GB-1000

Firewall Appliance

High Availability

User's Guide

H$_2$A

High Availability
Highly Available

Global
Technology
Associates, Inc.

Copyright

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 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

Document Information

GNAT Box High Availability User’s Guide Version 1.0, December 2001

Version Information

GNAT Box System Software version 3.2.2 December 2001

Problems

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

Support: +1.407.482.6925

Electronic Contact Information

General Email: info@gta.com

Support Email: support@gta.com

Website: http://www.gta.com

3rd Printing December 2001

Contents

Introduction

H_2A™, Global Technology Associates, Inc.’s high availability option, is a cost-effective and resilient network security solution. The High Availability feature for the GB-1000 Firewall Appliance allows two GB-1000 systems to work in tandem to ensure network access and security.

The feature is part of the GNAT Box system software and is enabled with an activation code, so there is no additional software to install. Using that and the H_2A’s fast configuration, you can have a highly available firewall system running in minutes. Plus, H_2A is totally transparent to end-users, so no obvious changes are required to your existing network configuration.

Unlike other high availability solutions, GTA’s H_2A does not require special cabling to join the two HA systems.

GTA’s High Availability Solution...

When the H_2A feature is enabled on two GB-1000 systems, the systems operate as one virtual GB-1000. Only one system is functioning as a firewall; the other remains in standby, ready to take over if the primary system stops broadcasting. End users see one firewall, regardless of which physical system is operational.

A GTA H_2A configuration doesn’t follow the standard master/slave approach. The two systems don’t directly communicate with each other; each system operates independently, checking the integrity of its own network interfaces and listening to HA information broadcasts.

The system with the highest priority in the HA group is the operational firewall (master) while the other operates in standby (slave). Upon detecting no more master HA broadcasts, a standby system will assume the role of the master. The system will continue to operate in the master mode until another system in the HA group with a higher priority becomes operational and thus assumes the role of the master.

When a system looses connectivity on any of its HA configured network interfaces, it switches from its current mode to Init, a diagnostic mode in which the system continally tests its network interfaces. Once it verifies that it has connectivity again, it enters either the Standby (Slave) or Master mode, depending on its priority among the operational systems.

Note: *At this time, GTA's H_2A solution does not exchange state information. When a switch occurs, active connections are lost, affecting long-lived connections like telnet.*

...versus the Standard Approach

In a standard master/slave configuration, the slave communicates directly with the master to determine if the the master system is operating correctly. If the slave perceives that the master is not fully operational, it takes over the firewall operations. This approach has some flaws – the most serious being the assumption that if the slave has trouble communicating with the master, then the master is not operating properly; of course, the trouble could be with the slave system.

Requirements

- Two identical GB-1000 systems
- One static IP address on the External network
- One static IP address for the Protected network
- GNAT Box® system software version 3.2 or higher
- Valid H_2A activation code for each system.

About this User's Guide

This User's Guide is intended for the firewall administrator who is already familiar with the GB-1000 and the GNAT Box system software. The guide lists the requirements for using H_2A; how to activate, configure and operate the H_2A option for GB-1000; and defines the terms used in this guide. The manual is organized to make it easy to use, both as a tutorial and as a reference source. It is not intended to repeat material available in other documentation such as the *GNAT Box® User's Guide version 3.2.1 or GNAT Box User's Guide 3.2.2 Addendum.*

Documentation conventions

The following documentation conventions are used in the guide:

Bold type	Terms introduced and explained for the first time. Names of on-screen buttons and menu items.
SMALL CAPS	Fields.
`Courier`	Text that appears on the screen.

High Availability Modes

When a GTA Firewall has the H_2A feature enabled, it will be operate in one of three High Availability modes. The system will change modes depending on its status and the status of other systems in the HA group. All HA modes are determined and set by each HA system and not from external inputs. All mode changes are logged.

Init mode

Each time an HA-enabled system starts up, it enters the **Init** mode. In Init mode, the system always assumes the worst: that its network interfaces are not functioning properly, and it has no connections to local networks. Once in Init mode, the system begins to test its network interfaces by directing packets from each HA Network Interface to the beacons in the beacon list. If valid responses are received from at least one beacon assigned to each HA network interface, then the HA system will switch to **Standby** (Slave) mode.

