



Firewall Product Functional Summary

1. Product Version

Vendor Name: Global Technology Associates, Inc.

Product Version: GNAT Box Firewall System Family, Version 3.2.5

Date of Publication: 28 May 2002

2. Executive Overview

Global Technology Associates' GNAT Box Firewall System Family of firewalls is based on the GNAT Box System Software - the original cost effective Internet firewall system. Introduced in 1996 with a sub \$ 1,000 price and an unlimited user license, the GNAT Box Firewall System led the way defining a new class of firewall systems. Unlike many of its newly arrived imitators the GNAT Box Firewall System is a fully capable firewall, and is not limited in functionality. The GNAT Box Firewall System was truly a revolutionary firewall product that was built around the concepts of simplicity, power and affordability. The GNAT Box Firewall System software is a totally self-contained system, which integrates both an operating system and innovative hybrid firewall technology into a single high performance compact system. The GNAT Box Firewall System is available in several different forms: 1) The GNAT Box Pro, GTA's classic software only based system where the entire runtime system boots off and is totally contained on a single 3.5" 1.44Mb floppy diskette. 2) The GB-Flash GNAT Box Firewall System, where the GNAT Box Firewall System software is delivered pre-installed on a 16Mb flash module that the user installs in his own hardware. 3) The GB-1000 Firewall/VPN Appliance, where the GNAT Box Firewall System software is delivered as a self-contained firewall appliance designed for medium to large enterprise with need for unlimited users licenses and options like High Availability. 4) The RoBoX Firewall Appliance, where the GNAT Box Firewall System software is delivered as a self-contained firewall appliance designed for remote or branch offices needed 25 or fewer concurrent user licenses.

The GNAT Box System is a comprehensive firewall system that prevents unauthorized access from the untrusted network, completely hides your internal network, and provides transparent network access to users on the protected hidden network. The system utilizes stateful packet inspection and application firewall techniques combined with a powerful network address translation system. Unlike some firewall systems, the GNAT Box provides the user with complete transparent network access to external and private service networks for TCP, UDP, and ICMP based applications. In addition, the system supports transparent network access for unusual application protocols such as: FTP, Archie, gopher, RealAudio/RealVideo, StreamWorks, VDOLive, CU-SeeMe, VXtreme, Vosaic, NTT AudioLink, NTT SoftwareVision, Apple Quicktime Streaming protocol, Microsoft Netmeeting and RTSP-based applications. The GNAT Box Firewall System also includes a built-in IPsec VPN.

The system is managed either from a simple, easy-to-use, GUI console interface or remotely from either a web browser client or from a Windows client. Since the GNAT Box System has very minimal hardware requirements and is highly efficient in operation, many organizations can utilize existing or seemingly outdated hardware. The system is supplied on all products excluding the RoBoX Firewall Appliance with an unlimited license, making the GNAT Box System Software family of firewalls ideal for organizations of all sizes. The GNAT Box System Software family of firewalls is the price/performance market leader.

3. Overview of firewall product functional summary program

3.1. Scope and purpose of firewall product functional summaries

The purpose of the firewall product functional summary program is twofold:

- To provide a structured format in which vendors can describe the distinguishing features and advantages of their products
- To provide a structured format from which potential firewall customers can compare and contrast the features and design principles of firewall products

The summary format used in the program has been derived through an open process including firewall vendors, agencies of the computer security community, and the firewall customer community. This cooperative effort is a voluntary program.

3.2. Security and design principles

When designing computer security systems, as with other mission critical systems, it is important that the basic design principles of the system be sound, and that the implementation be of high quality. When choosing a computer security system, it is important for the customer to be able to judge the capabilities and design principles of the system in terms of the protections required by that customer's intended deployment of the system. The functional summary program permits computer security product manufacturers to present their products and designs in the best possible light, while adhering to a format that encourages accurate product comparison. The summary format requests information from the vendor about design decisions made in a number of important areas, yet tries to permit the response to be as free-form as necessary so as not to constrain the vendor within the bounds of a narrow definition of what constitutes a "firewall."

