highest Priority)	25
GB-1000 B (Lower Priority)	26
Upgrade an Existing GB-1000	26
Merge Configuration	26
Edit Configuration	27
Configure the Existing GB-1000	28
Upgrade Examples	29
New GB-1000 (Highest Priority) Example	29
Existing GB-1000 (Lower Priority)	29
Remote Access Filters	30
Log Messages	30
Example of State Change Email Notifications	35
Entering INIT Mode	35
Entering Slave Mode	35
Entering Master Mode	35
INDEX	37

1 Introduction

About H₂A

H₂A, Global Technology Associates, Inc.'s High Availability option, is a cost-effective and resilient fail-over system for secure 24/7 network access. Two or more GB-1000 Firewall Appliances together create a system that acts as a single firewall. The H₂A High Availability option for GB-1000's allows you to maintain network security and access. With H₂A's fast, transparent fail-over, you're assured that firewall downtime doesn't equal network downtime.

The feature is easy to use. Set up two or more systems anywhere on the same network, enter the activation codes, and begin customizing the H₂A option. That's it: no special cabling and no extra software. With GTA's fast configuration, your H₂A solution can be operational in minutes.

An H₂A system is transparent to end users, requiring no obvious changes to the existing network configuration. It appears to the network as one firewall, regardless of which physical system is functioning as the virtual firewall.

Inside GTA's High Availability Solution

Once your H₂A option has been activated and configured on your firewalls, the H₂A system works transparently to ensure constant firewall coverage and seamless maintenance of your GB-1000 configurations.

To determine which GB-1000 functions as the virtual firewall, each firewall in the H₂A chain is assigned a priority number. The GB-1000 with the highest priority will function as the virtual firewall (in master mode), while the others function as standby firewalls (in slave mode).

Each firewall chain listens to network activity, continuously scanning for broadcasts of HA status information. The firewall in master mode broadcasts its identity (the virtual firewall IP address) and priority number. If master broadcasts stop, a firewall in slave mode takes over as the virtual firewall until a GB-1000 in the chain with a higher priority becomes operational.

Note

H₂A does not exchange state information, so active connections are lost when a switch occurs, affecting long-lived connections such as telnet.

Features

- 24/7 network security and access.
- Easy installation—no special cabling.
- Simple configuration, with no additional software.
- Easy management with GNAT Box System Software user interfaces.
- Cost-effective fail-over solution.

Requirements

The H₂A High Availability solution requires:

- Two or more GB-1000's with identical hardware and software configurations.
- GNAT Box System Software version 3.2 or higher.
- One static IP address on the External Network.
- One static IP address for the Protected Network.

Registration & Activation

If you have not yet registered your firewall products, go to www.gta.com, click on Support, and then click on the GTA Support Center link. This takes you to the login screen. Click New Account, enter your profile information, then choose a user ID and password. Click Add to save the form.

In the login screen, enter your user ID and password. In the Make a Selection screen, click Support Center, then Product Registration. Enter your product serial numbers and firewall activation (unlock) codes, then click Submit.

Feature Activation Codes

Optional features on GTA Firewalls require activation codes. A separate H₂A activation code is entered on the Features screen of each system in the H₂A chain. When an activation code is entered correctly, the description column will indicate “GB-1000 3.x–High Availability.” Enter both feature activation codes before configuring either system. Activation codes are system specific, so make sure to enter the appropriate activation code for each system.

Note

If the feature code does not appear, please contact GTA support, putting your serial number and Support Center User ID in the message subject.

The feature activation code can be found in Registered Products by selecting the serial number of your GTA Firewall on GTA Support. Copy the feature activation code and enter it in the Features screen in the next available row. Click Save. The appropriate license will be displayed.

Note

Enter the H₂A feature activation code for each firewall in the H₂A chain before configuring any of the firewalls for high availability.

Copy Protection

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

Installation Support

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

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

Installation support covers only the aspects of configuration related to installation and activation of a H₂A High Availability within the first 30 days of purchase of the feature. This support covers setting up the GNAT Box H₂A High Availability in its default setting.

If you need further assistance, contact the GTA Sales staff to purchase a support contract. Contracts range from support by the incident to full coverage for a year. Other avenues for assistance are available through the GNAT Box Mailing List and Forum, found at www.gta.com, or through an authorized GTA Channel Partner.

Documentation

This Feature Guide is designed to be used in conjunction with the **GB-1000 PRODUCT GUIDE** and the **GNAT BOX SYSTEM SOFTWARE USER’S GUIDE**. This guide lists requirements, and explains how to activate, configure and operate an H₂A system.

Documentation Conventions

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

Documentation Conventions

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

Notes are indicated by an indented, italicized headline.

The note body copy is further indented.

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

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

Additional Documentation

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

Documentation Map

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

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

2 HA Concepts

The following concepts are specific to high availability and to the GNAT Box System Software H₂A feature.

High Availability Modes

When a GTA Firewall has the H₂A feature enabled and configured, it will operate in one of three modes: master, slave or init. Each system will shift modes depending on its operational status and priority number, and the status and priority number of other systems in the H₂A chain. HA modes are determined by the individual H₂A firewall, not from any external source. All mode changes are logged.

Init Mode

Each time an HA-enabled system starts up, it assumes that its network interfaces are not functioning properly, and that it has no connections to local networks. It enters the init, or diagnostic, mode.

In init mode, the system is temporarily out of the H₂A chain. It tests its network interfaces by directing packets from each HA network interface to the beacons on its beacon list. If valid responses are received from at least one beacon assigned to each HA network interface, the H₂A firewall will switch to slave or master mode, and re-enter the H₂A chain as a standby or master unit.

If a firewall in the H₂A chain loses connectivity on any of its network interfaces, it will switch to init mode and continuously test its connections. When it regains connectivity, it will re-enter the H₂A chain as a standby or master unit.

Standby (Slave) Mode

In standby (slave) mode, the H₂A firewall listens (via UDP, port 77) for HA broadcast traffic from other members of the H₂A chain. The HA broadcast traffic will include information that indicates the priority number of the firewall functioning in master mode. The standby systems will compare the priority number extracted from the HA broadcasts to its own priority; if it determines that the priority number of the current master unit is lower than its own, it will switch to master mode.

