H2A

High Availability Feature Guide

Global Technology Associates, Inc.

Global Technology Associates
3361 Rouse Rd, Suite 240
Orlando, FL 32817

Tel: +1.407.380.0220
Fax. +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table Of Contents

Introduction

About H_2A - High Availability

H_2A, 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 H_2A-capable GTA firewalls create a system that acts as a single firewall allowing you to maintain network security and access. With H_2A's fast, transparent fail-over, you're assured that firewall downtime doesn't equal network downtime.

H_2A is easy to configure and use. Set up two or more systems anywhere on the same network, enter the activation codes, and begin customizing the H_2A option. That's it. No special cabling and no extra software. With GB-OS' fast configuration, your H_2A solution can be operational in minutes.

An H_2A system is transparent to end users, requiring no obvious changes to the existing network's 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 H_2A option has been activated and configured on your firewalls, the H_2A system works transparently to ensure constant firewall coverage and seamless maintenance of your GTA firewall configurations.

To determine which GTA firewall functions as the virtual firewall, each firewall in the H_2A chain is assigned a priority number. The GTA firewall 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 High Availability 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 GTA firewall in the chain with a higher priority becomes operational.

Note

H_2A 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.
- Cost-effective fail-over solution.

Requirements

H_2A - High Availability requires:

- Two or more H_2A-capable GTA firewalls with identical hardware and software configurations.
- One static IP address on the external network.
- One static IP address for the protected network.
- H_2A - High Availability option for each firewall in the H_2A chain.

Registration & Activation

If you have not yet registered your firewall products, go to the GTA Online Support Center (https://www.gta.com/support/center/login/). In the login screen, enter your user ID and password. Click the **Register Product** link and enter your product serial numbers and firewall activation (unlock) codes, then click **Submit**.

If you do not already have a GTA Online Support Center account, click the **Create an Account Now!** link on the GTA Online Support Center login screen.

Feature Activation Codes

Optional features for GB-OS require activation codes. High Availability activation can be automated or entered manually through the GB-OS Web interface. High Availability can only be activated after your GTA Firewall UTM Appliance has been registered through the GTA Online Support Center.

Automatic Activation

High Availability can be automatically activated through the GB-OS Web interface. Navigate to **Configure>Configuration>Runtime>Update**. If no updates display, click on **Check Now**. All available feature codes and runtime updates will display. Click on **Update** and High Availability will be automatically installed.

Manual Activation

To manually activate High Availability, retrieve the feature activation code by logging into the GTA Online Support Center and navigate to **View Your Registered Products.** Select the serial number of your GTA Firewall UTM Appliance to display the activation code.

Next, login to GB-OS and navigate to **Configure>System>Activation Codes**. Click the **New** icon to enter the feature activation code in the next available line. **Save** the section. When an activation code is entered correctly, the Description field will indicate “GB-*X*–High Availability”, where *X* is your firewall’s product number.

Note

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

Note

Enter the H_2A feature activation code for each firewall in the H_2A chain before configuring any of the firewalls for High Availability.

About this Guide

This feature guide is a supplement to the *GB-OS User's Guide*. It lists requirements, and explains how to activate, configure and operate an H_2A system.

Conventions

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

Bold Italics	Emphasis
Italics	Publications
Blue Underline	Clickable hyperlink (email address, Web site or in-PDF link)
Small Caps	On-screen field names
`Monospace Font`	On-screen text
Condensed Bold	On-screen menus, menu items
BOLD SMALL CAPS	On-screen buttons, links

High Availability Concepts

The following concepts are specific to High Availability and to the GB-OS H_2A feature.

High Availability Modes

When a GTA firewall has the H_2A 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 H_2A chain. High availability modes are determined by the individual H_2A firewall, not from any external source. All mode changes are logged.

Init Mode

Each time an H_2A-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 removed from the H_2A chain. It tests its network interfaces by directing packets from each H_2A network interface to the beacons on its beacon list. If valid responses are received from at least one beacon assigned to each H_2A network interface, the H_2A firewall will switch to standby or master mode, and re-enter the H_2A chain as a standby or master unit.

If a firewall in the H_2A 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 H_2A chain as a standby or master unit.

Standby (Slave) Mode

In standby (slave) mode, the H_2A firewall listens for H_2A broadcast traffic from other members of the H_2A chain. The H_2A 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 H_2A 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 H_2A network interfaces to the H_2A master MAC address; send out H_2A broadcasts messages which include the system's priority in the H_2A chain, and continue to listen for H_2A broadcasts.

However, in the master mode, the system is listening for High Availability broadcasts from a GTA firewall in the H_2A 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 their 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 H_2A 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 unreachable. If all the hosts (beacons) associated with an interface fail to respond, then H_2A assumes there is a problem with the network interface. The firewall will switch to init mode, 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 UTM Appliance as a beacon, deselect the Stealth Mode option in **Configure>Security Policies>Preferences** on the firewall which you will use as a beacon.

Broadcast Port and Multi-cast Address

H_2A - High Availability broadcasts are transmitted by default as broadcast packets from broadcast port UDP 77 at the multi-cast address 224.0.0.18.

H_2A Network Interface

An H_2A network interface is any network interface on a GTA firewall that has been configured for High Availability. When a network interface is configured for H_2A, it will be included in the network connectivity testing performed by the H_2A feature. The failure of any H_2A network interface (for instance, 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 H_2A 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 two or more systems in an H_2A chain share the same priority number, the unit which becomes the master first will retain master mode.