3.3. Terms and definitions

Since the network security field is dynamic and rapidly growing, new techniques and terms are constantly being brought into use. To provide a basis for clear communication, a simple glossary of terms and definitions is provided as a part of the summary format. Vendors are welcome to define their own terminology, distinct from the terms in the glossary, but are requested to provide definitions in the glossary section for new terminology that is coined, and to annotate them as such. Readers of this document are encouraged to peruse the glossary section for annotations and definitions of such new terms as may appear.

4. Product Overview

The GNAT Box Firewall System is a revolutionary firewall product family; a totally self-contained network security solution that is simple to install and operate. The GNAT Box Firewall System is a turnkey system that runs either on customer supplied Intel-based hardware or on a GNAT Box appliance such as the GB-1000 Firewall Appliance. The network security system and the operating system are an integrated package, so the GNAT Box System software is not installed on top of an existing operating system, but rather is the operating system.

Self-Contained Single Function

The GNAT Box Firewall System's self-contained approach has many advantages over other systems that are installed on top of existing operating systems. First and foremost, the GNAT Box Firewall System software has a single function: security. It's not clutter with other non-security applications that can possibly have a detrimental effect on security. A single self-contained approach makes the GNAT Box System simpler than overly burdened complex systems. As complexity increases, the possibility that bugs and security holes can be exploited increases, often in an exponential manner. Installing a security application on an existing operating system can be problematic. Today, the many variations in standard operating systems,

with their updates, patches and version releases, makes it is quite likely that the security software installed on such a system may have security compromises from the day it is installed. Systems that rely on standard operating systems put the burden on the administrator. The administrator must have the most current patches, updates and releases installed and configured in order for the security software to function properly. The GNAT Box System does away with this problem by providing a total solution; operating system and firewall in one package.

Hybrid System

The GNAT Box System is a hybrid firewall. It combines stateful packet inspection, application firewall techniques and network address translation to provide a robust, high performance network security system. The system melds the network security functionality into the operating system, thus keeping all firewall functions always loaded in memory. This means that the latency associated with swapping and the loading and unloading of specific applications never occurs on the GNAT Box System. The result is high performance. It's well documented that application and proxy-based firewalls suffer greatly due to the large latency overhead. They also generally demand large expensive hardware platforms in an attempt to solve this design flaw. Their approach is "get a bigger hammer." The GNAT Box System approach is "get simple and smart."

Network Address Translation

The GNAT Box System completely hides the internal protected network from the external unprotected network. The network address translation feature dynamically translates an unlimited number of unregistered IP addresses into a single registered IP address on the external network. The GNAT Box System also provides a facility to implement a static network address translation scheme if desired. The GNAT Box System fully supports RFC-1918 addressing schemes.

Simple

The GNAT Box System is simple to install, configure and operate. The system software can be installed and configured in just a few minutes. You don't have to be a Unix guru or an NT expert, because there are no drivers to install, no complex operating system to configure and no expensive hardware to purchase. The GNAT Box System provides three GUI user interfaces, one for local use on the system console and the others for remote administration. The system is remotely managed and administered via a web browser from your favorite environment be it NT, Windows95, Macintosh or Unix or via a Windows 98/NT client.

Powerful

The GNAT Box System is a powerful high performance system supporting over 32, 000 concurrent connections on GTA firewalls with unlimited users and 10,000+ on the RoBoX Firewall Appliance. The system is completely transparent for standard TCP, UDP and ICMP applications. In addition, GNAT Box supports many hard to handle applications such as: RealAudio/Video, Vxtreme, Vosaic, VDOLive, StreamWorks, CU-SeeMe, NTT SoftwareVision, NTT AudioLink, Apple Quicktime Streaming, Microsoft Netmeeting and RTSP applications.

Affordable

The GNAT Box System is the most cost-effective firewall family on the market today. Its low price, unlimited user license, and minimal hardware requirements make it a clear winner. Moreover, with the GNAT Box System you eliminate the need for expensive administrative overhead. No other firewall family comes close to delivering the price to performance of the GNAT Box Firewall System family.

The GNAT Box System has minimal hardware requirements. Given of its highly efficient design, the GNAT Box System can utilize hardware that may be considered too slow or obsolete for today's demanding desktop environments. The system supports 10 and 100 Mbps Ethernet, Gigabit Ethernet, Token Ring, FDDI (UTP, SAS and DAS), PPP ISDN, PPP Async modems. The system does not use a hard disk drive, so there's no chance of a disk crash or any need for costly backup equipment. The GNAT Box System's total "in memory" design means that power outages or accidental shutdowns will not

damage or corrupt the system.

