

GNAT *Box* VPN

and

VPN Client

with SoftRemoteLT from SafeNet, Inc.



Feature Guide

a *GNAT Box*
System Software Option



Copyright

© 1996-2003, Global Technology Associates, Incorporated (GTA). All rights reserved.

GTA acknowledges all trademarks appearing in this document. This product includes software developed by the University of California, Berkeley, and its contributors. Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

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

GNAT Box is a registered trademark of Global Technology Associates, Incorporated.

RoBoX is a trademark of Global Technology Associates, Incorporated.

SafeNet VPN client SoftRemoteLT is a trademark of SafeNet, Inc.

All other products are trademarks of their respective companies.

Version Information

SafeNet VPN client SoftRemoteLT version 8.0.2

October 2002

GNAT Box System Software version 3.3.2

November 2002

Technical Support

GTA's direct customers in the USA should email GTA via the contact information listed below. Other customers should contact their local GTA authorized reseller.

Contact Information

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

Support: support@gta.com

Document Information

GNAT Box VPN Feature Guide
with GNAT Box System Software Version 3.3.2

November 2002 – updated 2/6/03

Contents

1 INTRODUCTION	1
About GNAT Box VPN	1
Features	1
Requirements	2
About VPN Client	2
Registration & Activation	3
Feature Activation Codes	3
Installation Support	4
Additional VPN Client Licenses	4
Documentation	5
Documentation Conventions	5
Additional Documentation	6
2 VPN CONCEPTS	7
Overview	7
Authentication & Integrity	7
Confidentiality	8
VPN Operation	8
Packet Flow	9
Outbound	9
Inbound	10
Tunnels	10
Null Tunnel Mode	10
Encapsulating Security Payload (ESP)	11
Access Control	11
Hash Algorithms	12
Encryption Methods	13
Manual Key Exchange VPN	14
Internet Key Exchange (IKE) VPN	14
Mobile IKE	17
3 VPN CONFIGURATION	19
Overview	19
VPN Objects	19
Default VPN Objects	19
Interface Variations	22
VPN Authorization	23
Remote Access Filters	26
Manual Key Exchange	26
IKE	26
Mobile IKE	26
IP Pass Through Filters	26

Examples	27
Manual Key Exchange	27
IKE Configuration	30
4 CLIENT INSTALL & CONFIGURATION	35
Overview	35
Quickstart	35
VPN Client User Interface	36
VPN/SafeNet Taskbar Icons	36
VPN Client Menu	37
Installation	39
Mobile VPN Client Activation Code	39
Software Installation	40
Uninstalling	42
Configure the VPN Client	42
1. Start the Security Policy Editor	43
2. Add a New Connection	43
3. Remote Party Identity and Addressing	44
4. My Identity	45
5. Security Policy	47
6. Authentication (Phase I)	48
7. Key Exchange (Phase II)	48
8. Save the Security Policy	49
Firewall Configuration	50
User Authorization	50
VPN Objects	52
Remote Access Filters	53
IP Pass Through Filters	54
Mobile User Authentication	56
Remote Access Filter	57
Mobile VPN Example	58
5 TROUBLESHOOTING	61
VPN Client Q&A	61
GTA Firewall Log Messages	61
VPN Client Log Viewer	62
APPENDIX	69
VPN Client Examples & Worksheet	69
INDEX	71

1 Introduction

About GNAT Box VPN

A Virtual Private Network (VPN) is essentially a system that allows a private and secure network connection over a potentially insecure public network. A VPN extends a company's ability to exchange data and communications confidentially anywhere that a public network is in place. Using a VPN, employees, clients and partners can access necessary information while not breaching the security of the company's internal network. Between two firewalls, a VPN provides secure gateway-to-gateway communications.

The benefits of VPN include: global connectivity, even for small companies; improved security; more cost effective than a physical network connection; less time and money spent when connecting remote users; simplified network topology; and telecommuting support.

GNAT Box System Software's VPN facility is based on the Internet Engineer Task Force (IETF) Internet Protocol Security (IPSec) standard. IPSec is designed for use in interconnected systems of packet-switched computer communication networks. It provides for transmitting blocks from sources to destinations, which are identified by fixed-length addresses. The protocol is specifically limited in scope to provide the functions necessary to deliver a datagram from source to destination, so there are no mechanisms for other services found in host-to-host protocols.

Features

- Configuration of security policies.
- Easy to use graphical user interface.
- Creation and deployment of secure custom installations for easy setup.
- AES, 3DES, DES, Blowfish, Twofish, MD5, SHA-1 and SHA-2 encryption algorithms.
- Easy creation of VPN definition through the use of VPN Objects.
- Quickly enable and disable VPN authorizations.

Requirements

- Supported GTA Firewall.
(GB-Pro offers only gateway to gateway VPN.)
- GNAT Box System Software version 3.2 or higher.

VPN Client Requirements

- PC compatible with a Pentium 75 MHz processor or equivalent.
- Windows operating system: 32Mb-64Mb.
- 10 MB hard disk space.
- Native Microsoft TCP/IP protocol.
- Non-encrypting modem and native Microsoft PPP dialer for dial-up connections or Ethernet for network connections.
- Microsoft Internet Explorer 5.0 or later for viewing on-line help files.

About VPN Client

GNAT Box VPN Client is a Windows-compatible software product that secures data communications sent from a desktop or laptop computer across a public or private TCP/IP network. When the GNAT Box VPN Client operates on an unprotected public network, such as the Internet, it creates a virtual private network (VPN) between end users. GNAT Box VPN Client is not available for GB-Pro.

GNAT Box VPN Client is based on SafeNet VPN client SoftRemoteLT version 8.0.2, the most widely used VPN Client in the industry.

Note

The VPN Client supports X.509 certificates and so can be used with other IPSec VPN systems that support certificates. However, GTA Firewall systems do not currently support the use of certificates.

Network Applications

The GNAT Box VPN Client supports secure communications for client-to-gateway and client-to-client connections. “Road warriors” can telecommute to the main office through the Internet or another remote access method for secure client-to-gateway communications. Organizations requiring a low-cost solution for secure communications among their employees or members across a private LAN, WAN, or dial-up connection can use the GNAT Box VPN Client for secure client-to-client communications.

Interoperability

Because the GNAT Box VPN Client is an industry-standard IPSec VPN, it can interoperate with many IPSec-compliant devices from major equipment manufacturers. The GNAT Box VPN Client interoperates with IPSec-compliant gateways such as firewalls, VPN routers and gateway encryptors.

Compatibility

All NDIS-compliant Ethernet network interface cards (NICs) should be compatible with this product. Windows 95, 98, 2000, ME and XP are supported. Windows NT and 2000 servers and the plug-and-play feature on Windows NT notebook computers are not supported.

Registration & Activation

If you have not yet registered your firewall product, go to www.gta.com, click on Support and then the GTA Support Center link. This takes you to the login screen. Click New Account, enter your profile information and choose a user ID and password. Once you have completed the form, click Add to save it.

In the login screen, enter your user ID and password. In the Make a Selection screen, click Support Center, then Product Registration. Enter your product serial number and activation (unlock) code, then click Submit.

Feature Activation Codes

Optional features on GTA Firewalls require activation codes. VPN is provided with the GB-100, GB-1000, GB-Flash and RoBoX-25, and a single mobile client session is also included (GNAT Box System Software version 3.2 and up). The session is part of product activation on GB-100, GB-1000 and GB-Flash, but requires a separate feature activation code on RoBoX-25. (VPN is provided as an optional feature on RoBoX-10.) For multiple concurrent mobile client sessions, a license will be provided with a feature activation code that authorizes the desired number of concurrent sessions.

Note

If the feature code does not appear under Registered Products, please email support with your product serial number and Support Center User ID in the message subject.

The feature activation code for your license can be found in Registered Products by selecting the serial number of your GTA Firewall on GTA Support. Copy the feature activation code and enter it in the Features screen in the next available row. Click Save. The appropriate license will be displayed.

Copy Protection

Copying of GNAT Box System Software is allowed for backup purposes, but to activate your systems, you need a serial number and activation codes. Keep a copy of these codes; the codes will also continue to be available online at the GTA Support Center after completing product registration.

Installation Support

Installation ("up and running") support is available to registered users. If you have registered your product and need installation assistance during the first 30 days, contact the GTA Support team by email at support@gta.com.

Include in the email your product name, serial number, registration number, feature activation code numbers for your optional products, and a System or Hardware Configuration Report, if possible.

Installation support covers only the aspects of configuration related to installation and activation of a VPN option within the first 30 days of purchase of a firewall or VPN Client license. This support covers setting up the GNAT Box VPN Client in its default setting, configuring the firewall for VPN Client and confirming connectivity.

If you need further assistance, contact the GTA Sales staff to purchase a support contract. Contracts range from support by the incident to full coverage for a year. Other avenues for assistance are available through the GNAT Box Mailing List and Forum, found at www.gta.com, or through an authorized GTA Channel Partner.

Additional VPN Client Licenses

GB-Flash, GB-1000 and RoBoX-25 each include a license for one concurrent VPN Client session. If you would like to buy licenses for additional VPN Client sessions, contact the sales department.

Exception

The RoBoX-10 offers VPN as an option.

When purchasing an additional multiple VPN Client license, you will be able to access a newly generated feature activation code on GTA's website under Registered Products. This new code will activate the total number of VPN licenses purchased; if you initially had a five-user license and upgraded to 10, the new code will activate 10 total licenses.

You can add your new license in the next available line in the Features screen. It is not necessary to delete your old license as only the code for the highest number of VPN licenses will be active.

Documentation

This Product Guide explains how to set up and use the VPN and VPN Client. The **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** includes configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms

To see more examples of VPN and VPN Client configurations, go to the GTA Support Center on the www.gta.com website.

Documentation Conventions

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

Documentation Conventions

SMALL CAPS	Field names.
BOLD SMALL CAPS	Names of publications.
<i>Bold Italics</i>	Emphasis.
Courier	Screen text.
<brackets>	Names of keyboard keys, e.g., <Return>, <F12>.

Notes are indicated by an indented, italicized headline.

The note body copy is further indented.

"How to" sections are indicated by an indented, bold headline.

The "How to" body copy is unbolded and closed with a rule line.

Additional Documentation

Documentation is available for GTA Firewall product owners. Product Guides show how to install and set up GTA Firewall products. Feature Guides describe GTA optional features. The **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE** includes advanced configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms.

Documentation Map

Topic	Document Name	Location
Installation	Product Guides	Shipped w/product*
System Setup	Product Guides	Shipped w/product*
GNAT Box Concepts	Concepts	www.gta.com
Troubleshooting	User's Guide or Product Guides	Shipped w/product, CD*
Configuration examples	–	www.gta.com
Sample reports	–	www.gta.com
Ports & Services	User's Guide	Shipped w/product, CD*
Drivers & NICs (Pro, Flash)	Product Guides	Shipped w/product*
GTA Firewalls	Product Guides	Shipped w/product*
Content Filtering	Surf Sentinel Feature Guide	Shipped w/product*
High Availability	H ₂ A Feature Guide	Shipped w/product*
VPN	GNAT Box VPN Feature Guide	Shipped w/product*
VPN Examples	GB-VPN to VPN Tech Docs	www.gta.com
GBAdmin interface	User's Guide	Shipped w/product, CD*
GBAdmin Help	GBAdmin Online Help	Shipped w/product, CD*
Web interface	User's Guide	Shipped w/product, CD*
Console interface	Console Interface Tech Doc	www.gta.com

* All documents for registered products can also be found on the www.gta.com website.

2 VPN Concepts

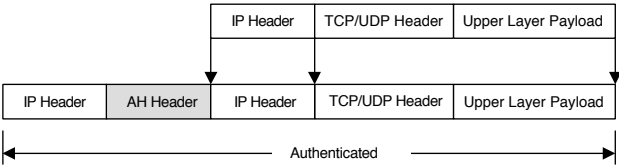
Overview

Security is a critical issue in the current implementation of the Internet Protocol (IPv4). In its growth, the Internet started attracting not only academic circles and research labs, but also banking, commerce and business sites. It is a growing market area yet to be exploited to its full potential. The lack of security is somewhat crippling. IPv4 does not provide measures to ensure that data being received has not been altered during transmission, or came from the claimed source. Without these measures, bank transactions can be altered, credit card numbers can be stolen, and other false data can be forged.

In an effort to overcome the security issues in IPv4 and utilize the public Internet as a secure communications network, the IETF developed the IPSec standard for Virtual Private Networking. IPSec focuses on the security that can be provided by the IP layer of the network, not application level security. The security requirements are divided into Authentication/Integrity and Confidentiality. These can be used independently or together to establish and maintain secure communications.

Authentication & Integrity

Authentication guarantees that the data received is the same as the data that was sent, and that the claimed sender is in fact the actual sender. Integrity means that the transmitted data has arrived at its destination without undetected alternation. The Authentication Header (AH) is a mechanism for providing strong integrity and authentication for IP datagrams. Security is provided by adding authentication information (to the IP datagram), which is calculated using all of the fields in the IP datagram (including the IP header, but also including the other headers and the user data). This does not change in transit. Authentication is sufficient for users who do not require confidentiality. Using only authentication for some types of packets reduces the time and resources involved for participating end systems computing authentication data. The authentication data is carried in its own payload; hence the systems that are not participating in the authentication may ignore it. Below are some examples of the IP header structures with and without the AH:

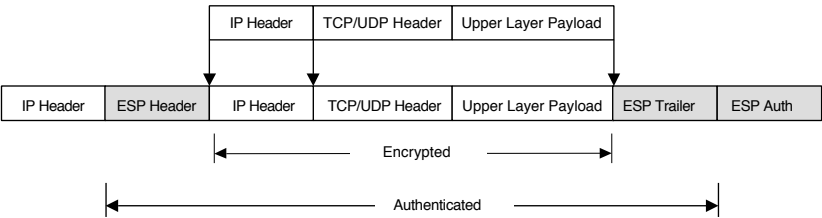


No Authentication Header

Confidentiality

Confidentiality means that the intended recipients of a communication know what is sent, but unintended parties cannot determine it. A mechanism commonly used for providing confidentiality is called encryption. IPSec provides confidentiality through Encapsulating Security Payload (ESP). ESP can also provide data origin authentication, connection-less integrity, and anti-reply service (a form of partial-sequence integrity). Confidentiality can be selected independent of all other services. There are two modes for providing confidentiality using ESP: tunnel mode and transport mode. Tunnel mode encapsulates an entire IP datagram within the ESP header; transport mode encapsulates the transport layer frame inside ESP. The GNAT Box System supports IPSec tunnel mode.

