GB-OS

VPN Gateway

& GTA Mobile VPN Client

Option Guide

VPNOG200506-01

Global Technology Associates, Inc.

Contents

Introduction

What is VPN?

VPN means Virtual Private Network.

- ***What makes it private?*** You can access resources on your network as if you were a second private network attached to the private (trusted) part of your network.
- ***What makes it virtual?*** You're not ***really*** accessing your private network from the private network: you're accessing it from a public or other untrusted network, such as the Internet. A combination of authentication, encryption and tunneling technologies are used to make sure that your data is transmitted securely, so you can trust your connection as if you would trust your normal private network connection.

VPN connections provide a way to access your protected data from an insecure location, all without compromising your network security.

VPNs vs. Standard NAT Tunnels

Standard tunnels can provide external access to your internal network. So why use a VPN?

VPNs provide ***more secure access*** than standard tunnels. VPN tunnels provide methods to assure authorization, data integrity, or privacy. As a result, VPN tunnels can secure even connections that normally do not provide encryption, authorization or integrity checking on their own.

Standard tunnels do not provide these VPN safety mechanisms!

VPNs are an ideal secure network solution for employees that travel or work from home. They also can serve to securely connect branch offices to a main office or data center.

GTA firewalls support the IPSec VPN standard; this provides interoperability with many third-party VPN products. IPSec VPNs can use a defined combination of:

- authentication keys
- anti-tampering hashes
- data encryption
- IP packet encapsulation

to ensure the identity, integrity, and privacy of your data transfers over public, untrusted networks. For more information, see Elements of IPSec VPN Security.

About IPSec VPN on GTA Firewalls

GTA firewalls provide IPSec controls for both mobile client (commuter-to-office) and gateway-to-gateway (office-to-office) VPN connections.

GTA firewall VPN is a security gateway version of the IPSec standard; the mobile VPN client provides the host version. For specific information on the GTA implementations of the IPSec standard, see Elements of IPSec VPN Security.

What's New: NAT Traversal; New VPN Client

Both the GTA firewall's VPN gateway and GTA Mobile VPN Client software now support NAT traversal (also known as "NAT-T") technology.

NAT traversal (RFC 3947 and RFC 3948) allows use of IPSec VPN over networks with NAT filters that deny IP protocol 50 (ESP), which is required for IPSec data protection. NAT traversal encapsulates ESP traffic within UDP port 4500 to bypass NAT filtering.

NAT traversal is automatic for both GB-OS 3.7 firewalls and the new VPN client, and requires no configuration.

The new GTA Mobile VPN Client is required to use NAT traversal. Previous versions of the GTA (GNAT Box) Mobile VPN Client do not provide RFC 3947 NAT traversal capabilities.

The VPN Gateway (Firewall) Component

GTA firewalls can function as VPN gateways, handling authentication and encryption for VPN tunnels.

The VPN gateway is configured on the firewall directly using the web administrative interface. VPN configurations are created in **VPN Objects**, and bound to an incoming authorization channel in either **Users** (for mobile VPN clients or a second VPN gateway with a dynamic IP address) or **VPNs** (where both VPN gateways have a static IP address).

GTA firewalls can interoperate with either another GTA firewall (for office-to-office VPNs) or a mobile VPN client (for commuter-to-office VPNs).

Because GTA firewalls support the IPSec VPN standard, GTA firewall VPNs are also interoperable with third-party products that also support the IPSec VPN standard. For information on creating a VPN between a GTA firewall and another VPN gateway, see additional documentation located on GTA's web site (http://gta.com/support/documents/).

Features

- ***NEW!*** NAT traversal
- Easy application of security policies
- Easy creation and revision of VPNs using VPN configuration objects
- Quickly enable and disable VPN authorizations
- AES-128, AES-192 and AES-256, 3DES, DES and Blowfish methods for confidentiality
- MD5, SHA-1 and SHA-2 one-way hash methods for data integrity
- Up to 4,096-bit Diffie-Hellman keys for authenticity

The Client Component

With the mobile VPN client option, GTA firewalls can also provide VPN protection to travelling employees or employees working from home.

Your mobile VPN client software is installed on the client computer. It serves to locally perform the authentication, encryption and other services that would normally be performed by a second VPN gateway. Mobile VPN client software negotiates the connection with your GTA firewall VPN gateway.

The GTA Mobile VPN Client is Microsoft ® Windows®-compatible VPN software. This client is new to the release of GB-OS version 3.7, which also supports NAT traversal.

Features

- ***NEW!*** NAT traversal
- Easy VPN setup
- Client-to-client and client-to-gateway VPNs
- Compatible with most versions of Microsoft® Windows® (including Windows XP Service Pack 2)
- DES, 3DES, and AES encryption methods for confidentiality
- MD5 and SHA-1 one-way hash methods for data integrity
- Up to 2,048-bit Diffie-Hellman keys for authenticity
- USB mode allows easy start/stop of VPN with insertion/removal of a USB drive

Minimum Requirements

- Microsoft® Windows® 95, 98, Me, NT 4 (Service Pack 6 or greater), 2000, XP
- Intel® Pentium® class or greater processor
- 10 MB unused hard disk space
- 128 MB RAM
- 56K dial-up modem, wireless (WiFi), Ethernet or other compatible network card

About This Guide

This guide shows how to use IPSec VPN on your GTA firewall and how to install, set up and use the GTA Mobile VPN Client, a program designed to connect mobile and remote users to a virtual private network.

Conventions

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

Bold Italics	emphasis
Italics	publications
Blue Underline	clickable hyperlink (email address, web site or in-PDF link)
SMALL CAPS	on-screen field names
`Monospace Font`	on-screen text
Condensed Bold	on-screen menus, menu items
BOLD SMALL CAPS	on-screen buttons, links

Organization of the chapters in this guide is divided according to relevance for firewall or client primarily, and secondarily by order of steps used to complete a task. For the location of specific topics, please see the table of contents or index.

If you encounter troubles while configuring the firewall or VPN client, a list of frequently asked questions, guidelines, and other solutions are available in Troubleshooting. To read about technical details of IPSec and GTA firewall VPN implementation, see Elements of IPSec VPN Security.

Additional Documentation

For additional instructions on installation, registration and setup of a GTA product, see applicable Quick Guides, FAQs or technical papers. For optional features, see the appropriate feature guide. Documentation is included with new GTA products, and is available for download from the GTA web site.

Note

For the latest documentation, check the GTA web site for PDFs and other formats.

These manuals and other documentation can also be found on the GTA web site (www.gta.com). Documents on the web site are either in plain text (*.txt) or portable document format (*.pdf) which requires Adobe Acrobat Reader version 5.0 or greater, Apple Preview or ghostview. A free copy of Adobe Acrobat Reader can be obtained at www.adobe.com.

GB-OS User's Guide	GB-OS firewall software features; web user interface, GBAdmin
GB-Commander Product Guide	GB-Commander for GTA firewalls
GTA Reporting Suite Product Guide	stand-alone reporting software
Mail Sentinel Option Guide	email anti-spam and anti-virus filtering optional feature
Surf Sentinel Content Filtering Option Guide	content filtering optional feature
H_2A High Availability Option Guide	high availability optional feature
GTA VPN Option Guide	VPN (virtual private networks) optional feature
www.gta.com	hardware specifications, current documentation, examples

Mailing List

To learn more about GB-OS, join the GTA staff-monitored email mailing list by sending a blank email to gb-users-subscribe@gta.com.

Support

Installation Support

Installation ("up and running") support is available to registered users. See GTA's web site for more information.

If you need installation assistance during the first 30 days after purchase, register your product and then contact the GTA support team by email at support@gta.com. Include your product name and serial number(s).

Support Contracts

If you need support for GTA products, a variety of support contracts are available. Contact GTA sales staff for more information. Contracts range from support by the incident, to full coverage for a year. Other assistance may be available through the GNAT Box Mailing List or through an authorized GTA Channel Partner.

Setup

Overview

This section explains configuration steps for an IPSec VPN on both the firewall and a client computer. It also provides configuration examples for common types of IPSec VPN setups.

Each GTA firewall VPN requires a minimum of two points: an initiator and a responder. The responder must be a GTA firewall; the initiator can be either a second VPN gateway or a mobile VPN client.

GTA firewall VPN setup requires configuration of both:

- GTA firewall
- GTA Mobile VPN Client ***or*** a second VPN gateway (e.g. GTA firewall)

Setup times will vary according to your VPN components, but can be completed in as little as 15 minutes.

Instructions for VPN setup with:

- Macintosh computers
- Third party firewalls
- Non-IPSec VPNs

are available at the GTA web site (http://gta.com/support/documents/).

For more information on IPSec VPN, see Elements of IPSec VPN Security.

On the GTA Firewall (VPN Gateway)

To use IPSec VPN with a GTA firewall, five firewall aspects ***must*** be configured in order:

1. Feature activation codes
2. VPN configuration objects
3. VPN or user authorization
4. Firewall (remote) access filters
5. Inbound (passthrough) traffic filters

Additionally, the second VPN gateway (GTA firewall or third-party VPN gateway) or mobile VPN client must be configured to reflect the same settings.

Entering Feature Codes

When a VPN option is purchased, feature activation codes are required for client-to-gateway VPNs. If you have purchased a mobile VPN client license package, enter its feature activation code into the **Features** section of the firewall configuration. Click **SAVE**.

If gateway-to-gateway VPN is not a standard feature of your firewall, and you have purchased a VPN option, also enter the VPN option's feature activation code and click **SAVE**.

Note

Feature activation codes for gateway-to-gateway VPNs are required only for GTA firewalls that are not sold with VPN as a standard feature. See your firewall's specifications for more information.

Creating VPN Configuration Objects

VPN objects contain information specific to VPN connections on your GTA firewall. This information includes aspects such as hash algorithms (for data integrity) and encryption methods (for data privacy). VPN configuration objects are applied to incoming VPN connections.

VPN Objects lists available VPN configurations.

VPN configuration objects are not activated until referenced by an authorization and allowed by firewall (remote) access and inbound traffic (passthrough) filters.

Four VPN objects exist by factory default:

- IKE
- Mobile
- Manual
- Dynamic (Anonymous)

These default VPN objects are useful templates for defining your own custom VPN. For example, the mobile VPN object is essentially IKE for VPN Client users; if you want to use a mobile VPN client, the mobile VPN object contains templated settings that may be useful to you. Meanwhile, the dynamic VPN object allows definition of VPN Phase I and local identity for any dynamically-addressed firewall or client connecting to a statically-addressed firewall.