Required Hardware

The GNAT Box Firewall System is available in three different forms: software only, software installed on a flash memory module and as a self-contained firewall appliance. All three forms utilize the same GNAT Box Firewall System software and offer the same level of security. However, the flash module and appliance form factors offer additional value added services not found on the standard system.

GNAT Box Pro

The GNAT Box Pro system fits entirely on and boots off a 3.5" floppy diskette. No hard disk is required or utilized.

Hardware Requirements

Intel or compatible 486, Pentium or Pentium Pro CPU

ISA or PCI based system

16 Mbytes RAM (minimum)

1 1.44 Mbytes 3.5" floppy diskette drive

2 Network cards (minimum)

1 Basic VGA display adapter

1 Parallel Port 1 CRT*

1 Keyboard**

* Not required for operation.

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

Optional System Hardware Components

1 Additional network card for Private Service network (PSN)

1 Serial Port - COM 1-4 (1645x/16550 UARTs only)

1 Async Modem (external or internal) for PPP connections

1 ISDN TA (external) with RS-232 interface for PPP connections

GB-Flash GNAT Box Firewall

The GB-Flash product is the GNAT Box Firewall System software delivered on a single 16Mb CompactFlash memory module. The flash memory module is inserted into an adapter card and connected to the primary IDE disk controller on the system motherboard. The GB-Flash product is identical to the GNAT Box Pro product, however it offers additional functionality in the form of: a built-in DNS server, a built-in DHCP server and the addition of IKE to the IPSec VPN.

Hardware Requirements

Intel or compatible 486, Pentium or Pentium Pro CPU

64 Mbytes RAM (minimum)

IDE disk controller interface

1 1.44 Mbytes 3.5" floppy diskette drive

2 Network cards (minimum)

1 Basic VGA display adapter

1 Parallel Port 1 CRT*

1 Keyboard**

* Not required for operation.

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

Optional System Hardware Components

1 Additional network card for Private Service network (PSN)

- 1 Serial Port - COM 1-4 (1645x/16550 UARTs only)
- 1 Async Modem (external or internal) for PPP connections
- 1 ISDN TA (external) with RS-232 interface for PPP connections

GB-1000 Firewall/VPN Appliance

There are no hardware requirements for the GB-1000 Firewall/VPN system since it is a totally self-contained firewall appliance. The GB-1000 has the following hardware characteristics:

- 4 10/100 high-speed Ethernet interfaces
- 1 DB-9 serial interface for the console
- 1 DB-9 serial interface for modem/pager use or ISDN TA connections
- 1 USB port
- 1 feature expansion slot (Gigabit Ethernet, Token Ring, or fiber Ethernet)

RoBoX Firewall Appliance

There are no hardware requirements for the RoBoX Firewall Appliance system since it is a totally self-contained firewall appliance. The RoBoX has the following hardware characteristics:

- 3 10/100 High-speed Ethernet Interface
- 1 DB-9 serial interface for the console

5. Vendor information

Global Technology Associates, a privately owned, US corporation, and developer of Internet Firewalls celebrates 10 years of business success in 2002. Since 1994, GTA has been an innovator in the Internet firewall field. With the introduction of the compact, cost-effective GNAT Box firewall in 1996, GTA was the vanguard leader in bringing firewalls to the small and medium size marketplace.

Products include a range of firewall products for all sizes of networks: from the GB-1000 Firewall/VPN rack-mount appliance for larger networks, and the new RoBoX desktop appliance for remote offices, to our software based GNAT Box Pro and GB-Flash offering flexible configuration options. All firewalls are powered by the GNAT Box System Software – simple, powerful, affordable.

