GNAT Box®

SYSTEM SOFTWARE

GTA Glossary

Global Technology Associates, Inc.

GTA Glossary **January 2004**

Technical Support

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's website 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 GTA authorized channel partner.

Tel: +1.407.482.6925 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

GNAT Box is a registered trademark of Global Technology Associates, Incorporated. RoBoX and Surf Sentinel are trademarks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. WELF and WebTrends are trademarks of NetIQ. Sun, Sun Microsystems and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. The Java product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/. SurfControl is a registered trademark of SurfControl plc. s

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA
Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: http://www.gta.com • Email: info@gta.com
Lead Development Team: Larry Baird, Richard Briley, Jim Silas, Brad Plank.
Technical Consulting: David Brooks. **Documentation:** Mary Swanson.

Contents

The GTA Glossary defines terms used in GNAT Box System Software and documentation; it also provides a collection of other relevant industry words, phrases and acronyms used in, or pertinent to, GNAT Box System Software and other GTA hardware and software products.

For more definitions and industry term discussions, see **techweb.com/encyclopedia**; **www.webopedia.com**; and **www.faqs.org**. These and many other online sites can provide you with more information about these concepts.

Numerals

3DES (Triple DES)

See *encryption algorithm*.

A

A record

See *zone file*.

access control

The control of who has, or what applications have, access to a network, server or other computer device.

access router

A router that connects your network to another network or networks. An access router enforces your Access Control Lists, effectively providing a level of protection for all hosts "behind" that router.

ACL (Access Control List)

A listing of users and their associated access rights. Rules for packet filters (typically routers, servers or security gateways) that determine which packets to pass and which to block. In GNAT Box System Software, ACL specifically refers to content filtering lists.

activation code

An activation code is an encode key of 35 characters which enables optional features on GTA Firewall and other GTA products. Activation codes are system specific and must be used on the system for which they were generated. **Example:** `E5FA6342-78E44D9D-59D1761B-45B4884D`

ACK

The acknowledgment sent to a transmitter to indicate that a receiver is ready to accept data; also used to acknowledge that data has been received without error.

ActiveX control

Active X controls typically add functionality such as toolbars, notepads and calculators to web pages run on Windows machines. They can be downloaded and executed by a web browser automatically, but unlike Java applets, (which are multi-platform), they have full access to the Windows operating system, with the attendant risk.

address spoof

Sending a message with a packet header modified so that it appears to come from a specific IP address. Validly used to prevent session timeouts. See *spoofing* under *attack*.

AES (Advanced Encryption Standard)

See *encryption algorithm*.

agent

In network management, the component of a system that responds to management requests and/or preprogrammed traps. In the client/server model, the component that prepares information and exchanges it for a client or server application.

AKEP (Authentication Key Exchange Protocol)

Key transport based on symmetric encryption allowing two parties to end up with a shared secret key.

algorithm

A set of mathematical rules (logic) used in the processes of encryption and decryption. See *encryption algorithm*.

alias

An assumed name address that routes a message to all real addresses associated with the alias. See also *IP Alias*.

AND

See *Boolean logic*.

ANSI (American National Standards Institute)

anti-replay protocol

Part of the IPSec standard, anti-replay ensures IP packet-level security by making it impossible to intercept packets and insert changed packets into the data stream. Both ESP and AH use anti-replay.

When a security association has been established between a sender and a receiver, their counters are initialized at zero. The first packet sent will have a sequence number of 1, the second 2, etc. The receiver verifies that the number on the packet is not that of a previously sent packet. When a replayed packet is detected, the program sends an error message, discards the packet, and logs the event with the date/time, source address, destination address and sequence number.

API (Application Program Interface)

A format used by an application program to communicate with the operating system or another control program such as a database management system or communications protocol. APIs are implemented by writing function calls in the program.

CMC (Common Messaging Calls)

A programming interface specified by the XAPIA as the standard messaging API for X.400 and other messaging systems. CMC is intended to provide a common API for applications that want to become mail enabled.

MAPI (Mail API)

A programming interface from Microsoft that enables a client application to send to and receive mail from Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft applications such as Outlook, the Exchange client and Microsoft Schedule use MAPI. Simple MAPI is an enhanced version of the Common Messaging Calls (CMC).

ARIN (American Registry for Internet Numbers)

An organization founded in 1997 to dispense IP addresses in North and South America, the Caribbean and sub-Saharan Africa. This was previous handled by Network Solutions, Inc., (InterNIC), which manages domain names. The European and Asian counterparts of ARIN are Researux IP Europeens (RIPE) and Asia Pacific Network Information Center (APNIC). www.arin.net.

ARP (Address Resolution Protocol)

A TCP/IP protocol used to obtain a node's physical address. A client station broadcasts to the network an ARP request containing the IP address of the node with which it wishes to communicate, and the target node sends back its physical address.

AS (Autonomous System)

A network of interconnected hosts, clients, etc., administered by a single set of management rules controlled by one entity.

ASCII (American Standard Code for Information Interchange)

A binary code for text, communications and printer control. It is used for most communications and is the built-in character code in most computers.

asymmetric key encryption

A separate but integrated user key pair comprised of one public key and one private key. Each key is one way, meaning that key used to encrypt cannot be used to decrypt information.

ATM (asynchronous transfer mode)

A network technology that supports both realtime voice and video and data. ATM establishes a logical circuit from end to end, guaranteeing quality of service (QoS). ATM is widely used as a backbone technology in carrier networks and large enterprises. It is highly scalable and supports multiple transmission speeds.

attack

Deliberate assault against a computer system or network to gain access, prevent service or otherwise intrude on or damage the system. See *hacker*.

brute force cracking

Trying to recover a crypto key by trying all reasonable possibilities.

bucket brigade

Attack against a public key exchange in which an attacker's key is substituted for the requested public key.

dictionary attack

A brute-force attack to reveal a password using obvious combinations.

DoS

Denial of Service. An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted.

DDoS

A distributed denial of service attack uses multiple computers throughout the network.

fragmentation, IP fragment attack

Fragmenting packets in such a way that they pass filters meant to protect against and drop certain packets or fragments. A type of DoS.

hijacking

An attack which takes over a live connection between two entities so as to masquerade as one of the entities.

ping flood

See many, many *pings* or *DoS*, above.

Ping of Death

A ping request with an invalid packet size value in the packet header crashes the target computer. See *Ping*.

replay, man-in-the-middle

A breach of security in which information is stored without authorization and then retransmitted to trick the receiver. A replay attack can be prevented using strong digital signatures that include time stamps and inclusion of unique information from the previous transaction such as the value of a constantly incremented sequence number.

smurf attack

A *spoof* attack in which ping requests (ICMP echo requests) are sent to a broadcast address on the target network. The return address is spoofed to the victim's address. Since a broadcast address is picked up by all nodes, it functions like an amplifier, generating hundreds of responses.

spoofing, address spoof

Attempting to gain access to a computer by sending a message with a packet header modified so that it appears to come from a trusted IP address. Also known as *IP spoof*. See *address spoof* for a valid use.

SYN flood attack

An assault on a network that prevents a TCP/IP server from servicing other users. It is accomplished by not sending the final acknowledgement to the server's SYN-ACK response in the handshaking sequence, which causes the server to keep signaling until it eventually times out.

authentication

The process of ensuring the identity of the connecting user or participants exchanging electronic data. Makes sure the person or server at either end of a connection is who they claim to be and not an impostor.

Authentication Header (AH)

The AH information is inserted between the IP header and the payload. An AH is used to ensure the integrity of the whole IP packet, including both the payload and the IP header. It does not provide data encryption.

autokey (Output Feedback [OFB] mode)

The block cipher mode in which the cipher is used to generate the key stream.

autokey system

A periodic substitution system in which the key, following the application of a previously arranged initial key, is generated from elements of the plain or cipher text of the message.

automatic filters

Generated by the system for transient events, i.e., a packet sent in response to a request from behind the firewall; connections triggered by selecting Automatic Accept All for an inbound tunnel; and Stealth mode. Has priority over the other filter types.