Below are some examples of how the typical IPv4 packets might look before and after applying ESP tunnel mode:



Packet with ESP Authentication Header

VPN Operation

Since the GNAT Box VPN operates in the IPSec tunnel mode, network address translation is not applied to the IP packets in the tunnel. System configurations that use unregistered IP addresses on the Protected Network (which GTA Firewalls do by default) will have IP packets transmitted with the unregistered IP address information in the source portion of the IP packet. This means that the two physical networks joined by the VPN must be on logically different networks, (e.g. 192.168.1.0/24 <--> 192.168.1.0/24 is not allowed).

All the following configurations are valid with the GNAT Box VPN:

- Unregistered Network - Unregistered Network
- Unregistered Network - Registered Network
- Registered Network - Registered Network

Note

Routing is crucial. When defining a VPN, ensure that packets to one network are routed back correctly on the other network. (If two GTA Firewalls are used, this function is performed automatically.)

Since the VPN tunnel completely encapsulates the IP packet, many commonly used IP protocols may be sent through the tunnel. The tunnel mode also allows the use of application protocols not normally supported in the NAT mode, such as Microsoft NetMeeting.

The GNAT Box VPN Client runs transparently at all times behind your other software applications.

Note

To initiate a VPN connection using authentication, run the GBAuth User Authentication utility. See Mobile Client Authentication in Chapter 4 for information about GBAuth.

Packet Flow

In order to illustrate both the inbound and outbound aspects of packet flow, this packet flow description assumes that two GNAT Box Systems are used, one on each side of the VPN.

Outbound

1. When a packet arrives on a Protected Network interface of the GNAT Box System, the VPN Security Associations (SA) are checked to determine if the destination is a VPN.
2. If the destination is not a remote VPN, then normal processing of the IP packet is performed.
3. If the destination is a remote VPN, then the IP Pass Through Filters rules are applied to the packet.
4. If the packet is accepted by an IP Pass Through Filter rule, then the VPN transformation defined in the VPN definition (SA) is applied.
5. If the packet is not accepted by a rule, it is rejected.

Inbound

The VPN packet arrives at the External Network interface of the remote GNAT Box System. The packet will be either an AH or ESP IP protocol packet.

1. When the VPN packet arrives at the External Network interface, Remote Access Filters are applied to the packet. A filter must be in place to accept a packet with either the AH or ESP protocol defined.
2. If no Remote Access Filter accepts the packet, it is rejected.
3. If a Remote Access Filter accepts the VPN packet, the SA table is searched to find a match. If a match is found, the appropriate transformation is applied to decode the packet.
4. Once the packet is successfully decrypted, IP Pass Through Filters are applied to determine if the packet will be accepted.
5. If a filter match is made, the packet is routed to the target IP address.
6. If no filter match is made, the packet is discarded.

Tunnels

The GNAT Box VPN is based on the IPSec standard using the tunnel mode. The tunnel mode seamlessly and securely establishes connections between networks without requiring any additional software to be installed on host machines. The GNAT Box performs the role of a security gateway by encrypting and routing packets to a remote 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 when utilizing unsupported protocols in the NAT mode between two GTA Firewall Protected Networks. To configure the VPN for the Null Tunnel mode, set AH to none and ESP to Null.

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.

Encapsulating Security Payload (ESP)

An ESP only protects 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.

Access Control

A VPN can provide the secure transport of data between two networks over an untrusted public network. However, it has no control over who can send/receive information and what data is passed between the two networks.

A VPN can be a cost-effective and productive facility, but if used incautiously, it can be a channel for unauthorized access from a remote network. The GNAT Box VPN facility addresses this issue with access control on the VPN tunnel. The GNAT Box VPN not only provides secure encrypted transport of data between two networks, it also provides facilities to control access on the encrypted tunnel. The GNAT Box implicit rule, “That which is not explicitly allowed is denied,” applies to VPN connections as well. VPN access control is provided at three points:

1. At the Protected Network interface through the use of IP Pass Through Filters to control the outbound access on the VPN tunnel.
2. At the External Network Interface through the use of Remote Access Filters. This access control point allows or disallows the acceptance of an IPSec packet from a remote network.
3. At the External Network Interface through the use of IP Pass Through Filters to control the inbound access on the VPN tunnel.

All the standard GNAT Box filter facilities below may be used to define access policies on the VPN tunnel for both inbound and outbound access:

- Source IP Address or Address Object
- Destination IP Address or Address Object
- Source Port
- Destination Port
- Protocol
- Time of Day/Day of Week
- Network Interface

Hash Algorithms

Hash Algorithms define the authentication method used in various aspects of the GNAT Box VPN. Each key exchange method uses the hash algorithm differently.

Manual Key Exchange

In the Manual Key Exchange method, the hash algorithm defines the Authentication Header (AH) transformation when used without an ESP specification. When both hash algorithm and ESP specifications are defined, the hash algorithm specifies the authentication portion of the ESP packet. When creating a Manual Key VPN, a key must be specified.

IKE Method

When using the IKE method, the hash algorithm is used to define the authentication method with the associated ESP encryption method. If no encryption method is selected, the hash algorithm defines the AH method.

Hash Key Length

The key length for the MD5 transformations is 128 bits, which is 16 ASCII characters or 32 hexadecimal characters. The key length for the SHA-1 transformations is 160 bits or 20 ASCII characters or 40 hexadecimal characters.

Supported Hash Algorithms

None	This selection indicates that AH will not be used in the Manual Key mode or in the IKE Mode. If None is selected here, then the ESP encryption method must have a value or be Null.
HMAC-MD5	The key will be padded to the minimum length.
HMAC-SHA-1	The key will be padded to the minimum length.
HMAC-SHA-2	The key will be padded to the minimum length.
All	With All selected the system will accept HMAC-SHA-1, HMAC-SHA-2 or HMAC-MD5, (negotiated). (Only available with IKE method.)

Encryption Methods

The Encryption Method defines the encryption used in the Encapsulated Security Payload (ESP) transformation.

Encryption Key Length

The Blowfish, CAST-128 and Twofish transformations use variable length keys, while AES, DES and 3DES use a fixed length key. If you exceed the maximum key length in these fields, you will generate an error and not be able to save the configuration until it is corrected. You may enter a shorter length key – the system will pad it to the minimum key size, e.g., in CAST-128, the key will be padded to 128 bits.

Supported Encryption Methods & Key Length

None	No encryption will be used, i.e., no ESP transformation. If None is selected here, then None cannot be selected for the hash algorithm authentication method.
Null	No key and no encryption, only IP encapsulation. This method will encapsulate any IP packet. This is useful when application protocols not supported by the GNAT Box System are used.
AES	128 bits. In Manual Key Exchange a key size of 16 ASCII chars or 32 Hex characters should be used.
Blowfish	40 to 448 bits. When using the Manual Key Exchange method, the length must be between 5-56 ASCII characters or 10-112 Hex characters.
CAST-128	40 to 128 bits. When using Manual Key VPN, the key length 5-16 ASCII characters or 10-32 Hex characters.
DES	64 bits. When using Manual Key VPN, the key length must be ASCII 8 characters or 16 Hex characters. Note: DES is often referred to as having 56 bits because one bit of each byte is used as a parity bit.
3DES	192 bits. When using Manual Key VPN, the key length must be 24 ASCII characters or 48 Hex characters. Note: 3DES is often referred to as having 168 bits because one bit of each byte is used as a parity bit.
Twofish	40 to 256 bits. When using Manual Key VPN the key length must be from 5 to 32 ASCII characters or 10-64 Hex characters.
Strong	Only available when using IKE. This indicates that the GNAT Box VPN will accept any of the encryption methods other than None or Null.

Preshared Encryption Keys

Preshared Encryption Keys are 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

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

Key Type

This choice list value indicates in which format the key will be specified. Either ASCII or HEX (Hexadecimal). If HEX is used only the valid hexadecimal values may be used.

Hexadecimal Characters

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Manual Key Exchange VPN

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. Once this manual exchange has been made, the keys will not change unless the tunnel is recreated.

Internet Key Exchange (IKE) VPN

IKE is the key exchange protocol used for exchanging cryptographic keys to dynamically establish security associations (SA) between two VPN peers. Initially, VPN peers must exchange Preshared keys. Using both keys, the IKE will dynamically establish a unique key for the peers using the SA. IKE will renegotiate SAs periodically based on the lifetime values established between the VPN peers.

IKE is performed in two phases. Each phase performs a unique function that authenticates and validates VPN connections. The specific functions of each phase are covered below:

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. This phase of the IKE connection establishes the initial SA and is used to authenticate subsequent Phase II exchanges. The GNAT Box IPSec VPN supports all the IPSec encryption algorithms for Phase I.

Exchange Mode, Main or Aggressive

The GNAT Box system normally operates in the Main mode, however if another vendors IPSec VPN is not capable of using the Main mode the Aggressive mode can be used. If the Aggressive mode is used, make sure that the other VPN system is configured to use IP Address at the identifier type. The GNAT Box VPN only supports IP Address as an identifier for VPN gateway to VPN gateway.

In the Mobile IKE configuration the Phase I specification cannot be set by the user. A fixed Phase I configuration of: Aggressive mode, Email Address Identifier, 3DES, SHA-1 and Diffie-Hellman Group 2 should be used by the GNAT Box VPN Client.

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.

Once Phase I has been authenticated and the SA has been established between the VPN peers, the Phase II exchange negotiates the encryption proposal used to encrypt the VPN data. The Phase II proposal specification is user configurable. Parameters that can be configured are:

PFS Key Group

Perfect Forward Secrecy (PFS) Key determines how a new key is generated. Using PFS ensures that a key used to protect a transmission, in whichever phase, cannot be used to generate any additional keys. In addition, the keying material for that key cannot be used to generate any new keys. Any one of the three PFS algorithms below may be used below to generate keys.

1. Diffie-Hellman Group 1
2. Diffie-Hellman Group 2
3. Diffie-Hellman Group 5

Note

To work correctly, both sides of a VPN must use the same PFS algorithm.

Security Association (SA)

Before an IP packet is secured by IPSec, a Security Association (SA) must be in place. A Security Association may be created manually or dynamically. The GNAT Box VPN offers implementations of manual keying, Internet Key Exchange (IKE) facility for dynamic key exchange and a special IKE mode for the mobile GNAT Box VPN client.

Identified by a unique IP Address, SPI (numeric ID) and security protocol (e.g., ESP, AH). The SA specifies the parameters for communication with the specified host.

Note

IKE and mobile VPN client support is only available on RoBoX, GB-100, GB-Flash and GB-1000.

Lifetime

Lifetime is a 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; the value cannot be configured by the user. Each phase has a separate lifetime: Phase I lifetime is 1.5 hours and Phase II is one hour.

Security Parameter Index (SPI)

The Inbound and Outbound Security Parameter Index are used to uniquely identify a Security Association (SA). The Inbound SPI will be the Outbound SPI on the remote side of the VPN. The Outbound SPI will be the Inbound SPI on the remote side of the VPN. The SPI should be unique for each SA, although the inbound and outbound SPI may have the same value. The minimum SPI value is 256.

Limits

The number of functional concurrent VPN tunnels is a function of how the tunnels are used, the encryption algorithm and the power of the CPU. See your product guide for the number of security associations (SA) available on your firewall.

Mobile IKE

The GNAT Box VPN has a special configuration IKE that supports the GNAT Box VPN Client. This configuration is specifically designed to address the dynamic nature of mobile clients in the field

Virtual IPs for Mobile VPN Clients

All GNAT Box VPN Clients require a virtual IP address. Since the VPN Client uses the ESP tunnel mode, both a gateway and network are required. (Tunnel mode implies network-gateway to gateway-network communications.) For a mobile client, the remote network consists of an unregistered single IP address. The gateway IP address of the mobile client is typically dynamic (e.g., dialup).

When planning for mobile client deployment, the administrator should select a virtual network that will be used for mobile clients. This network should be one of the IANA unregistered networks and should not be utilized anywhere on the local network. Individual IP addresses from this virtual network are then issued out one at a time to each mobile user.

The virtual IP addresses are used when creating access policies for mobile users. Policies can be set for the entire virtual network and for each individual mobile user.

3 VPN Configuration

Overview

In order to use the GNAT Box VPN, three functional areas must be configured: a VPN Definition using VPN Objects; Remote Access Filters; and IP Pass Through Filters.

For the VPN definition, the Security Association (SA) must exist on both sides of the VPN, with the remote side having an SA that is the mirror image of the local side.

To see more examples of VPNs, including static-to-dynamic gateway configurations, go to the GTA Support Center on the www.gta.com website.