5.1. Contact Information:

Contact name: Global Technology Associates, Inc.
Contact Business Hours: 8:30AM - 6PM EST
Contact telephone number: +1.407.380.0220
Contact FAX number: +1.407.380.6080
Contact Email address: info@gta.com
Contact Web URL: <http://www.gta.com>
Contact postal address: 3505 Lake Lynda Drive
Suite 109
Orlando, FL 32817

6. Product security architecture

6.1. Rationale

When describing a networked computer security system, there are several aspects of its design that must be taken into

consideration. A security system, such as a firewall, must be able to protect not only the systems connected to it; it must be able to protect itself. Generally, the mechanisms whereby this is accomplished are different. The firewall system's security is dependent on whatever security mechanisms the firewall has built into itself. The systems connected to the firewall's security are dependent on whatever security mechanisms the firewall provides to them. In some cases these mechanisms may be based on a common design feature. In others they may be a result of a combination of features. In this section we explain how the firewall protects itself and the systems connected to it. In cases where additional protections are provided, or additional protective relationships are provided, we will explain the design principles and operation of these protective relationships.

6.2. Security Architecture

The GNAT Box System is a totally self-contained network security solution that does not rely on any operating system. The network security system and the operating system are an integrated package, so the GNAT Box System is not installed on top of an existing operating system, but rather is melded into the operating system.

GNAT Box Terms and Concepts

External Network

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

Protected Network

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

Private Service Network

The Private Service network (PSN) (also often known as a DMZ network) is an optional service network that is located logically between the External network and the Protected network. The PSN isn't actually between the Protected and External networks, but nearly at a peer level with the Protected network. The PSN, however, is untrusted by the Protected network and by default no unsolicited packets are allowed to pass from the PSN to the Protected network. All hosts on the PSN are hidden from the External network, but completely accessible from the Protected network. The PSN is used in conjunction with the Tunnel facility to allow external access to hosts and services, such as web servers, FTP servers, email server, etc. By tunneling to a server on the PSN, an organization can allow public access to services while maintaining network security for the Protected network. To create a PSN, configure and/or add a third supported network interface to your GNAT Box System firewall. Since the PSN is hidden, unregistered IP addresses can be utilized.

Network Interface

A GNAT Box System network interface can be any supported network interface/card operating at any supported speed and utilizing any supported network topography. The GNAT Box System can operate with a combination of different network cards, thus performing network bridging functions between dissimilar networks.

External Network Interface

The External network interface is the network interface card that is attached to the External network. The External network interface requires a registered or legitimate IP address; only one registered IP address is required for the GNAT Box System. The External network interface can have up to 100 IP addresses using IP Aliasing.

Protected Network Interface

The Protected network interface is attached to the Protected network. The Protected network interface does not require a registered IP address (RFC 1918 addresses are recommended). The IP Aliasing Facility may be used on the Protected network interface.

Private Service Network Interface

The Private Service network (PSN) interface is optional. However, if you plan to offer public access to servers, such as a web server, it is highly recommended that you install a PSN interface. For many configurations of the GNAT Box System a PSN may not be required, such as on intranets or for outbound access only. The PSN interface does not require a registered IP address (RFC 1918 addresses are recommended). The IP Aliasing may be used on the PSN interface.

Eight Basic GNAT Box Concepts

1. Outbound packets originating from the Protected network can pass transparently through the GNAT Box to the External network and return.
2. Outbound packets originating from the Protected network can pass transparently through the GNAT Box to the PSN and return.
3. Outbound packets originating from the PSN can pass transparently through the GNAT Box to the External network and return.
4. Unsolicited packets arriving on the External network interface are blocked.
5. Unsolicited packets arriving on the PSN network interface, destined for the Protected network are blocked.
6. Packets originating from the External network may be directed to an IP address/Port combination on the PSN when an appropriate GNAT Box Tunnel and Remote Access Filter are in place.
7. Packets originating from the External network may be directed to an IP address/Port combination on the Protected network when an appropriate GNAT Box Tunnel and Remote Access Filter are in place.
8. Packets originating from the PSN may be directed to an IP address/Port combination on the Protected network when an appropriate GNAT Box Tunnel and Remote Access Filter are in place.

6.3. Product default operations

The GNAT Box System is based on the implicit rule, “That which is not expressly permitted is denied.” This rule applies to both inbound and outbound packets. Therefore, if all filters were to be deleted this implicit rule would still be operational for both inbound and outbound filters, thus disallowing packet flow both inbound and outbound.