B

backbone

A high-performance network of thick wire or fiber optic cables that enables data transmission within networks that are connected to it.

beacon

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

bit

The smallest element of computer storage, a single digit in a binary number (0 or 1). Eight bits make up a byte, which is equivalent to one alphanumeric character.

block

A string or group of bits that a block algorithm operates on; typical values are 40, 50, 64, 128, 512, 1024, …

block cipher/algorithms

Algorithms that operate on plain text in blocks (strings or groups) of bits.

Blowfish

See encryption algorithm.

Boolean logic

The "mathematics of logic," developed by George Boole in the mid-19th century. Its rules govern logical functions (true/false). As add, subtract, multiply and divide are the primary operations of arithmetic, AND, OR and NOT are the primary operations of Boolean logic.

bridge

An inter-networking switch usually operating at OSI Level 2, the Data Link Layer. A bridge expands a LAN or connects two LANs.

bridging mode

In default mode, a GTA Firewall acts as a firewall router, so that systems on the internal network see it as a gateway to the external network, and systems on the external network see the firewall as the gateway to the internal network.

Using bridging mode, a GTA Firewall acts as a bridging firewall, connecting networks transparently like a bridge, while filtering IP packets as a firewall.

A GTA Firewall in bridging mode can be inserted behind a router to the Internet between the router and the internal networks without changing IP addresses, gateways or any other network addresses.

A GTA Firewall in bridging mode can also be inserted in an internal network to separate networks that are at a peer level, or to further segregate Private Service Networks. This configuration allows two internal networks to communicate as one, while filtering IP traffic between them and preventing the passage of non-IP data (except ARP, which operates at both data link layer 2, and network layer 3).

In bridging mode, a GTA Firewall can be connected directly to a host, a switch, a router or a non-bridged GTA Firewall.

broadcast

In network terms, to send a datagram to an entire subnetwork.

browser

An interface that allows a user to view HTML pages in graphic or text-based format. Some examples are: Safari, Internet Explorer, Lynx (text-based), Netscape Navigator, Mozilla and Opera.

BSD UNIX (Berkeley Software Distribution UNIX)

A version of UNIX developed by the Computer Systems Research Group of the University of California at Berkeley from 1979 to 1993. BSD enhancements, known as the "Berkeley Extensions," include networking, virtual memory, task switching and large file names (up to 255 chars).

bus

A single data path to which all workstations directly attach, and on which all transmissions are available to every workstation. However, only the workstation to which a transmission is addresses can actually read it.

bypass

A flaw in a security device that allows messages to go around the security mechanisms.

byte (BinarY TablE)

A byte is made up of eight bits. A ninth bit may be used in the memory circuits as a parity bit for error checking. A byte holds the equivalent of a single alpha character or a symbol such as a decimal point or dollar sign. A byte can hold a single decimal digit (0 to 9), two numeric digits (packed decimal) or a number from 0 to 255 in binary.

C

CA (certificate authority)

A trusted third party who issues, revokes and manages certificates, validating that public keys are not compromised and that they belong to the correct owners.

CAST-128

See encryption algorithm.

CBR (Constant Bit Rate)

A uniform transmission rate, e.g., realtime voice and video traffic requires a CBR.

CDSA (Common Data Security Architecture)

A set of layered security services developed by The Open Group to address communications and data security in the Internet and intranet application space.

cell

fixed sized packets (the ATM standard is 53 octets, but proprietary lengths e.g. of 16 and 24 octets have been used). Cells are

identified and switched by means of a five byte header.

cell relay/switching

Used for high-speed transmission of multiple types of traffic, including voice, data and video.

certificate/digital certificate

An electronic document attached to a public key by a trusted third party which provides proof that the public key belongs to a legitimate owner and has not been compromised.

Certificate Revocation List (CRL)

A list of certificates that have been revoked before their scheduled expiration date.

CHAP (Challenge Authentication Protocol)

Session-based, two-way password authentication scheme.

checksum

A numeric value used to verify the integrity of a block of data. The value is computed suing a checksum procedure. A crypto checksum incorporates secret information in the checksum procedure so that it can't be reproduced by third parties that don't know the secret information.

CIDR (Classless Inter-Domain Routing)

A method for creating additional addresses on the Internet. CIDR reduces the burden on Internet routers by aggregating routes so that one IP address represents thousands of addresses that are serviced by a major backbone provider. All packets sent to any of those addresses are sent to the ISP. In 1990, there were about 2,000 routes on the Internet. Five years later, there were more than 30,000. Without CIDR, the routers would not have been able to support the increasing number of Internet sites.

Instead of the fixed 8, 16 and 24 bits used in the Class A-B-C network IDs, CIDR uses a variable network ID from 13 to 27 bits. For example, the CIDR address 204.12.01.42/24 indicates that the first 24 bits are used for the network ID.

CIPE (Crypto IP Encapsulation)

An ongoing project to build encrypting IP routers. The protocol used is as lightweight as possible. It is designed for passing encrypted packets between prearranged routers in the form of UDP packet. CIPE is not as flexible as IPSec but holds true to the original intended purpose: securely connecting subnets over an insecure transit network.

cipher

Encrypted plain text.

CBC (Cipher Block Chaining)

A block cipher mode that combines the previous block of ciphertext with the current block of plaintext before encrypting it; very widely used.

CTAK (cipher feedback)

A block cipher mode that feeds previously encrypted ciphertext through the block cipher to generate the key that encrypts the next block of ciphertext.

CFM (Cipher Feedback Mode)

A block cipher that has been implemented as a self-synchronizing stream cipher.

circuit switching

A method of handling traffic through a switching center, either from local users or from other switching centers, whereby a connection is established between the calling and called parties.

client

A device or application that makes use of the services provided by a server in a client/server architecture.

clustering

It generally refers to multiple computer systems that are linked together in order to handle variable workloads or to provide continued operation in the event one fails. A cluster of computer systems provides fault tolerance and/or load balancing. If one system fails, one or more additional systems are still available. Load balancing distributes the workload over multiple systems.

CMIP (Common Management Information Protocol)

The OSI layer 7 protocol for network management covering manager-to-agent and manager-to-manager communication from the International Organization for Standardization (ISO).

CMOT (CMIP over TCP)

CMOT is a network management architecture that uses the ISO CMIS/CMIP in a TCP/IP environment. Provides a means by which control and monitoring information can be exchanged between a manager and a remote network element.

CMS (Cryptographic Messaging Syntax)

A general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

CNAME (Canonical Name) record

See *zone file*.

coalesce data

To fuse or blend data files or logs together in order to save space. Some information is lost, but the blended data reflects the whole.

code

A system of instructions making up software. A system of symbols making up cipher text.

code group

A group of symbols assigned to represent a plain-text element.

COM port

In DOS systems, the name of a serial communications port. DOS supports four serial ports: COM1, COM2, COM3 and COM4. However, most software uses system interrupts to access serial ports, so that the four COM ports share two IRQ lines.

COMSEC (Communications Security)

Protection of all measures designed to deny to unauthorized persons information of value that might be derived from a study of communications.

common ports

See *port number*.

Configuration IP Address

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

connection mode, type

A logical connection set up between end systems prior to the data exchange. After data transfer the connection is terminated.

dedicated

Establishes a link when the firewall boots up and remains up until the interface is manually disabled, or the system is halted. Select for PPTP. The logical choice for PPPoE, as DSL is an "always on" connection. Select to test a configuration.

on-demand

Initiates and establishes a link with the remote site whenever a packet arrives on a Protected or PSN interface, destined for the External Network. The link will stay up as long as packets continue to be received before the time-out has expired.

on-enabled

When the interface is enabled, this type initiates a session and establishes a link with the remote site. The link will stay established until disabled. Requires manually enabling the External Network interface.

control vector

A string of bits of arbitrary length attached to a key that specifies the uses and restrictions for that key in the IBM Secret Key Management Protocol.

cookie (Persistent Client State HTTP Cookie)

A file or token that is passed from the web server to the web client that is used to identify the user and could record personal information such as ID & password, mailing address, credit card number, etc.

CRC (Cyclic Redundancy Check)

An algorithm used to detect data transmission errors.

CRMF (Certificate Request Message Format)

Used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA) for the purposes of X.509 certificate production.

CTS (Clear to Send)

The RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data. See RTS.