Standby (Slave) mode

Once the HA system determines that its network interfaces are operating properly, it enters the **Standby** (Slave) mode. In Standby, the HA system will begin to listen (UDP/77) for HA broadcast traffic from other members of the HA group. The HA broadcast traffic will include information that indicates the **Priority** of the system that is currently operating in the **Master** mode. In Standby mode, the HA system will compare the priority level extracted from the HA broadcasts from a system in the Master mode to its own Priority level. If the system determines that the priority level of the HA broadcast from the system operating in the Master mode is lower than its own priority, the system will switch to **Master** mode.

Master mode

A system enters the **Master** mode when it determines that it has a higher priority than a system currently operating in the Master mode, or there are no HA broadcasts, so it has the highest priority by default. Once in Master mode the system will:

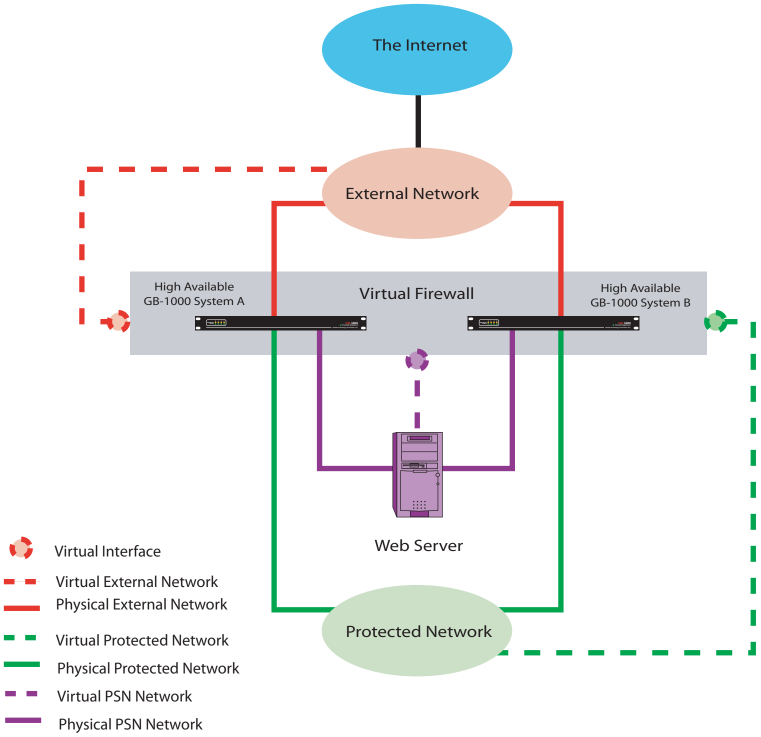
1. Change the physical MAC addresses of its HA network interfaces to the **HA Master MAC address.**
2. Begin sending out HA broadcasts (UDP/77) messages which include the system's priority in the HA group.
3. Continue to listen for HA broadcasts. However, in the Master mode, the system is listening for HA broadcasts from a system in the HA group with a higher priority. If the system in Master mode determines that another system in the HA group has a higher priority, then it drops back into Standby mode. When a system switches from the Master mode to any other mode, its MAC addresses will revert to original values.

Note: *In GNAT Box system software version 3.2.2, the system in Master mode has a unique virtual MAC address for each interface generated using a combination of the VRID (virtual router ID) number and the interface number. The IP address for the virtual Firewall does not change, but the virtual MAC address allows systems in non-recommended configurations to recognize and distinguish between the interfaces.*

The H_2A feature

Nearly all H_2A configuration is performed from a single system which then updates the other system in the HA group. Remember that the two systems in an H_2A configuration have identical hardware and software; because of this, configuration may be performed on either the system. You can configure H_2A from GBAdmin or the Web interface. Remember to verify that your Remote Access filters allow access.

When configuring the two systems, keep in mind the differencc between the **Configuration IP address** and the **Virtual Firewall IP address**. Configuration IP addresses should only be used by the administrator. End users will use only the Virtual Firewall IP address. This allows the end user to utilize the virtual firewall regardless of which physical system in the HA group is operating as the Master.