Note

For IPSec VPNs, a VPN object must define both Phase I and Phase II settings. Because the dynamic (anonymous) VPN object does not provide for entry of Phase II settings, it cannot be used as a template for IPSec VPN configuration.

Caution

The **DEFAULT** button in **VPN Objects** reverts the available configurations to these factory-default objects. Custom VPN configuration objects will be lost!

Key exchange, essential to authentication during IPSec VPN construction, can be accomplished either manually or automatically (with IKE).

In manual key exchange, Phase I settings cannot be user-configured.

In IKE (automatic key exchange), Phase I of the connection establishes an IKE security association that is later used to securely create an IPSec SA; it negotiates the VPN terms and authorizes the peer. Phase II establishes security associations (SAs) for IPSec, providing source authentication, integrity and confidentiality.

Example VPN objects for differing VPN setups (e.g. client-to-gateway, gateway-to-gateway) are provided in Examples.

To configure an IPSec VPN configuration object:

1. Click **Objects** then click **VPN Objects** in the GB-OS menu. Add (+) a new IKE VPN configuration object, or edit (✓) the existing IKE VPN configuration object. (Manual, mobile and dynamic VPN objects also exist and are similar, but will not be specifically covered here. For more information on their use, see Examples)
2. Enter a unique name and description for the configuration object, e.g. “Strong Encryption IPSec VPN”.
3. If you wish to require authentication with GBAuth, before using the VPN, check the **AUTHENTICATION REQUIRED** check box to require pre-authentication.
4. For the Local Gateway, select the interface object that will be the VPN gateway on ***this*** firewall. For the Local Network, select the subnetwork or manually indicate an IP address (with or without a subnet mask) to indicate which hosts the VPN may join on ***this*** firewall. (This is usually the internal/protected network.)
5. Define Phase I (IKE/IPSec negotiation) settings.
   - To force use of NAT traversal (UDP tunneling, a.k.a “NAT-T”) even if NAT is not present, check the **FORCE NAT-T PROTOCOL** check box.
   - To force use of a specific encryption algorithm, select **Aggressive** for the Exchange Mode; otherwise, select **Main**, which will automatically negotiate an encryption algorithm selection.
   - Enter the Local Identity of ***this*** firewall: select the type and value used during initial VPN validation, such as an IP address, domain name or email address value. (This must match the Remote Identity in the GTA Mobile VPN Client or second VPN gateway’s configuration.)
   - Select an encryption algorithm, hash method and key that will be used to encrypt, verify and authorize your IKE (IPSec VPN setup) exchange. Reasonable defaults have been provided for most connections; review your options and modify the selections as your security policies dictate.
   - Enter an integer in Lifetime to indicate the number of seconds before a VPN must be re-negotiated to protect from overexposed key attacks. This number must be greater than the maximum lifetime used by a connecting GTA Mobile VPN Client.
   - Enter an integer in DPD Interval (for dead peer detection) to indicate the number of seconds between each check for VPN activity.
6. Define Phase II (established IPSec VPN connections) settings.
   - Select an encryption algorithm, hash method and key that will be used to encrypt, verify and authorize your IPSec exchanges. Reasonable defaults have been provided for most connections; review your options and modify the selections as your security policies dictate.
   - Enter an integer in Lifetime to indicate the number of minutes before a VPN must be re-negotiated to protect from overexposed key attacks. This usually should not be the same number as the Phase I lifetime to prevent delays in VPN connections as both phases are re-negotiated.
7. Click **OK**. Click **SAVE**.

Creating Authorization

VPNs and **Users** applies a VPN configuration object to a type of authorized VPN or mobile VPN user’s connection.

After creating a VPN configuration using **VPN Objects**, use the **Authorization** section to apply a VPN configuration object to an authorized VPN or mobile VPN user, enable it, and define the IP addresses that hosts connected via VPN will use. Use **VPNs** for gateway-to-gateway VPNs with static IP addresses; use **Users** for client-to-gateway VPNs, or gateway-to-gateway VPNs where the second gateway has a dynamic IP address.

VPN authorizations are not active until allowed by firewall (remote) access and inbound traffic (passthrough) filters.

Authorization creates a loggable identity for VPN hosts and supplies some information necessary to the negotiation of the VPN connection.

To authorize a VPN connection:

1. If the second point on your VPN will be another VPN gateway with a static IP address, click **Authorization** then **VPNs.** If the second point on your VPN will be a mobile VPN client, or the second VPN gateway has a dynamic IP address, click **Authorization** then **Users**.
2. Add (**+**) or edit (✓) an authorized VPN or user.
3. If using **VPNs**, specify IKE or manual key exchange. This should mirror your intended selection of an IKE or manual VPN configuration object.
4. Enter a unique description for the authorized VPN/user, e.g. “Branch Office VPN” or “Database Administrator”.
5. If using **VPNs**, specify the identity of this VPN in the Local Identity field. (This should reflect the Remote Identity of the second VPN gateway.)
   If using **Users**, specify the Identity of the user, e.g. “vpnuser@example.com”. (This should reflect the Local Identity of the mobile VPN client or dynamically-addressed VPN gateway. It is not necessary for statically-addressed VPN gateways.)
6. If using Users, enter an authorization Method and enter a Password.
7. Un-check the **DISABLE** check box to enable the authorized VPN or user.
8. Select the VPN Object you made during while Creating VPN Configuration Objects.
9. Select a logical network that the initiating VPN host should join from Remote Network, or manually indicate the IP Address it should use while joined to the VPN. If using **VPNs**, enter the Remote Gateway that the attached VPN should use.
10. Enter the Pre-shared Secret that a VPN or user must present to initiate the VPN connection.
11. Click **OK**. Click **SAVE**.

Enabling Inbound VPN Connections

Enabling inbound connections for your VPN requires two functional elements:

- ***allowing authorization***
- ***allowing tunneling***

These are provided by remote access and passthrough filters. GTA firewalls consult these filters first, ***before*** deciding to authorize a VPN connection and then route the VPN connection.

Allowing Authorization

Remote access filters control permission for the initial connection made to the VPN gateway (firewall) to obtain authorization and set up SAs. This authorization must be obtained before the firewall will allow access to the VPN tunnel.

Note

Creation of VPN remote access filters assumes that the AH and ESP protocols (51 and 50, respectively) exist in the configured **IP Protocols**. If they have been deleted from your default set, you may manually re-create them. See the *GB-OS User's Guide* for more information.

Accept IPSec VPN packets (both AH and ESP IP protocols) from the VPN initiator. (If you are creating a non-IPSec VPN, the steps may be slightly different.)

To create remote access filters for your IPSec VPN:

1. Click **Filters** then **Remote Access**.
2. Add a new remote access filter by clicking an "up" or "down" triangle on a filter to indicate where in the prioritized list the filter should be placed. Placement near the top of the filter list is advisable to ensure that packet denial does not occur before the acceptance filter is evaluated.

Caution

The **DEFAULT** button in **Remote Access** reverts the available remote access filters to factory-defaults; one of these factory-default remote access filters will allow your VPN connections. However, if you click it, any custom remote access filters will be lost!

3. Enter a unique description for the filter, e.g. "Allow IPSec VPN: ESP Protocol".
4. Select "allow" as the TYPE.
5. Select the external network card as the INTERFACE.
6. Select ESP as the PROTOCOL.
7. Select "<ANY_IP>" as the OBJECT of the source (initiator) IP address.

Note

Initiators may have either a dynamic (DHCP) or static IP address; this will determine the type of the OBJECT for the source IP address. Mobile VPN clients usually have a dynamic IP address, so the source IP address of the remote access filter must be "<ANY_IP>" to accommodate the full range of IP addresses that the client may have. If you are establishing a gateway-to-gateway VPN with static IP addresses only, however, set the source IP address to that of the second VPN gateway.

8. Select the firewall's local VPN gateway IP address as the destination IP address OBJECT. (Remote access filters dictate access to the firewall itself, not to internal networks.)
9. Click **OK**. Click **SAVE**.
10. Repeat steps 2 through 9 for a UDP port 500 connection if your VPN uses IKE; also repeat it for UDP port 4500 if you wish to use NAT traversal (NAT-T). (The AH filter will be created automatically once you create the ESP filter.)

Allowing Tunnel Access

Passthrough filters perform the function of permission (as our remote access filter did for incoming connections in Allowing Authorization Access) but in a slightly different capacity: while remote access filters control connections that must be made ***to*** the firewall (such as the initial VPN authorization), passthrough filters control connections made ***through*** the firewall to a private network (such as the actual data transfer). If the authorization connection is permitted but the data connection is not permitted, the overall VPN construction will fail, providing *de facto* denial. A passthrough filter must be created to allow use of the VPN tunnel.

Since VPN connections do not receive NAT treatment, this causes the firewall to act as if is bridging the private and VPN subnetworks.

The passthrough filter can be general or specific: it can broadly apply to all connections between two subnetworks, or it can be as specific as connections between two specific hosts during a certain time of day for selected protocols. For IPSec VPNs, passthrough filters generally allow connections between the internal networks and the VPN client/network, regardless of the TCP port or time of day.

Generally you will need two passthrough filters for each VPN definition: one for inbound (creating the tunnel for VPN-to-protected network connections) and one for outbound (creating the tunnel for protected-to-VPN network connections).

In other words, a passthrough filter is directional, so a pair of them must be created to allow normal bi-directional connections.

Note

Passthrough filters for VPN definitions do not require entries in **Pass Through Host/Network**, because it is not a bridged connection.

To create passthrough filters for your IPSec VPN:

1. Click **Pass Through**. Click **Filters**.
2. Add a new remote access filter by clicking an "up" or "down" triangle on a filter to indicate where in the prioritized list the filter should be placed. Placement near the top of the filter list is advisable to ensure that packet denial does not occur before the acceptance filter is evaluated.

Caution

The **DEFAULT** button in **Filters** under **Pass Through** automatically creates a set of passthrough filters necessary by any authorized VPNs you have configured. However, if you click it, any custom remote access filters may be lost!

3. Enter a unique description for the filter, e.g. "Allow IPSec VPN: mobile user VPNuser".
4. Select "allow" as the TYPE.
5. Select the external network card as the INTERFACE (i.e. packets arriving on this network card should be filtered with this passthrough filter).
6. Select "any" as the PROTOCOL.
7. Select the ***original*** (non-VPN-encapsulated) source of the connection as the OBJECT of the source IP address. If your filter is for a mobile VPN client, this may be a single IP address rather than a whole network.

Note

The interface (network card) and the source/destination IP address together define the directionality of the passthrough filter. For example, a destination on the protected network arriving on the external interface marks an inbound passthrough filter; a source on the protected network arriving on the internal/protected interface marks an outbound passthrough filter.