VPN Objects

The VPN Objects list displays the name and description of all defined VPN Objects. VPN Objects are defined primarily by the `LOCAL GATEWAY` and `LOCAL NETWORK` fields. Other fields define how the connection will be protected and how the phases of the connection will be encrypted.

Default VPN Objects

Default VPN Objects are named `IKE`, `Manual` and `Mobile`. These defaults, once configured for your individual network, can fill most VPN requirements. `Mobile` is essentially an `IKE` VPN Object for VPN Client users.

Exception

GB-Pro systems have only the default `Manual` VPN object.

VPN Objects Fields

Disable	Check to disable all access for the selected object.
Name	Enter name by which the objects will be referenced.
Description	Enter a description of the object.
Mobile Authentication	Enabling this option requires a user to pre-authenticate using GBAuth. (The user ID and password for user authentication are set in User Authorization.) A Remote Access Filter must also be defined and enabled. See Chapter 4 for more information.
Local Gateway	An Interface name, IP alias or H_A group name assigned to an External Network interface on the local GTA Firewall. The encapsulated packets will appear at the remote gateway with this IP address listed as the source, therefore the IP address should be used as the remote (destination) gateway when Remote Access Filters are created for the VPN. After authorizing and saving a VPN, defaulting the filter set will create appropriate Remote Access Filters.
Force Mobile	Select if using an IP address protocol that requires the system to use dynamic protocol negotiation, such as system in which the external IP address is dynamic; deselect for static IP addresses.
Local Network	If you have defined an Address Object for the local network that is to be accessible via the VPN, select that object from the list. If not, enter the network IP address and mask of the local network, typically a Protected Network, PSN or a subnet of either.

Phase I

In IKE, a Phase One exchange establishes a security association by negotiating the terms of the VPN, authenticating the validity of the VPN peer, and setting connection parameters. Manual Key Exchange Phase I settings cannot be user-configured. For mobile connections, Phase I will default to Aggressive, 3DES, SHA-1 and Diffie-Hellman Group 2.

Exchange Mode	<p>Main: Static IP to Static IP. Set to Main when the connection is from one gateway with a static IP address to another static gateway, e.g., between two GTA Firewalls or a GTA Firewall to another vendor's VPN device.</p> <p>Aggressive: Static IP to Dynamic IP. Set to Aggressive when the connection is from a gateway with a dynamic IP address to one with a static IP address, i.e., VPN mobile connections, and most connections using PPP/PPPoE or DHCP.</p> <p>In either mode, if the vendor's VPN device has a setting or identification method, always set it to the IP address.</p>
---------------	---

Encryption Method	3DES, AES, Blowfish, DES, and Strong (Any). The encryption method that the GTA Firewall will accept from a connection initiator during Phase I. Blowfish will be used when the GTA Firewall initiates the connection.
Hash Algorithm	All, HMAC-MD5, HMAC-SHA-1; HMAC-SHA-2. The method that will be used for the Phase I authentication transformation. “All” allows the GTA Firewall to accept any of the hash algorithm encryptions for the Authentication Header (AH). MD5 will be used when the GTA Firewall initiates the connection.
Key Group	Any, Diffie-Hellman Group 1, 2 or 5. Select the key group for Phase I. Diffie-Hellman is a crypto-graphic technique that enables public keys to be exchanged in a way that derives a shared, secret (private) key at both ends. GNAT Box System Software uses Group 2 by default.

Phase II

In IKE, a Phase Two exchange establishes security associations for other protocols, providing source authentication, integrity, and confidentiality.

Encryption Method	3DES, AES, Blowfish, CAST-128, DES, None, Null, Strong, Twofish. Select the method for the Encapsulating Security Payload (ESP) transformation. When Strong is selected, any of the algorithms except None and Null will be accepted from the remote initiator. AES will be used when the GTA Firewall is the initiator. Null is a special case where there is only IP encapsulation. The Null method has little impact on performance. Null is useful when unsupported protocols are used in NAT mode between two firewalls.
Hash Algorithm	All, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2, None. Select the method that will be used for the Phase II authentication transformation. Selecting None will result in no AH (Authentication Header) transformation being applied to the packet.
Key Group	Any, Diffie-Hellman Group 1, 2 or 5. Select the key group for Phase II. On the GNAT Box VPN Client, this value is defined in the Security Policy section and is labeled PFS (Perfect Forward Secrecy) Key Group. With PFS, the compromise of a key exposes only the data protected by that key to unauthorized access.

Note

The GNAT Box IPSec VPN always has PFS and Replay Detection enabled. When communicating with another vendor's VPN device, enable PFS and Replay Detection on the other device. The anti-replay protocol prevents the insertion of changed packets into the data stream.



VPN Object List

GNAT-Box Edit VPN Object	
Disable:	<input type="checkbox"/>
Description:	DEFAULT: IKE VPNs
Name:	IKE
Mobile authentication required:	<input type="checkbox"/>
Local gateway:	EXTERNAL <input type="checkbox"/> Force mobile protocol
Local network	
Object:	Protected Networks <input type="text"/> IP Address: <input type="text"/>
Phase I	
Exchange mode:	main
Encryption method:	3des
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2
Phase II	
Encryption method:	aes
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>	

Default IKE, VPN Object

Interface Variations

GBAdmin has the list of VPNs at the bottom of the VPN Object screen. Select one of these list items to change it; add a VPN Object by clicking Add (+).

☐ Disable

VPN Objects

Name: ☐ Require mobile authentication.

Description:

Local gateway: ☐ Force mobile protocol

Local network:

Phase I

Exchange mode: Encryption method:

Hash algorithm: Key group:

Phase II

Hash algorithm: Encryption method:

Key group:

#	Name	Description
1	IKE	DEFAULT: IKE VPNs
2	MANUAL	DEFAULT: MANUAL VPNs
3	MOBILE	DEFAULT: MOBILE VPNs









VPN Object, Default IKE example (GBAdmin)

VPN Authorization

After creating a VPN definition using VPN Objects, use the VPN Authorization section to select a VPN Object, select which addresses it will apply to, and enable it. Some of the fields in VPN Authorization are only used for the VPN Client and mobile users. See Chapter 4 for more about VPN Client.

The supported VPN features vary depending on which platform the GTA Firewall is running. All of the flash-based products (GB-Flash, RoBoX, GB-100 and GB-1000) support automated key exchange (IKE), manual key exchange and mobile client. The floppy disk-based GB-Pro supports only manual key exchange.

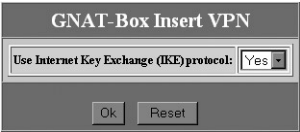
To authorize a new VPN in the Web interface, click the up or down arrow icon; to edit a VPN authorization, click on the check mark icon.

GNAT-Box VPNs				
Index	Action	Type	VPN object	Description
1	   	IKE	IKE	Jane User's Home Office
2	   	IKE	MANUAL	Mary Tester
<div>SaveReset</div>				

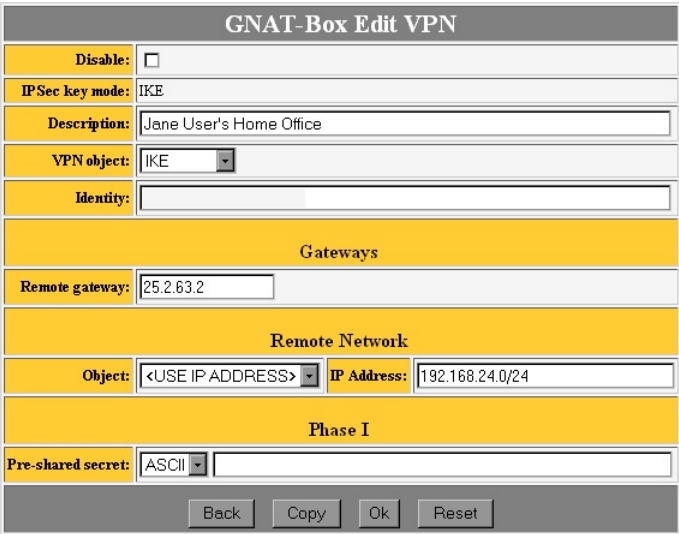
VPN List Screen

Select the Key Method

In the Web interface, a dialog box appears to prompt the administrator to select IKE or Manual mode. In GBAdmin, the IKE or Manual mode is selected on the main VPN screen.

A small dialog box titled "GNAT-Box Insert VPN". It contains a label "Use Internet Key Exchange (IKE) protocol:" followed by a dropdown menu currently set to "Yes". At the bottom are "Ok" and "Reset" buttons.

VPN key mode selection screen

A larger form titled "GNAT-Box Edit VPN". It has several sections: "Disable:" with a checkbox; "IPSec key mode:" with a dropdown set to "IKE"; "Description:" with a text field containing "Jane User's Home Office"; "VPN object:" with a dropdown set to "IKE"; "Identity:" with a text field. Below these is a yellow header "Gateways" with "Remote gateway:" set to "25.2.63.2". Another yellow header "Remote Network" follows, with "Object:" set to "<USE IP ADDRESS>" and "IP Address:" set to "192.168.24.0/24". A third yellow header "Phase I" is next, with "Pre-shared secret:" set to "ASCII" and an empty text field. At the bottom are "Back", "Copy", "Ok", and "Reset" buttons.

VPN Authorization

VPN Authorization Fields

Disable	When a VPN Authorization is created, deselect the DISABLE checkbox to activate the VPN. Check to disable all access for the selected VPN.
IPSec key mode	The key mode.
Description	Enter a brief description of VPN.
VPN Object	From the list of VPN Objects that you have created or from the default VPN Objects, select the definition of the VPN that you would like to authorize.

Identity	Enter user email address for user authentication. This field is used to associate the remote user with a preshared secret key. Use an email address to uniquely identify the user. (Only needed when “Force Mobile Protocol” is selected and using a dynamic to static VPN.)
Gateways	
Remote Gateway	Default is 0.0.0.0. Enter the IP address of the route (Destination) through which this VPN will pass, the gateway to the remote network. If the remote network is behind a GTA Firewall, then this IP address would be one assigned to the External Network interface. This IP address will also help determine routing of the packet.
Remote Network	
Object	Select a previously defined Address object.
IP address	If you selected “Use IP” to define the remote network, (Destination) enter the IP address of the remote network that resides behind the remote firewall. (If it is a GTA Firewall, then typically this will be the Protected Network, PSN or a subnet of either.) Use a mask to define the type of network (e.g., 255.255.255.0 or /24 for a Class C). A destination need not be an entire network.
IKE (Automated Key Exchange) Fields	
Phase I	
Preshared secret	Select ASCII or HEX* format value. Enter preshared as defined in VPN. This same key needs to be entered in the GNAT Box VPN Client Policy Editor when configuring the security policy. This field is case sensitive.
Manual Key Exchange Fields	
Encryption Key*	Select ASCII or HEX* format value. Enter encryption key as defined in VPN.
Hash Key	Select ASCII or HEX* format value. Enter the hash algorithm for the authentication transformation in ASCII or HEX format.
Security Parameter Index (SPI)	
Inbound/Outbound	Default is 256.

* Valid hexadecimal characters: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

Interface Variations

To create a new VPN in GBAdmin, click the Plus icon (+) on the toolbar or use the Insert Key on the keyboard; to edit an existing VPN, select the user in the list at the bottom of the screen and make changes.

Remote Access Filters

Manual Key Exchange

At least one Remote Access Filter that will accept an ESP VPN connection (IP protocol 50) from the remote side of the VPN gateway must be in place for Manual Key Exchange. A single generic Remote Access Filter may be used for multiple VPN connections, but a specific Remote Access Filter for the defined VPN provides the tightest security.

IKE

When using IKE, two Remote Access Filters are needed: one for the ESP Tunnel (IP protocol 50) and one to allow access for the IKE on UDP/500.

Mobile IKE

The remote gateway IP address is typically dynamic for mobile users, so a Remote Access Filters for IKE (UDP/500) and ESP must accept connections from any IP address. (Mobile IKE is used with the VPN Client. See the next chapter for more about configuring the firewall for mobile clients.)

IP Pass Through Filters

An IP Pass Through Filter that meets the local security policy and allows outbound access on the defined VPN is required. The filter can be as general or as specific as desired: it can allow any host on the local network outbound access to any remote host, for any protocol, at any time, or it can be limited to a specific local host with outbound access to a specific remote host for a given protocol at a specific time.

Generally, an inbound IP Pass Through Filter is created that allows the remote side of the VPN access to the local Protected Network. This filter does not have to be symmetrical to the outbound IP Pass Through Filter. Although typically a single inbound and outbound IP Pass Through Filter is created for a VPN definition, multiple filters may be required to meet an access policy.

Examples

Manual Key Exchange

This section provides an example of how a GNAT Box VPN is configured between two networks using the manual key exchange method.

Network A

Network Information

Protected Network:	192.168.1.0/24
GNAT Box External IP:	199.120.225.2
Mail Server:	192.168.1.100
Developer's Workstation:	192.168.1.225
Sales Group:	192.168.1.20 - 192.168.1.30

Address Objects

Name:	Protected Networks
Description:	DEFAULT: Protected Networks.

