



Whether your organization is operating an e-business platform that requires an ever present, safe and secure web site, or transferring, storing and processing electronic information across the Internet, or both, the single most important product you will require is a firewall. Specification of the appropriate product to provide a best fit with your organization's requirements is the key to success. Will it integrate with your network infrastructure? Will it enable you to implement your security policy effectively? There are many questions to be posed and answered if the product you install is to provide your organization with an effective defense against unwanted intrusion.

The GNAT Box Firewall system, which was the first incarnation of the GB-1000, was first introduced in 1996. Its popularity stemmed from the fact that it was simple to install, was booted and run from a single 3.5" floppy disk, and offered excellent value for money. While the GB-1000 Firewall Appliance would be unrecognizable to users of the original product, it has maintained its affordability and performance advantages in the marketplace.

Standard features include an unlimited user license, IPsec VPN capability, four high-speed 10/100 Ethernet interfaces, DHCP server, DNS server and encrypted remote management. These features, when combined with the ability to maintain over 32,000 concurrent sessions, make the GB-1000 a powerful product. Expansion options such as gigabit Ethernet, token ring, FDDI and fiber-based Ethernet are available. The GB-1000's engine is the ICSA certified GNAT Box firewall software. The more astute buyers of these products will research active operational installations in the marketplace and be reassured to find tens of thousands of sites, ranging from small businesses to multinationals, using this engine.

The GB-1000 houses a standard PC with a 660MHz Intel Celeron processor, 64Mb RAM and 16Mb of flash memory housed in a slimline, 1U-high case. There are four network interfaces, two of which are used for the protected and external networks respectively. The other two network interfaces can be defined as any of the three network types (Protected, External or PSN). These do not need to be configured during setup as only the external and protected network interfaces are required for initial configuration and testing of the GB-1000.

The use of standard operating systems within firewalls remains common. These operating systems are, of course, built to support many services outside the security function and, of necessity, do not focus on security to the exclusion of other functions. This may offer a secondary target to intruders unable to find a path through the firewall itself. The simple, easy-to-use, Windows interface is the front end to a proprietary operating system built specifically to operate the firewall and associated security functions.

An ever-increasing requirement for companies seeking to provide increased customer service across the Internet is the ability to host secure 'public' servers. This demilitarized zone

GB-1000 Firewall Appliance



by Michael Dickerson

Supplier: Global Technology Associates, Inc.

Price: on application

Contact: +1-407-380-0220

FAX +1-407-380-6080

info@gta.com

www.gta.com

FOR Excellent features and functionality coupled with unlimited licenses for large networks.

AGAINST None.

VERDICT Easy to install, configure and use. Provides organizations with a powerful firewall solution.

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★★
Overall Rating	★★★★★

(DMZ) can be provided by one or both of the two network interfaces available for such use in the GB-1000.

To install the GB-1000 administrators will need to connect the system to the local area network (LAN) and configure network settings to match the address scheme of the LAN. The GNAT Box system provides three user interfaces: console interface, web browser interface and GBAAdmin interface. The system used for testing purposes was a Windows NT 4.0 installation which enabled the use of the GBAAdmin interface on the administrator workstation (Windows 95, 98 and 2000 also support this interface). The IP address of the workstation needs to be changed to the same network as the GB-1000 to allow configuration.

The GBAAdmin interface is used as an offline configuration facility in the first instance but can be used as an online remote management client. All data transfers to the appliance are encrypted. There is a scrolling main menu which provides access to the nine configuration areas. These

are: basic configuration, authorization, routing, filters, IP pass-through (this means no network address translation is applied), NAT, runtime, reports and system activity. Each area contains menu items and status indications and offers a simple, methodical process of configuration. The heart of the system is GTA's network address translation (NAT) and stateful packet inspection engine. The stateful packet inspection facility monitors every IP packet passing through the system to ensure that NAT is performed for all packets passing through the system outbound. Only valid response packets or packets passing through user-defined tunnels (virtual private network functionality) are allowed to reach hosts on the protected or PSN networks from the external network (typically the Internet).


The console interface is a simple GUI-based tool consisting of hierarchical menus and pop-up boxes. Whilst this interface can be used to perform all configuration tasks it is best used for initial configuration and as a backup to the other interfaces.

The web browser interface allows remote administration using a frames-capable browser such as Microsoft Internet Explorer (version 3.0 or higher) or Netscape Navigator. It is possible to disable this facility or set it to a read-only mode which disallows remote updating. I found the web browser interface to be a slightly less effective management tool than the GBAAdmin interface, which is likely to be a reflection of the fact that most detailed configuration will take place onsite using the GBAAdmin interface. Checks and minor alterations are likely to be managed remotely through the web browser interface.

The GB-1000 includes a virtual private networking (VPN) facility as a standard system feature and is based on the IPsec standard using the tunnel mode. The VPN facility provides secure, encrypted data transfer between two discrete networks and requires three areas of configuration. Firstly a security association (SA) must be in place and configured. Secondly the system requires at least one remote access filter that will accept a VPN connection from the remote side of the VPN gateway. Lastly an IP pass-through filter that allows outbound access on the defined VPN is required. This should be implemented in accordance with organizational security policy.

GB-1000 now has a built-in http content-filtering facility (CyberNOT). This facility is activated by purchasing an annual license subscription. The content filtering facility operates with the traditional or transparent proxy mechanisms. CyberNOT features include 12 different categorizations, a database automatically updated on a weekly basis, daily updates downloadable though CyberNOT subscription. The service now contains over 3 million URLs gained by research in many languages. GB-1000 also integrates with the market leading URL control tool, Websense. This is an automated database of known inappropriate websites

Recommending the GB-1000 is not a difficult decision. Global Technology Associates have produced an upgraded system that rectifies a great number of problems apparent in earlier versions, but have also managed to add significant features. Care has been taken to retain its ease of use, allowing administrators an effective management tool that will provide operational benefits quickly. A hidden cost to unwary buyers is expensive licensing arrangements whereby an organization must include all the nodes on their network regardless of those who actually utilize the firewall. The GB-1000 has a simple unlimited user license which means huge potential savings to organizations with large networks.

The GB-1000 firewall appliance looks firmly set to build on the success of its predecessors and provide an easy-to-use, feature-rich firewall. 

Contact Information:



Global Technology Associates, Inc.
3505 Lake Lynda Dr., Ste. 109
Orlando, FL 32817
+1-407-380-0220 +1-407-380-6080 fax
info@gta.com www.gta.com