8. Select the ***original*** (non-VPN-encapsulated) destination of the connection as the OBJECT of the destination IP address.
9. Click **OK**. Click **SAVE**.
10. Repeat steps 2 through 9 for the outbound connection (packets arriving on the protected interface with a destination on the external network).

On the Client Computer

If laptop computers and other non-gateway servers and computers will connect to your GTA firewall VPN, install and configure GTA Mobile VPN Client software on those computers.

Mobile VPN client software is available for purchase separately from an authorized GTA Channel Partner or GTA sales.

These instructions assume that your VPN client computer is not behind a router that requires modification.

Installing the VPN Client Software

With GB-OS version 3.7, a new mobile VPN client has been introduced to complement the new NAT traversal (NAT-T) features.

The installation process for the GTA Mobile VPN Client is typical for Windows®-compatible software.

To install the GTA Mobile VPN Client software:

1. Log in to the Windows computer as an administrator.
2. Uninstall any other VPN client software.

Caution

All other IPSec VPN client software (e.g. Nortel Contivity, SafeNet or Cisco VPN Client) should be removed prior to installation of the GTA Mobile VPN Client. Concurrently installed VPN client software can cause instability of your computer.

3. Start the installer. Click the **NEXT** button. Read the license agreement; if you agree to the terms, click the **YES** button.
4. Choose an installation location for the software, e.g. C:\ProgramFiles\GTA\Mobile VPN Client. Click the **NEXT** button. Click the **NEXT** button. Click the **FINISH** button.
5. Reboot your computer and log in again.
6. A window for the VPN client will appear. Enter the serial number for the VPN client software.

Note

Without a valid ***VPN client serial number*** the software will operate in a trial mode for 30 days only.

7. The VPN client will start; its icon will appear in your system tray (next to the clock). Click it to view the configuration window.

Note

Closing the configuration window will not stop the VPN client. To quit the VPN client, right-click the icon in the tray and select **Quit**.

Configuring the VPN Client Software

To connect your computer with the GTA firewall VPN, you must first provide your mobile VPN client software with the required VPN settings.

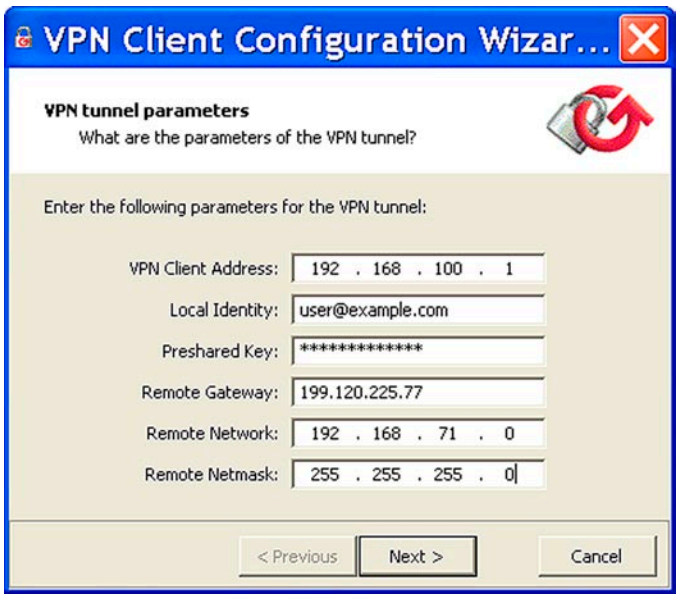
Use the worksheet to collect settings for your VPN client. Enter them if required by tunnel, Phase I or Phase II setup. Once your VPN client is configured, start/stop your VPN connection as desired.

For more information on advanced mobile VPN client features such as automatic start/stop of your VPN connection, see Advanced Mobile Client Setup.

Note

You may use the wizard to configure your software. It will configure the client for a connection compatible with default GB-OS firewall settings. If you elect to use the VPN client configuration wizard, you do not need to complete the manual configuration instructions in this section.

To use the configuration wizard, select **VPN Configuration** then **Wizard** and complete the available fields. Click **NEXT** and then **FINISHED**. (Click **?** for help.)



Using the GTA Mobile VPN Client's Configuration Wizard

VPN Settings Worksheet

Settings for your VPN client software must match your firewall's VPN settings. If you do not manage your firewall, consult your network administrator to obtain matching VPN settings.

These settings must match the VPN configuration object and authorization settings on your GTA firewall.

Firewall IP address/domain name:_____

Phase I

Pre-shared secret:_____

IKE

Encryption:_____

Hash (authentication):_____

Key (group):_____

Lifetime:_____

Dead peer detection (DPD) interval:_____

Advanced

Aggressive or main mode: aggressive

IKE port: 500

Local ID:_____

Remote ID:_____

Phase II

Protected network IP address w/ mask:_____

VPN client's IP address w/ mask:_____

ESP

Encryption:_____

Hash (authentication):_____

Key (group):_____

Lifetime:_____

Mode: tunnel

Entering Preferences (Parameters)

Parameters for phase lifetime and dead peer detection (DPD) don't need to match the settings of your GTA firewall, but agreement is beneficial.

To enter the lifetimes and dead peer detection intervals for Phase I and Phase II of your VPN:

1. Start your VPN client software (or click its item in the system tray to show a configuration window).
2. Click **PARAMETERS**.
3. Enter your IKE and IPSec (Phase I and Phase II) lifetimes in the LIFETIME area. Numbers are in seconds. Times specify when keys should be renewed and security associations recreated. Smaller times are generally more secure, although they can add performance overhead to the VPN.

Note

The maximum lifetimes for the mobile VPN client must be less than the lifetime indicated by the firewall.

4. Enter your check interval for dead peer detection (DPD). Do ***not*** enter 0.
5. Leave **BLOCK NON-CIPHERED CONNECTION** unchecked unless you wish to force ***all*** connections, including traffic with a non-VPN destination, through the VPN tunnel.
6. Entry of other DPD retry and replay window information are not necessary.
7. Click **SAVE & APPLY**.
8. Proceed to configuring Phase I.

Configuring Phase I (IKE)

Phase I settings must match your GTA firewall settings.

Default settings for Phase I are AES-192 encryption, SHA-1 hashes and Group 2 (1,024-bit) keys.

To enter the Phase I settings of your VPN:

1. Start your VPN client software (or click its item in the system tray to show a configuration window).
2. Click **Configuration**.
3. Right-click **Configuration** and select **New Phase I**. A new sub-item to the **Configuration** tree will appear; it will have a default name, such as CnxVpn1, that you may change in the NAME field.
4. Enter a new NAME if desired, with no spaces or special characters, e.g. "OfficePhaseI".
5. Select the INTERFACE (network card) that will be used (select * to indicate all available network cards).
6. Enter the REMOTE GATEWAY, which should be the external IP address or domain name of your GTA firewall.
7. Enter the PRESHARED KEY (secret) for your VPN connection and then CONFIRM it.

Note

Certificate-based authentication is not currently supported by GTA firewalls, but may be used if you are connecting to another GTA Mobile VPN Client. Consult your network administrator to determine if certificates can be used.

8. Enter IKE settings such as ENCRYPTION, AUTHENTICATION, and KEY GROUP.
9. Click **ADVANCED**.
   Check the **AGGRESSIVE MODE** check box. Add UDP port 500.
   Enter your LOCAL ID; the VALUE will be the email address indicated in your firewall's **Users** configuration, so select the TYPE indicating "email address".
   Enter the REMOTE ID of the firewall; the VALUE should be the external IP address of the firewall, so select the TYPE indicating "IP address".
   Click **OK**.
10. Proceed to configuring Phase II.

Manually Entering Phase I Settings in the GTA Mobile VPN Client

Configuring Phase II (IPSec)

Phase II settings must match your GTA firewall settings.

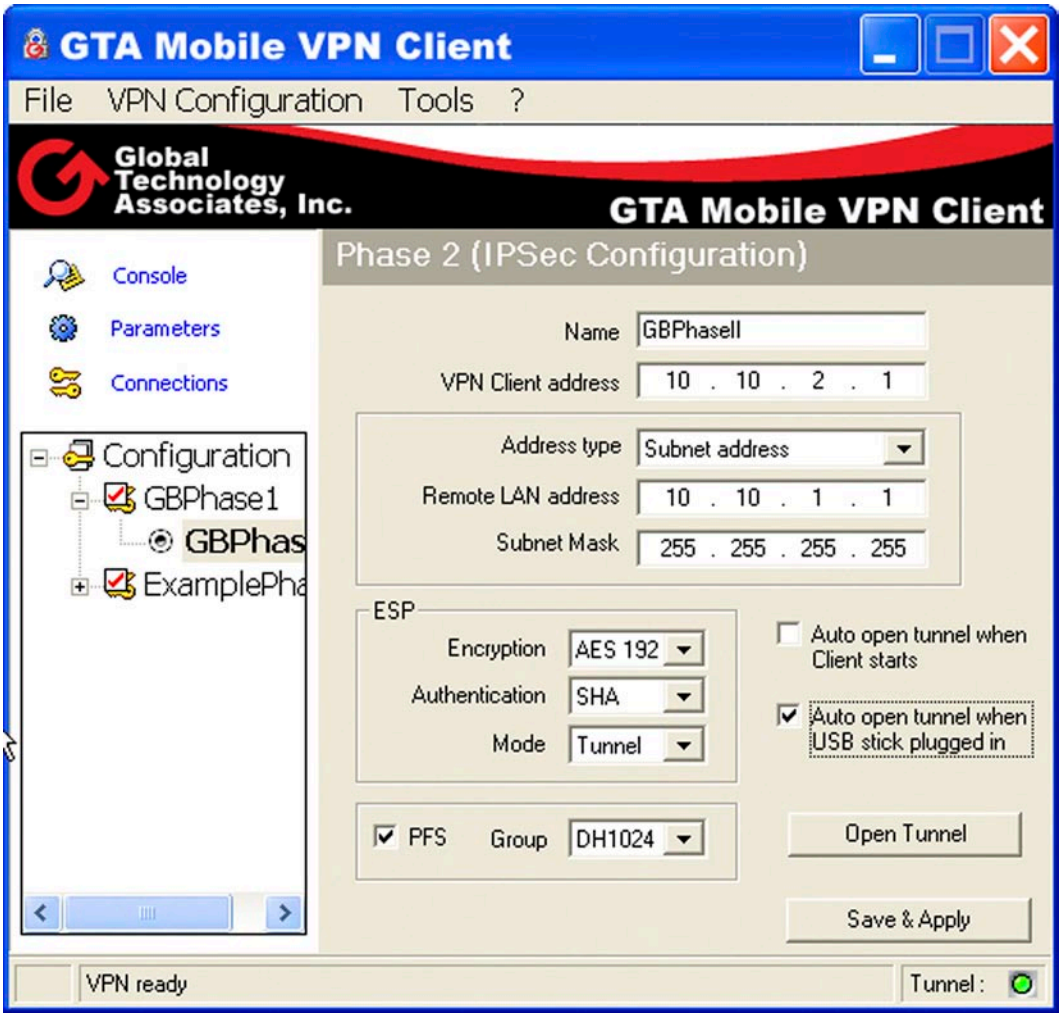
Default settings for Phase II are AES-192 encryption, SHA-1 hashes and Group 2 (1,024-bit) keys.