Index 1

Object:	USE IP ADDRESS
IP Address:	192.168.1.0/24

VPN Authorizations

Key exchange:	MANUAL
Description:	VPN to B
VPN object:	MANUAL
Remote network:	172.16.0.0/16
Remote gateway:	204.96.116.15
Encryption Key:	12345678
Authentication:	12345678
SPI:	Inbound: 256
	Outbound: 256

VPN Objects

Name:	MANUAL
Description:	DEFAULT: MANUAL VPNs
Authentication required:	no
Gateway:	EXTERNAL
Force mobile protocol:	no
Local network:	192.168.1.0/24
Phase 1	(Ignore for manual vpn)

Phase 2

Encryption Method: 3DES
HASH Algorithm: HMAC-SHA-1
Key Group: Diffie-Hellman Group 2

Remote Access Filters

Description: VPN: Allow ESP connections (VPN to B).
Type: Accept
Interface: ANY
Protocol: ESP (50)
Source: 204.96.116.15
Destination: EXTERNAL

IP Pass Through Filters

1. Description: Allow only developer's workstation to access any host on the remote R&D network.
 Type: Accept
 Interface: Protected
 Protocol: ALL
 Source: 192.168.1.225/32
 Destination: 172.16.2.0/24

2. Description: Allow the sales group to access the database server on remote network, web browser only.
 Type: Accept
 Interface: Protected
 Protocol: TCP
 Source: Sales Group
 Destination: 172.16.1.50/32
 Destination Port: 80

3. Description: Allow anyone on the remote network to access the local mailserver with POP3 and SMTP.
 Type: Accept
 Interface: External
 Protocol: TCP
 Source: 172.16.0.0/16
 Destination: 192.168.1.100/32
 Destination Ports: 25, 110

Network B

Network Information

Protected Network: 172.16.0.0/16
 GNAT Box External IP: 204.96.116.15
 GNAT Box Protected IP: 172.16.1.1
 Database Server: 172.16.1.50
 R&D Network: 172.16.2.0

Address Objects

Name: Protected Networks
 Description: DEFAULT: Protected Networks.

Index 1

Object: USE IP ADDRESS
 IP Address: 172.16.0.0/24

VPN Authorizations

Key exchange: MANUAL
 Description: VPN to A
 VPN object: MANUAL
 Remote network: 192.168.1.0/24
 Remote gateway: 199.120.225.2
 Encryption Key: 12345678
 Authentication: 12345678
 SPI: Inbound: 256
 Outbound: 256

VPN Objects

Name: MANUAL
 Description: DEFAULT: MANUAL VPNs
 Authentication required: no
 Gateway: EXTERNAL
 Force mobile protocol: no
 Local network: 172.16.0.0/16
Phase 1 (Ignore for manual VPN)
Phase 2
 Encryption Method: 3DES
 HASH Algorithm: HMAC-SHA-1
 Key Group: Diffie-Hellman Group 2

Remote Access Filters

Description: VPN: Allow ESP (VPN to A)
Type: Accept
Interface: ANY
Protocol: ESP
Source: 199.120.225.2
Destination: EXTERNAL

IP Pass Through Filters

- Description: Allow remote Network A full access to any host.
Type: Accept
Interface: EXTERNAL
Protocol: ALL
Source: 192.168.1.0/24
Destination: 172.16.0.0/16
- Description: Allow all users access to remote Network A mailserver
Type: Accept
Interface: PROTECTED
Protocol: TCP
Source: 172.16.0.0/16
Destination: 192.168.1.100/32
Destination Port: 25, 110

IKE Configuration

This section provides an example of how a GNAT Box VPN is configured between two networks protected by GTA Firewall systems, using the IKE method.

Network A

Protected Network: 192.168.1.0/24
External Interface: 199.120.225.2
Protected Interface: 192.168.1.1

Address Objects

Name: Protected Networks
Description: DEFAULT: Protected Networks.
Index 1
Object: USE IP ADDRESS
IP Address: 192.168.1.0/24

VPN Authorizations

Key exchange: IKE
 Description: VPN to B
 VPN object: IKE
 Remote network: 172.16.0.0/26
 Remote gateway: 204.96.116.15
 Preshared Secret: 123456789

VPN Objects

Name: IKE
 Description: DEFAULT: IKE VPNs
 Authentication required: no
 Gateway: EXTERNAL
 Force mobile protocol: no
 Local network: Protected Networks

Phase 1

Mode: Main
 Encryption Method: 3DES
 HASH Algorithm: HMAC-SHA-1
 Key Group: Diffie-Hellman Group 2

Phase 2

Encryption Method: AES
 HASH Algorithm: HMAC-SHA-1
 Key Group: Diffie-Hellman Group 2

Remote Access Filters

1.

Description: VPN: Allow ESP (VPN to B).
 Type: Accept
 Interface: ANY
 Protocol: ESP
 Source: 204.96.116.15
 Destination: EXTERNAL
2.

Description: VPN: Allow IKE (VPN to B).
 Type: Accept
 Interface: ANY
 Protocol: UDP
 Source: 204.96.116.15
 Source Port: 500 or Blank
 Destination: Object – EXTERNAL
 Destination Port: 500

IP Pass Through Filters

1. Description: Allow inbound from Network B (Network A).
 Type: Accept
 Interface: EXTERNAL
 Protocol: ALL
 Source: 172.16.0.0/16
 Destination: 192.168.1.0/24

2. Description: Allow outbound from network A to B (Network A).
 Type: Accept
 Interface: PROTECTED
 Protocol: ALL
 Source: 192.168.1.0/24
 Destination: 172.16.0.0/16

Network B

Protected Network: 172.16.0.0/16
External Interface: 204.96.116.15
Protected Interface: 172.16.1.1

Address Objects

Name: Protected Networks
Description: DEFAULT: Protected Networks.
Index 1
Object: USE IP ADDRESS
IP Address: 172.16.0.0/24

VPN Authorization

Key exchange: IKE
Description: VPN to A
VPN object: IKE
Remote network: 192.168.1.0/24
Remote gateway: 199.120.225.2
Preshared Secret: 123456789

VPN Objects

Name: IKE
Description: DEFAULT: IKE VPNs
Authentication required: no
Gateway: EXTERNAL
Force mobile protocol: no
Local network: Protected Networks B

Phase 1

Mode: Main
 Encryption Method: 3DES
 HASH Algorithm: HMAC-SHA-1
 Key Group: Diffie-Hellman Group 2

Phase 2

Encryption Method: AES
 HASH Algorithm: HMAC-SHA-1
 Key Group: Diffie-Hellman Group 2

Remote Access Filters

1. Description: VPN: Allow ESP (VPN to A).
 Type: Accept
 Interface: ANY
 Protocol: ESP
 Source: 199.120.225.2
 Destination: EXTERNAL
2. Description: VPN: Allow IKE (VPN to A)
 Type: Accept
 Priority: Information
 Interface: ANY
 Protocol: UDP
 Source: 199.120.225.2
 Source Port: 500 or Blank
 Destination: EXTERNAL
 Destination Port: 500

IP Pass Through Filters

1. Description: Allow inbound from Network A (Network B).
 Type: Accept
 Interface: EXTERNAL
 Protocol: ALL
 Source: 192.168.1.0/24
 Destination: 172.16.0.0/16
2. Description: Allow outbound to Network B to A (Network B).
 Type: Accept
 Interface: PROTECTED
 Protocol: ALL
 Source: 172.16.0.0/16
 Destination: 192.168.1.0/24

4 Client Install & Configuration

Overview

When the GNAT Box VPN Client is installed on your Microsoft Windows® workstation, it secures communications between your system and a remote network protected by a GTA Firewall system or other vendor's VPN device. For each security policy, the GNAT Box VPN Client transparently intercepts IP packets destined for the specified remote network and transmits them securely to the remote GTA Firewall system or other vendor's device. The remote GTA Firewall system decrypts the packets and routes them to the target host. Because the GNAT Box VPN Client operates transparently at the IP level, it requires no modification to work seamlessly with all your IP applications.

The GNAT Box VPN Client gives you all the tools you need to implement public key for secure communications and allows you to import or configure your security policy in its Security Policy Editor.

To see more examples of VPN Client configurations, including connecting a remote VPN client to multiple discontinuous networks, go to the GTA Support Center on the www.gta.com website.

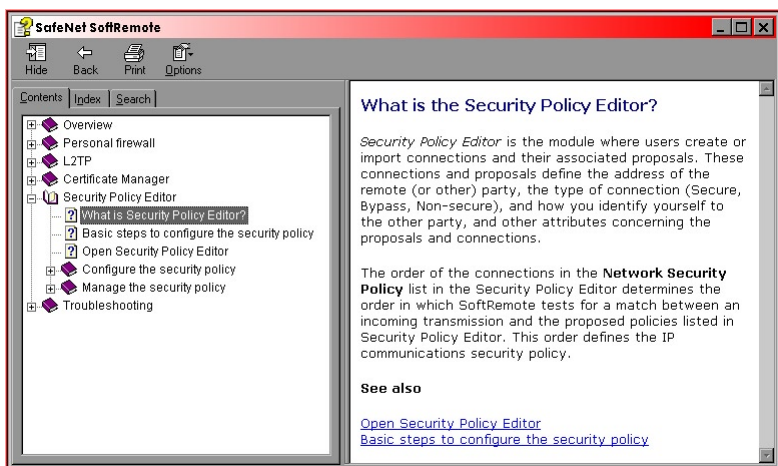
Quickstart

To set up the GNAT Box VPN Client:

1. Install GNAT Box VPN Client software. The software can be installed on Windows 95, 98, ME, XP, NT or 2000.
2. Obtain digital certificates if you are using the GNAT Box VPN Client with other VPN systems that use/require them. Because the GTA Firewall system uses preshared keys, digital certificates are not required if you are using GTA Firewalls only. You can obtain digital certificates manually, or automatically using SafeNet's Certificate Manager. For instructions, go to Contents and Index under the SafeNet Help menu.
3. Configure a security policy in Security Policy Editor.

VPN Client User Interface

This section describes the parts of the software and how to access use them. Additional information can be found in the GNAT Box VPN Client Help system, which is accessed from the task bar or Start Menu.



VPN Client Help

After you have installed the GNAT Box VPN Client and rebooted your system, you should have the VPN “S” icon (the SafeNet logo) in the system tray on your task bar. (If you click Remove Icon from the program menu, the system tray icon will be deleted from the task bar. It will re-display on reboot.)

Note

Some options that appear in the SafeNet client interface are not used by GNAT Box VPN Client.

VPN/SafeNet Taskbar Icons

The VPN icon changes to reflect the current status of your connection. These changes may occur too rapidly to be seen in the icon status; the most important icon symbols to look for are the “key” that means you have a secure connection, and the vertical red bar, which indicates that you are transmitting insecure data. The meanings of the symbols are:

**Disabled**

Grey icon with a red strike. The security policy is deactivated. If this icon appears after installation, the GNAT Box VPN Client service did not start properly. If restarting your computer does not start the service, the application may need to be reinstalled.

**Ready**

Icon with no key or bar. Service is ready to establish a connection.

**Not Secure**

Icon with a red bar. No secure connections have been established, and insecure data is being transmitted.

**Secure, Not Transmitting**

Icon with a key. At least one secure connection is established, but no data is being transmitted.

**Secure, Transmitting Insecure**

Icon with a key and red bar. At least one secure connection is established, but only insecure data is being transmitted.

**Secure, Transmitting Secure**

Icon with a key and green bar. At least one secure connection is established, and only secure data is being transmitted.

**Secure, Transmitting Secure and Insecure**

Icon with a key, green bar and red bar. At least one secure connection is established; both secure and insecure data is being transmitted.

VPN Client Menu

Right-clicking on the VPN icon in the icon tray will display the GNAT Box VPN Client menu. You can access the same functions from the GNAT Box VPN Client entry in your Start Menu.

Security Policy Editor

The Security Policy Editor is the software module in this application where you create connections and their associated proposals and list them in a hierarchical order that defines an IP data communications security policy. You can define multiple policies and selectively activate/deactivate them from this software module.

Certificate Manager

Not used in the GNAT Box VPN Client.

Deactivate Security Policy

This function allows you to deactivate your current security policy and allow all communications to be transmitted without security. This item is a toggle; once deactivated, the menu item will read Activate Security Policy.

Reload Security Policy

Whenever you try to modify your existing security policy and save it while a secure connection is active, you will be prompted to reset your active connection. If you click “No,” you can keep your changes and wait until the connection is no longer active to save.

Warning!!

This action overwrites your existing security policy and resets (drops) any active connections.

Remove Icon

This action will remove the GNAT Box VPN icon from the icon tray, thus disabling access to GNAT Box VPN functions from the task bar. The icon will not be displayed until you restart your system.

Log Viewer

Log Viewer displays the communications log, a diagnostic tool that lists the IKE negotiations.

Connection Monitor

The Connection Monitor utility displays statistical and diagnostic information for each active connection in the security policy. This utility is designed to display the actual security policy settings configured in the Security Policy Editor and the security association (SA) information established during Phase I IKE negotiations and Phase II IPSec negotiations.

Help

Provides access to the VPN Client help engine.

About GNAT Box VPN Client

Displays information about the release and build of the VPN Client.

Installation

If you are installing from a CD-ROM, open the directory that contains the GNAT Box VPN Client and locate the Setup icon. Double-click the Setup icon.

If you are installing from an Internet download, locate the download file and double-click on the self-extracting file.

Note

Since the download file needs to be decompressed and temporary files created, an installation via Internet download of the VPN Client software will initially require about twice as much disk space as an installation from CD. Once the software is installed and temporary files deleted, this disk space will again be available.

Mobile VPN Client Activation Code

GB-100, GB-1000, GB-Flash and RoBoX-25 running system software version 3.2.x and above include a single mobile client session. Since support for a single client session is built in, no activation code is required for a single client session, except for in RoBoX-25, which requires a second activation code (provided). For multiple concurrent mobile client sessions, you must purchase the desired license, (e.g., five concurrent sessions, etc.) The activation code is then available on the GTA Support site.

Note

RoBoX-10 provides VPN as an optional feature.

In order to enable your GTA Firewall to allow multiple concurrent mobile VPN Client sessions, you will need to enter your mobile client activation key code on the Features configuration screen on your GTA Firewall. You can do this with either GBAAdmin or the Web interface.