Note

GTA recommends selecting a unique priority number for each H_2A unit.

VRID

The VRID (Virtual Router ID) is what defines an H_2A chain. All members of an H_2A chain should be assigned the same VRID. Valid VRID values are 1-4079 for GB-OS 6.1.0 and above. (GB-OS 6.0.x and lower are 1-15.). GB-Ware in an High Availability environment on VMWare should use the same priority.

Virtual Firewall

The virtual firewall appears as a single system to network users, but actually consists of all physical GTA firewalls in the H_2A chain. The virtual firewall has virtual IP addresses and IP aliases that represent the H_2A 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 use the virtual firewall, regardless of which physical firewall in the H_2A 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 H_2A 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 address of a unit and the virtual IP address assigned to the H_2A chain.

Physical (Configuration) IP Addresses

A physical IP address is the IP address of a network interface on a GTA firewall. It is the IP address that appears in **Configure>Network>Interfaces>Settings**. In an H_2A configuration, physical IP addresses are used only for configuration, they should be accessed only by the administrator.

Virtual (Master) MAC Address

In an H_2A 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 GTA firewall.

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 H_2A 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.

Installation and Configuration

Overview

This following sections illustrate a new H_2A system setup, using at least two public (registered) IP addresses. See Reference A: H_2A on Two Subnets for examples of other configurations: a system with only one public IP address, and an H_2A upgrade of a GTA firewall. Nearly all H_2A configuration is performed from a single GTA firewall that updates the other firewalls in the H_2A 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.

H_2A System Location

The firewall in an H_2A 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 new configuration has been tested. The diagram below shows an H_2A - High Availability network pair.

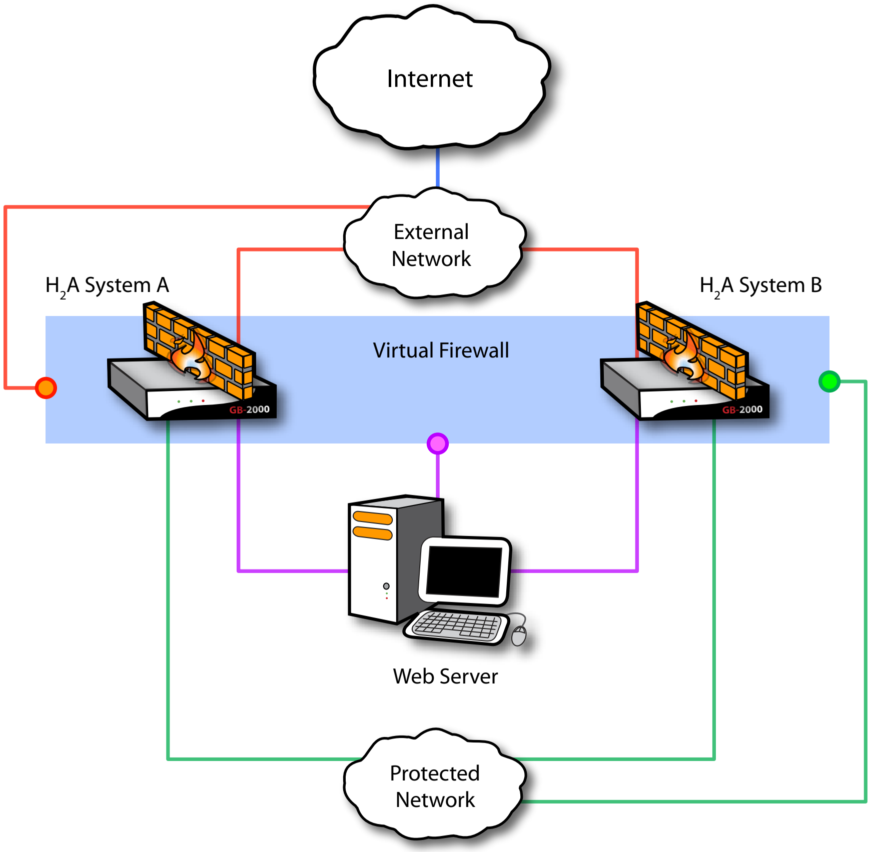


Figure 3.1: *H_2A - High Availability Network Pair Diagram*

Creating a H_2A Virtual Firewall

Install your GTA firewalls that will become the H_2A virtual firewall in your network. To safely configure High Availability settings without effecting network security, be sure all GTA firewalls that will be configured are operating in Test mode.

To toggle Test mode:

1. Navigate to **Configure>Configuration>Change Mode.**
2. Select Test mode.
3. Select **Submit.**

Choose the physical (configuration) IP addresses to configure the **Configure>Network>Interfaces>Settings** sections for each firewall. (Your current interface IP addresses will become the virtual firewall IP addresses on the new system.)

Create a backup (by using the **Configure>Configuration>Import/Export** screen) 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 Reference B: Upgrading an Existing GTA Firewall to High Availability for more information on merging a GTA firewall configuration.

Note

Use the *GB-OS User's Guide* as a reference for initial firewall set up and for more information on configuration options.

Creating individual security policies to allow H_2A firewalls to communicate with one another is not necessary. Policies are generated automatically by the High Availability service and use IP addresses entered in the HA Nodes address object (configured using the Object Editor, located at **Configure>System>Objects>Address Objects**.

System Examples

These IP addresses and other data are used as examples in the configuration sections that follow. Enter the appropriate data for your network. Firewall A is selected as the highest priority firewall.