To enter the Phase I settings of your VPN:

1. Start your VPN client software (or click its item in the system tray to show a configuration window).
2. Right-click on the Phase I configuration you created earlier. Select **Add Phase II**. A new sub-item to the **Configuration** tree will appear, underneath your Phase I configuration; it will have a default name, such as CnxVpn2, that you may change in the NAME field.
3. Enter a new NAME if desired, with no spaces or special characters, e.g. “OfficePhaseII”.
4. Enter the VPN CLIENT ADDRESS, which is the IP address your computer will use when attached to the firewall’s internal network.
5. Select the ADDRESS TYPE. This will be a subnet address if you are connecting to the firewall’s internal network; it will be a single IP address if you are connecting to only one host such as another GTA Mobile VPN Client.
   Enter the REMOTE HOST / LAN ADDRESS. This will be the IP address of the firewall’s internal network with subnet mask if you are connecting to the firewall’s internal network; if you are connecting to only one host, it will be the IP address of that host.
   If you are connecting to the firewall’s internal network, also enter the SUBNET MASK for that network.
6. Enter ESP settings such as ENCRYPTION, AUTHENTICATION and GROUP (Diffie-Hellman key group). Note that these settings may be different than those used in Phase I.
7. Select the tunnel MODE.
8. Check the **PFS** (perfect forward secrecy) check box.
9. If you wish your VPN connection to start automatically upon start of the VPN client software, check the **AUTO OPEN TUNNEL WHEN CLIENT STARTS** check box.
10. Click **SAVE & APPLY**. If you wish to start your VPN connection immediately, click **OPEN TUNNEL**.

Note

Creating a complete VPN configuration does not automatically open that VPN connection. To start or stop a VPN connection, see Starting and Stopping VPN Connections.



Manually Entering Phase II Settings in the GTA Mobile VPN Client

Starting and Stopping VPN Client Connections

Your VPN client software can be configured to automatically start or stop your VPN connection. This can be particularly useful if your primary network traffic must use the VPN, or if you always use the same VPN settings. You can also select to start and stop your VPN connections manually.

For a fully automated VPN solution, you may also elect to automatically start your VPN client software, which can then automatically start or stop your VPN connection. For more information on automatic startup of your VPN client, see Startup Modes.

To manually start and stop your VPN connection:

1. Start your VPN client software (or click its item in the system tray to show a configuration window).
2. Click a Phase II configuration item in the **Configuration** tree. Click **OPEN TUNNEL** to start the VPN connection.
3. Click **CONNECTIONS** to view your open VPN connections.
4. To stop a VPN connection, click the VPN connection and click **CLOSE TUNNEL**.

If you wish to automatically start your VPN connection, there are two choices:

- Connection startup that automatically occurs when the VPN client software starts
- Connection startup that automatically occurs when a USB drive / stick containing the configuration is plugged into your computer, if the VPN client software is already running

As mentioned above, these automatic VPN connection startup methods can be conveniently combined with the automatic startup of the VPN client software itself for fully automated VPN use.

To automatically start your VPN connection:

1. Start your VPN client software (or click its icon in the system tray to show a configuration window).
2. Click a Phase II configuration item in the **Configuration** tree.
3. If you wish your VPN connection to start automatically upon start of the VPN client software, check the **AUTO OPEN TUNNEL WHEN CLIENT STARTS** check box.
4. If you wish your VPN connection to start automatically upon insertion of a USB drive/stick containing a VPN client configuration, check the **AUTO OPEN TUNNEL WHEN USB STICK PLUGGED IN** check box.
5. Click **SAVE & APPLY**.
6. If you are using automatic connection startup that occurs upon insertion of a USB drive/stick, Insert the USB drive/stick. Select **File** then **Export VPN Configuration** from the menu. Choose the location of the USB drive/stick and save the exported configuration there.

Note

If you are using automatic connection startup that occurs upon insertion of a USB drive / stick, you may also choose to automatically stop your VPN connection when you remove the USB drive. For more information, see USB Drive Mode.

Examples

The VPN configuration you choose will vary based upon the answer to two questions:

- Do both initiator and responder have static IP addresses?
- Is key exchange manual or automatic (IKE)?

The following examples show configuration cases for manual vs. IKE key exchange and dynamic vs. static IP addresses.

All listed objects and configurations should be enabled. Any other options, if not listed, may be defined but are not necessary to achieve a functional configuration.

Note

Example configurations contain fictional descriptions, IP addresses and subnet masks used for illustration: internal or private network IP addresses that will be connected to the VPN are listed as the protected network, with IP addresses of 192.168.*.*, for example; in your implementation, however, those settings may contain a different IP addresses, or connect to your PSN rather than your protected network.

To use the following examples, replace IP addresses and subnet masks with your own network settings.

Note

Instead of merely attaching a whole interface (network card) as defined in **Network Information**, these examples attach an address object to the VPN.

Using address objects in your VPN objects allow for more flexible groupings of hosts that should be attached to the VPN: several disparate individual subnetworks or hosts may be defined in an address object, whereas an interface object would require attachment of the entire interface subnetwork, and would not allow simultaneous attachment of PSN hosts.

Note

Depending on the type of your VPN, the firewall may use more than one VPN object to create a connection. Particularly for connections with dynamically-addressed hosts, the firewall will use the dynamic VPN object during Phase I, and then use the **Users**-selected VPN object during Phase II.

Client to Gateway: Dynamic/Static IP Addresses & IKE

The identifying characteristics of this type of VPN include:

- Static external IP address on the firewall, as set in **Network Information**, but dynamic external IP address on the VPN client
- Firewall-compatible settings in the VPN client, and mobile VPN objects selected in **Users** for the statically-addressed firewall

Field Name	***Responder:*** GTA firewall with static IP address
External IP Address	200.200.200.200
In **Objects>Addresses:**	
Name	Protected Networks
Description	DEFAULT: Protected networks
Type	IP Addresses
Object	<USE ADDRESS>
Address	192.168.2.0/24 (hosts that should be attached to your VPN)
In **Objects>VPN Objects:**	
Description	DEFAULT: MOBILE VPNs
Name	MOBILE
Local Gateway	<EXTERNAL>
Local Network	Protected Networks (or the address object for VPN-attached hosts, as defined above)
Force Mobile Protocol	unchecked
Exchange Mode	aggressive
Local Identity	(uses dynamic VPN object)
Encryption Method [Phase I]	(uses dynamic VPN object)
Hash Algorithm [Phase I]	(uses dynamic VPN object)
Key Group [Phase I]	(uses dynamic VPN object)
Lifetime [Phase I]	(uses dynamic VPN object)
DPD	(uses dynamic VPN object)
Encryption Method [Phase II]	AES-192
Hash Algorithm [Phase II]	HMAC-SHA1
Key Group [Phase II]	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase II]	60 (in minutes)
In **Authorization>Users:**	
Name	Example User
Description	Database administrator
Identity	vpnuser@example.com
Method	<Password>
Password	(N/A unless you also set up GBAuth, LDAP or RADIUS authentication)
VPN Object	MOBILE (or the VPN configuration object, as defined above)
Remote Network	<USE ADDRESS> 192.168. 1.1 (the IP address the attached GTA Mobile VPN Client should use)
Pre-shared Secret	$%23Aty! (a long, randomized series of characters that must be identical to the PRESHARED KEY in the GTA Mobile VPN Client)
In **Filters>Remote Access:**	

Field Name	***Responder:*** GTA firewall with static IP address
Description	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<UDP>
Priority	5 - notice
Object [Source Address]	<ANY_IP>
Source Ports	500, 4500
Object [Destination Address]	<EXTERNAL>
Destination Ports	500, 4500
In **Filters>Remote Access:**	
Description	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ESP> (IP protocol 50)
Priority	5 - notice
Object [Source Address]	<ANY_IP>
Source Ports	(may be left blank)
Object [Destination Address]	<EXTERNAL>
Destination Ports	(may be left blank)
In **Pass Through>Filters:**	
Description	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ALL>
Priority	5 - notice
Object [Source Address]	192.168.1.0 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Source Ports	(may be left blank)
Object [Destination Address]	<Protected Networks> (or the address object defined above)
Destination Ports	(may be left blank)
In **Pass Through>Filters:**	
Description	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)

Field Name	***Responder:*** GTA firewall with static IP address
Type	Accept
Interface	<ANY> or <PROTECTED>
Protocol	<ALL>
Priority	5 - notice
Object [Source Address]	<Protected Networks> (or the address object defined above)
Source Ports	(may be left blank)
Object [Destination Address]	192.168.1.0 (the VPN IP address of the GTA Mobile VPN Client)
Destination Ports	(may be left blank)

Field Name	***Initiator:*** GTA Mobile VPN Client with dynamic IP address
External IP Address	dynamically assigned (DHCP, PPPoE, etc.)
In **Parameters**:	
Authentication (IKE) [Default Lifetime]	1800 (seconds)
Authentication (IKE) [Minimal Lifetime]	120 (seconds)
Authentication (IKE) [Maximal Lifetime]	28800 (seconds; must be less than LIFETIME in the GTA firewall's **VPN Objects** PHASE I)
Encryption (IPSec) [Default Lifetime]	1200 (seconds)
Encryption (IPSec) [Minimal Lifetime]	120 (seconds)
Encryption (IPSec) [Maximal Lifetime]	28800 (seconds; must be less than LIFETIME in the GTA firewall's **VPN Objects** PHASE II)
Check Interval [DPD]	30 (dead peer detection in seconds)
In **Configuration**>**Phase I (Authentication)**:	
Name	OfficePhaseI (a descriptor for your VPN; may not contain spaces or non-alpha-numeric characters; changing this value will change its name in the **Configuration** menu tree)
Interface	* (network cards or modems that the VPN will use)
Remote Gateway	200.200.200.200 (the external IP address of the VPN gateway in **Network Information**)
Preshared Key	$%23Aty! (a long, randomized series of characters that must be identical to the PRE-SHARED SECRET in the GTA firewall's **Users**; this password value will be obscured, and only character length will be visible)
Confirm	$%23Aty! (re-enter the PRESHARED KEY to confirm correct entry; this password value will be obscured, and only character length will be visible)
Encryption	3DES (equivalent to the IKE encryption in the GTA firewall's **VPN Objects** PHASE I)
Authentication	SHA (equivalent to the IKE HMAC-SHA1 hash in the GTA firewall's **VPN Objects** PHASE I)
Key Group	DH1024 (equivalent to the IKE group 2 Diffie-Hellman key in the GTA firewall's **VPN Objects** PHASE I)
Aggressive Mode [Advanced]	checked (equivelent to EXCHANGE MODE in the GTA firewall's **VPN Objects** PHASE I)
Value [Advanced Local ID]	vpnuser@example.com (equivalent to the Identity in the GTA firewall's **Users**)
Type [Advanced Local ID]	Email