Master Mode

Once in master mode, a system will change the physical MAC addresses of its HA network interfaces to the HA master MAC address; send out HA broadcasts (UDP/77) messages which include the system's priority in the H₂A chain, and continue to listen for HA broadcasts.

However, in the master mode, the system is listening for HA broadcasts from a GB-1000 in the H₂A chain with a higher priority. If it finds one that has a higher priority number, it will drop into slave mode and become a standby unit. When a system switches from master to any other mode, its MAC addresses revert to original values.

General Terms

Beacon

A beacon is the IP address of a host, used as a target to test network connectivity. A beacon IP address must be statically assigned to a network device able to respond to pings, and on the same logical subnet as the interface's configuration (physical) IP address. Good choices for beacons are separate systems that normally always run, such as routers, web servers, DNS servers or mail servers.

For each beacon on each interface, the H₂A firewall will send two ping packets a second. If the firewall fails to receive a reply five times in a row, the host will be marked as down. If all the hosts (beacons) associated with an interface fail to respond, then the H₂A assumes there is a problem with the network interface. The firewall will change its mode to init, send a log message, and continue to test the network interfaces.

Note

A firewall in stealth mode cannot be used as a beacon, because the External Network interface will not respond to pings. GTA Firewalls are in stealth mode by default, in compliance with ICSA (International Computer Security Association) firewall standards. If you wish to use a GTA Firewall as a beacon, deselect the Stealth mode field in Filters -> Preferences on the firewall which you will use as a beacon.

Broadcast Port and Multi-cast Address

High Availability broadcasts are transmitted by default as broadcast packets from on broadcast port UDP 77 at the multi-cast address 224.0.0.18.

HA Network Interface

An HA network interface is any network interface on a GB-1000 system that has been configured for High Availability. When a network interface is configured for HA, it will be included in the network connectivity testing performed by the H₂A feature. The failure of any HA network interface (i.e., no response from the specified beacons) will cause the system to change from the current HA mode to init mode.

Priority

The priority number is a number between 1 and 255 that ranks the systems in an H₂A chain. The system with the highest priority number and confirmed communications with its beacons will be the master unit and process network traffic as the virtual firewall.

If the priority number is the same for two or more systems in an H₂A chain, the unit with the highest configuration IP address will become the master unit. (E.g., in an HA pair with the physical addresses 192.168.71.253/24 and 192.168.71.252/24, the unit with .253 as the last octet will be the master unit.) The selected unit will be the master any time it is online and operational, unless priority numbers or physical IP addresses change.

Note

GT A recommends selecting a unique priority number for each H₂A unit.

VRID

The VRID (virtual router ID) defines an H₂A chain. All members of an H₂A chain should be assigned the same VRID. Valid VRID values are 1-15.

Virtual Firewall

The virtual firewall appears as a single system to network users, but actually consists of all physical GB-1000 systems in the H₂A chain. The virtual firewall has virtual IP addresses and IP aliases that represent the H₂A chain, and are referenced by hosts in order to send data through or to the firewall.

End users will see and use only the virtual firewall and the virtual firewall IP addresses. This allows the end user to utilize the virtual firewall, regardless of which physical firewall in the H₂A chain is operating as the master unit.

Virtual IP Addresses

A virtual IP address is an address assigned to a network interface on the virtual firewall and configured on the HA configuration screen; or, an IP alias assigned to the virtual firewall. Virtual IP addresses and IP aliases can be of any interface type – Protected, External or PSN. They belong to the virtual firewall: keep in mind the difference between a physical (configuration) IP addresses of a unit and the virtual IP addresses assigned to the H₂A chain.

Physical (Configuration) IP Addresses

A physical IP Address is the IP address of a network interface on a GB-1000; it is the IP address that appears in Network Information. In an HA configuration, physical IP addresses are used only for configuration; they should be accessed only by the administrator.

Virtual (Master) MAC Address

In an H₂A chain, the master unit acting as the virtual firewall uses a special MAC address, (instead of the MAC address assigned to its network interface), to differentiate it further from the physical GB-1000 unit.

IANA (Internet Assigned Numbers Authority) has assigned a range of numbers for high availability system MAC addresses: 00:00:5E:00:01:xx. In an H₂A chain, the master unit MAC address will be 00:00:5E:00:01:xx, in which “xx” is a unique number derived from the VRID assigned to the system and the interface number.

Note

The special MAC address assigned to the virtual firewall allows systems to recognize and further distinguish between the firewalls. The virtual IP address does not change.

3 Installation & Configuration

Quickstart

These are the basic steps for replacing an old firewall with an H₂A system.

1. Set up an isolated network for configuration of the new firewalls.
2. Connect the first GB-1000 (GB-1000 A).
 - a. Configure Preferences and Network Information with your configuration IP addresses, then enter the H₂A feature activation code in Features.
 - b. Configure High Availability using the virtual IP addresses you have selected, usually the IP addresses from your existing firewall system.
 - c. Assign this firewall the priority number for the master mode unit.
3. Connect the second GB-1000 (GB-1000 B).
 - a. Configure Preferences, Network Information and H₂A feature codes.
 - b. Configure High Availability using the data from the first system.
 - c. Assign this firewall the priority number for the slave (standby) unit.
4. Complete the configuration of GB-1000 A.
 - a. Using configuration data from your existing firewall, configure GB-1000 A according to your company policy.
 - b. Create and enable high availability Remote Access Filters.
 - c. Edit Local Gateway in VPN Objects to reference HA address objects.
5. Test the new configuration.
 - a. With power off, connect GB-1000 A to the network.
 - b. Turn off the power to your old firewall.
 - c. Power on and test GB-1000 A as you would any GTA Firewall.
6. Once you have completed testing the GB-1000 A to your satisfaction, connect your designated standby firewall (GB-1000 B) into your network.
7. Use the Update Slave function to transfer configuration data from the master mode unit to the standby unit.
8. Once you have completed testing the GB-1000 B to your satisfaction, test the system fail-over by powering off GB-1000 A, then powering it back on.