GNAT Box can easily be configured in a few minutes, the administrator needs only to supply the IP addresses and netmasks of the network interfaces and the default route. The system’s default filters are generated based on the IP addresses supplied by the system administrator. These filters are configured to block all inbound connections and allow outbound connections from the internal protected and private service networks.

By default the GNAT Box will log all packets that are rejected, and all outbound sessions upon the connection termination.

6.4. Protection of the firewall system

The GNAT Box System is a dedicated security system. It is not a general purpose computing platform, so services other than the admin user interface are offered on the system. Additionally:

- There is no command shell.
- There are no user accounts on the system.
- The admin user interface is protected with an account and password.
- The remote administration interface can be disabled, only allowing system administration from the local console.
- Update capability can be disabled for the remote administration interface, thus only allowing a browse capability.
- By default only hosts on the protected network are give access to the remote administrative interface.

6.5. Protection of attached networks and hosts

The GNAT Box System completely hides all IP addresses on the internal protected network and private service network (if one exists). Not only are these IP addresses hidden, but even if the addresses were known to a user on the external network, they would be inaccessible, because by default the GNAT Box System does not accept any unsolicited connections from the external network. Hosts on the protected and private service networks can transmit packets to the external network and receive replies to these packets transparently without revealing their IP addresses or compromise their security. This is accomplished by a combination of the GNAT Box System's stateful packet inspection and network address translation facilities.

When an inbound connections is desired a GNAT Box System tunnel should be configured to a particular service on a host residing on the private service network. When a tunnel is created in this manner, if for some reason an intruder compromises the tunneled service to the target host, the intruder will be isolated on the private service network.

Any unauthorized access attempts are logged by GNAT Box System.

7. Product features and mechanisms

7.1. Outbound Services

When an IP packet arrives on the GNAT Box's Protected network interface, after Outbound filtering, the engine determines where the packet should be sent and performs the necessary modifications on the packet (i.e. network address translation), if required. Then routes the packet to the correct network interface. Translation is performed if the destination host is on the External or PSN networks. If translation is performed, the IP packet's source address will be modified to be that of the network interface, that is the route to the destination IP address of the packet. When a response packet returns to the GNAT Box, the packet is inspected to determine if the packet is in fact a response on an active transparency circuit. If the packet is accepted, it is then modified with the originating reply IP address and routed on to the Protected network.

The GNAT Box transparently supports all standard TCP, UDP and ICMP applications. No proxies or modified applications are required for outbound access through the GNAT Box. Off the shelf applications operate normally as expected.

Applications such as telnet, ftp (both normal and PASV), DNS, http (web), https, SSL, ping, traceroute, gopher, WAIS, NFS, rlogin, SSH, RCP, SMTP, POP3, lpr, SNMP, IMAP, netbios, who, ntp, rtsp, tftp H323, ICQ, uucp, X-11, XDMCP, finger, AOL, Compuserve are supported just to name a few.

GNAT Box has transparent support built-in for many difficult and hard to handle application protocols. These applications include:

- RealAudio/Video
- Vosaic
- Vxtreme
- VDOLive
- StreamWorks
- CU-SeeMe
- PPTP
- Archie

- NTT AudioLink
- NTT SoftwareVision
- Apple Quicktime Streaming
- Microsoft NetMeeting
- RSTP Applications
- Net2phone
- Oracle*8

7.2 Tunnels / Inbound Services

In its default configuration, the GNAT Box System does not listen for any unsolicited inbound packets. It only responds to reply packets (those packets which are returning in response to packets that originated from the Protected or PSN). If you need to allow unsolicited connections to internal hosts, use the GNAT Box System's Tunnel facility.

A Tunnel is a GNAT Box facility that allows a host on an external network to be able to initiate a TCP or UDP session with a host on an otherwise inaccessible host for a specific service. This is done by mapping a visible IP address and port (service) to target IP address and service. This mapping can be performed for all services (host to host tunneling) or more typically for a given service. Common tunnels include: SMTP (email), FTP, WWW, SQLnet and telnet. Tunnels can be created to hosts on both the PSN and the Protected network.

Outbound Packets from the PSN - The PSN works the same as the Protected network, except that the PSN cannot reach the Protected network. If a host on the PSN attempts to reach a host on the Protected network, the connection will be refused. Additionally, the following message will be generated to the console (if syslog is enabled then it will also be sent to the log server): "Warning: Attempt by DMZ to access protected network."