D

DDNS

See *Dynamic DNS*.

default route (gateway)

The default route is generally the router IP address that connects the network to the Internet. The default route is the gateway where any non-local IP packets are sent. If you have selected the PPP device or enabled DHCP or PPPoE on an external network interface, then the Default Route field will be disabled; this value will be set by the selected protocol (PPP, PPPoE or DHCP).

A default route must always be on the same logical network as the External network interface, the only exception being a GTA Firewall PPP connection. DES (Data Encryption Standard)

U.S. data encryption standard adopted in 1976 as FIPS 46 by IBM with input from NSA. Basis for 3DES. See encryption algorithm.

DES (Data Encryption Standard)

See encryption algorithm.

deprecate

In programming, to make items in the code invalid or obsolete. When items are planned for deletion in future releases of a compiler or rendering engine, they are said to be deprecated. They should be removed from source code in subsequent program revisions.

In standard English, to express disapproval of; deplore or to belittle. See *depreciate*.

depreciate

In standard English, to lessen the price or value of or to think or speak of as being of little worth; to belittle.

In tax usage, refers to the lessening in value associated with use and age, as in the depreciation of the value of a car. Eventually, an item is no longer considered of value, and is removed from a list of valuable items, hence the confusion with the word *deprecate* when uses in a programming reference.

DES

See *encryption algorithm*.

device driver

A software component that controls a peripheral device. For data link devices, it manages the process of sending and receiving data across the data link.

DHCP (Dynamic Host Configuration Protocol)

ISPs use the DHCP to assign mobile clients an IP address that is good only for the duration of a dial-in phone call.

dial-up access

The connection of a computer to a network through the use of a modem and a public telephone network.

Diffie-Hellman

See encryption algorithm.

digital certificate

See certificate.

DLL (Dynamic Link Library)

A library of executable functions that can be used by a windows application.

DMZ

See *Private Service Network*.

DNS (Domain Name Server)

A distributed database of information used to translate domain names into Internet Protocol (IP) addresses. See *zone file*.

DDNS

See Dynamic DNS.

RDNS (Reverse DNS)

IP address to host name translation.

doorknob twist

A doorknob twist occurs when a connection is attempted on a port for which there is no service or tunnel in place and a filter has accepted the packet. A Doorknob Twist usually indicates that the firewall is misconfigured.

domain

A domain represents a level of the hierarchy in the Domain Name Space and is represented by a domain name. For example, the domain name "icsa.net" represents the second level domain "icsa" which is a subset, or subdomain, of the top level domain "net," which is in turn a larger subset of the total Domain Name Space.

domain name

A textual name assigned to a host on the Internet. The Domain Name Service (DNS) protocol translates between domain names and numerical IP addresses.

deactivation

The process of removing a domain name from the zone files for the top level domains. When a domain name is deactivated, the Domain Name Server no longer has the information needed to match the domain name with its corresponding IP address.

fully qualified domain name

Complete domain name for a specific computer (host) on the Internet, consisting of a host, domain, and top-level domain; e.g., gtafirewall.example.com, or www.gta.com.

dongle

See hardware key block.

DoS (Denial of Service) attack

See *attack*.

DTE (Data Terminating Equipment)

Typically a terminal or computer; the source or destination of signals on a network.

DCE (Data Connecting Equipment)

Typically a modem.

dynamic routing

The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Dynamic DNS (DDNS)

Automates the process of advising DNS servers when the automatically assigned IP address for a network device is changed, ensuring that a specific domain name always points to the correct machine. The domain name tracks the dynamic address so that other users on the Internet can easily reach the domain, allowing you to host a website, FTP server or email server, even when your IP address is dynamic.

GTA's Dynamic DNS service allows you to connect your dynamic IP address using a third-party DDNS service. The currently used External IP address on the GTA Firewall will update to the selected service each time the IP address changes, or once every month, whichever comes first.

E

EAP (Extensible Authentication Protocol)

Protocol for PPP authentication.

EDI (Electronic Data Interchange)

The direct, standardized computer-to-computer exchange or business documents (purchase orders, invoices, payments, inventory analyses, and others) between an organization and its suppliers and customers.

email proxy

Used to configure an SMTP proxy for inbound email on TCP port 25. Email Proxy can be used to shield an internal email server from unauthorized access and reduce or eliminate unsolicited email (spam). The Email Proxy will respond on any IP address assigned to the External Network interface, unless a tunnel is created on TCP port 25. An inbound tunnel on TCP port 25 will bypass the Email Proxy for the IP address

specified in the tunnel definition; if using Email Proxy, do not create an inbound tunnel on the same IP address and port.

encryption algorithm (engine)

A formula used to turn data into a secret code. Each algorithm uses a string of bits known as a "key" to perform the calculations. The larger the key (the more bits in the key), the greater the number of potential patterns can be created, thus making it harder to break the code and descramble the contents.

Most encryption algorithms use the block cipher method, which codes fixed blocks of input that are typically from 64 to 128 bits in length. Some use the stream method, which works with the continuous stream of input. Sample algorithms:

3DES (Triple DES)

Uses three applications of the DES cipher in EDE (Encipher-Decipher-Encipher) mode with totally independent keys.

AES (Advanced Encryption Standard) aka, Rijndael

GTA's recommended encryption. An encryption standard developed by the NIST to protect sensitive (unclassified) U.S. government information. Rijndael is the name given to the algorithm by its developers, cryptographer researchers Dr. Joan Daemen and Dr. Vincent Rijmen. Some of Rijndael's advantages are: key setup time and agility; low memory requirements; defense against power and timing attacks; such defense's impact on Rijndael's performance.

Blowfish

Blowfish is a high security encryption alogorithm designed by Bruce Schneier, the author of Applied Cryptography. It is very fast, is considered secure and is resistant to linear and differential analysis.

A symmetric block cipher system that can be used as a replacement for the DES or IDEA encryption algorithms. It takes a variable-length key, from 32 to 512 bits.

CAST-128

A 12- or 16-round Feistel cipher that has a blocksize of 64 bits and a keysize of up to 128 bits. Appears to have strength in accordance with its keysize and has good encryption/ decryption performance.

DES (Data Encryption Standard)

A secret key cryptography method that uses a 56-bit key, based on an IBM algorithm which was further developed by the U.S. National Security Agency. It uses the block cipher method which breaks the text into 64-bit blocks before encrypting them.

Diffie-Hellman

The first public-key algorithm, invented in 1976. A cryptographic technique that enables sending and receiving parties to exchange public keys in a manner that derives a shared, secret key at both ends. In Diffie-Hellman, each party raises the common number to a random power and sends the result to the other. The received number is raised to the same random power. Both parties come up with the same.

MD5 (Message Digest 5)

A popular one-way hash function developed by Ronald Rivest (the "R" in RSA) which is used to create a message digest for digital signatures. MD5 is faster than SHA-1, but is considered less secure. MD5 is similar to the previous MD4 method as both were designed for 32-bit computers, but MD5 adds more security since MD4 has been broken. The earlier MD2 function was designed for 8-bit computers. See one-way hash function and encryption algorithm.

SHA-1 (Secure Hash Algorithm-1)

A one-way hash algorithm used to create digital signatures. SHA was developed by the NIST (National Institute for Standards and Technology), and SHA-1 is a revision to the standard released in 1994.

Twofish

Twofish is a block cipher by Counterpane Labs. It has a 128-bit block; 128-, 192-, or 256-bit key; and 16 rounds. Twofish was one of the five Advanced Encryption Standard (AES) finalists. According to the NIST, all five of the finalists for the AES were sufficient to be the new AES.
`www.counterpane.com`

enterprise

The collection of systems, computers, networks, etc., that users depend on for information transfer, processing and management.

ESP (Encapsulating Security Payload)

The IPSec protocol that provides the security services of confidentiality, traffic flow confidentiality, connectionless integrity, data origin authentication, and anti-replay.