High Availability Network Diagram

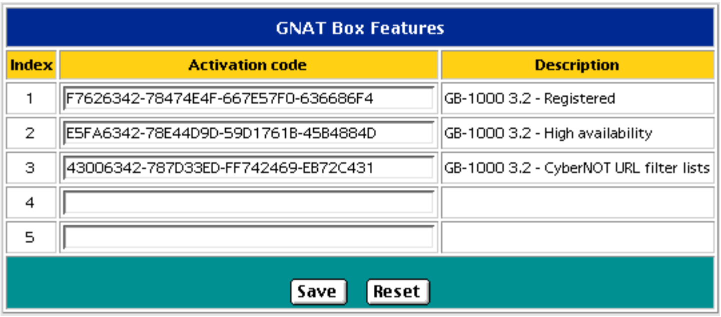
Pre-configuration

Save a copy of your current firewall configuration on your workstation prior to making changes for the H_2A option.

Before configuring the H_2A feature on your GB-1000 firewall systems, make sure that each has a valid High Availability activation code; IP addresses assigned to a Protected Network interface accessible by the other system; and Remote Access filters allowing access on the Protected Network interface (TCP/77, the same as RMC/GBAdmin).

Activate H_2A with Feature Codes

A separate H_2A activation code is entered on the **Features** screen of each system in the HA group. When the activation code is correctly entered, the description column will indicate "**GB-1000 3.2–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.



GNAT Box Features

Index	Activation code	Description
1	F7626342-78474E4F-667E57F0-636686F4	GB-1000 3.2 - Registered
2	E5FA6342-78E44D9D-59D1761B-45B4884D	GB-1000 3.2 - High availability
3	43006342-787D33ED-FF742469-EB72C431	GB-1000 3.2 - CyberNOT URL filter lists
4		
5		

Features Screen (Web)

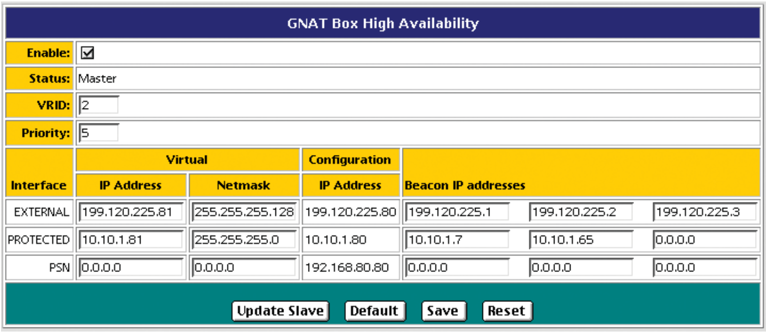
Upgrading an Existing GB-1000

If you are upgrading an existing GB-1000 firewall installation with the HA option, you may want to use the current IP addresses on the Virtual Firewall so that users are not affected by the changes.

In order to use the current IP addresses for the Virtual Firewall, change the IP addresses assigned to the NICs on the Network Information screen to free up existing IP addresses so they can be assigned to the Virtual Firewall. If possible, select new IP addresses that are one number lower or higher than the current IP addresses. If you change your existing IP addresses, do so prior to performing the HA configuration process.

Configure the Master System

In this guide, the Master system will be configured first, then the Standby system. Select the system you will designate as Master.

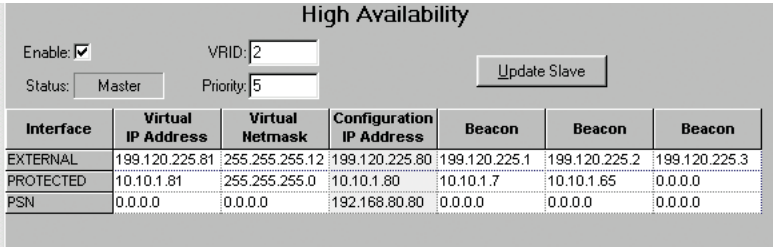


GNAT Box High Availability

Enable:	☑
Status:	Master
VRID:	2
Priority:	5

	Virtual		Configuration			
Interface	IP Address	Netmask	IP Address	Beacon IP addresses		
EXTERNAL	199.120.225.81	255.255.255.128	199.120.225.80	199.120.225.1	199.120.225.2	199.120.225.3
PROTECTED	10.10.1.81	255.255.255.0	10.10.1.80	10.10.1.7	10.10.1.65	0.0.0.0
PSN	0.0.0.0	0.0.0.0	192.168.80.80	0.0.0.0	0.0.0.0	0.0.0.0

