



GNAT

for VxWorks

A Gateway Network Address Translator

GNAT is a high performance network address translator (NAT) for VxWorks®. Its core engine maps internal to external addresses using port translation (NAPT) based on pre-defined mapping rules. Its small footprint and robustness have been specifically designed for use in an embedded environment. **GNAT**'s unprecedented flexibility and ease of customization make it the NAT of choice in embedded networking applications.

GNAT Operation

GNAT typically operates on a gateway between an internal and external network. It does this by creating "local" internal networks, which are connected to the external network (e.g. the Internet) using a single routable (public) IP address in the minimum configuration. **GNAT** maintains an address translation table containing active mappings of internal/external IP addresses and port numbers. Mappings are created dynamically based on rule-matching when a packet makes its way through **GNAT**. Based on these, each IP datagram sent out with an internal IP source address has the source address

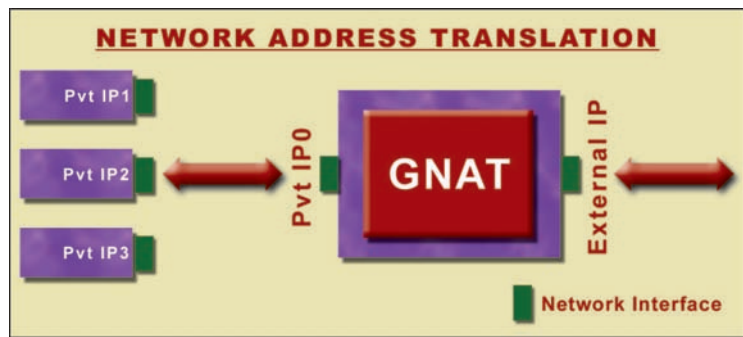
replaced by the appropriate external IP address and is re-injected into the packet stream. This process is reversed when a packet is received, since the mappings allow **GNAT** to determine the original requestor to which the packet should be forwarded. Mappings are automatically deleted after a pre-configured inactivity time period.

Inbound & Outbound Mappings

GNAT includes a redirection command to redirect inbound packets to a specified internal IP address (or multiple addresses for round-robin based load balancing). This allows external devices to initiate connections to internal NAT-ed nodes which may be necessary if the internal nodes are running servers (such as ftp, http, etc.), which require access from the outside. Further, **GNAT** supports redirection in the outgoing direction to allow services such as DNS port forwarding from the internal network. **GNAT** also allows the selection of ports for outbound NAPT with explicit or automatic port range selection, and supports the "map-block" command which uses an algorithm to determine

Features

- ❖ Many-to-one address translation and many-to-many round-robin translations.
- ❖ Conserves IP addresses.
- ❖ Supports bi-directional translation.
- ❖ Includes reference ALG implementation for FTP (including inbound, passive connections).
- ❖ Includes reference ALG implementation for PNA streams.
- ❖ Supports ICMP ID mapping and "from/to-specific" rules.
- ❖ Integrates with firewalls for dynamic firewalling.
- ❖ Extremely small footprint.
- ❖ Low network latency.
- ❖ Easily controlled by web server through string based CLI.
- ❖ Supports rule numbering and per-rule aging of NAT entries.
- ❖ Supports MSS value clamping.
- ❖ Validated on big & little endian architectures including PowerPC, MIPS, ARM / XScale, and X86.
- ❖ Royalty-free full-source distribution.



what the translated source address and range of available ports should be.

Local Network Privacy

A useful feature of **GNAT** is its ability to hide private IP addresses on its internal side. The nodes on the internal network may freely establish connections with external nodes. However, connections from the external side may be blocked or tightly controlled. **GNAT** can allow specific connections, or even no connections, to be established in this direction. **GNAT** thus offers security by assigning nodes on the internal network non-routable private IP addresses that cannot be easily accessed from potential threats on the outside.

VxWorks Edition Features

- ❖ Designed exclusively for VxWorks and VxWorks based Platforms
- ❖ Native support for VxWorks 5.3.x, 5.4.x, 5.5.x, 6.0 and AE
- ❖ Enhanced memory management and partition support
- ❖ Tornado Project Facility (IDE) integration
- ❖ Integrated with Tornado and VxWorks build and install methodology
- ❖ Requires no special VxWorks or networking source

Dynamic Firewall Interface

GNAT private IP address-hiding complements the perimeter security of IP packet filtering firewalls. A unique feature of **GNAT** allows the association of a NAT mapping with a firewall rule. When the NAT entry is created, it also opens a firewall window. This allows for a convenient way to enable a dynamic firewall rule, allowing activity at specific ports when a connection is initiated from the internal side. The firewall window is closed when the NAT entry expires.