How Tunnels Work

When an IP packet arrives at a GNAT Box System Firewall and it is not a response packet for an active connection and the Remote Access Filters allow the packet, it is compared against user defined Tunnels. If the destination IP address and port match the entrance of a Tunnel, a new connection is created. This new connection will automatically change the destination address and port of all packets arriving on this connection to be those given for the end of the Tunnel. Additionally, all response packets originating from the Tunnel's destination host will have the source address and port changed back to the Tunnel's beginning as the packets are transmitted back to the originating host.

Great care should be taken when configuring servers that will be the target of such tunnels. The recommended and secure method of tunneling is to use the PSN.

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

7.3 IP Aliasing

An IP Alias is the GNAT Box System facility that allows the External network interface to have multiple IP addresses. This facility is useful, if multiple targets on the PSN or Protected network are required for the same service (port) via the Tunnel facility (e.g. multiple webservers). All IP aliases must be registered or legitimate IP addresses, although they need not be from the same network.

7.4 NAT

Network Address Translation, or NAT, is one of the primary features of the GNAT Box System. The NAT facility used in the GNAT Box System is always active and is available in two forms: dynamic translation and static translation.

The default NAT form is a dynamic many-to-one scheme, in which all IP addresses located on the Protected network (and all connected networks attached) and the PSN are translated to a single IP address. This single IP address is the primary

address of the External network interface. The other form of NAT that is available, is a static translation method, referred to in the GNAT Box System as Mapping. The Mapping facility allows the GNAT Box administrator to specify a static mapping address scheme, such that a given address or subnet is mapped to a specific IP address assigned (aliased) to the External network interface.

7.5 Static IP Mapping

Mapping is a GNAT Box facility that allows an internal IP address or subnet to be statically mapped to an external IP address during the network address translation process. Typically, mapping is used with targets on the External network interface. Mapping is not useful unless IP aliases have been assigned to the target network interface, since by default all IP addresses on the Protected network are dynamically assigned to the real IP address of the outbound network interface.

7.6 VPN Support

The GNAT Box Firewall System has a built-in IPSec VPN facility. The system's IPSec VPN operates in the ESP tunnel mode that provides a VPN gateway for all hosts protected by the firewall. Because the ESP tunnel mode is utilized unregistered IP addresses can be used to access a remote network over the VPN tunnel. The basic GNAT Box System provides IPSec manual key exchange, while the GB-Flash and GB appliance systems provide both manual key exchange and IKE automated key exchange.

The GNAT Box System also provides transparent operation of many third party VPN implementations. Two of the most common VPNs: Microsoft Corporation's PPTP and Data Fellows SSH are supported transparently. Other VPN solutions, such as hardware based systems typically operate transparently with the GNAT Box System.

7.7 Filters

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

Basic GNAT Box Filter Concepts

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

sequentially against each filter until one of two events occurs:

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

Comparison Parameters

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

Source IP Address

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

Source Netmask

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

Source Port

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

Destination IP Address

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

Destination Netmask

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

Destination Port

The destination port can be: a single port, multiple ports or a range of ports. The specified Destination Port(s) are compared to the destination port of the IP packet to see if a match exists. If no Destination Port is specified, any destination port is

accepted. Destination ports are often called services since certain well known services have been assigned dedicated port numbers. Historically, well know services, typically those provided by servers, were defined to be ports in the range from 1 to 1024. However, with the explosive growth of the Internet, this limited range of ports has been exhausted and new services have ports assigned outside this range.

Network Interface

The network interface parameter allows a filter specification to define which network interface the packet must have arrived at in order to be matched.

Protocol

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

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

Filter Actions

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

Alarm

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

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

Email

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

Stop Interface

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

Pager

This filter action requires that an optional modem be attached to one of the supported serial interfaces (COM 1-4). This modem must be dedicated to the pager function. The modem may be either external or an internal modem card. Only numeric

paggers are supported. Because pager systems can vary from country to country there is no guarantee that the pager function will operate in all countries.