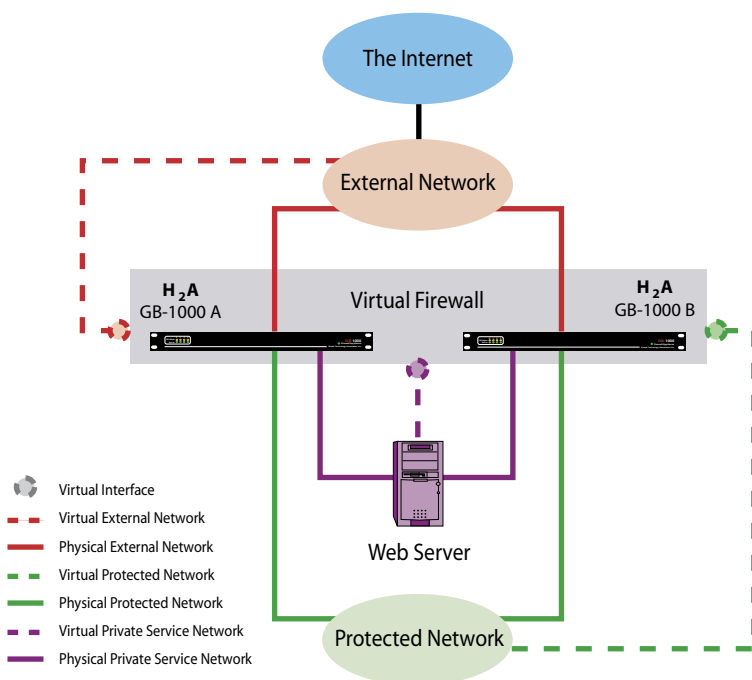
If your configuration passes this final test, your H₂A system is up and running.

Overview

This following sections illustrate a new H₂A system setup, using at least two public (registered) IP addresses. See the Appendix for examples of other configurations: a system with only one public IP address, and an H₂A upgrade of a GB-1000. Nearly all H₂A configuration is performed from a single GB-1000 that updates the other firewalls in the H₂A chain. Units may be configured in any order when setting up a new system; however, GTA recommends configuring the master unit first, especially when upgrading, in order for the administrator to test and verify the new configuration before transferring it to the standby units.

H₂A System Location

The firewall in an H₂A chain must be on the same network, but need not be in the same physical location. Plan the physical layout of your chain, but do not begin to integrate them into your network until the the new configuration has been tested. The diagram below shows an H₂A High Availability network pair.



H₂A High Availability Network Pair Diagram

Set Up H₂A Firewalls

Set up an isolated network on which to configure the GB-1000's. Choose the physical (configuration) IP addresses to configure the Network Information sections for each firewall. (Your current interface IP addresses will become the virtual firewall IP addresses on the new system.)

Caution

Create the HA system in an isolated environment; to avoid IP address conflicts, do not connect the new GB-1000 to the network until the entire system is ready to take over as the virtual firewall.

Make a copy of your current firewall configuration for reference. If you are replacing a GTA Firewall, you may be able to merge the current configuration onto your new firewalls. See the upgrade to H₂A instructions in the Appendix for more information on merging a GTA Firewall configuration.

Use the **GB-1000 PRODUCT GUIDE** as a reference for initial setup of a GB-1000, and use the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** for more information on GTA Firewall configuration options.

New System Examples

These IP addresses and other data are used as examples in the following sections. Enter the appropriate data for your network. GB-1000 A is selected as the highest priority firewall.

Router	199.120.225.1
Mail Server	192.168.71.110
Workstation	192.168.71.25

GB-1000 A (Highest Priority)

External IP Address	199.120.225.80/24
Protected IP Address	192.168.71.80/24

HA Configuration

VRID	10
Priority	20
HA-External	
Virtual IP Address	199.120.225.254
Beacons	199.120.225.253, 199.120.225.252, 199.120.225.251
HA-Protected	
Virtual IP Address	192.168.71.254
Beacons	192.168.71.253, 192.168.71.252, 192.168.71.251

GB-1000 B (Lower Priority)

External IP Address	199.120.225.79/24
Protected IP Address	192.168.71.79/24

HA Configuration

VRID	10
Priority	10
HA-External	
Virtual IP Address	199.120.225.254
Beacons	199.120.225.253, 199.120.225.252, 199.120.225.251
HA-Protected	
Virtual IP Address	192.168.71.254
Beacons	192.168.71.253, 192.168.71.252, 192.168.71.251

Set Up GB-1000 A

Connect the first GB-1000 (GB-1000 A). Choose any one of the identical firewalls. Using the **GB-1000 PRODUCT GUIDE**, set up the unit and configure Preferences and Network Information using your configuration IP addresses for this firewall, then enter the H₂A feature activation code in Feature Codes.

Select the Services -> High Availability menu item in GBAdmin or the Web to display the HA configuration screen. If you do not see the High Availability item, make sure you have entered the H₂A feature code.

Configure High Availability using the virtual IP addresses you have selected, usually the IP addresses from your existing firewall system. Assign this firewall the priority number for the master mode unit. The HA firewall with the highest priority number, as well as confirmed communications with beacons, will operate in master mode unless it loses connectivity.

Note

Not all network interfaces must be configured as HA interfaces. If you do not wish to use an interface for HA, leave the VIRTUAL IP ADDRESS field and the BEACON fields blank. You can deselect an HA interface by deleting the data from the BEACON fields.

GNAT-Box High Availability				
Enable:	<input checked="" type="checkbox"/>			
Status:	Feature disabled			
VRID:	<input type="text" value="14"/>			
Priority:	<input type="text" value="2"/>			
Email notification:	<input checked="" type="checkbox"/>			
Name	Interface	Virtual IP address	Beacon IP addresses	
HA-EXTERNAL	EXTERNAL	<input type="text" value="199.120.225.254"/>	<input type="text" value="199.120.225.253"/>	<input type="text" value="199.120.225.252"/>
HA-PROTECTED	PROTECTED	<input type="text" value="192.168.71.254"/>	<input type="text" value="192.168.71.253"/>	<input type="text" value="192.168.71.252"/>
<input type="button" value="Update Slave"/> <input type="button" value="Default"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>				

HA configuration – GB-1000 A

High Availability Fields

Enable	Enable the H ₂ A feature.
Status	When using the high availability option, this field displays the firewall's current mode: init (diagnostic), slave (standby) or master. This field is not editable.
VRID*	Virtual Router ID. Enter a value between 1 and 15. The VRID is used to identify the H ₂ A chain, so all firewalls in each H ₂ A chain must have the same VRID. If you are upgrading an existing H ₂ A configuration, make sure that your VRID number is between 1 and 15.
Priority*	Enter a priority number between 1 and 255. The firewall with the highest priority number will be the master unit when operational.
Email Notification	Select to have status change notification sent to the email address entered in the Preferences section. If enabled, DNS should be configured (Basic Configuration -> DNS). Both the email address and a configured DNS are required for the email notification feature.
Name	<p>By default, the name will be HA-<Interface Name>, where <Interface Name> is the logical name assigned to an interface in Network Information. To change the name assigned to the HA IP Address, type over the existing name.</p> <p>Note: If you change the HA name, you must change references to it elsewhere in the configuration, e.g. in objects and filters.</p>
Interface*	Select the interface object that represents this interface. This object corresponds to the logical name assigned to the physical network interface. If you change the logical name, you will need to re-select the Interface Object from the dropdown list. Interfaces may be used only once in H ₂ A. In GBAdmin, an interface that has already been selected will not appear in successive dropdown lists.