An ESP protects only the contents of the payload, not any associated header. Therefore it is possible to change any field in the IP packet carrying an ESP without causing a security violation. The contents of the ESP header are unknown to anyone not possessing information about the transformation and SA needed to recover the protected data.

ethernet

Ethernet is an approach for local area networks using copper wire or cable connections. Ethernets have been developed for 10 Mbytes/sec, 100 Mbytes/sec and higher speed applications. Ethernets use a protocol called CSMACD which stands for "Carrier Sense, Multiple Access, Collision Detect". "Multiple Access" means that every station is connected to a single copper wire (or set of wires). "Carrier Sense" means that before transmitting data, a station checks the wire to see if any other station is already sending something. If the LAN appears to be idle, then the station can begin to send data. For the "Collision Detect" part, two stations can begin to send data at the same time, and their signals will "collide" nanoseconds later. When such a collision occurs, the two stations stop transmitting, "back off", and try again later after a randomly chosen delay period.

executable contents

Data with contents that represent an executable computer program that is capable of modifying persistent data on a host computer.

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, GNAT Box 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. GNAT Box provides no security for hosts located on the External network. See Protected and Private Service Networks.

F

fault resilient

Systems that recover quickly after failure.

fault tolerant

Systems able to continue non-stop when a failure occurs.

FDDI (Fiber Distributed Data Interface)

An ANSI standard specifying a packet-switched LAN-to-LAN backbone for transporting data at high throughput rates over a variety of multimode fibers. FDDI addresses the bottom two layers of the OSI model.

field

A field is a name or tag given to a set of similar data inputs. For example a field might be "name," while Bob and Alice are two inputs to the field.

file

A collection of records stored and handled as a single unit. For example, an executive telephone book may be a file consisting of the names, titles and telephone numbers of the executives listed in the company's human resources database.

firewall

A device, installed at the point where network connections enter a site, that applies rules to control the type of networking traffic that flows in and out.

FR (Frame Relay)

Packet-mode switching interface for handling high-speed data and interconnecting LANs and WANs in low error-rate environments. A streamlined version of X.25, uses variable packets (frames) as the transfer format with less overhead and

sequence checking. Error checks occur only at the destination point.

fragmentation

If a packet is too large to be sent across a link as a single unit, a router can fragment the packet., splitting it into multiple parts which the receiver is able to put together again. Once fragmented, a packet will not be put back together until it reaches its destination. Fragmentation can be undesirable for reasons including:

• If any fragment from a packet is dropped, the entire packet needs to be retransmitted.

• It imposes extra processing load on the routers that have to split the packets.

• In some configurations, fragments are blocked because they don't contain the header information for a higher layer protocol (e.g., TCP) needed for filtering.

G

gateway

A computer that performs protocol conversion between different types of networks or applications. Gateways function at layer 4 and above in the OSI model. They perform complete conversions from one protocol to another rather than simply support one protocol from within another, such as IP tunneling. Sometimes routers can implement gateway functions.

Also, a computer that acts as a go-between two or more networks that use the same protocols. In this case, the gateway functions as an entry/exit point to the network. See proxy server, default route.

GRE (Generic Routing Encapsulation)

A general purpose encapsulation protocol which can be encapsulated in a delivery protocol and forwarded. RFC 2784.

GUI (Graphical User Interface)

A graphics-based user interface that incorporates icons, pull-down menus and a mouse. The GUI has become the standard way users interact with a computer. The three major GUIs are Windows, Macintosh and Motif, the latter being used in UNIX.

H

hacker

A person who writes programs in assembly language or in system-level languages, such as C.The term has come to be synonymous with "cracker," a person who utilizes computer knowledge to break into or otherwise utilize or damage someone else's computer system, previously called a cracker.

cracker

One who breaks security on a system. Coined in defense against press misuse of hacker.

script kiddie

A cracker without skills; one who uses scripts and programs written by others; one who indiscriminantly uses JavaScript from other peoples' pages in their own HTML pages; anyone who writes or uses code without understanding how the code works.

hardware encryption

Plain text is encrypted by hardware devices online between the host computers.

link hardware encryption

Performed through a series of switches (nodes) before the data reaches its destination, an encryption device is needed at each node. The source and destination are kept secret; the header need not be in clear text; the encryption devices are transparent to the data on the line; and the data doesn't affect processors at each end.

hardware key block (dongle)

A copy protection device supplied with software that plugs into a port. The software sends a code to that port, and the key responds by reading out its serial number, which verifies its presence to the program. The key hinders software duplication, because each copy of the program is tied to a unique number, and the key has to be programmed with that number. The key also acts as a pass-through to the printer or other peripheral.

hash code

See message digest.

hash function

An algorithm that turns a variable-sized amount of text into a fixed-sized output (hash value). Hash functions are used in creating digital signatures.

one-way hash function

In cryptography, an algorithm that generates a fixed string of numbers from a text message. The "one-way" means that is extremely difficult to turn the fixed string back into the text message. One-way hash functions are used for creating digital signatures for message authentication.

headers

Formatted information attached to the front of data sent through a computer network contain information used to deliver and process correctly the data being sent.

hexadecimal

A number system with a base of 16. The base 16 numbering system is used as a shorthand for representing binary numbers. Each half byte (four bits) is assigned a hex digit.

Base	16	10	2	16	10	2
	Hex	Dec	Bin	Hex	Dec	Bin
	0	0	0000	A	10	1010
	1	1	0001	B	11	1011
	2	2	0010	C	12	1100
	3	3	0011	D	13	1101
	4	4	0100	E	14	1110
	5	5	0101	F	15	1111
	6	6	0110			
	7	7	0111			
	8	8	1000			
	9	9	1001			

hierarchical trust

A graded series of entities that distribute trust in an organized fashion, commonly used in X.509 issuing certifying authorities.

HLD (High Level Designator)

Indicates the entry or exit point of a block in the network.

high availability

A multiprocessing system that can quickly recover from a failure. There may a minute or two of downtime while one system switches over to another, but processing will continue. Also: RAS (reliability, availability, serviceability); *fault resilient*.

HA Broadcast Port

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

HA Master MAC Address

The system in the HA group that is operating in the Master mode uses a special MAC address. The normal MAC address that is assigned to the NIC is replaced with the HA Master MAC address. This MAC address is: 00:00:5E:00:01:xx, where "xx" is the VRID number. Each interface has a unique VRID, generated by combining the VRID with the interface number.

HA Network Interface

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

Master Mode

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

1. Change the physical MAC addresses of its HA network interfaces to the HA Master MAC address.

2. Begin sending out HA broadcasts (UDP/77) messages which include the system's priority in the HA group.

3. Continue to listen for HA broadcasts. However, in the Master mode, the system is listening for HA broadcasts from a system in the HA group with a higher priority. If the system in Master mode determines that another system in the HA group has a higher priority, then it drops back into Standby mode. When a system switches from the Master mode to any other mode, its MAC addresses will revert to original values.

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

Init Mode

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

Standby Mode

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

HMAC

A mechanism for message authentication that combines an iterative cryptographic hash function such as MD5 or SHA-1 with a secret shared key.

hops

Point-to-point links in a transmission path, where each link is terminated at a network device such as a router or gateway. Additional hops add to processing time. Although each point-to-point link is a hop, the number of network devices between the starting and destination points is the number of hops.

host

A computer system that resides on a network and is capable of independently communicating with other systems on the network. A host is accessed by a user working at a remote location. The computer that contains the data is the host and the computer at which the user is working is the terminal.

host address

The address used by others on the network to communicate with a particular host.

host name

System name assigned to the firewall. GTA recommends using a *fully qualified domain name* as the host name for your GTA Firewall. Host names must be unique. If your network DHCP servers make IP address assignments based on the system name, enter the host name, often assigned by an ISP.

hypertext

Associated with information on the World Wide Web. Any text that contains "links" to other documents. Specifically, words or phrases in one document that are user selectable and which cause another document to be retrieved and displayed. These "links" usually appear in a different color than the main text and are underlined.

HTML (HyperText Markup Language)

HTTP (Hypertext Transfer Protocol)

The protocol used by WWW servers and clients to exchange hypertext data.

I

IANA (Internet Assigned Numbers Authority)

See ICANN.

ICANN (Internet Corporation for Assigned Names and Numbers)

A non-profit, international association founded in 1998 and incorporated in the U.S. It is the successor to IANA (Internet Assigned Numbers Authority), which manages Internet addresses, domain names and the huge number of parameters associated with Internet protocols (port numbers, router protocols, multicast addresses, etc.). ICANN provides a list of accredited registrars in addition to Network Solutions that accept domain registrations. www.icann.org.