Application Level Gateways

Some TCP and UDP protocols embed addressing information in the payload of packets. For example, during an "active" FTP connection, the client informs the server of its IP address & port number and then waits for the server to open a connection to that address. **GNAT** has to monitor these packets and modify them on the fly to replace the client's IP address (which is on the internal network) with the NAT-ed address. This requires defining specialized application level gateway modules (ALGs) for such protocols. **GNAT** supplies an implementation of the FTP ALG which can be used as a reference for any other protocols that require a specialized ALG. Further, **GNAT** includes support for inbound connections to an FTP server on the internal network, including passive connections. **GNAT** also includes other proxies for PNA based streams, netbios-DGM packets and "rcmd" transparent proxy.

Portable Private Networks

GNAT's setup of a "local" network on its internal side, with its own private IP address scheme, allows for maximum address portability since this network can be connected to any external network without any IP address change for the internal nodes. This is particularly useful in embedded environments where the "local" network may be part of a single embedded system. **GNAT** allows such applications to refer to the internal addresses without reference to the external IP address in use, which may change based on DHCP assignment, or inclusion of the embedded devices in a customer network.

Management Framework

GNAT supports a customizable management interface that can be programmatically controlled or presented through a string-based command layer, which can be easily controlled through a web-server or structured data files such as XML or via a CLI. Support for rule numbering, usage statistics, specific "from-to" rules, and rule-specific age settings allow for maximum management flexibility. Management of nodes on the internal network is also eased, since they can be assigned private IP addresses that do not change even if the external IP address changes based on connection to different external networks.

Built for VxWorks

The VxWorks edition of **GNAT** is a drop-

Also Available

- ❖ **SSHield**
Secure Shell
- ❖ **SSLimSecure**
Secure Sockets and TLS
- ❖ **ClassHopper**
Alternate Queuing Disciplines

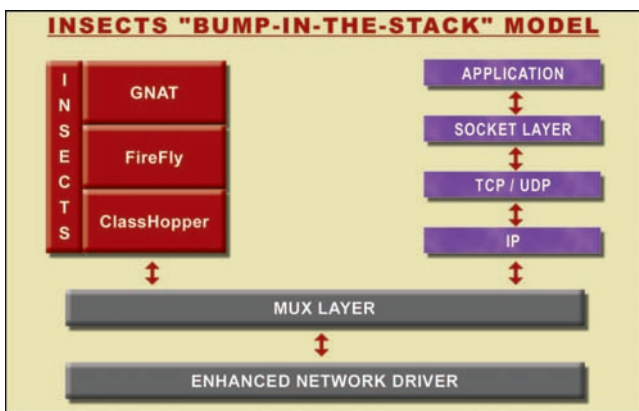
Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized implementations of **GNAT** including support for hardware acceleration using network processors and ASICs.

Customization Flexibility

- ❖ Support for port number ranges.
- ❖ Configurable timeout and NAT table size.
- ❖ Extensible architecture to support Application Level Gateways (ALGs).
- ❖ Support for selectively disabling the incoming or outgoing direction on each interface.
- ❖ Available in full-source format.
- ❖ Customization hooks and callouts.

in component for *VxWorks 5.x, 6.0 and AE*. It has been extensively validated on a variety of CPU architectures, and this minimizes development and integration efforts. **GNAT** is especially optimized for **VxWorks** and **VxWorks** based Platforms such as PNE and PCD, with support for multi-tasking and memory partitions, and transparently works with the native network stack in **VxWorks** or with **TeamF1**'s **NetF1** high-performance stack as well as other third-party stacks. Like the other members of the **INSECTS** suite, it is built as a network service that binds itself with the MUX layer, thereby guaranteeing compatibility with any **VxWorks** application with minimal to no changes, and without any special network stack source code requirement.



Email: sales@TeamF1.com
Web: www.TeamF1.com
Ph: 510-505-9931 ext. 5
Fax: (510) 505-9941



© 2002-2004 TeamF1, Inc.