Table 3.1: System Examples

System	Setting
Router	199.120.225.1
Firewall A (Highest Priority)	
External IP Address	199.120.225.80/24
Protected IP Address	192.168.71.80/24
H_2A Configuration	
VRID	10
Priority	20
H_2A External	
Virtual IP Address	199.120.225.254/24
Beacons	199.120.225.253, 199.120.225.252, 199.120.225.251
H_2A Protected	
Virtual IP Address	192.168.71.254/24
Beacons	192.168.71.253, 192.168.71.252, 192.168.71.251

Table 3.1: System Examples

System	Setting
Firewall B (Lower Priority)	
External IP Address	199.120.225.79/24
Protected IP Address	192.168.71.79/24
H_2A Configuration	
VRID	10
Priority	10
H_2A External	
Virtual IP Address	199.120.225.254/24
Beacons	199.120.225.253, 199.120.225.252, 199.120.225.251
H_2A Protected	
Virtual IP Address	192.168.71.254/24
Beacons	192.168.71.253, 192.168.71.252, 192.168.71.251

Setting Up Firewall A

Connect the first GTA firewall (Firewall A). Using the *GB-OS User's Guide*, set up the unit and configure **Configure>Network>Interfaces>Settings** using your configuration IP addresses for this firewall, then enter the H_2A feature activation code in **Configure>System>Activation Codes**.

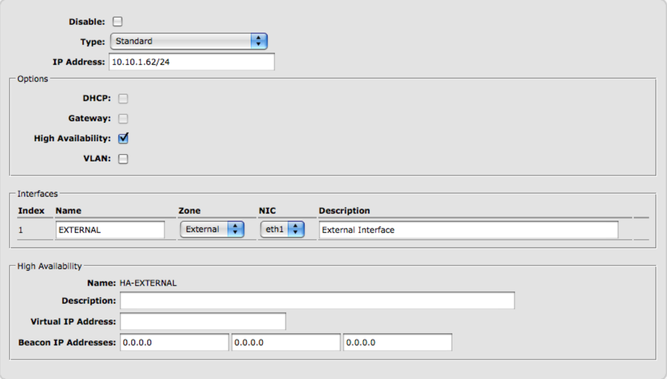
Configuring the H_2A - High Availability Interfaces

After the appropriate feature activation codes have been entered, navigate to **Configure>Network>Interfaces >Settings** to configure the H_2A - High Availability interfaces. Select **EDIT** to modify an existing interface or select **NEW** to define a new interface. If you receive a **REQUIRES ACTIVATION CODE** statement, make sure you have entered the H_2A activation code.

Select the High Availability checkbox and enter the High Availability Virtual IP addresses and beacons.

Note

Not all network interfaces must be configured as High Availability interfaces. If you do not wish to use an interface for H_2A, leave the HIGH AVAILABILITY box unchecked. You can deselect a configured H_2A interface by enabling the DISABLE field.



Disable: □

Type: Standard

IP Address: 10.10.1.62/24

Options

DHCP: □

Gateway: □

High Availability: ☑

VLAN: □

Interfaces

Index	Name	Zone	NIC	Description
1	EXTERNAL	External	eth1	External Interface

High Availability

Name: HA-EXTERNAL

Description:

Virtual IP Address:

Beacon IP Addresses: 0.0.0.0 0.0.0.0 0.0.0.0

Figure 3.2: *Configuring an H_2A Interface*

Note

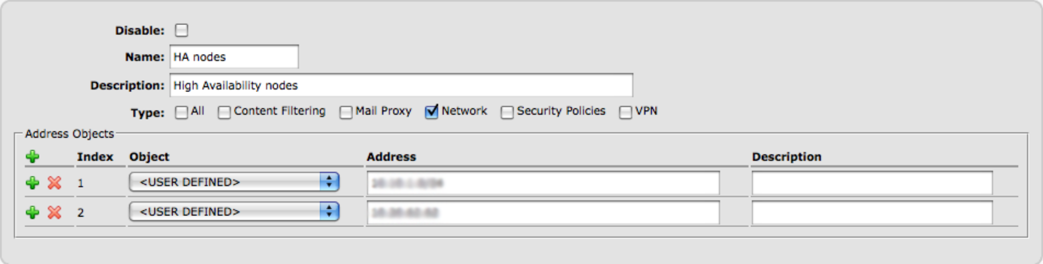
Imported Virtual IP must include a netmask.

Table 3.2: Configuring an H$_2$A Interface

Field	Description
Disable	Disables the H$_2$A interface.
Options	
High Availability	Check the High Availability box to configure the interface for High Availability.
High Availability	
Name	By default, the name will be `HA-X`, where ***X*** is the logical name assigned in the above settings.
Description	A brief description for the H$_2$A interface (e.g., `External HA Interface`)
Interface	The interface object, as defined in **Configure>Network>Interfaces>Settings**, that is being applied to the H$_2$A interface.
Virtual IP Address and Net Mask	Enter the virtual IP address and netmask that will be used for a given network interface.
Beacon IP Addresses	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.

Defining HA Nodes

Once the High Availability interfaces have been configured, define the High Availability nodes. To do so, navigate to **Configure>Objects>Address Objects** and select **EDIT** or **NEW**.