ICMP (Internet Control Message Protocol)

An IP protocol used for monitoring and control of an IP network. [RFC 792]

ICSA (International Computer Security Association)

A membership organization founded in 1989 with the purpose of providing education and a clearing house for computer security issues. Formerly NCSA (National Computer Security Association) Now a division of Trusecure. www.icsa.net.

Identity Certificate

A signed statement which binds a key to the name of an individual and has the intended meaning of delegating authority from that named individual to the public key.

IETF (Internet Engineering Task Force)

Founded in 1986, the IETF is a mostly volunteer organization of working groups dedicated to identifying problems and proposing technical solutions for the Internet. www.ietf.org.

IGMP (Internet Group Management Protocol)

The standard for IP multicasting used to establish host memberships in multicast groups on a single network. IGMP provides for a host to inform its local router that it wishes to receive transmissions addressed to a specific multicast group. The router then is able to determine which multicast traffic should be forwarded to each of its hosts.

IGP (interior gateway protocol)

A protocol used to interconnect the members (host, clients, etc.) of an autonomous system or network.

Internet Key Exchange (IKE)

IKE is the key exchange protocol used for exchanging cryptographic keys for dynamically establishing security associations between two VPN peers.

IMAP (Internet Message Access Protocol)

Protocol for retrieving email messages from a mail server.

implicit rule

That which is not explicitly allowed is denied. This means that if all filters are deleted, there is no inbound or outbound packet flow.

inbound tunnel

See entry under *tunnel*.

Index of Coincidence (IC)

The ratio of observed number of coincidences in a given body of text to the number of coincidences expected in a sample of random text of the same size.

indicator

An element inserted within the text or heading of the message to serve as a guide to the selection of derivation and application of the correct system and key for the prompt decryption of the message.

in-line encryptor

A product that applies encryption automatically to all data passing along a data link.

integrity, data integrity

Having assurance that data is transmitted without undetected alteration.

ICV (Integrity Check Value)

InterNIC (Internet Network Information Center)

Under a cooperative agreement with the National Science Foundation (NSF), certain companies (called interNICs) administer second level domain name registration services in the top-level domains, e.g., com, net, mil, org. Some provide information and education services. AT&T provides directory and database services.

internet; Internet

See network.

internetwork switches

Switches that connect multiple data networks; classified according to the OSI protocol level at which they operate. Bridges are internetworking devices operating at Level 2, the Data Link level. Routers operate at OSI level 3, the Network Level and gateways operate at any level above Level 3.

interoperability

The condition achieved among communications-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between them and their users.

interval

A distance between two points or occurrences, especially between recurrent conditions or states. The number of units between a letter, digraph, code group, and the recurrence of the same letter, digraph, counting either the first or second occurrence of both.

intranet

See network.

invalid packets

Packets that are not the expected size or have an invalid option bit; e.g., an ICMP port unreachable packet must have at least 28 bytes. Invalid packets are dropped silently by default, but can be logged, if desired.

I/O port (Input/Output port)

A pathway into and out of the computer. Also, an address used for input or output.

IP (Internet Protocol)

Moves packets of data from node to node. See TCP/IP.

IPv4 (Internet Protocol Version 4)

The current implementation of the Internet Protocol.

IPv6 (Internet Protocol Version 6)

The next version IP protocol, completed in 1997 by the IETF. IPv6 is backward compatible with and designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses.

IPv6 increases the address space from 32 to 128 bits, providing for practical purposes an unlimited number of networks and systems. It also supports quality of service (QoS) parameters for realtime audio and video.

IP address

The standard way to identify a computer connected to the Internet. Each IP address consists of eight octets expressed as four numbers between 0 and 255, separated by periods, for example: 176.31.23.13.

The TCP/IP packet uses 32 bits to contain the IP address, which is made up of a network and host address (netid and hostid). The more bits used for network address, the fewer remain for hosts. Certain high-order bits identify class types and some numbers are reserved. The Class Number is the decimal value of the high-order eight bits, which identifies the class type. Class C addresses have been expanded using the CIDR addressing scheme.

IP Alias

The GNAT Box system software facility that allows a network interface to have multiple IP addresses. If used on an External Network interface connected to the Internet, IP aliases must be registered IP addresses.

IP Pass Through

GTA term for "no NAT." Allows a host, subnet or network to be defined that will not have *NAT* applied to packets from specified

IP addresses. By default, IP Pass Through-designated IP addresses are configured for outbound only. If the connection protocol calls for a secondary inbound connection from an external host to the originating internal host, *virtual cracks* are created to allow the secondary connection.

IPSec (IP Security) protocols

The IPSec protocols provide for security of Internet Protocol (IP) communications where routing and relaying of data between network nodes are managed. Two protocols are described, AH and ESP.

IRQ (Interrupt ReQuest)

A hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

ISDN (Integrated Services Digital Network)

Supports transmission of voice, data, and image-based communications in an integrated form.

ISP (internet service provider)

An organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private lines such as T1. Large services may also provide proprietary databases, forums and other services.

J

Java

A programming language developed by Sun and modeled after C++ to generate cross-platfrom applications. Java applications can be run stand-alone or can be called by web pages and run on a user's machine (applet) or run on a Web server (servlet).

K

keep alive

A packet sent by one end of a connection to notify the other end to remain connected.

key, keyword, key sequence

A sequence of symbols that used with a cryptographic algorithm enables encryption and decryption. The security of the cryptosystem is dependent on the security of the key.

key exchange

The process for getting session keys into the hands of the conversants.

key strength, cipher strength

The number of bits in the key. The greater the number of bits, the stronger the key.

private key/public key

Traditional cryptography, such as DES, uses a secret key, in which the sender and receiver use the same key to encrypt and decrypt. It's fast, but the key is not transmitted securely.

Public-key cryptography, such as RSA, uses both a private and a public key. Each recipient has a private key that is kept secret and a public key. The sender looks up the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message. Owners never need to transmit their private keys so they are not vulnerable.

L

L2TP (Layer 2Tunneling Protocol)

A protocol from the IETF for creating virtual private networks (VPNs) over the Internet. It supports non-IP protocols such as AppleTalk and IPX as well as the IPSec security protocol. It is a combination of Microsoft's Point-to-Point Tunneling Protocol and Cisco's Layer 2 Forwarding (L2F) technology.

LAN (Local Area Network)

A network that consists of a single type of data link and can reside entirely within a physically protected area.

LDAP (Lightweight Directory Access Protocol)

A protocol used to access a compliant directory listing. LDAP will provide a method for searching email addresses on the Internet, eventually leading to a global white pages. LDAP is a sibling protocol to HTTP and

FTP and uses the ldap:// prefix in its URL. LDAP is a simplified version of the DAP protocol, used to access X.500 directories.

lifetime

Value that specifies how long the IKE SA exists. The lifetime specifies a length of time and a specific amount of data. When either value is reached, the SA is terminated and the VPN peers will establish a new key. The software determines this value during each phase. Each phase has a separate lifetime.

Link Control Protocol (LCP)

link hardware encryption

See hardware encryption.

lockout

When a user is locked out for a specific duration because of login failure.

logical name

The name given to an interface; the name of the interface object.

M

MAC address

The unique serial number burned into Ethernet and Token Ring adapters that identifes that network card.

Manual Key Exchange

Manual key exchange is a means for exchanging cryptographic keys between VPN peers. Each side must manually enter both the remote and local shared key to initiate the VPN tunnel. The keys do not change.

mapping

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.

MD5 (Message Digest 5)

See one-way hash function and encryption algorithm.

message digest

A condensed text string that has been distilled from the contents of a text message. Its value is derived using a one-way hash function and is used to create a digital signature.

MIB (Management Information Base)

An SNMP structure that describes the device being monitored, what is obtainable from the it, and what can be controlled

MIME (multipurpose Internet mail extensions)

Lets one transfer non-textual data, e.g. graphics, etc.

mobile code blocking

Blocking for JAVA, JAVA Script and ActiveX objects is built into the GNAT Box systems. These objects or scripts appear in inbound HTML on TCP port 443, 80, 8000 and 8080.