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

SNMP Trap

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

Generate ICMP

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

Filter Action Notes

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

7. 8 Remote Access Filters

Remote Access Filters control inbound access primarily on Tunnels. Additionally, Remote Access Filters control inbound access to any network interface on the GNAT Box Firewall from any attached network. When the GNAT Box System is initially configured a set of default Remote Access Filters are generated. These filters (listed below) can be used as is, modified or deleted to suit the local network security policy.

At the heart of GNAT Box System is GTA’s network address translation and stateful packet inspection engine. The stateful packet inspection facility monitors every IP packet passing through the GNAT Box System to guarantee that:

- Network address translation is performed for all packets passing through the GNAT Box System outbound.
- Only valid response packets or packets passing through user defined tunnels are allowed to reach hosts on the Protected or PSN networks from the External network.

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

7. 9 Domain Name Service

Since the GNAT Box System provides network transparency for users on the Protected network, all DNS queries operate normally. Since the GNAT Box System hides all network addresses on both the Protected and PSN networks, providing DNS information to the external network is pointless as none of the IP addresses on the Protected network are directly accessible from the External network.

A split DNS scheme should be used with the GNAT Box System; that is a DNS server can operate on the Protected network serving DNS information for the Protected network. Information about hosts on the PSN may also be provided by this DNS server for use by hosts on the Protected network (hosts on the PSN would not have access to this server unless you created a tunnel to the Protected network from the PSN on port 53/UDP). A separate DNS server should be used to provide DNS information for users on the External network (the Internet). This external DNS server can reside anywhere that is accessible by external users. Typically, this DNS server is located at your Internet Service Provider, on an external host (in the case of an Intranet) or on the PSN with Tunnels on port 53 for both TCP and UDP. The external DNS server would typically have “A” records for the External network interface IP address and any alias IP addresses.

8. Product audit/event reporting and summaries

The GNAT Box System provides audit and event reporting directly on the main console and remotely via the Unix syslog facility. Through the user interface the administrator can configure the log/auditing facility as to how information will be logged for outbound packets, inbound tunnels and filters. By default all unauthorized accesses attempts for both inbound and outbound connections are recorded. Additionally each remote access and outbound filter can also be configured to a specific logging configuration.

9. Product testing methodology

- The GNAT Box System kernel is tested during the development process on special target test systems configured for diagnostic and kernel level debugging. Alpha and stress testing is performed on in-house test systems in a both simulated and real Internet environments.
- The GNAT Box System support software is tested on a module basis during the development process. Each module undergoes regression testing as enhancements and modifications are applied. In-house test systems are utilized for alpha and stress testing.
- Automated penetration tools in addition in-house security exploits are used to test the system.

10. Product performance attributes

The GNAT Box System is a high performance system. For user provided hardware systems, the system performance will vary depending upon the processor and network interface card types. For most customers a 486 CPU and ISA based network cards can easily support network connections of speeds up to and including a T-1 line. The best performance will be obtained with a Pentium class CPU and PCI based network cards.

The GNAT Box System can support a maximum of 32,768 concurrent sessions (10,000+ with the RoBoX Firewall Appliance) with a memory size of 32Mb. Configurations with 16Mb can support up to 16,000 concurrent sessions.

11. Product operational assumptions

The GNAT Box System uses standard Intel based hardware. The system supports 10, 100, 1000 Mbps Ethernet, Token Ring and FDDI (UTP, SAS and UTP) network interface cards. RoBoX Firewall Appliance supports only 10, 100 Mbps Ethernet. For user-supplied hardware GNAT Box System Firewalls any combination of supported network cards may be in the GNAT Box System, the cards need not be of the same type or manufacture. A PPP interface is also supported on the external network interface for external and internal asynchronous modems for dialout operation. The PPP interface also supports external ISDN TA's.

12. Product operational/management requirements and interface

The GNAT Box System is a very low maintenance system. Generally most of the systems management involves the installation and configuration, which typically takes about five minutes. Since the GNAT Box System has no hard disk, there is no need to worry about disk crashes or tape backups. The runtime system is contained on a single 3.5" floppy diskette that is easily backed up with a supplied utility for the GNAT Box Pro and on a CompactFlash module for other GNAT Box System Firewalls. The GNAT Box runtime system is loaded into memory at boot time and only accesses the floppy disk to save and read configuration data, therefore a loss of power or unexpected shutdown typically will not damage or corrupt the system. Additionally the GNAT Box System can be administer remotely, so a CRT and keyboard are not required for operation after the initial configuration. The system is designed to be simple to operate and maintain, therefore human

resources for the support of the system are minimal.