Disable: □

Name: HA nodes

Description: High Availability nodes

Type: □ All □ Content Filtering □ Mail Proxy ☑ Network □ Security Policies □ VPN

Address Objects

	Index	Object	Address	Description
	1	<USER DEFINED>	[redacted]	
	2	<USER DEFINED>	[redacted]	

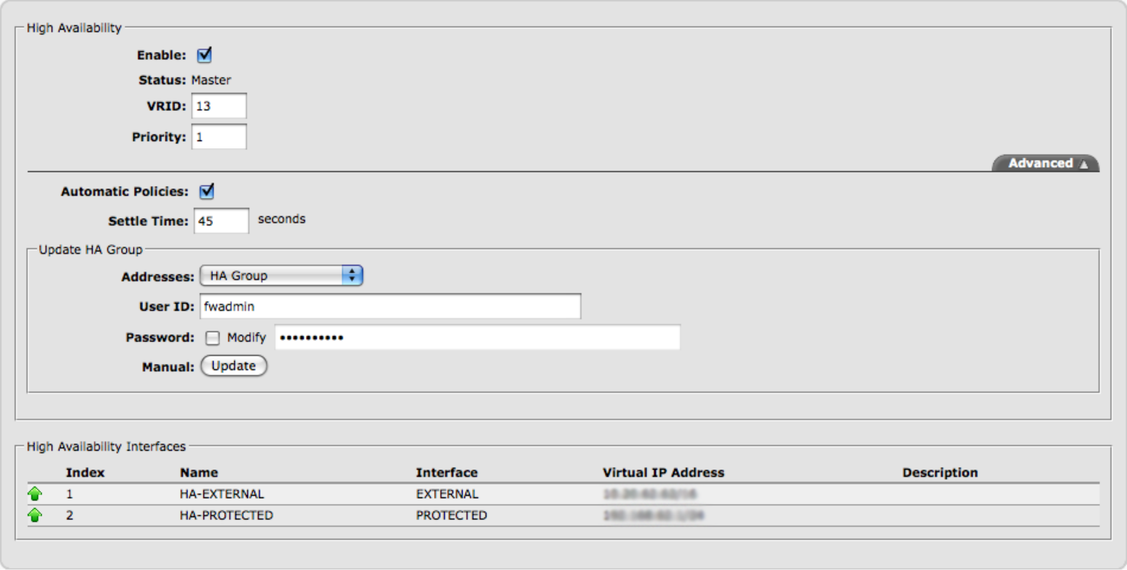
Figure 3.3: *Defining HA Nodes*

Select the HA Nodes object and enter both the logical and virtual IP address for all of the firewalls in the same VRID. Repeat this process for every HA node in the H$_2$A chain.

Once all interfaces have been entered, click **OK** and then **SAVE**. Once the H$_2$A - High Availability service has been enabled, the GTA firewall will automatically generate the required policies to allow all systems in the H$_2$A chain to communicate properly.

Configuring the H_2A - High Availability Option

Once the H_2A interfaces and nodes have been configured, configure the High Availability option by navigating to **Configure>Services>High Availability**.



High Availability

Enable: ☑

Status: Master

VRID: 13

Priority: 1

Automatic Policies: ☑

Settle Time: 45 seconds

Update HA Group

Addresses: HA Group

User ID: fwadmin

Password: □ Modify ••••••••••

Manual:

High Availability Interfaces

	Index	Name	Interface	Virtual IP Address	Description
⬆	1	HA-EXTERNAL	EXTERNAL	[redacted]	
⬆	2	HA-PROTECTED	PROTECTED	[redacted]	

Figure 3.4: *Configuring H_2A - High Availability*

Table 3.3: High Availability Fields

Field	Description
Enable	Enables the H_2A - High Availability feature.
Status	When H_2A has been enabled and configured, this field displays the firewall's current mode. See High Availability Modes for more information.
VRID	Virtual Router ID. Enter a value between 1 and 15. The VRID is used to identify the H_2A chain. Because of this, all firewalls that are to be placed in the same H_2A chain must share the same VRID.
Priority	Enter a priority value between 1 and 255. The firewall with the highest priority number will function as the master unit when operational.
Advanced	
Automatic Policies	A toggle to enable the firewall to generate an automatic set of policies to allow updates and accept HA Broadcast packets. Automatic policies use the HA node object and the GB-HA service group. Default is selected.
Settle Time	Settle time is used to control how long a firewall stays in a mode during HA transition before probing its beacons. This can be used to tune the firewall when it is connected to switches using Spanning Tree.
Update HA Group	
Addresses	A selection for a High Availability firewall or firewalls to update.
User ID	Enter the username for the system(s) to be updated.
Password	Enter or select to modify the system password.
Manual	Update button manual updates the HA group.

Configuring Firewall A

Complete the configuration of Firewall A using additional configuration data from your existing firewall. In addition, edit any configured IPSec Tunnels for the High Availability option. The configuration information from Firewall A will be transmitted to the other units in the H_2A chain after you have tested your new configuration.

Changing the Local Gateway for VPN Connections

After enabling the H_2A option and configuring your firewall, the Local Gateway in **Configure>VPN>Site to Site** must be edited to refer to the new HA interface. For example, if it previously pointed to **<External>**, the new Local Gateway may be **<HA-External>** (this is dependant on the HA interface's name).

Setting Up Firewall B

Setting up Firewall B requires completion of the same steps used to configure Firewall A. When configuring Firewall B, be sure to use the correct network information. For example, settings entered when defining Firewall A's HA interfaces will now be entered in Firewall B's HA Nodes address object. Defining additional configuration options is not necessary, since this information will be transmitted from Firewall A.