Field Name	***Initiator:*** GTA Mobile VPN Client with dynamic IP address
Value [Advanced Remote ID]	200.200.200.200 (the external IP address of the VPN gateway in **Network Information**)
Type [Advanced Remote ID]	IP Address
IKE Port [Advanced]	500
In **Configuration**>**Phase II (IPSec Configuration)**:	
Name	OfficePhaseII (a descriptor for your VPN; may not contain spaces or non-alpha-numeric characters; changing this value will change its name in the **Configuration** menu tree)
VPN Client Address	192.168. 1.1 (the IP address the attached GTA Mobile VPN Client should use, listed in the GTA firewall's **Users** Remote Network)
Address Type	Subnet Address (only use the Single Address option if the GTA firewall's attached network will consist of a single host)
Remote LAN Address	192.168.2.0 (the GTA firewall's attached network, such indicated by the protected networks address object)
Subnet Mask	255.255.255.0 (the GTA firewall's subnetwork mask, such indicated by the protected networks address object)
Encryption	3DES (equivalent to the IPSec encryption in the GTA firewall's **VPN Objects** Phase II)
Authentication	SHA (equivalent to the IPSec HMAC-SHA1 hash in the GTA firewall's **VPN Objects** Phase II)
Mode	Tunnel
PFS	checked (perfect forward secrecy is automatically used on GTA firewalls)
Group	DH1024 (equivalent to the IPSec group 2 Diffie-Hellman key in the GTA firewall's **VPN Objects** Phase II)

Client to Gateway: Dynamic IP Addresses & IKE

The identifying characteristics of this type of VPN include:

- Dynamic external IP addresses on ***both*** the GTA firewall, as set in **Network Information**, and the GTA Mobile VPN Client
- Default or edited Mobile **VPN Objects** selected in **Users**
- **Dynamic DNS** service on the GTA firewall must be configured; this enables the GTA Mobile VPN Client to connect through a domain name, without knowing the current IP address of the GTA firewall
- Firewall-compatible settings in the VPN client, and mobile VPN objects selected in **Users** for the statically-addressed firewall

Field Name	***Responder:*** GTA firewall with dynamic IP address
External IP Address	dynamically assigned
In Objects>Addresses:	
Name	Protected Networks
Description	DEFAULT: Protected networks
Type	IP Addresses
Object	<USE ADDRESS>
Address	192.168.2.0/24 (hosts that should be attached to your VPN)
In Services>Dynamic DNS:	
Services	DynDNS or ChangeIP (the dynamic DNS service provider you use)
Login User Name	dyndnsuser (the account's user name for your dynamic DNS service provider)
Login Password	m45GH234Vbbo (the account's password for your dynamic DNS service provider)
Host Name	examplefirewall.dyndns.org (the domain name your GTA Mobile VPN Client will use)
In Objects>VPN Objects:	
Description	DEFAULT: MOBILE VPNs
Name	MOBILE
Local Gateway	<EXTERNAL>
Local Network	Protected Networks (or the address object for VPN-attached hosts, as defined above)
Force Mobile Protocol	unchecked
Exchange Mode	aggressive
Local Identity	(uses dynamic VPN object; edit the default dynamic VPN object to contain a Domain Name type Local Identity such as examplefirewall.dyndns.org)
Encryption Method [Phase I]	(uses dynamic VPN object)
Hash Algorithm [Phase II]	(uses dynamic VPN object)
Key Group [Phase I]	(uses dynamic VPN object)
Lifetime [Phase I]	(uses dynamic VPN object)
DPD	(uses dynamic VPN object)
Encryption Method [Phase II]	AES-192
Hash Algorithm [Phase II]	HMAC-SHA1
Key Group [Phase II]	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase II]	60 (in minutes)
In Authorization>Users:	
Name	Example User
Description	Database administrator
Identity	vpnuser@example.com

Field Name	***Responder:*** GTA firewall with dynamic IP address
Method	<Password>
Password	(N/A unless you also set up GBAuth, LDAP or RADIUS authentication)
VPN Object	MOBILE (or the VPN configuration object, as defined above)
Remote Network	<USE ADDRESS> 192.168. 1.1 (the IP address the attached GTA Mobile VPN Client should use)
Pre-shared Secret	$%23Aty! (a long, randomized series of characters that must be identical to the PRESHARED KEY in the GTA Mobile VPN Client)
In **Filters>Remote Access**:	
Description	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<UDP>
Priority	5 - notice
Object [Source Address]	<ANY_IP>
Source Ports	500, 4500
Object [Destination Address]	<EXTERNAL>
Destination Ports	500, 4500
In **Filters>Remote Access**:	
Description	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ESP> (IP protocol 50)
Priority	5 - notice
Object [Source Address]	<ANY_IP>
Source Ports	(may be left blank)
Object [Destination Address]	<EXTERNAL>
Destination Ports	(may be left blank)
In **Pass Through>Filters**:	
Description	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)
Type	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ALL>

Field Name	***Responder:*** GTA firewall with dynamic IP address
Priority	5 - notice
Object [Source Address]	192.168.1.0 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Source Ports	(may be left blank)
Object [Destination Address]	<Protected Networks> (or the address object defined above)
Destination Ports	(may be left blank)
In **Pass Through>Filters:**	
Description	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)
Type	Accept
Interface	<ANY> or <PROTECTED>
Protocol	<ALL>
Priority	5 - notice
Object [Source Address]	<Protected Networks> (or the address object defined above)
Source Ports	(may be left blank)
Object [Destination Address]	192.168.1.0 (the VPN IP address used by the GTA Mobile VPN Client)
Destination Ports	(may be left blank)

Field Name	***Initiator:*** GTA Mobile VPN Client with dynamic IP address
External IP Address	dynamically assigned (DHCP, PPPoE, etc.)
In **Parameters**:	
Authentication (IKE) [Default Lifetime]	1800 (seconds)
Authentication (IKE) [Minimal Lifetime]	120 (seconds)
Authentication (IKE) [Maximal Lifetime]	28800 (seconds; must be less than LIFETIME in the GTA firewall's **VPN Objects** PHASE I)
Encryption (IPSec) [Default Lifetime]	1200 (seconds)
Encryption (IPSec) [Minimal Lifetime]	120 (seconds)
Encryption (IPSec) [Maximal Lifetime]	28800 (seconds; must be less than LIFETIME in the GTA firewall's **VPN Objects** PHASE II)
Check Interval [DPD]	30 (dead peer detection in seconds)
In **Configuration**>**Phase I (Authentication)**:	
Name	OfficePhaseI (a descriptor for your VPN; may not contain spaces or non-alpha-numeric characters; changing this value will change its name in the **Configuration** menu tree)
Interface	* (network cards or modems that the VPN will use)
Remote Gateway	examplefirewall.dyndns.org (the domain name of the VPN gateway in **Network Information**)
Preshared Key	$%23Aty! (a long, randomized series of characters that must be identical to the PRE-SHARED SECRET in the GTA firewall's **Users**; this password value will be obscured, and only character length will be visible)
Confirm	$%23Aty! (re-enter the PRESHARED KEY to confirm correct entry; this password value will be obscured, and only character length will be visible)
Encryption	3DES (equivalent to the IKE encryption in the GTA firewall's **VPN Objects** PHASE I)
Authentication	SHA (equivalent to the IKE HMAC-SHA1 hash in the GTA firewall's **VPN Objects** PHASE I)
Key Group	DH1024 (equivalent to the IKE group 2 Diffie-Hellman key in the GTA firewall's **VPN Objects** PHASE I)
Aggressive Mode [Advanced]	checked (equivelent to EXCHANGE MODE in the GTA firewall's **VPN Objects** PHASE I)
Value [Advanced Local ID]	vpnuser@example.com (equivalent to the Identity in the GTA firewall's **Users**)
Type [Advanced Local ID]	Email

Field Name	***Initiator:*** GTA Mobile VPN Client with dynamic IP address
Value [Advanced Remote ID]	examplefirewall.dyndns.org (the domain name of the VPN gateway in **Network Information**)
Type [Advanced Remote ID]	DNS
IKE Port [Advanced]	500
In **Configuration**>**Phase II (IPSec Configuration)**:	
Name	OfficePhaseII (a descriptor for your VPN; may not contain spaces or non-alpha-numeric characters; changing this value will change its name in the **Configuration** menu tree)
VPN Client Address	192.168. 1.1 (the IP address the attached GTA Mobile VPN Client should use, listed in the GTA firewall's **Users** Remote Network)
Address Type	Subnet Address (only use the Single Address option if the GTA firewall's attached network will consist of a single host)
Remote LAN Address	192.168.2.0 (the GTA firewall's attached network, such indicated by the protected networks address object)
Subnet Mask	255.255.255.0 (the GTA firewall's subnetwork mask, such indicated by the protected networks address object)
Encryption	3DES (equivalent to the IPSec encryption in the GTA firewall's **VPN Objects** Phase II)
Authentication	SHA (equivalent to the IPSec HMAC-SHA1 hash in the GTA firewall's **VPN Objects** Phase II)
Mode	Tunnel
PFS	checked (perfect forward secrecy is automatically used on GTA firewalls)
Group	DH1024 (equivalent to the IPSec group 2 Diffie-Hellman key in the GTA firewall's **VPN Objects** Phase II)

Gateway to Gateway: Dynamic/Static IP Addresses & IKE

The identifying characteristics of this type of VPN include:

- Static external IP address on ***one*** firewall, but dynamic external IP address on the ***second*** firewall, as set in **Network Information**
- Default or edited IKE objects selected in **VPNs** for the dynamically-addressed firewall, but mobile VPN objects selected in **Users** for the statically-addressed firewall