13. Product customer support

- Bug fixes within current version are provide free of charge to customers
- Minor updates (notated by the third number) are available free of charge to owners of current software versions.
- Major updates (notated by the first or second number) are provided for a nominal fee.

The GNAT Box System, typically once installed and configured requires little or no support. For those customers who wish to have support, GTA offers a variety of update and support plans domestically. Other plans domestically may be available from local suppliers of the GNAT Box. For customers outside the United States, maintenance plans are available but vary depending upon the geographical location.

Domestically in the United States

- Onsite installation is available.
- Onsite training is available.
- Configuration and installation support is included for the first 30 days.
- System update support is available for a nominal fee on an annual basis.
- System support is available at various response levels for a fee on an annual basis.

Internationally

- Onsite installation and training is available through local distributors and suppliers in all countries where the GNAT Box is sold.
- Maintenance plans are available, but vary depending upon the country.

14. Product interoperability considerations

- The GNAT Box System is designed primarily to operate as a gateway between a protected network and the Internet. However the GNAT Box is also ideal for usage as an intranet firewall between two private networks.
- The GNAT Box System only supports TCP/IP traffic to pass through the gateway.
- The GNAT Box System operates transparently with TCP, UDP and ICMP client based
- The GNAT Box System operates without modification with the SSH VPN both inbound and outbound.
- The GNAT Box System supports Microsoft Corporation's PPTP VPN without modification, both inbound and outbound.
- The GNAT Box System operates with many IPSec VPN gateway implementations.

15. Glossary

15.1. Format

Newly added terms or annotated/re-interpreted glossary terms specific to this document are prefaced with a mark to denote the change or addition. Readers of this document are requested to pay special attention to such terms.

15.2. Glossary of Terms

Abuse of Privilege: When a user performs an action that they should not have, according to organizational policy or law.

Application-Level Firewall: A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Authentication: The process of determining the identity of a user that is attempting to access a system.

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

Authorization: The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.

Bastion Host: A system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be “outside” Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., UNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

Challenge/Response: An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.

Chroot: A technique under UNIX whereby a process is permanently restricted to an isolated subset of the filesystem.

Cryptographic Checksum: A one-way function applied to a file to produce a unique “fingerprint” of the file for later reference. Checksum systems are a primary means of detecting filesystem tampering on UNIX.

Data Driven Attack: A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Defense in Depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

DNS spoofing: Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

Dual Homed Gateway: A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

Encrypting Router: see Tunneling Router and Virtual Network Perimeter.

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

Host-based Security: The technique of securing an individual system from attack. Host based security is operating system and version dependent.

Insider Attack: An attack originating from inside a protected network.

Intrusion Detection: Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

IP Splicing / Hijacking: An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

Least Privilege: Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

Logging: The process of storing information about events that occurred on the firewall or network.

Log Retention: How long audit logs are retained and maintained.

Log Processing: How audit logs are processed, searched for key events, or summarized.

Network-Level Firewall: A firewall in which traffic is examined at the network protocol packet level.

Perimeter-based Security: The technique of securing a network by controlling access to all entry and exit points of the network.

Policy: Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Proxy: A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Screened Host: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

Screened Subnet: A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.

Screening Router: A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.

Session Stealing: See IP Splicing.

Trojan Horse: A software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program.

Tunneling Router: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption.

Social Engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems.

Virtual Network Perimeter: A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks.

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

16. References to additional documents

17. Appendices

18. Functional Summary Program: Contacts

How to contact the functional summary program group, for more information or to participate:

Email: fwall-summaries@iwi.com

Web: <http://www.iwi.com>

(C)Copyright, 1995, Marcus J. Ranum, Information Warehouse! Inc. All rights reserved. This document may be freely published, mirrored, or reprinted, as long as this copyright message remains intact.

Format version: 1.0 RELEASE

Copyright © 2002 Global Technology Associates, Inc. All rights reserved.