Testing Firewall A's Configuration

To test Firewall A's new configuration, remove or turn off any existing firewalls and then switch Firewall A from Test mode to Live mode. To do so, navigate to **Configure>Configuration>Apply.**

To prevent IP addresses conflicts, do not power on any previously existing firewall when Firewall A is operating in Live mode.

Network Configuration

Following the instructions in this chapter, the transition to the H_2A system should be transparent to end users, though some users may see a brief disconnect for long-lived connections.

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.

Transmitting the Master Firewall's Configuration

Once Firewall A has been tested to your satisfaction, switch Firewall B from Test mode to Live mode.

Updating the Slave Firewall(s)

To transmit all the configuration data you have entered into Firewall A to Firewall B, navigate to the UPDATE HA GROUP section (found in **Configure>Services>High Availability**) on the Firewall A.

Note

Updating the HA Group is only available when the master firewall is operating in Live mode.

Updating the HA Group will update configuration information on units in the H_2A chain. The administrator must have the firewall administrator's user ID and password of the standby (slave) firewall. The standby unit must have an administrative user account with the ADMIN permission enabled. (This is part of initial configuration of the firewall, as configured using the *GB-OS User's Guide*.)

Updating the HA Group does not change:

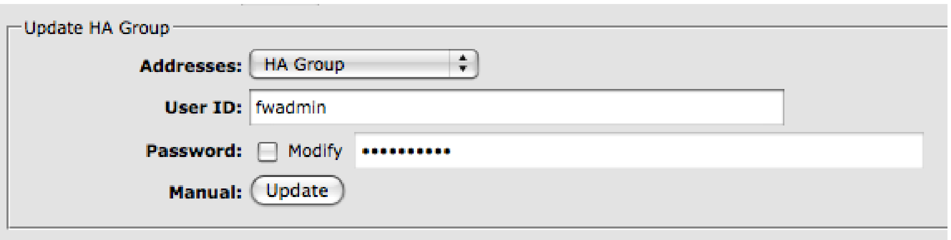
- Data on the **Configure>Network>Interfaces>Settings** screen.
- HA enabled interfaces
- Host name
- H_2A information (assuming H_2A has already been configured).

To Update HA Group:

1. Log on to master firewall and navigate to **Configure>Services>High Availability**.
2. Under the UPDATE HA GROUP section, select the address(es) of the systems to be updated.
3. Enter the administrative login credentials.
4. Click the UPDATE button to transfer configuration data from the master mode unit to the standby units. Updating will reboot the target firewall.

Note

Updating the HA Group can be used to update any firewall in the H_2A chain. However, for consistency, GTA recommends updating the lower priority firewalls from the highest priority firewall.



Update HA Group

Addresses: HA Group

User ID: fwadmin

Password: □ Modify ••••••••••

***Figure 3.5:** Updating the Slave Firewall*

Table 3.4: Updating the Slave Firewall

Field	Description
Addresses	The IP address of the slave firewall(es).
User ID	The slave firewall administrator's user ID.
Password	The slave firewall administrator's password.
Manual	Click the **UPDATE** button to update the HA Group.

Testing Fail-Over

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

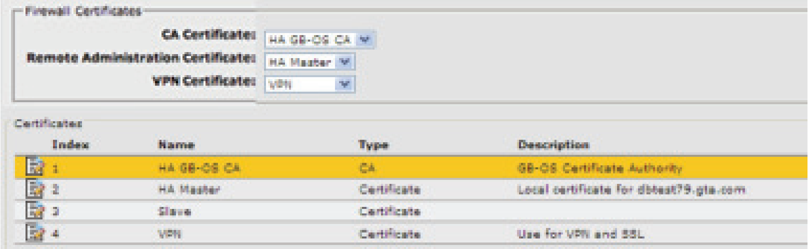
If the system performs satisfactorily on this final test, your H_2A system is up and running.

If you use remote administration on a non-standard port (not 443), include `:<port_number>` behind the firewall IP when updating the slave. For example: 192.168.71.254:`8080`

Certificates and High Availability

Each firewall must have a unique SSL certificate for web administration. However, the VPN certificate used for IPSec and SSL VPN Clients should be the same on both High Availability firewalls. Additionally, the firewalls should use the same GB-OS CA. To sync the certificates, perform the following:

1. On the Master firewall create the following certificates:
    a. GB-OS CA
    b. HA Master Certificate
    c. HA Slave Certificate
    d. VPN Certificate
2. Select the CA Certificate for the GB-OS CA.
3. Select the Remote Administration Certificate for the HA Master.
4. Select the VPN Certificate for the VPN.
5. Use the Update Slave function to push the certificates to the Slave firewall.
6. Login to the Slave firewall and select the HA Slave certificate for the Remote Administration Certificate.



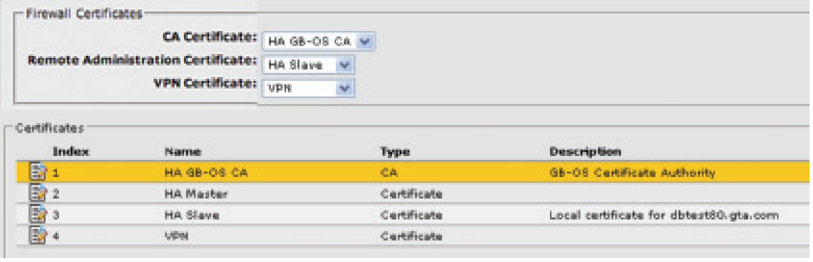
Firewall Certificates

CA Certificate: HA GB-OS CA
Remote Administration Certificate: HA Master
VPN Certificate: VPN