Features		
	Activation Code	Description
1	872709E7-1E0BA349-7DAD817C-FC8CC3D4	GB-1000 3.2 - Registered
2	872709E7-1E0BA349-7DAD817C-AABCC0D0	GB VPN Client - Registered

GBAdmin Interface Example

GNAT-Box Features		
Index	Activation code	Description
1	872709E7-1E0BA349-7DAD817C-FC8CC3D4	GB-1000 3.2 - Registered
2	872709E7-1E0BA349-7DAD817C-AA0BB0C0	GB VPN Client - Registered
3		
<div>Save Reset</div>		

Web Interface Example

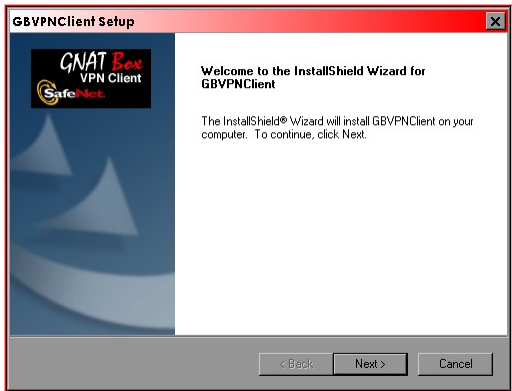
Enter the VPN Client activation code in any empty row and click Save. Upon re-display, the description field shows the appropriate VPN Client license. (See Feature Activation Codes in Chapter 1 for instructions.)

Note

When upgrading a VPN Client license, the feature code will activate the total number of VPN licenses purchased; if you initially had a five-user license and upgrade to 10, the new code will activate 10 total licenses.

Software Installation

Once the software installation begins, the first display will be the Welcome screen. Click Next to continue the installation or Cancel if you wish to abort the installation.

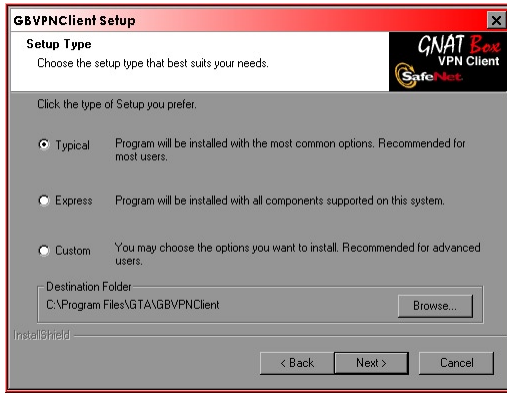


Opening Install Screen

The License Agreement will be displayed. Read the agreement, and if you agree to the terms, click Yes to proceed. If you don't agree to the terms of the agreement, click No and the installation process will terminate.

After accepting the License Agreement, the Setup Type screen will be displayed. Select the type of installation that best suits your needs. The default selection is "Typical." If you wish to install the GNAT Box VPN Client

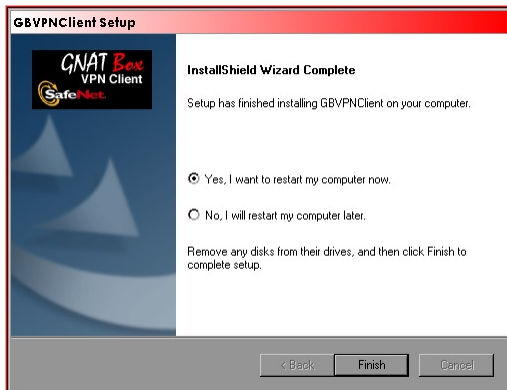
software in a directory other than the default, click Browse and select an alternative directory. Once you have made your selections, click Next to continue.



Setup type screen

Before the software is installed on your workstation the Summary screen will display your installation selections. Review the summary and if it is correct click Next to start copying files to your workstation. If the summary is not correct, click Back, correct your selections, and proceed.

The GNAT Box VPN Client files will be installed on your workstation. Once the copy procedure completes, the Restart screen will be displayed. You should restart your workstation before you attempt to use the GNAT Box VPN Client. After selecting “Yes, I want to restart my computer now,” click the Finish button to restart.



Restart Computer

Uninstalling

When you remove this software and its components, you can keep your security policy, digital certificates, and private keys. This is recommended if you are uninstalling to upgrade. Below is an example of how to uninstall under the Windows 2000 operating system. Procedures for other OS's will vary.

1. Click the Start button, then select Settings -> Control Panel -> Add/Remove Programs.
2. Select Change/Remove Programs, and from the list of currently installed programs, select GNAT Box VPN Client. Click Change/Remove.
3. In the GNAT Box VPN Client Setup dialog box, select the Remove radio button and click Next. In the Confirm Uninstall dialog box, click OK.
4. In the Uninstall Security Policy dialog box:
 - Click No to keep the security policy, certificates and private keys.
 - Click Yes to delete the security policy, certificates and private keys.
5. When the "Maintenance Complete" screen appears, restart your computer by selecting the "Yes" radio button, then click Finish.

Configure the VPN Client

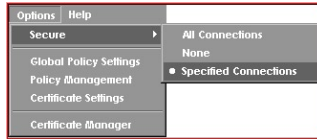
The next two sections provide information on setting up a mobile VPN Client and a GTA Firewall in their default configurations, in which the firewall accepts connections from the defined VPN Client. In a multiple VPN setup, each VPN Client must be configured, and each user must be defined on the firewall. You may enable and disable individual mobile users as needed.

Note

The Security Policy Editor may be configured while inactive or active. However, it may not be configured while Options -> Secure -> None is selected from the menu.

1. Start the Security Policy Editor

Click the VPN icon in the task bar or select the Policy Editor from the Start menu. From the Policy Editor Options menu, you must select Secure>Specified Connections in order to be able to edit your new policy.



Options/Secure Menu

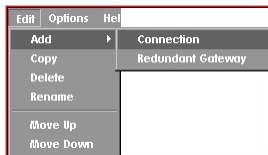
From the Options menu, select Global Policy Settings. Check the “Allow to Specify Internal Network Address” option.



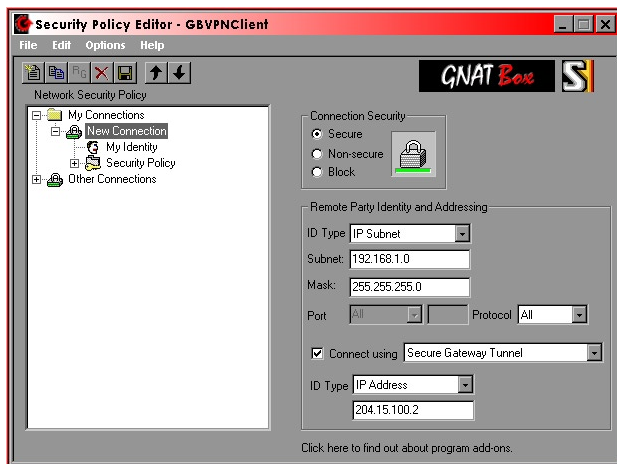
Global Policy Settings dialog box

2. Add a New Connection

Click the Add a New Connection icon from the task bar or select Add Connection from the Edit menu. A policy named “New Connection” will be displayed in the policy list. Highlight the policy name and rename it by typing over the existing text.



Edit Menu

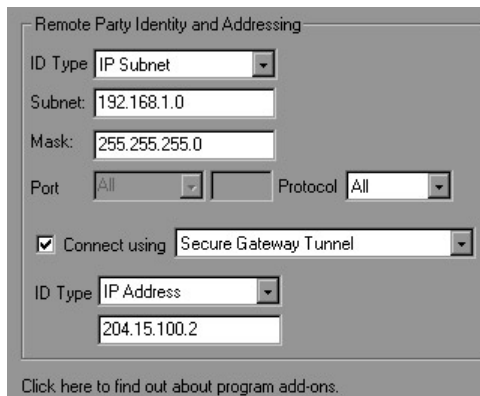


New Connection added

The Connection Security section should have the “Secure” radio button selected and the lock image should be green. Change this selection to “Non-secure” to disable the security policy if you wish or to “Block.” Connection Security selections are: Secure; Non-secure; Block.

3. Remote Party Identity and Addressing

In the Remote Party Identity and Addressing Section, you will specify information about the network protected by a GTA Firewall system accessed with the VPN Client.



Remote Party Identity and Addressing Section

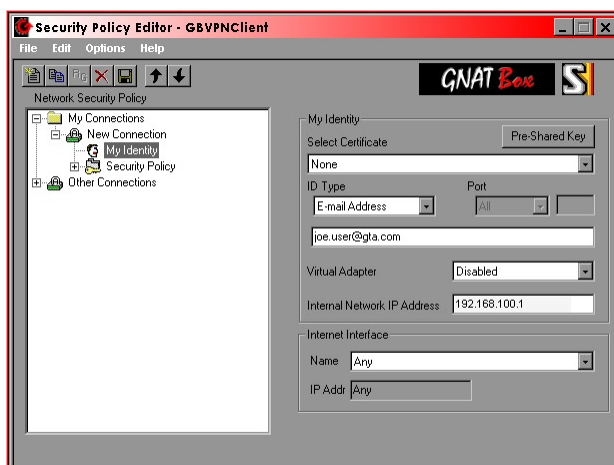
Remote Party Identity and Addressing Fields

ID Type	Select IP Subnet from the dropdown box.
Subnet	Enter the network address of the network protected by the GTA Firewall system, (e.g., 192.168.1.0).
Mask	Enter the netmask for the network specified in the Subnet field, (e.g. 255.255.255.0 for a class C network).
Port	Leave the protocol set to All.
Connect Using	Select option by clicking the checkbox, then select Secure Gateway Tunnel from the dropdown list.
ID Type	Select IP Address from the dropdown list.
IP Address	Enter the IP Address of the Gateway on your GTA Firewall system, generally the External network interface.

4. My Identity

Click on the “+” icon to expand the policy tree so the My Identity and the Security Policy icons are displayed.

Before configuring the My Identity Section, select the Security Policy icon and set the Phase I Negotiation Mode to Aggressive. See page 12 for an illustration of the Security Policy section. If this is not done before editing the My Identity Section, some required options will not be displayed.



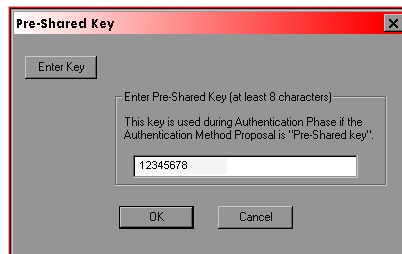
My Identity Section

My Identity Fields

Select Certificate	Set this field to None. Note: GNAT Box Firewalls use preshared keys, not certificates. If this field is not set to None, the Preshared Key button will not appear, and you will not be able to enter an email address under ID Type.
Preshared Key	Click the Preshared Key button to display the data entry dialog. Click the Enter Key button to enter your preshared key. Use a minimum of eight (8) characters. Your preshared key is not displayed in readable text. The preshared key entered here will be also be required to configure the firewall side of the VPN.
ID Type	Select Email Address. Enter your email address in the data entry field below the ID Type field, (e.g., joeuser@gta.com). Note: If you do not have the Email Address selection in the list, you have not selected Aggressive Mode in the Security Policy section.
Virtual Adapter	Disable (uncheck) this field.
Internal Network IP Address	Enter the virtual IP address issued to you by your firewall administrator, (e.g. 192.168.100.1).

Internet Interface

Name	Select the network device for which you will use this security policy. This is a dynamic list; you can use any listed device, depending upon your location. This means that it is possible to use the PPP adapter and then later use an Ethernet interface at a different location. Note: To use a modem (PPP) in Windows XP, select Any.
IP Address	This will display the IP address of the selected device. If you select the PPP adapter and no PPP connection is established, the IP Address field will display 0.0.0.0 until a valid IP address is obtained.



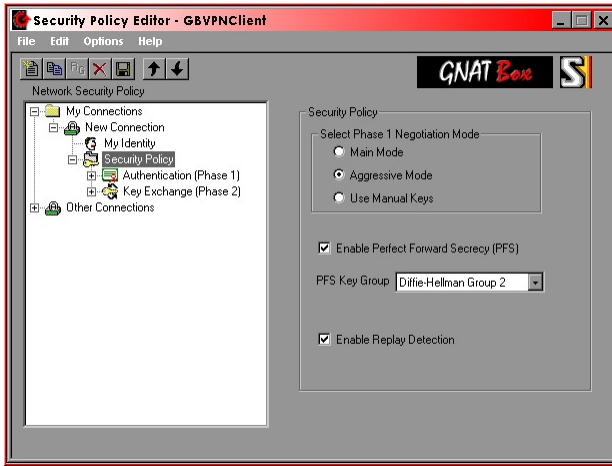
Preshared Key Dialog

Note

Record your preshared key in a safe and secure location.

5. Security Policy

Click on the “+” icon next to Security Policy to expand the tree, then select Security Policy.