High Availability Configuration Screen (Web)



High Availability

Enable: ☑ VRID: 2

Status: Master Priority: 5

Interface	Virtual IP Address	Virtual Netmask	Configuration IP Address	Beacon	Beacon	Beacon
EXTERNAL	199.120.225.81	255.255.255.12	199.120.225.80	199.120.225.1	199.120.225.2	199.120.225.3
PROTECTED	10.10.1.81	255.255.255.0	10.10.1.80	10.10.1.7	10.10.1.65	0.0.0.0
PSN	0.0.0.0	0.0.0.0	192.168.80.80	0.0.0.0	0.0.0.0	0.0.0.0

High Availability Configuration Screen (GBAdmin)

1. Select the **High Availability** menu item from the **Services** menu 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 H_2A feature code.)
2. Click the **Enable** checkbox to enable the HA feature.

> ***Note:*** *When the system has been configured and is running in the HA group, the* ***Status*** *field will display the current HA mode of the system, Init, Slave or Master.*

3. Enter a value between 0 and 15 for the **VRID** (Virtual Router ID). Both HA systems must have the same VRID. The VRID is used to uniquely identify the HA group.

Note: *If you are upgrading an existing H2A configuration, make sure that your VRID number is 0-15. VRID numbers ranged from 1-255 in version 3.2.1.*

4. Enter the **Priority** number between 1 and 255 for the HA system. The HA system with the highest Priority and confirmed communications with its beacons will operate in the **Master** mode. The system operating in Master mode will be the operational firewall and process network traffic as the virtual firewall.

Note: *If you do not set the priority number for the systems, the two firewalls will select the Master by automatically giving one system a higher priority number.*

5. Enter the **Virtual IP Address** and **Netmask** that will be used by the virtual firewall for a given network interface (these are the IP addresses the firewall users will use). By default, the Virtual IP address is one IP address higher than the **Configuration IP address** (Click the **Default** button to call up the default settings.)

   If you are upgrading an existing GB-1000 with the H_2A option and have replaced your previous IP addresses with new ones (as described previously), enter your previously assigned IP addresses in the Virtual IP Address fields.

6. The **Configuration IP Address** field is non-editable. The Configuration IP Address is the IP address assigned to a GB-1000 NIC. This is the IP address that the administrator will use to configure the GB-1000 system. Any change to the IP address assigned to the specified network interface on the **Network Information** screen will change the Configuration IP address on the HA configuration screen.

7. Enter up to three **Beacon IP Addresses**.

Note: *Normally, one beacon address is the Configuration IP address on the other H_2A system.* ***Do not make the other H_2A system your only beacon address.*** *This can lead to improper functioning of the HA group.*

The Beacon IP Addresses are used to help determine when a network interface has a problem. For each beacon listed, the GB-1000 will send two ping packets a second. If the system fails to receive a reply five times in a second, the host will be marked as down. If all the hosts (beacons) associated with an interface fail to respond, then the HA module assumes there is a problem with the network interface. The system will change its current HA mode to the **Init** mode, send a log message and continue to test the network interface.

8. Click **Save** to save the HA configuration information.
9. Select **Remote Access** from the **Filters** menu item. The High Availability option requires two Remote Access filters. These filters can be produced by clicking **Default** on the Remote Access Filter screen or created manually. Remember, if you **Default** and save the configuration, any custom filters will be lost; the system will create default filters according to the system configuration.