MTU (Maximum Transmission Unit)

A link layer restriction on the maximum number of bytes of data in a single transmission (i.e., frame, cell, packet). See also *fragmentation*.

Some typical values for MTUs, taken from RFC-1191:

MTU	Where Commonly Used
65535	Hyperchannel
17914	16 Mbit/sec token ring
8166	Token Bus (IEEE 802.4)
4464	4 mbit/sec token ring (IEEE 802.5)
1500	Ethernet
1500	PPP (typical; can vary widely)
576	X.25 Networks

Path MTU

The smallest MTU of any link on the current path between two hosts. This may change over time since the route between two hosts, especially on the Internet, may change over

time. It is not necessarily symmetric and can even vary for different types of traffic from the same host.

DF (Don't Fragment) bit

This is a bit in the IP header that can be set to indicate that the packet should not be fragmented by routers, but instead an ICMP "can't fragment" error is returned sent to the sender and the packet is dropped.

ICMP Can't Fragment Error

This error (type 3 (destination unreachable), code 4 (fragmentation needed but don't-fragment bit set)) is returned by a router when it receives a packet that is too large for it to forward and the DF bit is set. The packet is dropped and the ICMP error is sent back to the origin host. Normally, this tells the origin host that it needs to reduce the size of its packets if it wants to get through. Recent systems also include the MTU of the next hop in the ICMP message so the source knows how big its packets can be. Note that this error is only sent if the DF bit is set; otherwise, packets are just fragmented and passed through.

MSS (maximum segment size)

MSS can be announced during the establishment of a TCP connection to indicate to the other end the largest amount of data in one packet that should be sent by the remote system. Normally the packet generated will be 40 bytes larger than this; 20 bytes for the IP header and 20 for the TCP header. Most systems announce a MSS that is determined from the MTU on the interface that the traffic to the remote system passes out from the system through.

Path MTU Discovery (PMTU-D)

One solution to the problem of fragmentation is Path MTU Discovery. The idea behind it is to send packets that are as large as possible while still avoiding fragmentation. A host does this by starting by sending packets that have a maximum size of the lesser of the local MTU or the MSS announced by the remote system. These packets are sent with the DF bit set. If there is some MTU between the two hosts which is too small to pass the packet successfully, then an ICMP can't fragment error will be sent back to the source. It will then know to lower the size; if the ICMP message includes the next hop MTU, it can pick the correct size for that link immediately, otherwise it has to guess.

MX (Mail Exchange)

See *zone file*.

N

name server

A computer that has both the software and the data (zone files) needed to match domain names to IP addresses

name service

A service that provides individuals or organizations with domain name-to-IP address matching by maintaining and making available the hardware, software, and data needed to perform this function.

NAT (Network Address Translation)

A router connecting two networks together; one designated as inside is addressed with either private or obsolete addresses that needs to be converted into legal addresses before packets are forwarded onto the other network (designated as outside).

An IETF(Internet Engineering Task Force) standard that allows an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet and vice versa. It also serves as a firewall by keeping individual IP addresses hidden from the outside world. See proxy server.

NetBIOS (Network Basic Input/Output)

Network programming interface allowing applications to communicate across a network.

netmask

In a GTA Firewall configuration, when not applied to a network address, the netmask is a means to specify a single IP address or a group of contiguous IP addresses.

network

See also: *Protected, External and Private Service Networks*. A collection of devices and connectors that create a physical connection to allow communication between users, usually differentiated by being reached by using a common network address. For purposes of discrimination, a network is a group of devices linked by a common network addresses, either separate or part of an internet, and separate or part of THE Internet;
i.e., "This office's network is linked to three other networks to make up our company internet (physical structure). Our company internet carries the information exchanged and generated by people within our intranet, including those who can become part of our internet by a virtual (VPN) link. Our customers can reach us through an extranet that includes access to some information that is also available to our intranet, some of which is housed within our internet and some housed on servers accessed over the Internet (whole world internet). Our employees can access information over the Internet from the World Wide Web only if we authorize it."

extranet

(1) A subset of a body of knowledge common to and available to a particular organization that is available to a group outside the organization;
(2) the group defined by access to this knowledge subset.

Internet

The physical networked structure that underlies the worldwide, omnipresent information exchange.

internet

A connected group of two or more networks. (The Internet is an internet, but an internet is not THE Internet.; an internet may or may not be connected to THE Internet.) Also: internetwork

intranet

(1) A body of knowledge common to a particular organization over a network, internet (internetwork), and/or the Internet that is denied to all others;
(2) the group defined by such access.

subnet

A portion of a network defined by the subset of a network address to which it belongs. (This concept is somewhat analogous to the four-digit zip code addition that specifies which part of that zip code area the address belongs.)

World Wide Web

Refers to the entire virtual space for information exchange created by the Internet. Also: WWW; Web.

network adapter

See NIC.

network encryption

Crypto services applied to information above the data link level but below the application software level. This allows crypto protections to use existing networking services and existing application software transparently.

network transparency

Network Transparency is a term used to describe the function that allows host systems residing on hidden networks (PSNs and Protected Networks) to send packets to and receive replies from hosts on external networks in a transparent manner. Network Transparency is implemented as part of the GNAT Box stateful packet inspection facility. The state of all connections is maintained by the system in a series of tables aong with other connection information that ensures that only authorized packets are accepted. Network Transparency allows GTA Firewalls to operate without the need for permanent holes in the firewall as required by typical IP filtering.

Network Time Protocol (NTP)

An Internet protocol used to synchronize the clocks of computers to some time reference. NTP is an Internet standard protocol originally developed by Professor David L. Mills at the University of Delaware.

NIC (Network Information Center)

See InterNIC.

NIC (Network Interface Card)

Also network adapter. A printed circuit board that plugs into both the clients (personal computers or workstations) and servers and controls the exchange of data between them. It provides services at the data link level of the network, which is also known as the "access method" (OSI layers 1 and 2).

A transmission medium, such as twisted pair, coax or fiber optic, interconnects all adapters to network hubs or switches, or in the case of a bus network, to each other. Ethernet, Token Ring and Apple's LocalTalk are common network adapters. The equivalent circuitry may be built directly into the motherboard.

NIST (National Institute of Standards & Technology)

The standards-defining agency of the U.S. government, formerly the National Bureau of Standards. www.nist.gov.

node

A point of concentrated communications; a central point of communications. Switching devices are often called nodes because they form the junctions between routes or trunks in a data network.

Null Tunnel Mode

In the Null Tunnel mode, no encryption or authentication is used. This mode is useful when only IP encapsulation is desired, such as to utilize unsupported protocols in the NAT mode between two GNAT Box protected networks. To configure the VPN for the Null Tunnel mode, set AH to none and ESP to Null.

O

object

In programming, an item that can be identified, selected and moved or manipulated. An object can be a program, a picture, a chart, a shape or a software entity containing data and/or executables.

octet

An eight-bit storage unit. In the international community, octet is often used instead of byte.

octal

A numbering system that uses eight digits. It is used as a shorthand method for representing binary characters that use six bits. Each three bits (half a character) is converted into a single octal digit.

Open System Interconnection (OSI)

A system capable of transparently operating in telecommunications environments of dissimilar computers. Usually refers to the International Standard Organization (ISO) seven layered protocol model for the exchange of information between open systems

P

packet

A sequence of data and control characters (binary digits) in a specified format that is switched/transferred as a whole.

packet-switching

The process of routing and transferring data by means of addressed packets so that a channel is occupied only during the transmission of the packet. No physical connection is necessary. The packets are routed throughout the network towards their destination where the entire message is reconstructed. Upon completion of the transmission, the channel is made available for the transmission of other traffic.

PAP (Password Authentication Protocol)

An authentication protocol that allows PPP peers to authenticate on another, does not prevent unauthorized access but merely identifies the remote end.

parse

Collecting and organizing into components; for example, compilers parse source code so it can be translated into object code. Parsing consists of two activities, lexical analysis and semantic parsing. Lexical analysis divides strings into components and semantic parsing determines the meaning of the strings.

password, pass code

A sequence of characters or words that a subject submits to a system for purposes of authentication, validation, or verification.