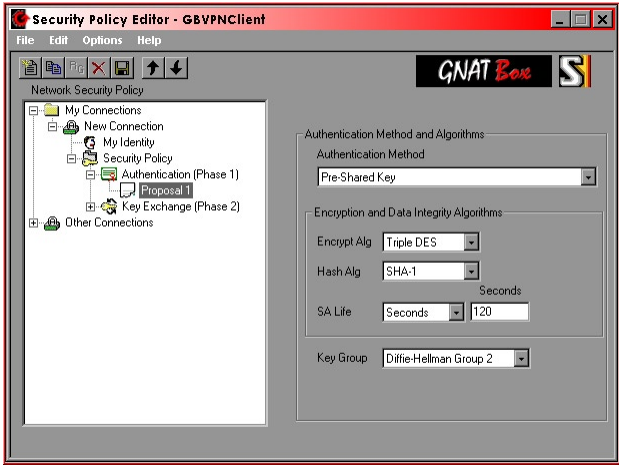
Security Policy Section

Security Policy Fields

Select Phase I Negotiation Mode	Select the Phase I Negotiation Mode to Aggressive.
Enable Perfect Forward Secrecy	Select this item (PFS).
PFS Key Group	Select Diffie-Hellman Group 2. On the GTA Firewall Mobile VPN configuration screen this value is the Phase II Key Group parameter.
Enable Replay Detection	Select this item.

6. Authentication (Phase I)

Click the “+” icon next to Authentication (Phase I) to expand the tree. There will be one proposal labeled Proposal 1. Click on Proposal 1 to display it.



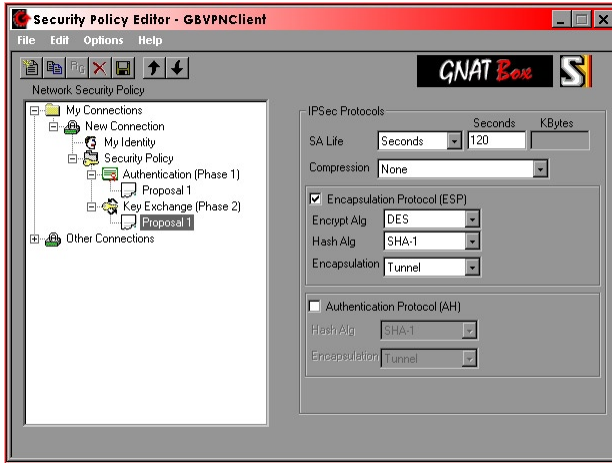
Authentication (Phase I) Proposal 1

Authentication (Phase I) Fields

Authentication Method	Select Preshared Key.
Encryption Alg	Select Triple DES.
Hash Alg	Select SHA-1.
SA Life	Select Seconds and set a value greater than 120 and less than 10 minutes (600 seconds). The default is 120 seconds. For slower connections (i.e., dial-up connections , which do not have a static IP address) it is often advantageous use a value near the minimum of 120.
Key Group	Select Diffie-Hellman Group 2.

7. Key Exchange (Phase II)

Click the “+” icon next to Key Exchange (Phase II) to expand the tree. One proposal is labeled Proposal 1. Click on Proposal 1 to display it.



Key Exchange (Phase II) Proposal 1

Key Exchange (Phase II) Fields

SA Life	Select Seconds and set a value greater than 120 and less than 10 minutes (600 seconds). The default is 120 seconds. For slower connections (e.g., dial-up connections, which do not have a static IP address) it is often advantageous use a value near the minimum of 120.
Compression	Select None.
Encapsulation Protocol	Select this item. (ESP)
Encrypt Alg.	Select DES, Triple DES or Null. Your firewall administrator should tell you which algorithm to use.
Hash Alg.	Select either MD5 or SHA-1. Your firewall administrator should tell you which hash algorithm to use.
Encapsulation	Select Tunnel.
Authentication Protocol (AH)	Deselect.

8. Save the Security Policy

Click on the “Disk” icon in the tool bar or use the File menu and select Save Changes. Your new policy will now be active. If you wish to deactivate the policy select the Non-secure option on the main policy display.

When your policy is enabled, only network packets destined for an IP address in the specified remote Protected Network will be encrypted. Packets to all other destinations will be transmitted normally.

Firewall Configuration

This provides a brief overview of the mobile client configuration procedure.

Your firewall administrator should configure a Mobile VPN definition for you. The administrator should have the following information:

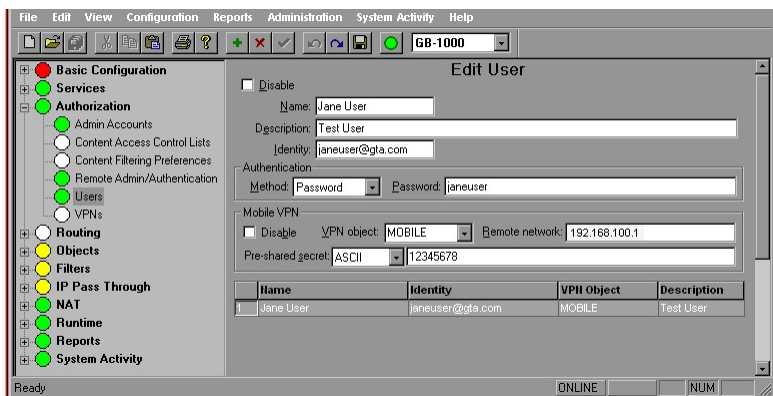
1. Your preshared key.
2. Your virtual IP address.
3. Your email address.
4. Your Phase II settings: Encryption Algorithm, Hash Algorithm and PFS Key Group.

The firewall configuration steps are:

1. Create an appropriate VPN Object (Definition), authorize the VPN and create the User.
2. Create Remote Access Filters for both IKE (UDP/500) and ESP protocols.
3. Create IP Pass Through Filters to allow both inbound and outbound access policies for the mobile client.

User Authorization

The Remote Network is the internal network IP address entered in the My Identity section of the GNAT Box VPN Client policy definition. The netmask should always be /32 or 255.255.255.255 (specifying a single host). Enter the Email address that you used in the My Identity section of the policy. Enter the preshared key you entered in the policy definition. The IDENTITY and PASSWORD fields are required by GBAuth User Authentication.



User Authorization (GBAdmin)

GNAT-Box Edit User	
Disable:	<input type="checkbox"/>
Name:	Jane User
Description:	Test User
Identity:	jjaneuser@gta.com
Authentication	
Method:	Password
Password:	jjaneuser
Mobile VPN	
Disable:	<input type="checkbox"/>
VPN object:	MOBILE
Remote Network:	192.168.100.1
Pre-shared secret:	ASCII 12345678
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>	

User Authorization (Web)

User Authorization Fields

Disable	Check to disable all access for the selected user
Name	Enter full name of the user
Description	Enter description of user
Identity	Enter user email address for user authentication
Authentication	
Method	Password method
Password	Enter password for user authentication
Mobile VPN	
Disable	Check to disable VPN access for the selected user
VPN Object	Select a previously defined VPN object
Remote Network	Enter IP address of the remote network
Preshared secret	Select ASCII or HEX value. Enter preshared secret as defined in VPN in ASCII or HEX format

VPN Objects

VPN Objects have three initial, default VPN Objects: IKE, Manual and Mobile. These defaults, once configured for your individual network, can fill most VPN requirements. IKE and Mobile default objects are similar, so either can be used as a pattern for mobile configurations.

You may either edit a default object directly, or select the default object and copy it using the Insert key or the Add (+) icon. The copy will retain all the settings of the default, but leave the name and description blank.



VPN Object List

GNAT-Box Edit VPN Object	
Disable:	<input type="checkbox"/>
Description:	DEFAULT: MOBILE VPNs
Name:	MOBILE
Mobile authentication required:	<input type="checkbox"/>
Local gateway:	EXTERNAL <input type="checkbox"/> Force mobile protocol
Local network	
Object:	Protected Networks IP Address: <input type="text"/>
Phase I	
Exchange mode:	aggressive
Encryption method:	3des
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2
Phase II	
Encryption method:	3des
Hash algorithm:	hmac-sha1
Key group:	Diffie-Hellman group 2
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>	

VPN Object, Default Mobile

Apply your changes to the VPN section by saving the section. See page 19 of this guide for field descriptions for VPN Objects

Mobile VPN Objects Fields

Disable	Check to disable all access for the selected VPN.
Name	Enter VPN name.
Description	Enter description.
Mobile Authentication	Check box to require mobile authentication.
Local Gateway	Select the Interface Object (interface or alias name) from the dropdown list.
Force Mobile Protocol	Leave Force Mobile Protocol deselected.
Local Network	Enter the IP Address/Mask or select the Object for the local (internal) network.

Phase I

Set mode, ESP, HASH, and Key Group.

Exchange Mode	Select Aggressive mode from drop-down list.
Encryption	Select the encryption method specified in the Phase I Method section of your VPN Client policy definition.
Hash Algorithm	Select the Hash Algorithm used in the Phase I section of the policy definition.
Key Group	Set the Key Group to the PFS Key Group value you specified in Phase I of the policy definition.

Phase II

Set ESP, HASH, and Key Group.

Encryption	Select the encryption method specified in the Phase II Method section of your policy definition.
Hash Algorithm	Select the Hash Algorithm used in the Phase II section of the policy definition.
Key Group	Set the PFS Key Group to the value you specified in the Security Policy section in the policy definition.

Note

Set encryption algorithm to None (Null), DES or 3DES, as in Phase II in VPN Client.

Remote Access Filters

If you already have Remote Access Filters (RAFs) in place for a remote GTA Firewall system VPN, you may only need to modify your filters. Since the IP address of the mobile client will typically be dynamic, you need to create a Remote Access Filter to allow the IKE (UDP/500) protocol to be accepted from any IP. This means your filter will need to have the source IP address set to “ANY_IP”. Additionally, you will need to have a filter that accepts the ESP protocol (IP protocol 50) from any IP.

After setting up your VPNs, you may also default your filters, then select and enable the appropriate filters. Defaulting Remote Access Filters will create filters based on the information you have provided, and erase filters that have been customized. If you have customized filters, save a copy of your configuration if you want to use the Default option. This will allow you to copy and paste or enter customized filters by hand.

Access to IKE from Mobile Clients

A Remote Access Filter should allow the IKE method to be used by a VPN Client when accessing the VPN tunnel.

- | | |
|-------------------|---|
| Description: | VPN: Allow access to IKE from mobile clients. |
| Type: | Accept |
| Interface: | ANY |
| Protocol: | UDP |
| Source: | ANY_IP |
| Destination: | ANY_IP |
| Destination Port: | 500 or Blank |

ESP Connections from Mobile Clients

Define Remote Access Filters to accept IKE/ESP connections.

- | | |
|---------------------|---|
| Description: | VPN: Allow ESP connections from mobile clients. |
| Type: | Accept |
| Interface: | ANY |
| Protocol: | ESP (50) |
| Source Object: | ANY_IP |
| Destination Object: | ANY_IP |

IP Pass Through Filters

Create IP Pass Through Filters per your corporate security policy. You will need to create at least two IP Pass Through Filters for mobile VPN Client access: one for inbound access from the mobile client and the other for outbound access to the mobile client. You can create individual filters for each mobile client, use a general filter for all mobile clients, or use a combination of the two.

For a general IP Pass Through Filter set, group your mobile VPN users in a single virtual network (e.g. 192.168.100.0). For example, the two IP Pass Through Filters listed below allow all mobile users (192.168.100.0/24) to have access to any host on the internal network (192.168.1.0/24). Likewise, any host on the internal network has access to any host with a mobile virtual IP address. Remember, this is only available if an active VPN is established.

1. Description: Allow inbound access from mobile clients.
 Type: Accept
 Interface: External
 Protocol: ALL
 Source: 192.168.100.0/24
 Destination: 192.168.1.0/24

2. Description: Allow outbound connections to mobile clients.
 Type: Accept
 Interface: Protected
 Protocol: ALL
 Source: 192.168.1.0/24
 Destination: 192.168.100.0/24

A more restrictive policy example that only allows mobile VPN clients access to a mail server (192.168.1.10) with POP3 (TCP/110) and SMTP (TCP/25) protocols would be implemented in the following manner:

1. Description: Allow only SMTP and POP3 inbound access from mobile clients.
 Type: Accept
 Interface: External
 Protocol: TCP
 Source: 192.168.100.0/24
 Destination: 192.168.1.10
 Destination Port: 25,110

2. Description: Allow outbound connections to mobile clients.
 Type: Accept
 Interface: Protected
 Protocol: ALL
 Source: 192.168.1.0/24
 Destination: 192.168.100.0/24

Enable default filter for Authentication (optional).

Description: Allow user access to authentication server.
 Type: Accept
 Interface: ANY
 Protocol: TCP
 Source: ANY_IP
 Destination: ANY_IP
 Destination Port: 76

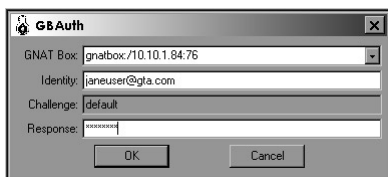
Mobile User Authentication

The GBAuth User Authentication utility program allows the mobile client user to pre-authenticate by entering an identity and password set in the GNAT Box User Authorization screen.

If the Mobile Authentication Required checkbox has been selected on the GTA Firewall, the user must run GBAuth before initiating a VPN connection. This will display a dialog box similar to the one below.

Note

The appropriate Remote Access Filter must be enabled. The Remote Access Filter defaults in GNAT Box System Software contains a filter that will be enabled if this box is checked.



GBAuth, VPN Authorization screen

Enter the name or IP address of the GTA Firewall in the GNAT Box field or select it from the drop-down box. Enter an identity (the email address specified in the GTA Firewall User Authorization section) in the IDENTITY field, then click OK or press <Return>. The cursor will move to the RESPONSE field. Enter the password from User Authorization, then click OK. If the identity or password is not recognized, a "Validation failed" box will appear.



Authentication Failed

If the information is correct, a dialog box will appear, saying "You have been Authenticated." Now you may initiate a VPN connection through the firewall.



Authenticated Successfully

If the authentication is successful, the GBAuth icon will appear on the task bar. By right-clicking on the GBAuth taskbar icon, you can close the utility, open to re-authenticate, or open the About box.