The two required Remote Access filters are:

1. Allow the system to receive HA broadcasts.

```
     Description: Allow high availability protocol.
            Type: Accept
       Interface: ANY
        Protocol: UDP
       Source IP: Object - "ANY_IP"
     Source Port: Zero or blank for any
  Destination IP: 224.0.0.18/32
Destination Port: 77
```

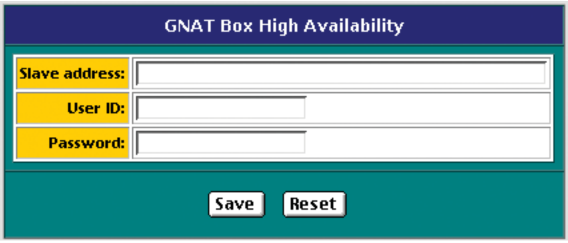
2. Allow the system to receive IGMP for HA.

```
     Description: Allow IGMP
            Type: Accept
       Interface: ANY
        Protocol: 2
       Source IP: Object - "ANY_IP"
     Source Port: Leave blank for any
  Destination IP: 224.0.0.18/32
Destination Port: Zero or blank for any
```

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

Update the Standby System

Click the **Update Slave** on the High Availability screen.



GNAT Box High Availability

Slave address:

User ID:

Password:

Update Standby/Slave Dialog (Web)

In the **Slave address** field enter the **Configuration IP Address** of the system you are designating the Standby system. Enter an Admin User ID for the slave system in the **User ID** field. This Admin User ID must have both RMC and Admin options enabled for the account. Enter the password for the User ID in the **Password** field and press **Save** to upload and save the configuration information to the Standby system.

The Master system (the one with the highest priority) is now configured and the standby/slave system has the latest configuration data.

Complete Standby System Configuration

Since the **Update Slave** function performs most of the configuration on the Standby system, there are only a few manual configuration changes. These changes need only be performed once, since these data fields are static and are not updated by the Update Slave function.

Note: *The Slave Update function does not update:*
- *Any data on the Network Information screen.*
- *Any data on the Preferences section.*
- *Feature Codes.*
- *Enterprise Server fields.*

After the update has been performed from the Master system, connect to the Standby system using the Configuration IP address with either the Web or GBAdmin interface. On the Standby system:

1. Select the **High Availability** menu item from the **Services** menu.

2. Edit the **Beacon IP Addresses**. If you are using the Standby system as a beacon IP for the Master system, one beacon IP address on the list will be that of the Standby system. Change this IP address to that of the Master's Configuration IP Address so that the master will serve as a beacon for the Standby system.
3. Change the **Priority** to a lower value than the Master, a number between 1 and 255. The HA system with the lowest Priority and confirmed communications with its beacons will operate in Standby mode.

> ***Note:*** *If you do not set the priority number for the systems, the two firewalls will select the Master by automatically giving one system a higher priority number.*

Administration Notes

- Use Configuration IP addresses to access the firewall systems with either GBAdmin or the Web user interfaces.
- Make all configuration changes to the primary (master system) then use the Update Slave function to apply the changes to the slave system.
- **User Configuration**
  Hosts on the protected network(s) should have their default route/gateway pointing to 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. Access from the external network (the Internet) to inbound tunnels should also use the Virtual IP Address assigned to the External network interface.

> ***Note:*** *DHCP is not recommended in the H_2A configuration.*

H_2A Setup Example

The following example illustrates the setup of a High Availability group.

Hosts

Router: 199.120.225.1

Mail Server: 192.168.1.110

Workstation: 192.168.1.25

Physical GB-1000 Systems

GB-1000 System 1

VRID: 10

Priority: 8

External

Configuration IP Address: 199.120.225.79/255.255.255.0

Beacons: 199.120.225.80, 199.120.225.1

Protected

Configuration IP Address: 192.168.1.79/255.255.255.0

Beacons: 192.168.1.80, 192.168.1.110

GB-1000 System 2

VRID: 10

Priority: 7

External

Configuration IP Address: 199.120.225.80/255.255.255.0

Beacons: 199.120.225.79, 199.120.225.1

Protected

Configuration IP Address: 192.168.1.80/255.255.255.0

Beacons: 192.168.1.79, 192.168.1.110

Virtual Firewall System

External

Virtual IP Address: 199.120.225.78/255.255.255.0

Protected

Virtual IP Address: 192.168.1.78/255.255.255.0

Glossary

Activation Code

An activation code is an encode key of 35 characters which enable optional features on the GB-1000 system. Activation codes are system specific and must be used on the system they were generated for. To use the GB-1000 High Availability feature a valid H2A activation code must be installed on each system in the HA group.

```
    Example:   E5FA6342-78E44D9D-59D1761B-45B4884D
```

Beacon

A host that is used as a target to test network connectivity. A beacon can be any network device with an assigned static IP address and accessible on a local network attached to a HA system. Each HA system should include the other system in its beacon list. For each beacon in the beacon list the HA system will send a ping packet every 1/2 second. Good choices for beacons are systems that are normally always running, such as routers or mail servers.