PCMCIA card

A credit card size memory or PC card that meets the PC Card Standard developed jointly by the Personal Computer Memory Card International Association (PCMCIA) and the Japan Electronic Industry Development Association (JEIDA).

PDC (Primary Domain Controller)

A Windows NT service that manages security for its local domain. Every domain has one PDC, which contains a database of usernames, passwords and permissions.

BDC (Backup Domain Controller)

PFS (Perfect Forward Secrecy)

Compromise of a single key will permit access only to data protected by that key. For PFS to exist the key used to protect transmission of data must not be used to derive any additional keys, and if the key used to protect transmission of data is derived from some other keying material, that material must not be used to derive any more keys.

Any one of the three PFS algorithms below may be used below to generate keys.

Diffie-Hellman Group 1

Diffie-Hellman Group 2

Diffie-Hellman Group 5

Phase I

In IKE, a phase one exchange establishes a security association. This phase negotiates the terms of the VPN, authenticates the validity of the VPN peer, and sets the parameters of the VPN connection.

Phase II

In IKE, a phase two exchange establishes security associations for other protocols. This phase provides source authentication, integrity, and confidentiality to all messages.

physical network address

A host address on a data link.

ping

An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Ping also functions like a domain name (DNS) server, because "pinging" a domain name will return its IP address. Mike Muuss, who wrote ping, said that the name comes from the sound a sonar signal response makes. Ping is commonly believed to be an acronym of Packet INternet Groper.

POP (Post Office Protocol)

An Internet protocol for retrieving email from a server host.

port number

In a TCP/IP-based network such as the Internet, it is a number assigned to an application program running in the computer. The number is used to link the incoming data to the correct service.

well-known port/service

A protocol port number from 0 through 1023 that is widely used for a certain type of data on the network. For example, World Wide Web traffic (HTTP packets) is typically assigned port 80, FTP transfer is port 20, and Kerberos authentication is port 88.

PPP (Point-to-Point Protocol)

The communications protocol used to dial up the Internet over a serial link, such as an IDSN line. Developed by the Internet Engineering Task Force in 1994, it superseded the SLIP protocol. PPP establishes the session between the user's computer and the ISP using the Link Control Protocol (LCP), which also handles authentication (PAP, CHAP, etc.), compression and encryption.

The Multilink PPP protocol (MP, MPPP or MLPPP) bridges B channels for higher speed.

PPPoE (PPP over Ethernet)

A method for running the PPP protocol, commonly used for dial-up Internet connections, over Ethernet. Used by DSL and cable modem providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point

connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

PPTP (Point-to-Point Tunneling Protocol)

A specialized PPP (point-to-point) transport protocol for some Microsoft products. A PPTP connection allows a link from a non-routable internal IP address to an external IP address through the use of an internal PPTP server with a routable IP address.

preshared encryption keys

Only available when using the IKE VPN setup. The Preshared Encryption Key is used to initiate communication with the other side of the VPN. Hence, the Remote Key would be the Local Key of the VPN's other side. [Both side's Local Keys together are the Preshared Encryption Keys.] The Local and Remote Keys should be unique to their respective firewalls.

Note: The Local Key will remain the same for all IKE VPNs on a specific firewall.

private key, secret key

The privately held "secret" component of an integrated asymmetric key pair. See *key*.

Private Service Network

The Private Service network (PSN) (also known as a DMZ network) is an optional service network that is located logically between the External network and the Protected network, but nearly at a peer level with the Protected network. The PSN 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.

Protected Network

The Protected network is the network hidden behind the GNAT Box system. The term Protected network is used by GTA 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 by default not 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.

protocol

The procedures that are used by two or more computer systems so they can communicate with each other.

proxy server

Also called a "proxy" or "application level gateway," it is an application that breaks the connection between sender and receiver. By hiding the IP address of the receiver from the sender, it prevents the sender from obtaining internal addresses and details of a private network.

Proxy servers are available for common Internet services; e.g., an HTTP proxy is used for Web access, and an SMTP proxy is used for email. Proxies generally employ network address translation (NAT), which presents one organization-wide IP address to the Internet. It funnels all user requests to the Internet and fans responses back out to the appropriate users.

public key

A key used in public key crypto that belongs to an individual entity and is distributed publicly. Others can use the public key to encrypt data that only the key's owner can decrypt. See Key.

public key algorithm

A cipher that uses a pair of keys, a public key and private key, for encryption and decryption; also called an asymmetric algorithm.

R

RAID (Redundant Array of Independent Disks)

(Formerly, "inexpensive")

A disk subsystem that is used to increase performance and/or provide fault tolerance, a set of two or more hard disks with a disk controller that contains the RAID functionality. RAID improves performance by disk striping, which interleaves bytes across multiple drives, so that disks can be used simultaneously. See information pubished by the RAID Advisory Board at www.raid-advisory.com.

registry

See *ARIN*.

RDNS (Reverse DNS)

See *DNS*.

reboot

Reboot restarts the remote GTA Firewall. This action will terminate the Web interface's network connection to the web server.

replay detection

See *anti-replay protocol*.

RFC (Request for Comments)

A document that describes the specifications for a recommended technology. The IETF has published more than 2500 RFCs, all of which can be viewed at www.ietf.org/rfc.