Certificates

Index	Name	Type	Description
1	HA GB-OS CA	CA	GB-OS Certificate Authority
2	HA Master	Certificate	Local certificate for dbtest79.gta.com
3	Slave	Certificate	
4	VPN	Certificate	Use for VPN and SSL

Figure 3.6: *HA Master Certificates*



Firewall Certificates

CA Certificate: HA GB-OS CA
Remote Administration Certificate: HA Slave
VPN Certificate: VPN

Certificates

Index	Name	Type	Description
1	HA GB-OS CA	CA	GB-OS Certificate Authority
2	HA Master	Certificate	
3	HA Slave	Certificate	Local certificate for dbtest80.gta.com
4	VPN	Certificate	

Figure 3.7*: HA Slave Certificates*

Both firewalls will now use the same GB-OS CA to create certificates and will share the same VPN certificate. Once the firewall configuration is synchronized, update the slave. If the roles are reversed, any updates to the certificates (adding/removing) will use the same CA.

For more information on creating and editing certificates, please see the *GB-OS User's Guide*.

Troubleshooting

Log messages, reports and activity snapshots are your first reference for general troubleshooting. This section contains useful troubleshooting procedures and frequently asked questions for solving firewall configuration errors.

Troubleshooting issues discussed in this chapter are specific to the H_2A - High Availability option. For all other troubleshooting issues regarding your GTA firewall, please refer to the *GB-OS User's Guide*.

Guidelines

GTA Support recommends the following guidelines as a starting point when troubleshooting network problems:

- Start with the simplest case of locally attached hosts.
- Use IP addresses, not names. Your problem could be DNS.
- Work with one network segment at a time.
- Verify your firewall system configuration by using **Configure>Verify**. The verification check is the best method of ensuring that your system is configured correctly. Correct all errors and warnings listed.
- Your first tests should be connectivity tests. Ping and traceroute are very useful tools for testing connectivity.
- Make sure the network cabling is connected to the correct network interface. Some useful guidelines are:
  - Verify the network interface numbers, MAC addresses and logical names listed on the **Configure>Network>Interfaces>Settings** screen.
  - Use the logical elimination method. Connect a network cable to the first network interface and use the ping facility to test for connectivity with a host on the desired network. If unsuccessful, move the cable to the next network interface and perform the test again. Repeat until successful, or all network interfaces have been tested.
  - Generate a Configuration Report. Check the report to ensure all your network devices have been recognized by the system at boot time.

Frequently Asked Questions

Q: I've just connected my H_2A system. Why I can't see the other unit (or units) in my H_2A chain?

Check that all the cables are connected properly and to the correct interfaces. Verify that all the interfaces in **Configure>Network>Interfaces>Settings** and **Configure>Services>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 H_2A chain have identical VRID numbers. This number identifies the members of the H_2A chain to one another.

Q: 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.

Q: I can't ping the other firewalls in my H_2A chain; when one unit tries to use the other as a beacon, it can't be reached.

It could be that one or all of your GTA firewalls are set to stealth mode. In accordance with ICSA standards, GTA Firewall UTM Appliances operate in stealth mode by default. If you would like to turn off stealth mode, navigate to **Configure>Security Policies>Preferences** and uncheck (disable) stealth mode on all firewalls in the your H_2A chain.

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

If you have two or more separate H_2A chains, make sure that the VRID numbers for each chain are unique (e.g., H_2A chain 1 = VRID 5; H_2A chain 2 = VRID 10). This allows High Availability systems to distinguish between firewalls in their own chain, and those in a separate chain.

Q: 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 IP addresses on your physical interfaces, the Default Gateway field in **Configure>Network>Interfaces>Settings** must be set to an IP address on your virtual network, otherwise the network cannot identify your interface.

Q: Why does my interface not appear in the High Availability section?

H_2A systems cannot use dynamically assigned (DHCP / PPP) interfaces. Only interfaces with static IP addresses can be configured for use with the H_2A option.

Q: What does the verification message; "WARNING: Configuration modified, slave not updated" mean?

The verification message means the firewall configuration has been modified but that the other firewalls in the HA group have not been updated with the change. To update the other firewalls in the HA group go to **Configure>Services>High Availability** section and update the HA Group when all modifications are complete.

Reference A: H_2A on Two Subnets

An alternative setup for H_2A 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 Installation and Configuration to configure **Configure>Network>Interfaces>Settings** and **Configure>Services>High Availability**.

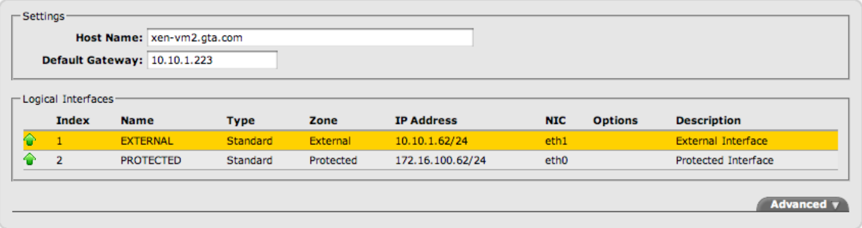
Configuring Firewall A

H_2A can be configured to use different networks for the configuration IP address and H_2A IP addresses. Using different networks, the administrator can configure the firewall to use RFC 1918 (private) IP address on the external network interface, so that only H_2A 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.