Beacon IP Address

A beacon’s IP address.

Configuration IP Address

This is an IP Address that is assigned to any NIC on the GB-1000 and appearing on the Network Information screen. Configuration IP addresses are only used to configure the GB-1000 and should not be used for any purpose other than configuration. Only the administrator should access the Configuration IP Address on the GB-1000.

HA Default Remote Access Filters

In order for a system to operate properly in a HA group two **Remote Access** filters must be in place. These filters are generated by default when the HA mode is enabled, and the Default button is pressed on the Remote Access filter summary screen. If the Remote Access filters have been customized then, these two filters need to be entered manually. The two filters are:

```
1.  Accept High Availability Protocol
    This filter accepts UDP broadcast on port 77 to the multi-
        cast address of 224.0.0.18.
    DEFAULT: Allow high availability protocol.
    Accept ANY UDP from "ANY_IP" to 224.0.0.18/32 77
2.  Accept IGMP Protocol
    This filter accepts IGMP protocol at the multi-cast address
        of 224.0.0.18.
    DEFAULT: Allow IGMP needed by high availability.
    Accept ANY 2 from "ANY_IP" to 224.0.0.18/32
```

HA Network Interface

Any network interface on the GB-1000 system that has been configured for HA use. When a network interface is configured for HA use it will be included in the network connectivity testing performed by the HA software. The failure (no response from the specified beacons) of any HA Network Interface will cause the system to change from the current HA mode to the **Init Mode**. Not all network interfaces on a GB-1000 have to be configured as HA Network Interfaces. If you wished not to use an interface as a HA Network Interface enter “0.0.0.0” as the Virtual IP address on the HA configuration screen.

HA Broadcast Port

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

HA Master MAC Address

The system in the HA group that is operating in the **Master mode** uses a special MAC address. The normal MAC address that is assigned to the NIC is replaced with the **HA Master MAC address**. This MAC address is: 00:00:5E:00:01:**xx**, where “xx” is the VRID number. *In GNAT Box system software version 3.2.2, each interface has a unique VRID, generated by combining the VRID with the interface number.*

Priority

This value determines how the GB-1000 system will operate in the HA group. An active healthy system with the highest priority in the HA group will assume the Master role in the HA group. If the priorities are the same for both systems in the HA group the GB-1000 that declares itself to be the Master first will stay the Master, until a change occurs in the HA group status. Valid priority values are: 1 - 255.

Standby/Slave Update

The **slave update** is a function that is executed by the administrator from the HA system with the highest priority. This function is executed from the HA configuration screen by clicking the “Slave Update” button. The **slave update** function will send configuration information to the other system in the HA group (one with a lower priority, hence, it will be operating in the Slave mode by default) and update it. To use the slave update function the slave system must have an admin user account that has both “**RMC**” and “**Admin**” permissions enabled. The Slave Update screen requires the administrator to enter both the admin user ID and password for the remote system.

Virtual Firewall

The virtual firewall consists of both physical GB-1000 systems in the HA group yet appears as a single system to network users.

Virtual Firewall IP Address

This is an IP address that is assigned to any of the NICs on the **Virtual Firewall**. Virtual Firewall IP addresses are configured on the HA configuration screen and can be of any interface type (Protected, External or PSN). The Virtual Firewall IP addresses are referenced by hosts that wish to send data through or to the firewall. These IP addresses should always be available despite which GB-1000 system is actively operating in the Master mode.

VRID

The VRID (Virtual Router ID) defines a HA Group. All members of an HA Group should have the same VRID. Valid VRID values are 0-15.

Global
Technology
Associates, Inc.

3505 Lake Lynda Drive, Suite 109
Orlando, FL 32817 USA