As long as the VPN is being used and data is being exchanged, the VPN automatically re-authenticates. One hour after initial authentication, GBAuth will ask the user to re-authenticate. Select Re-authenticate or Cancel. To close GBAuth, right-click on the taskbar icon and select Close.

Caution

Failing to re-authenticate or canceling authentication WILL NOT close an active VPN session.

Remote Access Filter

A default Remote Access Filter for mobile VPNs is set in the GNAT Box System Software. Once Mobile Authentication Required is checked, this filter can be enabled automatically by defaulting Remote Access Filters.

Note

If filters have never been saved, they are recalculated every time the system is restarted, according to the system parameters. If you have saved filters and then make changes to your GTA Firewall, using the Default button will recalculate your filters to match your system.

GNAT-Box Edit Remote Access Filter							
Description:	DEFAULT: Allow access to user authentication server.						
Disable:	<input type="checkbox"/>						
Type:	Accept	Interface:	<ANY>	Protocol:	TCP		
Priority:	5 - notice						
Action:	<input type="checkbox"/> Alarm <input type="checkbox"/> Email <input type="checkbox"/> ICMP <input type="checkbox"/> Pager <input type="checkbox"/> SNMP <input type="checkbox"/> Stop Interface Log: Default						
Time based:	<input type="checkbox"/> Time group is: <N/A>						
Source Address							
Object:	ANY_IP	IP Address:					
Source Ports							
Range:	<input type="checkbox"/>	0	0	0	0	0	0
		0	0	0	0	0	0
Destination Address							
Object:	ANY_IP	IP Address:					
Destination Ports							
Range:	<input type="checkbox"/>	76	0	0	0	0	0
Broadcast:	<input type="checkbox"/>	0	0	0	0	0	0
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>							

Mobile Authentication default filter

Mobile VPN Example

This section is an example of a GNAT Box VPN to VPN Client configuration.

GTA Firewall

Network

Protected Network: 192.168.1.0/16
External Interface: 199.120.225.2

User Authorizations

Name: Joe User
Description: Mobile VPN for Joe User
Identity: joe.user@gta.com

Authentication

Auth method: password
Password: "BuyGNATBox"

Mobile VPN

VPN object: MOBILE
Remote network: 192.168.100.1
Pre-shared secret: "BuyGNATBox"

VPN Objects

Name: MOBILE
Description: DEFAULT: MOBILE VPNs
Authentication required: no
Gateway: EXTERNAL
Force mobile protocol: no
Local network: Protected Networks

Phase 1

Mode: Main
Encryption Method: 3DES
HASH Algorithm: HMAC-SHA-1
Key Group: Diffie-Hellman Group 2

Phase 2

Encryption Method: 3DES
HASH Algorithm: HMAC-SHA-1
Key Group: Diffie-Hellman Group 2

Remote Access Filters

1. Description: Allow ESP connections from mobile clients.
 Type: Accept
 Interface: ANY
 Protocol: ESP (50)
 Source: ANY_IP
 Destination: 199.120.225.2/32

2. Description: Allow access to IKE from mobile clients.
 Type: Accept
 Interface: ANY
 Protocol: UDP
 Source: ANY_IP
 Source Port: 500 or Blank
 Destination: 199.120.225.2/32
 Destination Port: 500

IP Pass Through Filters

1. Description: Allow inbound from mobile client
 Type: Accept
 Interface: EXTERNAL
 Protocol: ALL
 Source: 192.168.100.1/32
 Destination: 192.168.1.0/24

2. Description: Allow outbound from network A mobile client.
 Type: Accept
 Interface: PROTECTED
 Protocol: ALL
 Source: 192.168.1.0/24
 Destination: 192.168.100.1/32

Mobile Client

Network

Virtual IP Address: 192.168.100.1/32

5 Troubleshooting

The section contains some common errors that may occur when using the VPN Client; information about how to use VPN Client's Log Viewer; and samples of a GTA Firewall's syslog facility. More information about the syslog (and all GTA Firewall systems) can be found in the **GNAT Box SYSTEM SOFTWARE USER'S GUIDE**.

VPN Client Q&A

Look for more Q&A on the GTA support website at www.gta.com.

Q: When I came in from the field and plugged my laptop into the office network, my Internet connection was suddenly not available.

A: When connecting to the network locally, disable the VPN Client. Otherwise, the attempted connections will interfere with one another.

GTA Firewall Log Messages

The following represent some of the log messages you can use to troubleshoot your VPN connection.

Starting IKE server after saving VPN sections or rebooting firewall. Licenses indicate the number of MOBILE USERS.

```
Dec  5 01:27:12 IKE: Licensed for 1 mobile client connections.
```

```
Dec  5 01:27:12 RMC: Starting IKE server.
```

Indicates a successful VPN connection set up:

```
Dec  5 01:27:11 IKE: IPSec-SA established 199.120.225.78-  
                  >199.120.225.80
```

```
Dec  5 01:27:11 IKE: IPSec-SA established 199.120.225.80-  
                  >199.120.225.78
```

Indicates a successful user connection:

```
Dec  5 01:27:11 IKE: License reserved for "joeuser@gta.com"
      (199.120.225.12---
```

Indicates a successful Authentication:

```
Dec  5 02:43:40 RMCauth: Authentication successful from
199.120.225.12
      for "joeuser@gta.com".
```

```
Dec  5 02:43:33 RMCauth: Accepted connection from 199.120.225.12.
```

Indicates a failed Authentication:

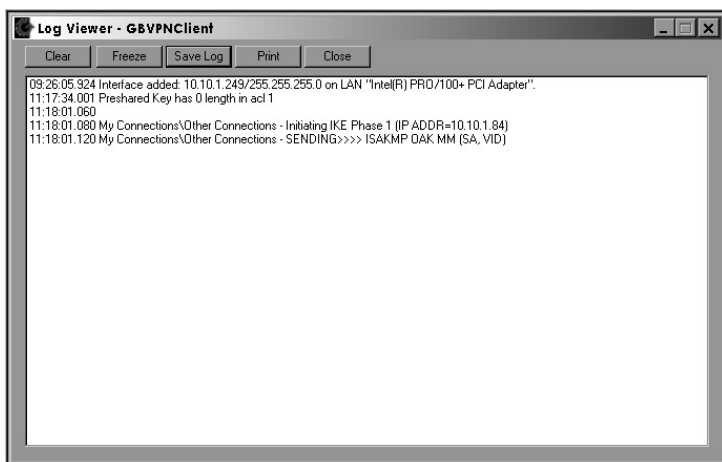
```
Dec  5 01:26:55 IKE: Authentication needed, access from
(199.120.225.12---199.120.225.78) for "joeuser@gta.com" denied.
```

VPN Expiring and renewing:

```
Dec  5 02:12:25 IKE: IPSec-SA established 199.120.225.78-
      >199.120.225.12
Dec  5 02:12:25 IKE: IPSec-SA established 199.120.225.12-
      >199.120.225.78
Dec  5 02:12:24 IKE: IPSec-SA expired 199.120.225.12->199.120.225.78
Dec  5 02:12:24 IKE: IPSec-SA expired 199.120.225.78->199.120.225.12
```

VPN Client Log Viewer

Log Viewer messages enable users to troubleshoot problems with establishing IPSec communications. The Log Viewer must be enabled for logging to occur.



Log Viewer

Log Viewer Message Format

Two types of messages can appear in the Log Viewer: error messages and IKE messages. For error messages, see [IKE Messages](#) in this section.

This is the format of IKE messages with a typical message logged in the Log Viewer:

```
01:38:02.570 Balt Corporate Access - SENDING>>>> ISAKMP OAK MM (SA)
```

Log Viewer Fields

	Definition	Message Segment
Message time	Time message is written to log	01:38:02.570
Connection name	Security Policy Editor connection name associated with the IKE activity	Balt Corporate Access
Transmit direction	Direction of IKE message: sending or receiving	SENDING>>>>
IKE message	IKE message indicating type of ISAKMP message being processed. IKE messages are defined in the SafeNet/Soft-PK Log Viewer IKE message table.	ISAKMP OAK MM (SA)

The table below shows examples of successful and failed IKE communication messages as a reference for interpreting the Log Viewer file.

Successful IKE Establishment

Description	Debug Messages
-------------	----------------

Successful Main Mode (MM) Negotiation (Pre-share) Successful SA established. Yellow key appears in SafeNet icon.	<pre> Pre-share - Initiating IKE Phase 1 (IP ADDR=IPSec peer) Pre-share - SENDING>>>> ISAKMP OAK MM (SA) Pre-share - RECEIVED<<<< ISAKMP OAK MM (SA) Pre-share - SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID) Pre-share - RECEIVED<<<< ISAKMP OAK MM (KE, NON) Pre-share - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS _ INITIAL _ CONTACT) Pre-share - RECEIVED<<<< ISAKMP OAK MM *(ID, HASH) Pre-share - Established IKE SA MY COOKIE 1f f5 e4 d 84 30 f9 5c HIS COOKIE 4c af 1f 2c 20 16 d0 ec Pre-share - Initiating IKE Phase 2 with Client IDs (message id: 61965C8D) Initiator = IP ADDR= your _ address, prot = 0 port = 0 Responder = IP ADDR= IPSec peer, prot = 0 port = 0 Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Pre-share - RECEIVED<<<< ISAKMP OAK QM *(HASH, SA, NOTIFY:STATUS _ RESP _ LIFETIME, NON, ID, ID) Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH) Pre-share - RECEIVED<<<< ISAKMP OAK QM *(HASH, NOTIFY:NOTIFY CONNECTED) Pre-share - Loading IPSec SA (Message ID = 61965C8D OUTBOUND SPI = 405 INBOUND SPI = 493B30CC) </pre>
Successful Aggressive Mode negotiation (pre-shared key) Successful SA established. Yellow key appears in SafeNet icon.	<pre> Pre-share - Initiating IKE Phase 1 (IP ADDR= IPSec peer) Pre-share - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID) Pre-share - RECEIVED<<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH) Pre-share - SENDING>>>> ISAKMP OAK AG *(HASH) Pre-share - Established IKE SA MY COOKIE 73 9c 76 19 4f 5e 35 c8 HIS COOKIE e9 94 9c 82 64 b2 fa 44 Pre-share - Initiating IKE Phase 2 with Client IDs (message id: 99F08C75) Initiator = IP ADDR= your _ address, prot = 0 port = 0 Responder = IP ADDR= IPSec peer, prot = 0 port = 0 Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Pre-share - RECEIVED<<<< ISAKMP OAK QM *(HASH, SA, NOTIFY:STATUS RESP _ LIFETIME, NON, ID, ID) Pre-share - SENDING>>>> ISAKMP OAK QM *(HASH) Pre-share - RECEIVED<<<< ISAKMP OAK QM *(HASH, NOTIFY:NOTIFY CONNECTED) Pre-share - Loading IPSec SA (Message ID = 99F08C75 OUTBOUND SPI = 189 INBOUND SPI = BA78A2CD) </pre>

Failed IKE Establishment

Description	Debug Messages
-------------	----------------

IPSec peer not responding; no key appears in SafeNet icon. Remote peer is either unreachable or not responding to SA request. Verify that IP connectivity exists to the local router and then to the IPSec peer.

```
Demo - Initiating IKE Phase 1 (IP ADDR=IPSec peer)
Demo - SENDING>>>> ISAKMP OAK MM (SA)
Demo - message not received! Retransmitting!
Demo - SENDING>>>> ISAKMP OAK MM (Retransmission)
Demo - message not received! Retransmitting!
Demo - SENDING>>>> ISAKMP OAK MM (Retransmission)
Demo - message not received! Retransmitting!
Demo - SENDING>>>> ISAKMP OAK MM (Retransmission)
Demo - Exceeded 3 IKE SA negotiation attemptsx
```

Failed Quick Mode (QM) negotiation. Improper IPSec peer configuration. Soft-PK was configured for three re-transmissions to establish SA.

```
Demo - Initiating IKE Phase 1 (IP ADDR=IPSec peer)
Demo - SENDING>>>> ISAKMP OAK MM (SA)
Demo - RECEIVED<<< ISAKMP OAK MM (SA)
Demo - SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID)
Demo - RECEIVED<<< ISAKMP OAK MM (KE, NON)
Demo - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:
STATUS INITIAL_CONTACT)
Demo - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
Demo - Established IKE SA
MY COOKIE 1f f5 e4 d 84 30 f9 5c
HIS COOKIE 4c af 1f 2c 20 16 d0 ec
Demo - Initiating IKE Phase 2 with Client IDs (message id:
61965C8D)
Initiator = IP ADDR= your_address, prot = 0 port = 0
Responder = IP ADDR= IPSec peer, prot = 0 port = 0
Demo - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
Demo - RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO
PROPOSAL_CHOSEN)
Received NO_PROPOSAL_CHOSEN message
Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission)
Demo - RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO
PROPOSAL_CHOSEN)
Received NO_PROPOSAL_CHOSEN message
Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission)
Demo - RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO
PROPOSAL_CHOSEN)
Received NO_PROPOSAL_CHOSEN message
Demo - SENDING>>>> ISAKMP OAK QM *(Retransmission)
Demo - RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO
PROPOSAL_CHOSEN)
Received NO_PROPOSAL_CHOSEN message
Exceeded retry attempts - deleting IPSec Security
Association
```