Field Name	***Initiator:*** GTA firewall with dynamic IP address	***Responder:*** GTA firewall with static IP address
External IP Address	dynamically assigned	200.200.200.200
In **Objects**>**Addresses**:		
Name	Protected Networks	Protected Networks
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	IP Addresses	IP Addresses
Object	<USE ADDRESS>	<USE ADDRESS>
Address	192.168. 1.0/24 (hosts that should be attached to your VPN)	192.168.2.0/24 (hosts that should be attached to your VPN)
In **Objects**>**VPN Objects**:		
Description	DEFAULT: IKE VPNs	DEFAULT: MOBILE VPNs
Name	IKE	MOBILE
Local Gateway	<EXTERNAL>	<EXTERNAL>
Local Network	Protected Networks (or the address object for VPN-attached hosts, as defined above)	Protected Networks (or the address object for VPN-attached hosts, as defined above)
Force Mobile Protocol	checked	unchecked
Exchange Mode	aggressive	aggressive
Local Identity	IP Address	(uses dynamic VPN object)
Encryption Method [Phase I]	AES-192	(uses dynamic VPN object)
Hash Algorithm [Phase II]	HMAC-SHA1	(uses dynamic VPN object)
Key Group [Phase I]	Diffie-Hellman group 2 (1024 bits)	(uses dynamic VPN object)
Lifetime [Phase I]	90 (in minutes)	(uses dynamic VPN object)
DPD	30 (in seconds)	(uses dynamic VPN object)
Encryption Method [Phase II]	AES-192	AES-192
Hash Algorithm [Phase II]	HMAC-SHA1	HMAC-SHA1
Key Group [Phase II]	Diffie-Hellman group 2 (1024 bits)	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase II]	60 (in minutes)	60 (in minutes)
In **Authorization**>**VPNs**:		
IPSec Key Mode	IKE	(no entry in **Authorization**>**VPNs**; equivalent information is entered in **Authorization**>**Users**)
Description	Home-to-office VPN	
Local Identity	firewall1@example.com	
VPN Object	IKE (or the VPN configuration object, as defined above)	
Remote Gateway	200.200.200.200 (the external IP address of the ***other*** VPN gateway)	

Field Name	***Initiator:*** GTA firewall with dynamic IP address	***Responder:*** GTA firewall with static IP address
Remote Network	<USE ADDRESS> 192.168.2.0/24 (the attached hosts on the ***other*** VPN gateway)	
Pre-shared Secret	$%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)	
In **Authorization**>**Users**:		
Name	(no entry in **Authorization**>**Users**; equivalent information is entered in **Authorization**>**VPNs**)	Home Firewall 1
Description		Home-to-office VPN
Identity		firewall2@example.com
Method		<Password>
Password		
VPN Object		MOBILE (or the VPN configuration object, as defined above)
Remote Network		<USE ADDRESS> 192.168. 1.0/24 (the attached hosts on the ***other*** VPN gateway)
Pre-shared Secret		$%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)
In **Filters**>**Remote Access**:		
Description	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<UDP>	<UDP>
Priority	5 - notice	5 - notice
Object [Source Address]	<USE ADDRESS> 200.200.200.200 (the external IP address of the ***other*** VPN gateway)	<ANY_IP>
Source Ports	500, 4500	500, 4500
Object [Destination Address]	<EXTERNAL>	<EXTERNAL>
Destination Ports	500, 4500	500, 4500
In **Filters**>**Remote Access**:		

Field Name	***Initiator:*** GTA firewall with dynamic IP address	***Responder:*** GTA firewall with static IP address
Description	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ESP> (IP protocol 50)	<ESP> (IP protocol 50)
Priority	5 - notice	5 - notice
Object [Source Address]	<USE ADDRESS> 200.200.200.200 (the external IP address of the ***other*** VPN gateway)	<ANY_IP>
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<EXTERNAL>	<EXTERNAL>
Destination Ports	(may be left blank)	(may be left blank)
In **Pass Through>Filters:**		
Description	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Destination Ports	(may be left blank)	(may be left blank)
In **Pass Through>Filters:**		
Description	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***out-bound***.)	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***out-bound***.)
Type	Accept	Accept
Interface	<ANY> or <PROTECTED>	<ANY> or <PROTECTED>

Field Name	***Initiator:*** GTA firewall with dynamic IP address	***Responder:*** GTA firewall with static IP address
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Destination Ports	(may be left blank)	(may be left blank)

Gateway to Gateway: Static/Static IP Addresses & IKE

The identifying characteristics of this type of VPN include:

- Static external IP addresses on ***both*** firewalls, as set in **Network Information**
- Default or edited IKE **VPN Objects** selected in **VPNs**
- Local Identity is not necessary, since static IP addresses serve as a constant element for identity

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
External IP Address	100.100.100.100	200.200.200.200
In **Objects>Addresses:**		
Name	Protected Networks	Protected Networks
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	IP Addresses	IP Addresses
Object	<USE ADDRESS>	<USE ADDRESS>
Address	192.168. 1.0/24 (hosts that should be attached to your VPN)	192.168.2.0/24 (hosts that should be attached to your VPN)
In **Objects>VPN Objects:**		
Description	DEFAULT: IKE VPNs	DEFAULT: IKE VPNs
Name	IKE	IKE
Local Gateway	<EXTERNAL>	<EXTERNAL>
Local Network	Protected Networks (or the address object for VPN-attached hosts, as defined above)	Protected Networks (or the address object for VPN-attached hosts, as defined above)
Force Mobile Protocol	unchecked	unchecked
Exchange Mode	main	main
Local Identity	IP Address	IP Address
Encryption Method [Phase I]	AES-128	AES-128
Hash Algorithm [Phase II]	HMAC-SHA1	HMAC-SHA1
Key Group [Phase I]	Diffie-Hellman group 2 (1024 bits)	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase I]	90 (in minutes)	90 (in minutes)
DPD	30 (in seconds)	30 (in seconds)
Encryption Method [Phase II]	AES-192	AES-192
Hash Algorithm [Phase II]	HMAC-SHA1	HMAC-SHA1
Key Group [Phase II]	Diffie-Hellman group 2 (1024 bits)	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase II]	60 (in minutes)	60 (in minutes)
In **Authorization>VPNs:**		
IPSec Key Mode	IKE	IKE
Description	Office-to-office VPN	Office-to-office VPN
Local Identity	(may be left blank)	(may be left blank)
VPN Object	IKE (or the VPN configuration object, as defined above)	IKE (or the VPN configuration object, as defined above)
Remote Gateway	200.200.200.200 (the external IP address of the ***other*** VPN gateway)	100.100.100.100 (the external IP address of the ***other*** VPN gateway)

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
Remote Network	<USE ADDRESS> 192.168.2.0/24 (the attached hosts on the ***other*** VPN gateway)	<USE ADDRESS> 192.168. 1.0/24 (the attached hosts on the ***other*** VPN gateway)
Pre-shared Secret	$%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)	$%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)
In **Filters**>**Remote Access**:		
Description	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)	Allow firewall to process IKE and NAT-T. (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<UDP>	<UDP>
Priority	5 - notice	5 - notice
Object [Source Address]	<USE ADDRESS> 200.200.200.200 (the external IP address of the ***other*** VPN gateway)	<USE ADDRESS> 100.100.100.100 (the external IP address of the ***other*** VPN gateway)
Source Ports	500, 4500	500, 4500
Object [Destination Address]	<EXTERNAL>	<EXTERNAL>
Destination Ports	500, 4500	500, 4500
In **Filters**>**Remote Access**:		
Description	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)	Allow firewall to process VPN encryption (ESP). (use the default mobile VPN filter as a template, even though there is no mobile VPN client)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ESP> (IP protocol 50)	<ESP> (IP protocol 50)
Priority	5 - notice	5 - notice
Object [Source Address]	<USE ADDRESS> 200.200.200.200 (the external IP address of the ***other*** VPN gateway)	<USE ADDRESS> 100.100.100.100 (the external IP address of the ***other*** VPN gateway)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<EXTERNAL>	<EXTERNAL>
Destination Ports	(may be left blank)	(may be left blank)
In **Pass Through**>**Filters**:		

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
Description	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Destination Ports	(may be left blank)	(may be left blank)
In **Pass Through>Filters:**		
Description	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)
Type	Accept	Accept
Interface	<ANY> or <PROTECTED>	<ANY> or <PROTECTED>
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Destination Ports	(may be left blank)	(may be left blank)

Gateway to Gateway: Static/Static IP Addresses and Manual Key Exchange

The identifying characteristics of this type of VPN include:

- Static external IP addresses on ***both*** firewalls, as set in **Network Information**
- Default or edited manual **VPN Objects** selected in **VPNs**
- ***Only Phase II settings of the manual VPN object are used*** (Phase I may be entered, but it is not used; instead, Phase I from the dynamic VPN object is used)
- Local Identity is not necessary, since static IP addresses serve as a constant element for identity

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
External IP Address	100.100.100.100	200.200.200.200
In **Objects>Addresses:**		
Name	Protected Networks	Protected Networks
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	IP Addresses	IP Addresses
Object	<USE ADDRESS>	<USE ADDRESS>
Address	192.168. 1.0/24 (hosts that should be attached to your VPN)	192.168.2.0/24 (hosts that should be attached to your VPN)
In **Objects>VPN Objects:**		
Description	DEFAULT: MANUAL VPNs	DEFAULT: MANUAL VPNs
Name	MANUAL	MANUAL
Local Gateway	<EXTERNAL>	<EXTERNAL>
Local Network	Protected Networks (or the address object for VPN-attached hosts, as defined above)	Protected Networks (or the address object for VPN-attached hosts, as defined above)
Force Mobile Protocol	unchecked	unchecked
Exchange Mode	main	main
Local Identity	IP Address	IP Address
Encryption Method [Phase II]	AES-192	AES-192
Hash Algorithm [Phase II]	HMAC-SHA1	HMAC-SHA1
Key Group [Phase II]	Diffie-Hellman group 2 (1024 bits)	Diffie-Hellman group 2 (1024 bits)
Lifetime [Phase II]	60 (in minutes)	60 (in minutes)
In **Authorization>VPNs:**		
IPSec Key Mode	Manual	Manual
Description	Office-to-office VPN	Office-to-office VPN
Local Identity		
VPN Object	Manual (or the VPN configuration object, as defined above)	Manual (or the VPN configuration object, as defined above)
Remote Gateway	200.200.200.200 (the external IP address of the ***other*** VPN gateway)	100.100.100.100 (the external IP address of the ***other*** VPN gateway)
Remote Network	<USE ADDRESS> 192.168.2.0/24 (the attached hosts on the ***other*** VPN gateway)	<USE ADDRESS> 192.168. 1.1/24 (the attached hosts on the ***other*** VPN gateway)
Encryption Key	<ASCII> $%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)	<ASCII> $%23Aty! (a long, randomized series of characters that must be identical on ***both*** VPN gateways)
Hash Key	<ASCII> GHij43#e@t (a long, randomized series of characters that must be identical on ***both*** VPN gateways)	<ASCII> GHij43#e@t (a long, randomized series of characters that must be identical on ***both*** VPN gateways)