Virtual IP address	Enter the virtual IP address that will be used for a given network interface. If the IP address is in the same network as the interface to which it is assigned, enter a single IP address, but if it is in a logically different network, use a subnet mask. (E.g.: If the interface is in the 10.10.10.0/24 network, and the virtual IP address is in the 199.120.225.0/24 network, use 199.120.225.1/24 to identify the virtual IP address.)
Beacon	Enter up to three beacon IP addresses. Use systems with very little downtime, such as routers, mail servers and web servers. Do not make other firewalls in the chain your only beacons; GTA recommends using at least two beacon IP addresses.

- **H₂A systems cannot use dynamically assigned interfaces.**

Note

All GTA Firewalls, version 3.3 and higher, are in stealth mode by default. A firewall in stealth mode cannot serve as a beacon, because it will not respond to pings. To use a GTA Firewall as a beacon, deselect the STEALTH MODE field in Filters -> Preferences.

Set Up GB-1000 B

Connect the second GB-1000 (GB-1000 B). Set up the second unit and configure Preferences and Network Information using your configuration IP addresses for this firewall, then enter the H₂A activation code in Features.

Select the Services -> High Availability menu item in GBAdmin or the Web to display the HA configuration screen. If you do not see the High Availability item, make sure you have entered the H₂A feature code.

Configure High Availability using the data from the first system, except the priority number. Beacon IP addresses for the standby unit can be the same as the master unit. Use the High Availability fields table in the previous section for more information.

Assign this firewall the priority number for the standby (slave mode) unit. H₂A firewalls with lower priority numbers, as well as confirmed communications with beacons, will operate in slave mode unless the higher priority firewall loses connectivity.

Caution

If you do not set the priority number for the systems, the two firewalls will select the master automatically.

Configure GB-1000 A

Complete the configuration of GB-1000 A using additional configuration data from your existing firewall. In addition, create the appropriate Remote Access Filters and VPN Objects for the high availability configuration. The configuration information from GB-1000 A can be transmitted to the other units in the H₂A chain after you have tested your new configuration.

Remote Access Filters

In order for a system to operate properly in a H₂A chain, two Remote Access Filters must be in place. These filters are generated (but not enabled) when the H₂A option is enabled and the Default option is used in Remote Access Filters. These filters can also be created manually.

Caution

If you default filters and save the configuration, your custom filters will be lost; the system will create filters according to the system configuration.

1. This filter accepts UDP broadcasts on port 77 to the multi-cast address of 224.0.0.18.

Description	Allow High Availability protocol.
Type	Accept
Interface	ANY
Protocol	UDP
Source	ANY_IP
Source Port	Blank
Destination	224.0.0.18/32
Destination Port	77

2. This filter accepts IGMP protocol needed by High Availability at the multi-cast address of 224.0.0.18.

Description	Accept IGMP Protocol
Type	Accept
Interface	ANY
Protocol	IGMP (2)
Source	ANY_IP
Source Port	Blank
Destination	224.0.0.18/32
Destination Port	Blank

Note

Order is very important. If you create these filters manually, position them before any deny filters.

Local Gateway in VPN Objects

After enabling the H₂A option and before setting up VPNs, the LOCAL GATEWAY fields in VPN Objects must be edited to refer to the new HA interface (address) objects.

Test Firewall Configuration

Test the new configuration. With power off, connect GB-1000 A to the network. Turn off the power to your old firewall. Power on and test the GB-1000 A as you would any firewall.

To prevent IP addresses conflicts, do not power on the old firewall with the new system in place.

Network Configuration

Following the instructions in this chapter, the transition to the H₂A system should be transparent to end users, though some users may see a brief disconnect for long-lived connections, and VPN users will need to re-authenticate.

If you encounter problems, check that the default route/gateway of hosts on the Protected Network(s) is the virtual IP address assigned to the Protected Network interface; other services provided by the firewall, such as DNS, are accessible from the virtual IP address assigned to each network interface; and access from the External Network (usually the Internet) to inbound tunnels uses the virtual IP addresses assigned to the External Network interface.

For more information, see Chapter 4 – Troubleshooting.

Configure GB-1000 B

Once the GB-1000 A has been tested to your satisfaction, connect your designated standby firewall (GB-1000 B) into the network and turn on power.

Update the Standby/Slave

To transmit all the configuration data you have entered into GB-1000 A to GB-1000 B, use the Update Slave function on the GB-1000 A.

The Update Slave (Standby) function updates configuration information on units in the H₂A chain. The administrator must have the user ID and password of the standby firewall. The standby unit must have an administrative user account with both “RMC” and “Admin” permissions enabled. (This is part of initial configuration of the GB-1000.)

The Update Slave function does not change:

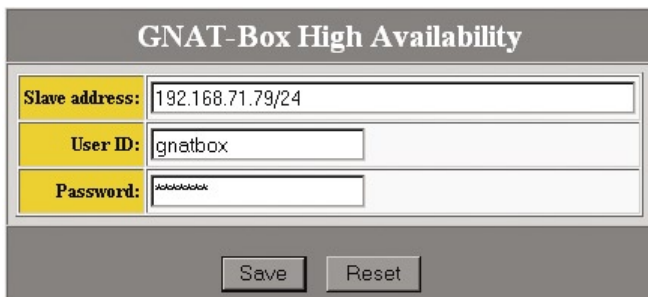
- Data on the Network Information screen.
- Data in the Preferences section.
- Feature codes.
- Enterprise Server fields.
- HA information (assuming HA has already been configured).