IKE Messages	
ISAKMP OAK MM (SA)	Message containing proposed parameters that will be used to secure sensitive exchange messages. ISAKMP proposal list exchange. Each proposal has a setting for encryption algorithm, hash algorithm, and Diffie-Hellman group. The agreed-on settings will be used to protect the final messages of MM and all of QM. Should the settings not be compatible, a NO PROPOSAL message will appear.
ISAKMP OAK MM (KE, NON)	The Diffie-Hellman exchange used as key material for securing sensitive exchange messages. ISAKMP Diffie-Hellman key exchange with nonce. The key, KE, is created by each party using an agreed-on formula, plugging values in the formula, and raising the result of the formula to the power of a secret value. As each party knows its secret exponent, it can take the KE received from the other party and raise that by its own exponent. If each party performs this procedure, both get a shared secret key. The nonce, NON, is a nonsense random value used in the calculation to add randomness to the KE.
ISAKMP OAK MM *(ID, HASH)	The party's identity used as authentication and a calculated hash as assurance of identification. ISAKMP message containing the identity that one party is using as identification to the other. This can be its IP address, domain name, e-mail address, or distinguished name. That identity must be accepted by the receiving party for a positive identification. The hash, HASH, is created by selecting bits of the message as samples, then sending these selected bits through an algorithm. The pattern for selection and the algorithm are agreed on in the MM proposal exchange as the hash algorithm setting. The asterisk indicates that this message is one of the final MM messages and is protected, encrypted, and hashed.
ISAKMP OAK QM *(HASH, SA, NON, ID, ID)	Proposed parameters to be used when securing the IP data, the two parties identification and nonces for a non-PFS exchange. IPSec exchange message containing a hash of the message contents, HASH, a list of the proposed parameters to be used on the user's data, SA, each party's nonce, and the identity of each party's identification, ID. The parameters agreed on will be IPSec protocol, ESP or AH; encryption algorithm, if ESP is to be used; hash algorithm; and if tunneling is to be performed. Hash algorithms and tunneling settings are for either ESP or AH. The responder in an IKE that did not use Perfect Forward Secrecy (PFS), because there were no KEs, sent this message. This means that the parties will reuse some of the agreed-on key when calculating the IPSec key. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.
ISAKMP OAK QM *(HASH)	The conclusion of the Quick Mode exchange containing a hash of the agreed-on key, protocol, the responder's SPI, and the two nonces. IPSec message used to finalize the entire exchange. This also provides a form of verification as the hash is calculated using the IPSec key, IPSec protocol agreed on, the other party's Security Parameter Index (SPI), and the two nonces each party used. The SPI is a reference number each party uses to keep track of the parameters and keys to be used for the traffic that is sent and received. For example, I would tell you my SPI so when you transmit a protected message to me, I know how to handle the message properly, and vice versa. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.
ISAKMP OAK MM (KE, NON, VID)	The Diffie-Hellman exchanged and nonce used as key material for securing sensitive exchange messages and the product vendor ID. ISAKMP message containing a Diffie-Hellman key, KE, nonce used to add randomness to the key, and a Vendor ID used to notify the receiver of the transmitting party's vendor. This can be used to associate what the transmitter's capabilities are and allow parameter preferences to be made as well as determining if the connection should be established.
ISAKMP OAK INFO *(HASH, NOTIFY, NO, PROPOSAL_CHOSEN)	Message indicating that the QM exchange parameters were incompatible, so the exchange failed. IPSec message viewed when the list of proposed parameters did not have any common settings for the transmitter. This means the IPSec parameters for each party must be verified. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.
ISAKMP OAK QM *(Retransmission)	Message indicating a previously sent message was sent again because no response was received in the allotted time. IPSec message sent when a previous message was not responded to in the configured time period. This indicates that one of the parties may not be available to complete the exchange. The asterisk indicates that this message is secured using the agreed-on ISAKMP parameters and key.

Sample Messages

```

Device A
Phase 1 – Authentication
1. MM ----->
   SA (Security Association) DES/SHA-1/DHG1; TDES/SHA-1/DHG2
2. <----- MM
   SA: TDES/SHA-1/DHG2
3. MM ----->
   KE (Diffie-Hellman a^x), NON (nonsense, random number)
4. <----- MM
   KE (Diffie-Hellman a^y), NON (nonsense, random number)
5. MM ----->
   ID (the identification of one party), HASH
6. <----- MM
   ID, HASH

*** Phase 1 Complete ***
Phase 2 – Key Exchange with Perfect Forward Secrecy (PFS)
1. QM ----->
   SA: ESP/DES/SHA-1; ESP/TDES/SHA-1; AH/MD5, KE, NON
2. <----- QM
   SA: ESP/TDES/SHA-1, KE, NON
3. QM ----->
   HASH

```

Message Explanations

During Phase I, IDs and parameters for protecting Phase II are established.

1. Device A sends a list of proposed parameters to protect the Phase II key exchange and the level of key strength it wants to use for Phase I's key exchange, not necessarily for both phases.
2. Device B selects the proposed parameters it prefers over the other proposals and send its selection to Device A. If none of the proposals fit its requirements, it sends a NO PROPOSAL message and the exchange ends. The two parties must be reconfigured to work.
3. Should the exchange continue, Device A calculates a number "a raised to x" where a is known by each device and x is a random number known only by Device A. The NON is a random number added to the calculation to add randomness.
4. Device B receives that message and performs a similar calculation.
5. Both sides exchange identification. Alternate subject fields—IP address, e-mail address and domain name—can be used as IDs. The ID is a field containing the information the party is using to identify itself.
6. If either side fails to accept the other's ID, the exchange ends. The two parties must be reconfigured.

If both sides are satisfied, Phase I completes and Phase II begins.

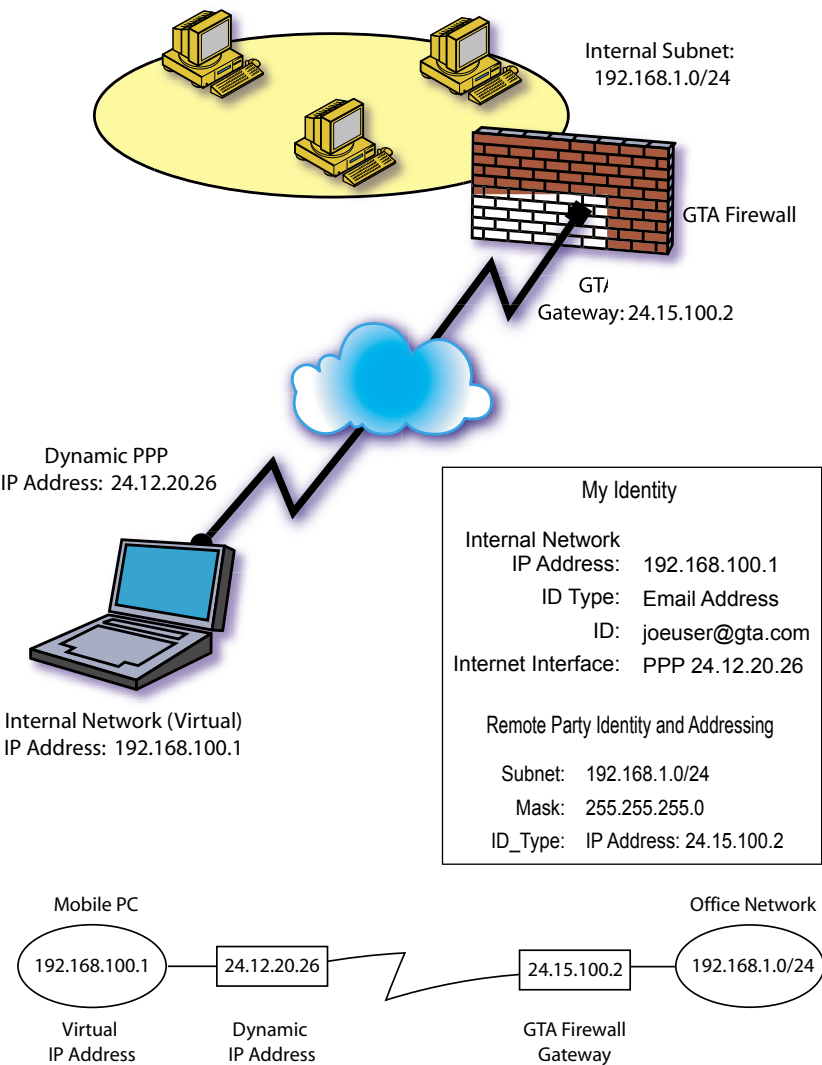
- Device A sends a list of proposed parameters using the new key material established in Phase I.

- Phase II concludes with a HASH—the IDs and NON's of each party and the responder's (Device B's) SPI to use when sending packets.

The two parties can now exchange data securely.

Appendix

VPN Client Examples & Worksheet



Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: _____ *Pro Network Netmask*Mask: _____ *Protected Network*

Protocol: ALL

Connect using Secure Gateway ☒

Tunnel: IP Address

ID_Type: _____ *Firewall's External Interface IP Address*

My IdentityPre-Share Key: Don't write it down *At least 8 characters*Internal Network IP Address: _____ *Virtual IP Address assigned by FW admin*

ID Type: Email Address

ID: _____ *Your Email Address*Internet Interface: _____ *PPP or a Ethernet NIC*

Security PolicyAggressive Mode: ☒ *Select this before you can select ID Type above*Enable PFS: ☒PFS Key Group: ☐ Diffie-Hellman Group 1 *Pick one For Phase II*☐ Diffie-Hellman Group 2☐ Diffie-Hellman Group 5Enable Replay Detection: ☒

Authentication (Phase I)

Encryption Alg: 3DES

Hash Alg: SHA-1

SA Life: _____ Seconds *(120-600 seconds)*

Key Group: Diffie-Hellman Group 2

Key Exchange (Phase II)SA Life: _____ Seconds *(120-600 seconds)*

Compression: NONE

Encapsulation Protocol (ESP): ☒Encryption Alg: ☐ DES ☐ 3DESHash Alg: ☐ SHA-1 ☐ MD5

Encapsulation: Tunnel

Index

Symbols

3DES 13

A

access control 11
activation code 5, 39
AES 13
algorithms 13
Anti-replay protocol 21
authentication 7, 62, 67, 70
Authentication Header 10, 21

B

benefits of VPN 1
Blowfish 13

C

CAST128 13
certificate
 GNAT Box support 2
 SafeNet support 2
Certificate Manager 38
client-to-client
 VPN client 2
client-to-gateway
 VPN Client 2
Compact Flash. *See* flash memory
compatibility 3, 66
concurrent sessions 3, 39
confidentiality 8
Configuration Report 4
conventions, documentation 5
Copyright ii
copy protection 4

D

default
 password. *See* factory settings
 Remote Access Filters 54
 user ID. *See* factory settings
 VPN Objects 52
DES 13
Diffie-Hellman 15
digital certificates 35, 42

discontinuous network
 VPN Client to 35

documentation 5
download 39
drivers and NICs 6

E

Email ii
Encapsulated Security Payload.
 See ESP
encapsulation 9
encryption algorithms, methods 13
ESP 11, 13
Exception 4, 19
Exchange Mode 15, 20

F

features of VPN 1
feature code. *See* activation code
flash-based products 23
Force Mobile Protocol 25

G

gateway. *See* default: route
gateway-to-gateway
 VPN 1
GB-Pro
 one default object 19
GBAdmin 6
GBAuth 9, 56
Global Policy Settings 43
GNAT Box System Software ii

H

H2A. *See* High Availability
hash algorithms 12
hash key length 12
help. *See* support
Help Menu 38
hexadecimal 14, 25
High Availability 6

I

identity 69
IETF IPsec standard 1
IKE 24, 61, 64, 66
inbound packet 10
insecure 1, 36

installation

software 40

installation support 4**integrity** 7**interoperability** 3**K****key length**

encryption (ESP) 13

hash 12

L**LAN/WAN** 2**license**

mobile client 3, 4, 39

lifetime, SA 16**logical networks**

must be different 8

Log Viewer 38**M****Manual Key Method** 24**MD5** 12, 21, 67**Mobile IKE** 15, 17, 26**Mobile Key Method** 24**mode** 64, 70**multiple discontinuous networks**

VPN Client to 35

my identity 45**N****NAT (network address translation)** 8**new connection** 43**Note.** *See* notes & warnings**notes & warnings** 2, 3, 4, 9, 13, 14,

16, 21, 38, 39, 42, 46, 53, 56, 57

caution 57

exception 4, 19

Null Tunnel Mode 10**O****outbound packets** 9**P****packet**

inbound 10

packets 8

outbound 9

packet flow 9**PFS (Perfect Forward Secrecy)** 15,
21, 66, 70**Phase I** 70**Phase II** 70**port protocol** 45**PPP** 69**preshared keys** 14**Protocol, anti-replay** 21**R****registration** 3, 6**remote party** 44**Remove Icon** 38**Replay Detection** 21**requirements** 2**Rijndael** 13**router** 65**routing problems** 9, 25**S****SafeNet** 63**Security Association (SA)** 16**security gateway** 10**Security Parameter Index** 16**security policy** 25, 35, 37, 38, 42, 44,
47, 54**Security Policy Editor** 63**SHA1, SHA2** 12, 21**software**

uninstall 42

software installation 40**support** 3, 19, 35, ii

installation 4

T**taskbar icons** 36**technical support.** *See* support**Telephone** ii**Terms** 6**trademark** ii**transparent**

VPN Client 9

troubleshooting 6**tunnel mode** 8, 10, 17**Twofish** 13**U****unauthorized access** 11**uninstall software** 42**unregistered IP** 8**User Authentication.** *See* GBAuth

user authorization 50

V

valid configurations 9

version ii

SafeNet 2

VPN Client

discontinuous networks to 35

VPN definition. *See* VPN Objects

VPN Objects 19

VPN tunnel 9

W

warning 11, 38

Web 6

Windows

compatible 2, 35, 46