RFC 1918 numbers

IANA has reserved the following three blocks of the IP address space for private internets:

```
10.0.0.0  - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Rijndael (AES)

See *encryption algorithm*.

RIP (Routing Information Protocol)

Evolving dynamic routing protocol, c.f. www.ietf.cnri.va.us/html.charters/rip-charter.html

router

An internetworking switch operating at the OSI Level 3, the Network Layer.

routing protocol

A formula used by routers to determine the appropriate path onto which data should be forwarded. The routing protocol also specifies how routers report changes and share information with the other routers in the network that they can reach.

EGP (Exterior Gateway Protocol)

A broad category of routing protocols designed to span different systems. Also, the original exterior gateway routing protocol, a distance vector protocol, superseded by BGP.

BGP

A path vector routing protocol used to span autonomous systems, developed by the IETF. BGP4 supports the CIDR addressing scheme.

RTS (Request To Send)

An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit. See *CTS*.

runtime

In GTA documentation, refers to the GTA software executable, e.g., "the GNAT Box System Software version 3.5 runtime."

S

SCSI (Small Computer System Interface)

A set of parallel interface standards developed by ANSI; used for attaching peripheral devices such as printers and drives to computers. SCSI interfaces provide for faster data transmission rates (up to 80 Mbytes per second) than standard serial and parallel ports. Because you can attach many devices to a single SCSI port, SCSI really is an input/output bus rather than a simple interface. Because there are many variants of SCSI, two SCSI interfaces may not be compatible.

Security Association (SA)

Identified by a unique triple of IP Address, SPI (numeric ID) and security protocol (e.g. ESP, AH). Specifies the parameters for communication connecting two hosts. Each two-way connection uses a minimum of two SAs, one for each direction of communication. Any time a defined VPN is active (in use, or not yet timed out), it will use at least two SAs.

serial number

The number used to identify an individual GTA hardware or software product. Each GTA Firewall, for example, has a serial number that must be entered in the Features screen, along with an *activation code*.

server

Computer devices or processes that provide service to clients in client/server architecture.

session

A single communication transaction.

session key

The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key or set of session keys is used for each communication session.

SGML (Standard Generalized Markup Language)

A set of rules developed by the ISO in 1986 for organizing and tagging elements of a document. The tags can be interpreted to format document elements in different ways. HTML interprets tags according to SGML rules.

SHA-1 (Secure Hash Algorithm-1)

See *encryption algorithm*.

SKIP (Simple Key Interchange Protocol)

A protocol that establishes session keys to use with IPSec protocol headers. SKIP data is carried in packet headers and travels in every IPSec-protected packet. Developed by Sun Microsystems, Inc.

SMTP (Simple Mail Transfer Protocol)

An Internet protocol for transmitting email between email servers.

SNMP (Simple Network Management Protocol)

A standard for managing IP devices, retrieving data from each device on a network and sending it to designated hosts. In its full implementation, SNMP enables both read and write access. In GNAT Box System Software, the SNMP facility is *read-only*. It does not allow the write access needed for control and configuration. The data, contained in a MIB (Management Information Base) and organized in report form, helps the administrator ensure optimal performance in the managed devices.

SNMP version 2 provides enhancements including security and an RMON (Remote Monitoring) MIB, which provides continuous feedback without being queried by the SNMP facility. SNMP version 3 introduced a revised nomenclature for SNMP, a new access method using authentication, and the ability to encrypt SNMP data packets.

SOCKS

A protocol that provides for firewall transversal for client-server applications.

sockets

The package of subroutines that provide access to TCP/IP on most systems.

SPI (Security Parameter Index)

Used to uniquely identify which SA should be applied to a packet. The SPI values should be unique for each SA. The inbound and outbound value may be the same for a given SA. Should be a value greater than 256.

SPI (Service Provider Interface)

The programming interface for developing Windows drivers under WOSA. In order to provide common access to services, the application (query, word processor, email program, etc.) is written to a particular WOSA-supported interface, such as ODBC

or MAPI, and the developer of the service software (database manager, document manager, print spooler, etc.) writes to the SPI for that class of service.

spoof

See *address spoof*.

SQL (Structured Query Language)

Set of commands used to create, access, query, modify, and otherwise manage relational databases.

SSL (Secure Sockets Layer)

In SSL, when a session is started, the server sends its public key to the browser, and the browser uses it to randomly generate a secret key. This is sent back to the server as key exchange for that session. Supports server and client authentication and maintains the security and integrity of the transmission channel. Developed by Netscape.www.netscape.com/eng/security/SSL_2.html.

Standby/Slave Update

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

stateful packet inspection

A firewall technology that monitors the state of a transaction to verify that an inbound packet's destination matches the source of a previous outbound request, assuring that the inbound packet was actually requested.

static address mapping

See *mapping*.

Static NAT

See *Network Address Translation*.

static routing

Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

stealth mode

Stealth mode is the factory set default for new GTA Firewall systems, activated at the system kernel level. The firewall will not respond to ICMP ping or traceroute requests, nor to UDP traceroute requests. Filters that allow pings, traceroutes, etc., from the External interface are not functional when the firewall is in stealth mode. The firewall will not respond with an ICMP message when a packet arrives for a port without a tunnel or service set on any External Network interface. Like all Automatic Filters, Stealth mode has priority over the other filter types.

string

A series of characters that do not mean anything in particular and that are manipulated as a group.

synchronous transmission

The entire message is sent with control information surrounding the text portion of the transmission.

T

TA (Terminal Address)

Terminal identifier in P1024B protocol.

T1, T3

A digital communications line which has a capacity of 1.544 Mbps (megabits per second); A digital communications line having a capacity of 44.736 Mbps.

TCP/IP (transmission control protocol/ internet protocol)

A communications protocol developed to internetwork dissimilar systems.

TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. UDP, which is part of the TCP/IP suite, is an alternate transport that does not guarantee delivery. It is widely used for realtime voice

and video transmissions where erroneous packets are not retransmitted.

TCP/IP is a routable protocol, and the IP part of TCP/IP provides the routing capability. In a routable protocol, all messages contain not only the address of the destination station, but the address of a destination network. Every client and server in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at startup.

telnet

Virtual terminal protocol that enables remote log-ons to computers across a network.

timeout

Timeouts define how long a connection should be idle before it is marked ready to close. The result of a connection reaching its timeout value differs for each IP protocol.

time server

See *NTP*.

token

A single element of a programming language, as used in parsing. A password as used in token authentication. A data item as used in token email. A data structure as used in token rings.

trace route

An Internet utility that describes the path in realtime from the client machine to the remote host being contacted. It reports the IP addresses of all the routers in between. Windows comes with its own Traceroue utility (TRACERT.EXE) that is executed from the command line.

transparency

Allowing an application to perform on a circuit/connection without impacting on the usual operations or the operators of the circuit. See Network Transparency.

transport mode

In IPSec protocols, transport mode generally refers to security associations between hosts. Security protection is extended to only selected portions of the association.

TTL (Time To Live)

Lifetime in seconds or number of transmissions of a packet.

tunnel, tunnel mode

A secure virtual connection through the Internet or an intranet. In IPSec, tunnel mode generally refers to a security association in which an "outer" IP header specifies the IPSec processing destination while an "inner" IP header specifies the ultimate destination of the packet. In IPSec protocols, tunnel mode is required for gateway to gateway security associations unless one gateway is acting as a host, then *transport mode* is allowed.

inbound tunnel, GNAT Box tunnel

Allows a host on an external network to be able to initiate a protocol with an otherwise inaccessible host for a specific service. Tunnels can be defined for both the External Network and the PSN; tunnels are only associated with inbound connections, so they are not used on a Protected Network interface. Tunnels can be created only for these inbound connections:

1. From the External Network interface to a host on the PSN.
2. From the External Network interface to a host on the Protected Network.
3. From the PSN interface to a host on the Protected Network.

A GNAT Box inbound tunnel should not be confused with a VPN, which provides secure gateway-to-gateway tunneling, IP Pass Through or GNAT Box System Software's bridging mode.

U

UDP (User Datagram Protocol)

Defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol.

unexpected packets

If a packet is valid, but not expected by the state table, the firewall denies it, e.g., a packet can only generate a single ICMP port unreachable response; a second one may indicate an *ICMP replay* attack; also, an unexpected packet may be a packet that does not have the correct flags during TCP's three-way handshake.

URL (Uniform Resource Locator)

Address that defines the route to a web page or other file on a web server that contains the protocol prefix, port number, domain name, subdirectory names and file name. Port 80 is the default port if none is defined. See the following explanation of the sample URL: `http://www.example.com/sub/fuzzy.htm:80`

http:	protocol
//	separators
www	prefix
.example.com	domain
/sub	subdirectory
/fuzzy.htm	HTML file
:80	port

V

virtual crack

Traditional IP filtering requires that holes be created in the firewall to allow packets to be accepted for arbitrary inbound connections. Since many application protocols create arbitrary secondary inbound connections, additional holes must be created to accept a wide range of possibilities.

A virtual crack is part of the GNAT Box stateful packet inspection technology which allows secondary inbound connections to be accepted without a dedicated hole in the firewall. A virtual crack is automatically configured when the GTA Firewall detects the signature of a nonstandard protocol packet passing outbound using secondary connections. The virtual crack stays in place until the connection is shut down, expires due to inactivity, or the expected protocol event does not occur, (e.g., a client crash). For more information, see *IP Pass Through*.

virtual firewall

The virtual firewall consists of both physical GTA Firewall systems in an H2A group yet appears as a single system to network users.

Virtual Firewall IP Address

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

VPN (Virtual Private Network)

A private network built atop a public network. Hosts within the private network use encryption to talk to other hosts. The encryption excludes hosts from outside the private network even if they are on the public network.

VRID (Virtual Router ID)

VRID defines a HA Group. All members of an HA Group should have the same VRID. Valid VRID values are 0-15.

W

well-known port/service

See port number.

WAN (Wide Area Network)

A network that connects host computers and sites across a wide geographical area.

WELF (WebTrends Enhanced Log Format)

The format used by GTA Firewalls to record log messages. For more information about WELF, see `www.netiq.com/partners/technology/welf.asp`.

X

X.500

An OSI protocol for managing online directories of users and resources, called a "Directory Information Base" (DIB) or white pages. It provides a hierarchical structure that fits a standard classification system, by country, state, city, street, family, etc. The goal is to have a global directory.

XML (Extensible Markup Language)

An open standard used for defining data elements on a web page. It has tags similar to HTML, but it allows a web page to function like a database record.

Z

zone file

A zone is the portion of the total domain name space stored on a particular name server. Zone files in DNS server databases contain the information needed to match domain names to IP addresses through lookup (host name to IP address), reverse lookup (IP address to host name), and a file of host names and IP addresses for name servers on that maintain the root domains. See *DNS*.

A record

IP address entry in a database.

CNAME (Canonical) name

Alias of an IP address. A statement in a DNS database (zone file) that assigns an alias to the true (canonical) name of the server.

MX record

Entry in a domain name database that identifies the mail server responsible for handling email for the domain.