Log on to GB-1000 A and open the High Availability screen. Click the Update Slave button to transfer configuration data from the master mode unit to the standby unit (GB-1000 B).

Note

The Update Slave function can be used to update any firewall in the H₂A chain. However, for consistency, GTA recommends updating the lower priority firewalls from the highest priority firewall.

In the **SLAVE ADDRESS** field, enter the Configuration IP address of the unit to be updated. Enter an administrative user ID for the slave system in the **USER ID** field. This user ID must have both RMC and Admin options enabled. Enter the password for the User ID in the **PASSWORD** field and press **Save** to upload and save the configuration information to the unit, which now has the latest configuration data.



The image shows a web-based configuration form titled "GNAT-Box High Availability". It contains three input fields: "Slave address:" with the value "192.168.71.79/24", "User ID:" with the value "gnatbox", and "Password:" with a masked value "*****". Below these fields are two buttons: "Save" and "Reset".

Update Standby/Slave

If you have more than one standby unit, repeat the steps in this section and the next for each additional firewall.

Test Fail-over

Once you have successfully tested GB-1000 B, test the system fail-over by powering off GB-1000 A, then powering it back on. Using the same tests you ran for GB-1000 A, test the connectivity of GB-1000 B. Repeat the steps in this section for each additional firewall.

If the system performs satisfactorily on this final test, your H₂A system is up and running.

4 Troubleshooting

Q&A

- 1. I've just connected my H₂A system. Why I can't see the other unit (or units) in my H₂A chain?**
 - Check that all the cables are connected properly and to the correct interfaces.
 - Verify that all the interfaces in Network Information and High Availability have been properly identified with both physical and virtual IP addresses, and that all names are valid.
 - Verify that all units in your chain have identical VRID numbers. This number identifies the members of the chain to one another.
- 2. The firewall I thought was going to be in master mode is in slave mode. Why?**
 - Check that the priority number in the firewall you have designated the master is higher than that of the other firewalls. Priority numbers range from 1-255, with 255 being the highest priority number. GTA recommends that all firewalls in a chain have unique priority numbers.
 - The firewall could be in init mode, either because its interfaces are down, or because it cannot ping its beacons.
- 3. I can't ping the other firewalls in my H₂A chain; when one unit tries to uses the other as a beacon, it can't be reached.**
 - It could be that one or all of your GTA Firewalls are set in stealth mode. In accordance with ICSA standards, GTA Firewalls are in stealth mode by default. If you would like to turn off stealth mode, open Filters -> Preferences and uncheck (disable) stealth mode on all firewalls in the your high availability system.

4. Why are none of the GTA Firewalls in the chain in master mode? All are in standby (slave) mode.

- If you have more than one H₂A system (in other words, you have two or more separate H₂A chains), make sure that the VRID numbers for each chain are unique: e.g., H₂A chain 1 = VRID 5; H₂A chain 2 = VRID 10. This allows high availability systems to distinguish between firewalls in their own chain, and those in a separate chain.

5. User connections have the IP address of the unregistered network as their source. Why?

- Check your physical interface IP addresses. If you use private, unregistered (RFC 1918) IP addresses on your physical interfaces, the DEFAULT GATEWAY field in Network Information (or the fields in Gateway Selector, if it is being used) must be set to an IP address on your virtual network, otherwise the network cannot identify your interface.

Appendix

H₂A on Two Subnets

An alternative setup for H₂A uses only one public (registered) IP address that is routable on the Internet. If you have a limited number of public IP addresses, or you want to increase security by limiting access, use this example with the instructions in Chapter 3 to configure Network Information and High Availability.

Configure the GB-1000 A

H₂A can be configured to use different networks for the configuration IP address and HA IP addresses. Using different networks, the administrator can configure the firewall to use an RFC 1918 (private) IP address on the External Network interface, so that only H₂A will use the public IP address.

The default gateway assigned to the firewall must be the same as the router's public IP address, 199.120.225.253. The 10.0.0.253 router IP address is used primarily as a firewall beacon.

Note

If Protected Network user IP addresses are NAT'ed to the External Network IP address and users are unable access to the Internet, check that the default gateway is using the router's public IP address.

GNAT-Box Network Information					
Logical Interfaces					
Logical Name	Type	IP Address	NIC	DHCP	Gateway
EXTERNAL	External	10.0.0.254/24	fxp1	<input type="checkbox"/>	<input type="checkbox"/>
PROTECTED	Protected	192.168.71.254/24	fxp0	<input type="checkbox"/>	<input type="checkbox"/>

Network Information using private (RFC 1918) IP addresses

Host name:	GB-1000
Default gateway:	199.120.225.253

Public IP address for Default Gateway (registered IP address of the router)

HA Configuration

If the virtual IP address is on a different network than its associated physical IP address, use a subnet mask with the virtual IP address.

In the illustration below, the HA-EXTERNAL virtual IP address (199.120.225.254/24) is entered with a subnet mask because the network is different from the physical External Network (10.0.0.254/24). The HA-PROTECTED virtual IP address (192.168.71.253) does not require a mask because it is on the same network as the Protected Network interface (192.168.71.254/24).

Beacon IP Addresses

Beacon IP addresses for the HA-EXTERNAL interface should be from the same network (10.0.0.0/24) as the physical External Network IP address and the network router. Beacon IP addresses for the HA-PROTECTED interface may be from the same network as the virtual IP address.

GNAT-Box High Availability				
Enable:	<input checked="" type="checkbox"/>			
Status:	Master			
VRID:	14			
Priority:	20			
Email notification:	<input checked="" type="checkbox"/>			
Name	Interface	Virtual IP address	Beacon IP addresses	
HA-EXTERNAL	EXTERNAL	199.120.225.254/24	10.0.0.253	<input type="checkbox"/>
HA-PROTECTED	PROTECTED	192.168.71.253	192.168.71.1	<input type="checkbox"/>
	PSN			<input type="checkbox"/>
<div> <input type="button" value="Update Slave"/> <input type="button" value="Default"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>				

HA Configuration for limited IP addresses

Static Address Mapping

Map all services on the physical External Network interface to the HA-EXTERNAL address object or an IP alias on the External Network interface to ensure that services which originate from the firewall are NAT'ed correctly.

Caution

If static mapping is not done, services will be NAT'ed as the External Network IP address instead of the virtual IP address.