Settings

Host Name: xen-vm2.gta.com

Default Gateway: 10.10.1.223

Logical Interfaces

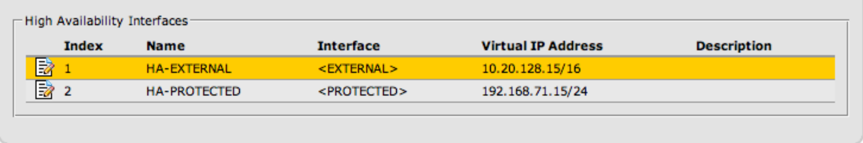
Index	Name	Type	Zone	IP Address	NIC	Options	Description
1	EXTERNAL	Standard	External	10.10.1.62/24	eth1		External Interface
2	PROTECTED	Standard	Protected	172.16.100.62/24	eth0		Protected Interface

Figure A.1: *Network Settings Using Private (RFC 1918) IP Addresses*

H_2A 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 Figure A.2 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).



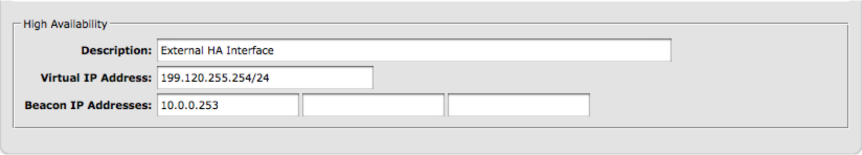
High Availability Interfaces

Index	Name	Interface	Virtual IP Address	Description
1	HA-EXTERNAL	<EXTERNAL>	10.20.128.15/16	
2	HA-PROTECTED	<PROTECTED>	192.168.71.15/24	

Figure A.2: *H_2A Configuration*

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.



High Availability

Description: External HA Interface

Virtual IP Address: 199.120.255.254/24

Beacon IP Addresses: 10.0.0.253

Figure A.3: *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.

Note

For more information on configuring static address mapping, see the *GB-OS User's Guide*.

Two Subnets Example

Continue the configuration and testing of your High Availability configuration using the instructions in Installation and Configuration and the example below.

Table A.1: Two Subnets Example

System	Setting
Router	199.120.225.253, 10.0.0.253
Firewall 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
H$_2$A Configuration	
VRID	14
Priority	20
H$_2$A External	
Virtual IP Address	199.120.225.254/24
Beacons	10.0.0.253
H$_2$A Protected	
Virtual IP Address	192.168.71.253/24
Beacons	192.168.71.1, 192.168.71.2, 192.168.71.3
Firewall B (Lower Priority)	

Table A.1: Two Subnets Example

System	Setting
External IP Address	10.0.0.252/24
Protected IP Address	192.168.71.252/24
Default Gateway	10.0.0.253
H_2A Configuration	
VRID	14
Priority	10
H_2A External	
Virtual IP Address	199.120.225.254/24
Beacons	199.120.225.253
H_2A Protected	
Virtual IP Address	192.168.71.253/24
Beacons	192.168.71.1, 192.168.71.2, 192.168.71.3

Reference B: Upgrading an Existing GTA Firewall to High Availability

This section illustrates how to add a second firewall to your network and upgrade your existing H_2A-capable GTA firewall to High Availability. These instructions can also be used when upgrading two existing GTA firewalls to an HA configuration.

To set up your H_2A system, leave the existing GTA firewall in place and configure the new GTA firewall.

Set up the new GTA firewall in its factory default configuration using the instructions in the *GB-OS User's Guide*, then upload your existing configuration onto the new firewall.

Updating the New Firewall's Configuration

Export the existing GTA firewall's configuration so that it may be uploaded to the new GTA firewall using the instructions below.

1. Open a Web browser and connect to the existing GTA firewall's Web interface.
2. Navigate to **Configure>Configuration>Import/Export**.
3. Select the Live radio button, and then click the **Download** button. Save the existing firewall's configuration in an easy to remember location, such as the desktop.
4. Next, log in to the new GTA firewall's Web interface and navigate to **Configure>Configuration> Import/Export.**
5. Select the Test radio button, and browse the configuration file's location.
6. Under the Preserve Section, select the Activation Codes radio button to preserve the codes while importing the configuration.
7. Select the **Upload** button to upload the configuration.

CAUTION

If you do not preserve the activation codes, you must re-enter the new firewall's serial number and activation codes after the existing firewall's configuration has been uploaded, since this will have been overwritten.

The new GTA firewall will have now have the existing firewall's configuration uploaded to it's Test mode configuration. To apply the Test mode to the Live mode configuration, navigate to **Configure>Configuration>Apply**, select the Apply Test Configuration and then the **Submit** button.

Editing the New Firewall's Configuration

After updating the new firewall's configuration, re-connect to the new firewall using the existing firewall's protected network IP address.

Using the instructions in Installation and Configuration, configure the **Configure>Network>Interfaces> Settings**, **Configure>System>Contact Information** and **Configure>Services>High Availability** screens. Make this firewall your designated master unit by giving it the higher priority number.

Verify that any security policies, tunnels and objects which previously referenced the EXTERNAL interface object now use the HA-EXTERNAL object.

Typically, a GTA Firewall uses the external IP address when performing services such as DNS lookups, email alarms, Web Filtering registration verification and network time. 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 Installation and Configuration.

Configuring the Existing Firewall

With your new GTA firewall in place on your network, you can now connect the old firewall to an isolated network and edit the configuration using the instructions in Installation and Configuration to configure the existing firewall as the H_2A chain's slave firewall.

Assign a lower priority number to this GTA firewall to make it the designated slave firewall.