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
Inbound SPI	256 (an integer, 256 or greater, that must be identical on ***both*** VPN gateways)	256 (an integer, 256 or greater, that must be identical on ***both*** VPN gateways)
Outbound SPI	256 (an integer, 256 or greater, that must be identical on ***both*** VPN gateways)	256 (an integer, 256 or greater, that must be identical on ***both*** VPN gateways)
In **Filters**>**Remote Access**:		
Description	Allow firewall to process VPN encryption (ESP). (use the default ESP VPN filter as a template)	Allow firewall to process VPN encryption (ESP). (use the default ESP VPN filter as a template)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ESP> (IP protocol 50)	<ESP> (IP protocol 50)
Priority	5 - notice	5 - notice
Object [Source Address]	<USE ADDRESS> 200.200.200.200 (the external IP address of the ***other*** VPN gateway)	<USE ADDRESS> 100.100.100.100 (the external IP address of the ***other*** VPN gateway)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<EXTERNAL>	<EXTERNAL>
Destination Ports	(may be left blank)	(may be left blank)
In **Pass Through**>**Filters**:		
Description	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)	Allow VPN traffic to be tunneled inbound. (use DEFAULT: VPN, allow ***inbound***.)
Type	Accept	Accept
Interface	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)	<ANY> or <EXTERNAL> (the network card that will be receiving VPN traffic)
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Destination Ports	(may be left blank)	(may be left blank)

Field Name	***Initiator:*** GTA firewall with static IP address	***Responder:*** GTA firewall with static IP address
In **Pass Through**>**Filters**:		
Description	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)	Allow VPN traffic to be tunneled outbound. (use DEFAULT: VPN, allow ***outbound***.)
Type	Accept	Accept
Interface	<ANY> or <PROTECTED>	<ANY> or <PROTECTED>
Protocol	<ALL>	<ALL>
Priority	5 - notice	5 - notice
Object [Source Address]	<Protected Networks> (or the address object defined above)	<Protected Networks> (or the address object defined above)
Source Ports	(may be left blank)	(may be left blank)
Object [Destination Address]	192.168.2.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)	192.168.1.0/24 (the internal IP address of hosts attached to the ***other*** VPN gateway)
Destination Ports	(may be left blank)	(may be left blank)

Advanced Mobile Client Setup

The new GTA Mobile VPN Client has several new features to enable use on servers, desktop computers or laptop computers.

Hidden Mode

The VPN client software can be configured to run as a service that cannot be user-modified.

When “hidden”, the VPN client software will still have an icon visible in the system tray; however, clicking the icon will not show a configuration window.

A special tool called VpnHide.exe must be used to set the visibility.

To hide/unhide the VPN client software:

1. Download VpnHide.exe from http://www.thegreenbow.fr/bin/VpnHide.exe.
2. Start VpnHide.exe.
3. Click **VISIBLE** or **INVISIBLE**.
4. Click **OK**.

USB Drive Mode

The VPN client software can be configured to open and close your VPN connection when a USB drive containing the VPN configuration is inserted or removed.

To use the USB-activated VPN connection handling:

1. Insert the USB drive (also sometimes called a pen drive or USB stick).
2. Start the VPN client software.
3. Select **File** then **Configuration Mode** from the menu.
4. Click **USB STICK (PLUG-IN AUTOMATIC DETECTION)**.
5. Enter the location of the USB drive, or click the ... button to browse to its location.
6. Click **OK**.
7. Configure your VPN as usual, or copy / export your current VPN configuration onto the USB drive.
8. To start your VPN connection, plug in your USB drive. To stop the connection, eject / remove the USB drive. (Your VPN client software must remain running to automatically start and stop your VPN.)

The VPN client software can be returned at any time to normal operation by clicking **LOCAL (LOCAL DRIVE, CLASSIC MODE)** in **Configuration Mode**.

Startup Modes

The VPN client software can be configured to start a VPN connection upon boot, login, or manually.

These different startup modes can provide the VPN connection upon boot (e.g. when a service on your server requires a VPN), or upon login (e.g. when VPN connection is part of your enforced usage policy).

A special tool called VpnStart.exe must be used to set the startup mode.

To set the startup mode of the VPN client software:

1. Download VpnStart.exe from http://thegreenbow.fr/bin/VpnStart.exe.
2. Start VpnStart.exe.
3. Select a start mode.
   Click **BOOT** to start a VPN connection upon boot, as if the VPN were a service.
   Click **LOGIN** to start a VPN connection upon user login.
   Click **MANUAL** to start a VPN connection using the normal manual start mode for the software.
4. Click **OK**.

Console and Configuration Tools

Configuration Management

The mobile VPN client software allows configurations to be imported and exported.

Importing and exporting configurations facilitates configuration deployment and troubleshooting. Administrators may configure a VPN settings on their computer and then send that configuration to the VPN user. VPN users can also export their configurations for troubleshooting by the network administrator.

Exported VPN client configurations may be opened and edited in a plain text processor such as Notepad. Corrected VPN configurations can also be imported.

To export / import a VPN configuration:

1. Start the VPN client software.
2. Select **File** then **Import VPN Configuration** or **Export VPN Configuration**.
3. Select a location for the file. A VPN client configuration file will have the ".tgb" file extension.
4. Click **OPEN** or **SAVE**.

Console / Logs

The VPN client software maintains a console which allows you to view current VPN activity. This activity may contain useful debugging information by providing feedback messages and component status.

Optionally, you can save the output of the console to a log file for viewing in a text editor such as Notepad.

To view the console/log:

1. Start the VPN client software.
2. Select **Tools** then **Console** from the menu.
3. If the console has been stopped, click **START** to begin logging.
4. To save the log to a text file, click **SAVE FILE**.

The console messages / log can be filtered in the console. A series of pull-down menus at the bottom of the VPN console window cause less or more log information to be displayed. The default information (level 0 for each setting) is usually sufficient for debugging purposes.

Label	*Name*	*Description*
Misc	Miscellaneous	The degree of logging detail for low-level messages.
Trpt	Transport	The degree of logging detail for UDP transport mode.
Msg	Message	The degree of logging detail for IKE decoding.
Cryp	Crypto	The degree of logging detail for cryptographic exchanges.
Timr	Timer	The degree of logging detail for timers.
Sdep	Sysdep	The degree of logging detail for IKE interfaces with IPSec
SA	Security Associations	The degree of logging detail for SA management.
Exch	Exchange	The degree of logging detail for IKE exchanges.
Nego	Negotiation	The degree of logging detail for Phase I and Phase II negotiation.
Plcy	Policy	Not used.
All	All	The degree of logging detail for all subsystems.

Troubleshooting

On the GTA Firewall

FAQ

1. Mobile VPN clients cannot connect to the firewall.

First use ping and / or traceroute to verify that VPN client connections can reach the firewall without use of the VPN. Then check that you have correctly configured the required remote access and passthrough filters. Finally, check that all mobile VPN clients have accounts with VPN configuration set up in **Users**, referencing a valid VPN configuration object in **VPN Objects**.

Log Messages

GTA firewalls log common problems such as denied VPN connections.

VPN connections tunnel network traffic over untrusted networks using authentication and encryption for security. If an IKE type of VPN is used, IKE messages may appear in the log ("`IKE server`"); another key identifier is "`type=mgmt, vpn`".

When the IKE service starts up due to firewall reboot or saving a VPN configuration section, the startup is logged, along with the number of allowed concurrent mobile users.

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall"
pri=5 msg="WWWadmin: Starting IKE server." type=mgmt src=192.168.71.2 srcport=2206
dst=192.168.71.254 dstport=80 duration=2
```

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2002-08-30 14:12:18" fw="ipsec" pri=5
msg="Licensed for 100 mobile client connections. type=mgmt,vpn
```

Failed VPN authentications are logged with the account name.

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall"
pri=5 msg="RMCauth: Accepted connection" type=mgmt src=199.120.225.78 srcport=2197
dst=199.120.225.200 dstport=76
```

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall" pri=4
msg="RMCauth: Authentication failure for 'support@gta.com'." type=mgmt src=199.120.225.78
srcport=2197 dst=199.120.225.200 dstport=76 duration=4
```

Security Associations

By default, each IPSec security association (SA) creation is logged. Most VPN connections require two SAs.

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall" pri=5
msg="IPsec-SA established type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall" pri=5
msg="IPsec-SA established type=mgmt,vpn src=24.170.164.183 dst=199.120.225.200
```

Security associations may expire. After expiration, they must be renewed or the connection will be closed.

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="ipsec" pri=5
msg="IPsec-SA established type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="ipsec" pri=5
msg="IPsec-SA expired type=mgmt,vpn src=199.120.225.200 dst=24.170.164.183
```

Mobile Client VPN Authentication and Connection

Mobile clients must authenticate first before establishing a connection.

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall"
pri=5 msg="RMCauth: Accepted connection" type=mgmt src=199.120.225.78 srcport=2170
dst=199.120.225.200 dstport=76
```

```
Mar 4 21:06:44 firewall.example.com id=firewall time="2005-03-04 21:06:44" fw="firewall" pri=6
msg="RMCauth: Authentication successful for 'support@gta.com'." type=mgmt src=199.120.225.78
srcport=2170 dst=199.120.225.200 dstport=76 duration=4
```

Attempts to connect without authentication will be denied.

```
Mar 4 21:06:44 pri=4 msg="Authentication needed, access for 'support@gta.com' denied."
type=mgmt,vpn src=65.33.234.134 dst=199.120.225.78
```

If the user is already authenticated from one IP address and they attempt to authenticate from a second IP address, the connection will be denied. The user's VPN lease must expire before login will be permitted.