GNAT-Box Static Address Mappings			
	From		To
Index	Object	IP Address	Interface
1	EXTERNAL		HA-EXTERNAL
2	???		???

Static Address Mapping

Continue the configuration and testing of your high availability configuration using the instructions in Chapter 3 and the examples in this section.

Two Subnets Examples

Router IP Address 199.120.225.253
 10.0.0.253

GB-1000 A (Highest Priority)

External IP Address 10.0.0.254/24
 Protected IP Address 192.168.71.254/24
 Default Gateway 199.120.225.253

VRID 14
 Priority 20

HA-External

Virtual IP Address 199.120.225.254/24
 Beacons 10.0.0.253

HA-Protected

Virtual IP Address 192.168.71.253
 Beacons 192.168.71.1, 192.168.71.2, 192.168.71.3

GB-1000 B (Lower Priority)

External IP Address	10.0.0.252/24
Protected IP Address	192.168.71.252/24
Default Gateway	10.0.0.253
VRID	14
Priority	10
HA-External	
Virtual IP Address	199.120.225.254/24
Beacons	199.120.225.253
HA-Protected	
Virtual IP Address	192.168.71.253
Beacons	192.168.71.1, 192.168.71.2, 192.168.71.3

Upgrade an Existing GB-1000

This section illustrates how to add a second firewall to your network and upgrade your existing GB-1000 to high availability. These instructions can also be used when upgrading two existing GB-1000's to an HA configuration.

To set up your H₂A system, leave the existing GB-1000 in place and configure the new GB-1000.

Set up the new GB-1000 in its factory default configuration using the instructions in the **GB-1000 PRODUCT GUIDE**, then merge your existing configuration onto the new firewall.

Merge Configuration

Download the configuration from your current firewall so it can be accessed by the new GB-1000. Merge this configuration into the GB-1000 with GBAdmin or the Web interface, using the instructions below.

Merge a Configuration Using GBAdmin

1. On the new GB-1000, open GBAdmin and go to File -> Merge. A warning dialog will appear saying, "Operation will overwrite current settings; do you wish to continue?" Select Yes to overwrite the factory default settings on the GB-1000.
2. In the Merge dialog box select: SOURCE: File and INFORMATION TO MERGE: Configuration only. Click Browse, then find and select your saved configuration (e.g., GB332.GBcfg).
3. Save the configuration by clicking the Save All Sections icon.

Upload a Configuration Using the Web Interface

1. Open a web browser connection to your new GB-1000 and go to Administration -> Upload Configuration.
2. In the Upload Configuration dialog box, click Browse, then find and select your saved configuration (e.g., GB332.GBcfg).
3. Click Submit to upload the configuration to the new GB-1000.

Caution

Using the Web interface, you must re-enter the serial number, registration and HA feature code, as this will be overwritten during the merge.

GNAT-Box Network Information					
Logical Interfaces					
Logical Name	Type	IP Address	NIC	DHCP	Gateway
EXTERNAL	External	199.120.225.254/24	fxp1	<input type="checkbox"/>	<input type="checkbox"/>
PROTECTED	Protected	192.168.71.254/24	fxp0	<input type="checkbox"/>	<input type="checkbox"/>
PSN	PSN	192.168.250.254/24	fxp2	<input type="checkbox"/>	<input type="checkbox"/>

Network Information for the existing firewall

Edit Configuration

After merging the configuration, re-connect to the new GB-1000 using the merged configuration's Protected Network IP address.

Using the instructions in Chapter 3 of this guide, configure the Network Information, Preferences and High Availability sections. Make this firewall your designated master unit by giving it the higher priority number.

Verify that Remote Access Filters which previously referenced the EXTERNAL interface object now use the HA-EXTERNAL interface object; that tunnels which reference the EXTERNAL Interface Object now reference the HA-EXTERNAL interface object; that VPN Objects reference the new HA objects.

Typically, a GTA Firewall uses the External IP address when performing services such as DNS lookups, email alarms, Surf Sentinel registration verification and NTP. To ensure that these queries will be NAT'ed correctly after an upgrade, verify that Static Address Mappings which reference the EXTERNAL interface object now point to the HA-EXTERNAL object.

After you have verified the configuration, integrate it into your network and test it using the instructions in Chapter 3.

GNAT-Box Network Information					
Logical Interfaces					
Logical Name	Type	IP Address	NIC	DHCP	Gateway
EXTERNAL	External	199.120.225.252/24	fxp1	<input type="checkbox"/>	<input type="checkbox"/>
PROTECTED	Protected	192.168.71.252/24	fxp0	<input type="checkbox"/>	<input type="checkbox"/>
PSN	PSN	192.168.250.252/24	fxp2	<input type="checkbox"/>	<input type="checkbox"/>

New GB-1000 Network Information

GNAT-Box High Availability						
Enable:	<input checked="" type="checkbox"/>					
Status:	Master					
VRID:	14					
Priority:	255					
Email notification:	<input checked="" type="checkbox"/>					
Name	Interface	Virtual IP address	Beacon IP addresses			
HA-EXTERNAL	EXTERNAL	199.120.225.254	199.120.225.1	199.120.225.2	199.120.225.3	
HA-PROTECTED	PROTECTED	192.168.71.254	192.168.71.1	192.168.71.2	192.168.71.3	
HA-PSN	PSN	192.168.250.254	192.168.250.1	192.168.250.2	192.168.250.3	
			Update Slave	Default	Save	Reset

Virtual IP addresses configured using existing IP addresses

Configure the Existing GB-1000

With your new GB-1000 in place on your network, you can now connect the old firewall to an isolated network and edit the configuration using the instructions in Chapter 3 for the standby firewall.

Assign a lower priority number to this GB-1000 to make it the designated standby unit.

Once you have completed this, integrate the unit back into the network and complete the configuration by using the Update Slave function from the new GB-1000. Once the unit is in place and you have verified the new configuration, test fail-over by turning the master mode unit off.

If this final test is successful, your H₂A system is up and running.

Note

GB-1000 firewalls in an HA configuration must have identical hardware and software. If your old firewall is not on the same version as your new firewall, the old unit must be upgraded.