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 GTA firewall. Once the unit is in place and you have verified the new configuration, test fail-over by turning the master firewall off.

If this final test is successful, your H_2A system is up and running.

Reference C: Log Messages

GB-OS uses WELF formatted log messages by default.

HA Updated from Web Interface

```
Dec 11 21:58:23 fw.gta.com id=firewall time="2006-12-11 21:58:23" fw="Firewall A" pri=5
msg="WWWadmin: Update of 'High Availability'." type=mgmt src=192.168.71.12 srcport=3162
dst=192.168.71.254 dstport=443
```

Switch to MASTER MODE

```
Dec 9 18:55:58 fw.gta.com id=firewall time="2006-12-09 18:55:58" fw="Firewall A" 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="2006-12-09 18:55:52" fw="Firewall A" 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="2006-12-11 21:58:23" fw="Firewall A" 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 config file, must be 0..255"
type=mgmt
```

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

```
id=firewall time="2006-12-30 10:35:43" fw="Firewall A" 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="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HApinger: Exiting."
type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Exiting." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Removed IP address
192.168.71.78 /32 from interface fxp0." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Updated MAC address
for interface fxp0 to 00:d0:68:00:09:58." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Removed IP address
10.254.254.81/32 from interface fxp1." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Updated MAC address
for interface fxp1 to 00:d0:68:00:09:59." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=6 msg="NAT: Default address for
interface fxp1 set to 10.254.254.80." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=6 msg="NAT: Default address for
interface fxp0 set to 192.168.71.80 ." type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="WWWadmin: Removing
static routes." type=mgmt src=192.168.71.12 srcport=2453 dst=192.168.71.80 dstport=443

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=6 msg="WWWadmin: Adding static
routes." type=mgmt src=192.168.71.12 srcport=2453 dst=192.168.71.80 dstport=443

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" 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="2006-12-30 10:35:43" fw="Firewall A" pri=6 msg="alarms: Reinitializing."
type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HA: Starting."
type=mgmt

id=firewall time="2006-12-30 10:35:43" fw="Firewall A" pri=5 msg="HApinger: Starting."
type=mgmt
```

```
id=firewall time=”2006-12-30 10:35:43” fw=”Firewall A” pri=5 msg=”alarms: Server ready.”
type=mgmt

id=firewall time=”2006-12-30 10:35:43” fw=”Firewall A” pri=4 msg=”HA: Switching to init
mode, Starting.” type=mgmt

id=firewall time=”2006-12-30 10:35:43” fw=”Firewall A” pri=6 msg=”alarms: Email not
enabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:43” fw=”Firewall A” pri=6 msg=”alarms: Enterprise
server not enabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp1 set to 10.254.254.80.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp0 set to 192.168.71.80 .” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=6 msg=”HAstateChange: Adding
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Default
route set to 10.254.254.1.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
old objects .” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘ANY_IP’.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘Protected Networks’.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘EXTERNAL’.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘PROTECTED’.” type=mgmt

id=firewall time=”2006-12-30 10:35:44” fw=”Firewall A” pri=4 msg=”alarms: WARNING: email
not enabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=4 msg=”HA: Switching to slave
mode, beacons ok.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp1 set to 10.254.254.80.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp0 set to 192.168.71.80 .” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=6 msg=”HAstateChange: Adding
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Default
route set to 10.254.254.1.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
old objects .” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘ANY_IP’.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘Protected Networks’.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘EXTERNAL’.” type=mgmt

id=firewall time=”2006-12-30 10:35:51” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘PROTECTED’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=4 msg=”HA: Switching to master
mode, no higher priority ‘master’ found.” type=mgmt
```

```
id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HA: Updated MAC address
for interface fxp0 to 00:00:5e:00:01:25.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HA: Added IP address
192.168.71.78 /32 to interface fxp0.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HA: Updated MAC address
for interface fxp1 to 00:00:5e:00:01:24.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HA: Added IP address
10.254.254.81/32 to interface fxp1.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp1 set to 10.254.254.81.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=6 msg=”NAT: Default address for
interface fxp0 set to 192.168.71.78 .” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=6 msg=”HAstateChange: Adding
static routes.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Default
route set to 10.254.254.1.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Removing
old objects .” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘ANY _ IP’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
address object ‘Protected Networks’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘EXTERNAL’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add
interface object ‘PROTECTED’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add HA
interface object ‘EXTERNAL’.” type=mgmt

id=firewall time=”2006-12-30 10:35:57” fw=”Firewall A” pri=5 msg=”HAstateChange: Add HA
interface object ‘PROTECTED’.” type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=5 msg=”HAstateChange: Gateway
selector disabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=6 msg=”alarms: Reinitializing.”
type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=6 msg=”gblogd: Reinitializing.”
type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=5 msg=”alarms: Server ready.”
type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=6 msg=”alarms: Email not
enabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=5 msg=”HAstateChange: Stopping
NTP service.” type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=6 msg=”alarms: Enterprise
server not enabled.” type=mgmt

id=firewall time=”2006-12-30 10:35:59” fw=”Firewall A” pri=5 msg=”HAstateChange: Setting
internal DNS servers to 192.168.71.9.” type=mgmt
```

Copyright

Technical Support

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

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

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

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

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

Trademarks & Copyrights

GB-OS and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

Some products include software developed by the OpenSSL Project (http://www.openssl.org/)..

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3361 Rouse Rd, Suite 240 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • **Fax**: +1.407.380.6080 • **Web**: http://www.gta.com • **Email**: info@gta.com