GNAT-Box Network Information					
Logical Interfaces					
Logical Name	Type	IP Address	NIC	DHCP	Gateway
EXTERNAL	External	199.120.225.252/24	fxp1	<input type="checkbox"/>	<input type="checkbox"/>
PROTECTED	Protected	192.168.71.252/24	fxp0	<input type="checkbox"/>	<input type="checkbox"/>
PSN	PSN	192.168.250.252/24	fxp2	<input type="checkbox"/>	<input type="checkbox"/>

Re-IP old firewall to new addresses

Upgrade Examples

New GB-1000 (Highest Priority) Example

External IP Address 199.120.225.253/24
 Protected IP Address 192.168.71.253/24
 PSN IP Address 192.168.250.253/24

VRID 10

Priority 20

HA-External

Virtual IP Address 199.120.225.254
 Beacons 199.120.225.249, 199.120.225.252,
 199.120.225.251

HA-Protected

Virtual IP Address 192.168.71.254
 Beacons 192.168.71.249, 192.168.71.252,
 192.168.71.252

Existing GB-1000 (Lower Priority)

External IP Address 199.120.225.252/24
 Protected IP Address 192.168.71.252/24
 PSN IP Address 192.168.250.252/24

VRID 10

Priority 10

HA-External

Virtual IP Address 199.120.225.254
 Beacons 199.120.225.253, 199.120.225.249,
 199.120.225.251

HA-Protected

Virtual IP Address 192.168.71.254
 Beacons 192.168.71.253, 192.168.71.249,
 192.168.71.251

Remote Access Filters

1. This filter accepts UDP broadcasts on port 77 to the multi-cast address of 224.0.0.18.

Description	Allow High Availability protocol.
Type	Accept
Interface	ANY
Protocol	UDP
Source	"ANY_IP"
Destination	224.0.0.18/32
Destination Port	77

2. This filter accepts IGMP protocol needed by High Availability at the multi-cast address of 224.0.0.18.

Description	Allow IGMP
Type	Accept
Interface	ANY
Protocol	2
Source	"ANY_IP"
Destination	224.0.0.18/32

Log Messages

GNAT Box System Software now uses WELF formatted logs by default.

HA Updated from Web Interface

```
Dec 11 21:58:23 fw.gta.com id=firewall time="2002-12-11 21:
58:23" fw="GB-1000A" pri=5 msg="WWWadmin: Update of
'High Availability'." type=mgmt src=192.168.71.12 src-
port=3162 dst=192.168.71.254 dstport=443
```

Switch to MASTER MODE

```
Dec 9 18:55:58 fw.gta.com id=firewall time="2002-12-09 18:
55:58" fw="GB-1000A" pri=4 msg="HA: Switching to master
mode, no higher priority 'master' found." type=mgmt
```

Switch to SLAVE MODE

```
Dec 9 18:55:52 fw.gta.com id=firewall time="2002-12-09 18:
55:52" fw="GB-1000A" pri=4 msg="HA: Switching to slave
mode, beacons ok." type=mgmt
```

Switch To INIT MODE

```
Dec 11 21:58:23 fw.gta.com id=firewall time="2002-12-11 21:
58:23" fw="GB-1000A" pri=4 msg="HA: Switching to init
mode, Starting." type=mgmt
```

Unable to reach a beacon address

```
Dec 30 10:18:49 pri=4 msg="HApinger: No reply from
10.254.254.1" type=mgmt
```

Error Message with wrong priority

```
Dec 11 20:28:31 pri=3 msg="HA: wrong priority (256) in con-
fig file, must be 0..255" type=mgmt
```

Error message VRID is greater than 15

```
Dec 11 22:07:24 odin.gta.com id=firewall time="2002-12-11
22:07:24" fw="GB-1000A" pri=3 msg="HA: vr_id greater
than 15" type=mgmt
```

Sample log output: a successful update of HA service running on the firewall in master mode

```
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A"
pri=5 msg="WWWadmin: Update of 'High Availability'."
type=mgmt src=192.168.71.12 srcport=2453 dst=192.168.71.80
dstport=443
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HApinger: Exiting." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Exiting." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Removed IP address 192.168.71.78 /32 from in-
terface fxp0." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Updated MAC address for interface fxp0 to 00:
d0:68:00:09:58." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Removed IP address 10.254.254.81/32 from inter-
face fxpl." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Updated MAC address for interface fxpl to 00:
d0:68:00:09:59." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxpl set to
10.254.254.80." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxp0 set to
192.168.71.80 ." type=mgmt
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="WWWadmin: Removing static routes." type=mgmt
src=192.168.71.12 srcport=2453 dst=192.168.71.80 dst-
port=443
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="WWWadmin: Adding static routes." type=mgmt
src=192.168.71.12 srcport=2453 dst=192.168.71.80 dst-
port=443
```

```
id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="WWWadmin: Default route set to 10.254.254.1."
type=mgmt src=192.168.71.12 srcport=2453 dst=192.168.71.80
dstport=443

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="alarms: Reinitializing." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HA: Starting." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="HAPinger: Starting." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=5
msg="alarms: Server ready." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=4
msg="HA: Switching to init mode, Starting." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="alarms: Email not enabled." type=mgmt

id=firewall time="2002-12-30 10:35:43" fw="GB-1000A" pri=6
msg="alarms: Enterprise server not enabled." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxpl set to
10.254.254.80." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxp0 set to
192.168.71.80 ." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Removing static routes." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=6
msg="HAstateChange: Adding static routes." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Default route set to 10.254.254.1."
type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Removing old objects ." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Add address object 'ANY_IP'."
type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Add address object 'Protected Net-
works'." type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Add interface object 'EXTERNAL'."
type=mgmt

id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=5
msg="HAstateChange: Add interface object 'PROTECTED'."
type=mgmt
```

```
id=firewall time="2002-12-30 10:35:44" fw="GB-1000A" pri=4
  msg="alarms: WARNING: email not enabled." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A"
  pri=4 msg="HA: Switching to slave mode, beacons ok."
  type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=6
  msg="NAT: Default address for interface fxp1 set to
  10.254.254.80." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=6
  msg="NAT: Default address for interface fxp0 set to
  192.168.71.80 ." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Removing static routes." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=6
  msg="HAsstateChange: Adding static routes." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Default route set to 10.254.254.1."
  type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Removing old objects ." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Add address object 'ANY_IP'."
  type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Add address object 'Protected Net-
  works'." type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Add interface object 'EXTERNAL'."
  type=mgmt
id=firewall time="2002-12-30 10:35:51" fw="GB-1000A" pri=5
  msg="HAsstateChange: Add interface object 'PROTECTED'."
  type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=4
  msg="HA: Switching to master mode, no higher priority
  'master' found." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
  msg="HA: Updated MAC address for interface fxp0 to 00:
  00:5e:00:01:25." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
  msg="HA: Added IP address 192.168.71.78 /32 to interface
  fxp0." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
  msg="HA: Updated MAC address for interface fxp1 to 00:
  00:5e:00:01:24." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
  msg="HA: Added IP address 10.254.254.81/32 to interface
  fxp1." type=mgmt
```

```
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxpl set to
10.254.254.81." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=6
msg="NAT: Default address for interface fxp0 set to
192.168.71.78 ." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Removing static routes." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=6
msg="HAsstateChange: Adding static routes." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Default route set to 10.254.254.1."
type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Removing old objects ." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add address object 'ANY_IP'."
type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add address object 'Protected Net-
works'." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add interface object 'EXTERNAL'."
type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add interface object 'PROTECTED'."
type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add HA interface object 'EXTER-
NAL'." type=mgmt
id=firewall time="2002-12-30 10:35:57" fw="GB-1000A" pri=5
msg="HAsstateChange: Add HA interface object 'PROTECT-
ED'." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A"
pri=5 msg="HAsstateChange: Gateway selector disabled."
type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=6
msg="alarms: Reinitializing." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=6
msg="gblogd: Reinitializing." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=5
msg="alarms: Server ready." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=6
msg="alarms: Email not enabled." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=5
msg="HAsstateChange: Stopping NTP service." type=mgmt
```

```
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=6
  msg="alarms: Enterprise server not enabled." type=mgmt
id=firewall time="2002-12-30 10:35:59" fw="GB-1000A" pri=5
  msg="HAsstateChange: Setting internal DNS servers to
  192.168.71.9." type=mgmt
```

Example of State Change Email Notifications

Entering INIT Mode

```
Subject: GNAT Box - HA mode change
From: fw@gta.com
To: support@gta.com
Date: Mon, 30 Dec 2002 10:46:02 -0500 (EST)
NOTIFICATION TYPE: HA mode change
NAME: GB-1000 (HA-Master)
DATE: Mon 2002-12-30 10:46:02 EST
CONFIGURATION: EXTERNAL=10.254.254.80
PROTECTED=10.10.1.80
```

Entering INIT Mode.

.....

Entering Slave Mode

```
Subject: GNAT Box - HA mode change
From: fw@gta.com
To: support@gta.com
Date: Mon, 30 Dec 2002 10:46:09 -0500 (EST)
NOTIFICATION TYPE: HA mode change
NAME: GB-1000 (HA-Master)
DATE: Mon 2002-12-30 10:46:09 EST
CONFIGURATION: EXTERNAL=10.254.254.80
PROTECTED=10.10.1.80
```

Switching from INIT to Slave Mode.

.....

Entering Master Mode

```
Subject: GNAT Box - HA mode change
From: fw@gta.com
To: support@gta.com
Date: Mon, 30 Dec 2002 10:46:17 -0500 (EST)
NOTIFICATION TYPE: HA mode change
NAME: GB-1000 (HA-Master)
DATE: Mon 2002-12-30 10:46:17 EST
CONFIGURATION: EXTERNAL=10.254.254.80
PROTECTED=10.10.1.80
```

Switching from Slave to Master Mode.

.....

Index

A

activation code 2

B

beacon 8, 16

broadcast port 8

C

cables 2, 21

caution 13, 16, 17, 25, 27

cfg. *See* Configuration: copy

Configuration Report 3

connecting 2

connectivity 7, 9, 14, 16, 20

Console interface 5

conventions, documentation 4

copyright ii

copy protection 3

D

default

button, filters 17

route 18

settings 3, 8

diagnostic mode. *See* init mode

different subnets 23

DMZ. *See* PSN

documentation 4

drivers and NICs 5

dynamic interfaces 16

E

email, GTA ii

email notification 15

enable HA 15

Encapsulated Security Payload.
See ESP

F

factory settings, defaults. *See* default:
settings

fail-over 1, 8, 11, 20, 28

test 20

feature code. *See* activation code

filter order 17

G

gateway. *See* default: route

GBAAdmin 5

GNAT Box System Software ii

GTA Mailing List 3

H

HA network interface 9

help. *See* support

highest priority 9, 13, 19, 21

I

IGMP 17

init mode 7

installation support 3

interface object 15

L

Local Gateway

VPN Objects 18

location 12

log messages 30

M

MAC address, virtual 10

mapping 25

master MAC address. *See* MAC ad-
dress, virtual

master mode 8

merge configuration 26

mode

high availability 7

init 7

master 8

mode, stealth 16

multi-cast address 8, 17, 30

N

name field 15

network pair 12

notes & warnings 1, 2, 3, 8, 9, 10, 14,
15, 16, 17, 19, 23, 28

caution 13, 16, 17, 25, 27

notification 15

O

order, filter 17

P

pair, network 12

partners, GTA 3

physical firewall 9

ping 8, 21

ping, can't 21

port 77 7, 17, 30

primary mode. *See* master mode

priority mode. *See* master mode

priority number 9, 15
 caution 16

PSN 10

public IP address 12, 23

Q

quickstart method 11

R

re-connect 27

registered IP address. *See* public IP
 address

registration 2, 5

Remote Access Filters 17

RFC 1918 22, 23. *See also* public IP
 address

routable on the Internet. *See* public IP
 address

S

setting. *See* default: settings

slave mode. *See* standby mode

standby mode 7

start HA 15

state information 1

static mapping 25, 27

status 15. *See also* mode: high avail-
 ability

stealth mode 16, 21

support 2, ii
 installation 3

T

technical support. *See* support

telephone ii

telnet 1

terms 4

test fail-over 20

test mode. *See* init mode

trademark ii

troubleshooting 5

two subnets 23

U

UDP 7, 17, 30

Update Slave 19

upgrade your existing GB-1000 26
up and running 3

V

valid names 21

version ii

version upgrade 28

virtual firewall 9

 IP address 10

 MAC address 10

virtual IP address field 16

virtual router ID 9, 15

VRID. *See* virtual route ID

VRID, unique 22

W

Web interface 4

WELF 30

wrong HA mode 21