```
Mar 4 21:06:44 pri=4 msg="Unable to aquire license, access for 'user@example.com' denied."
type=mgmt,vpn src=200.200.200.200 dst=100.100.100.100
```

On the GTA Mobile VPN Client

FAQ

1. My mobile VPN client software says it is in a 30-day evaluation mode.

If the VPN client serial number was not correctly entered during installation, or if you clicked **TRIAL** during installation instead of entering a serial number, the VPN client software will function for 30 days in an evaluation mode.

Enter the VPN client serial number you received with your mobile VPN option purchase for the VPN client software to exit evaluation mode.

2. My Internet connection does not work when I return to the office.

Your VPN connection may still be active, even though it is not necessary while inside your office LAN. Stop the VPN connection. You might also need to restart your browser or other network application before you can use the non-VPN connection on your office LAN.

3. The GTA Mobile VPN Client will not start a VPN on Windows XP.

Windows XP has a feature called fast user switching. This means that multiple users may be logged in and running programs at the same time (including VPN software), even when only one user is actively using the mouse and keyboard.

If another user is logged in to Windows XP and has started a VPN connection, you will not be able to start a VPN; the other user is already using those VPN resources.

To start your VPN, first ask the other user to log in and stop their VPN connection. Then you may log in to your own account and start your own VPN.

Log Messages

Incorrect Remote Gateway

An incorrect value was used for the external IP address of the GTA firewall (VPN gateway). This should match the remote gateway in the GTA firewall's mobile **VPN Objects**.

```
103901 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]
```

```
103906 Default ipsec _ get _ keystate: no keystate in ISAKMP SA 00D9CBC8
```

Incorrect Pre-shared Key

An incorrect value was used for the pre-shared secret (key). This value must match the pre-shared secret specified for the account in the GTA firewall's **Users**.

```
101901 Default message _ recv: invalid cookie(s) 303a3fce1772c7b7 8505c95b1034c3c6
```

```
101901 Default dropped message from 199.120.225.117 due to notification type INVALID _ COOKIE
```

```
101901 Default SEND Informational [NOTIFY] with INVALID _ COOKIE error
```

Incorrect Local ID Value

An incorrect value for the local identity of the VPN client was used. In most cases, this should be the email address specified for the account in the GTA firewall's **Users**.

```
101202 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]
```

Incorrect Local ID Type

An incorrect type for the local identity of the VPN client was used. In most cases, the type should be **Email**.

```
100731 Default ike _ phase _ 1 _ send _ ID: invalid ip address: Bad file descriptor WSA(11001)
```

```
100731 Default exchange _ run: doi->initiator (00D95C58) failed
```

Incorrect Remote ID Value

An incorrect value for the remote identity of the GTA firewall was used. In most cases, this should be the IP address specified in the GTA firewall's mobile **VPN Objects**.

```
101325 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

101325 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]

101325 Default ike _ phase _ 1 _ recv _ ID: received remote ID other than expected
200.200.200.200
```

Incorrect Remote ID Type

An incorrect type for the remote identity of the GTA firewall was used. In most cases, the type should be **IP Address**.

```
101447 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

101447 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]

101448 Default ike _ phase _ 1 _ recv _ ID: received remote ID other than expected
199.120.225.117

101455 Default ipsec _ get _ keystate: no keystate in ISAKMP SA 00F7BD40
```

Incorrect Phase I Settings

An incorrect Phase I (IKE) setting was used. These settings should match the GTA firewall's dynamic **VPN Objects** PHASE I settings.

```
104041 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

104041 Default transport _ send _ messages: giving up on message 00DAF350

104041 Default recvfrom (164, 0011FD70, 65536, 0, 0011FCEC, 0011FCE8): WSA(10054)
```

Incorrect Phase II Settings

An incorrect encryption, authentication or key group was used in Phase II settings. These settings should match the GTA firewall's mobile **VPN Objects** PHASE II settings.

```
104401 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

104401 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]

104402 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [HASH] [NAT _ D] [NAT _ D]

104402 Default phase 1 done: initiator id vpnuser@example.com, responder id 200.200.200.200

104402 Default (SA VPN-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY _ EXCH] [NONCE]
[ID] [ID] [NAT _ OA]

104402 Default RECV Informational [HASH] [NOTIFY]

104402 Default RECV Informational [HASH] [NOTIFY] with NO _ PROPOSAL _ CHOSEN error
```

Incorrect Phase II Authentication Settings

An incorrect value was used for Phase II authentication (hash) settings. This value should match the GTA firewall's mobile **VPN Objects** PHASE II settings.

```
105935 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

105935 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]
```

```
105935 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [HASH] [NAT _ D] [NAT _ D]

105935 Default phase 1 done: initiator id support-GB2@gta.com, responder id 199.120.225.117

105935 Default (SA VPN-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY _ EXCH] [NONCE]
[ID] [ID] [NAT _ OA]

105935 Default RECV Informational [HASH] [NOTIFY] with NO _ PROPOSAL _ CHOSEN error
```

Incorrect Phase II Key Group Settings

An incorrect value was used for Phase II key group (Diffie-Hellman) settings. This value should match the GTA firewall's mobile **VPN Objects** PHASE II settings.

```
110213 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [SA] [KEY _ EXCH] [NONCE] [ID] [VID]
[VID] [VID] [VID]

110213 Default (SA VPN-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY _ EXCH] [NONCE] [ID]
[NAT _ D] [NAT _ D] [VID] [VID]

110213 Default (SA VPN-P1) SEND phase 1 Aggressive Mode [HASH] [NAT _ D] [NAT _ D]

110213 Default phase 1 done: initiator id support-GB2@gta.com, responder id 199.120.225.117

110213 Default (SA VPN-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY _ EXCH] [NONCE]
[ID] [ID] [NAT _ OA]

110213 Default RECV Informational [HASH] [NOTIFY] with NO _ PROPOSAL _ CHOSEN error
```

Elements of IPSec VPN Security

IPSec, a secure network connection standard (RFC 2401) designed by IETF (Internet Engineering Task Force), provides two implementations: transport mode and tunnel mode. The tunnel mode implementation applies to VPN gateways, such as GTA firewall VPNs.

GTA firewall VPNs provide:

- Authorization
- Data integrity
- Data privacy

GB-OS IPSec tunnels (VPNs) cause the original IP packet to be:

1. Encrypted to hide contents from interceptors
2. Hashed to resist tampering
3. Authorized with keys and/or authentication to validate transmission according to your security policies
4. Encapsulated within another IP packet to provide routing for the “sealed” original packet

GTA firewall VPN is essentially a tunnel and a security processing service for your IP traffic, both tunneling and securing packet contents. All GTA firewall VPN-secured traffic receives encapsulation by a secondary IP packet layer after it is secured.

Because this security and encapsulation is agnostic to the contents, all IP protocols can be secured with GTA firewall VPN, including TCP (and its higher-level protocols like HTTP or SSH), UDP, ICMP and others.

Caution

Varying degrees of data integrity and confidentiality are provided by the hashes, keys and encryption algorithms you elect to use. GTA recommends that you carefully select each one based upon the strength and performance needs of your VPN.

IPSec’s security benefits arise from the secure creation of authorized, encrypted connections. IPSec connections utilize some auxiliary TCP and UDP connections to negotiate a secure connection before actual transmission of user data occurs.

During the creation of an IPSec VPN connection:

1. Hosts (including clients or gateways) exchange keys.
2. Hash and encryption methods are negotiated with identities being assured by the keys from step 1.
3. Security associations (SAs) are created on each host to contain the agreed security transformations and associated keys for each VPN destination from step 2.
4. Data transmission receives the protection designated by the established rules of the SAs from step 3 until they expire or are deleted.

Automatic IPSec key exchange and IPSec SA initialization is provided using the IKE standard (RFC 2407 and RFC 2409). (Manual key exchange is supported, but not recommended because of the security risks inherent in overexposed keys.)

IPSec VPNs on GTA firewalls require the use of AH and ESP protocols (IP protocols 51 and 50). Key exchange and other IKE negotiations may also require the use of UDP port 500. If ESP traffic is blocked, GTA firewall VPNs will use NAT traversal (RFC 3947 and RFC 3948) to tunnel ESP traffic using UDP port 4500.

For more information on the IP packet transformations that occur during a GTA firewall VPN connection, see TCP/IP Packets: IPSec VPN Packet Structure. For more information on IPSec packet processing specific to GTA firewalls, see GTA firewall VPN Packet Processing. For more information on the IETF standards applying to IPSec or IKE, see the applicable RFCs: RFC 2401 (IPSec), RFC 2409 (IKE), RFC 2407 (IKE's role in IPSec), RFC 2402 (AH) and RFC 2406 (ESP).

Verifying Authorization

Verifying identity through authentication is an important step of secure computing. Identity allows policies to be applied based on the trustworthiness and relevance of the data source. For example, an incoming connection may have both privacy and tamper-proofness (data integrity), but unless you know the sender and authorize their activities, you don't truly know what data you are allowing onto your network.

IPSec VPN can provide authorization during the Phase I (IKE) part of VPN initialization. ***The GTA firewall implementation of IPSec VPN requires authorization; VPN will not activate without an authorization that references a VPN configuration object.***

The source of the authorization can be provided in two separate ares of GTA firewall configuration. For gateway-to-gateway GTA firewall VPNs, the identity is checked by **VPNs**; for mobile client GTA firewall VPNs, identity is checked by **Users**.

Verifying Data Integrity

Verifying data integrity (tamper-proofing) is also an important part of secure computing. Integrity assures that the data has not been tampered with to introduce unwanted data, including trojans and viruses. For example, you may intend to accept the sender and content of a packet, but unless you can assure that a third party has not altered it, you don't truly know what data you are allowing onto your network.

Data integrity is ensured during both Phase I and Phase II of IPSec VPN creation by keys and hashes. Separate keys and hashes may be selected for either phase. Key and hash preferences for a GTA firewall VPN connection are configured in **VPN Objects**.

Note

Keys uniquely identify the host establishing the connection; hashes are computed using the data and the key, and therefore a hash of a packet's data is only verifiable by a destination who knows the secret of the sender's original key.

The selection of a key and a hash method is generally a balance between performance, technical requirements, and strength. Larger keys are generally considered better, but come at the price of performance, for example. GTA firewalls provides reasonable defaults for many VPNs, but you may wish to select a greater key length or a different hash algorithm to suit your needs.

Ensuring Data Privacy

Ensuring data privacy is usually (but not always) a part of secure computing. Privacy allows sensitive data to be hidden from unauthorized parties. For example, you may trust the source and integrity of data, but don't want others to be able to read it while in transit to your network. Common reasons for data privacy include the transmission of financial and personal data.

Privacy is ensured during both Phase I and Phase II of VPN creation by encryption algorithms. Separate encryption methods may be selected for either phase.

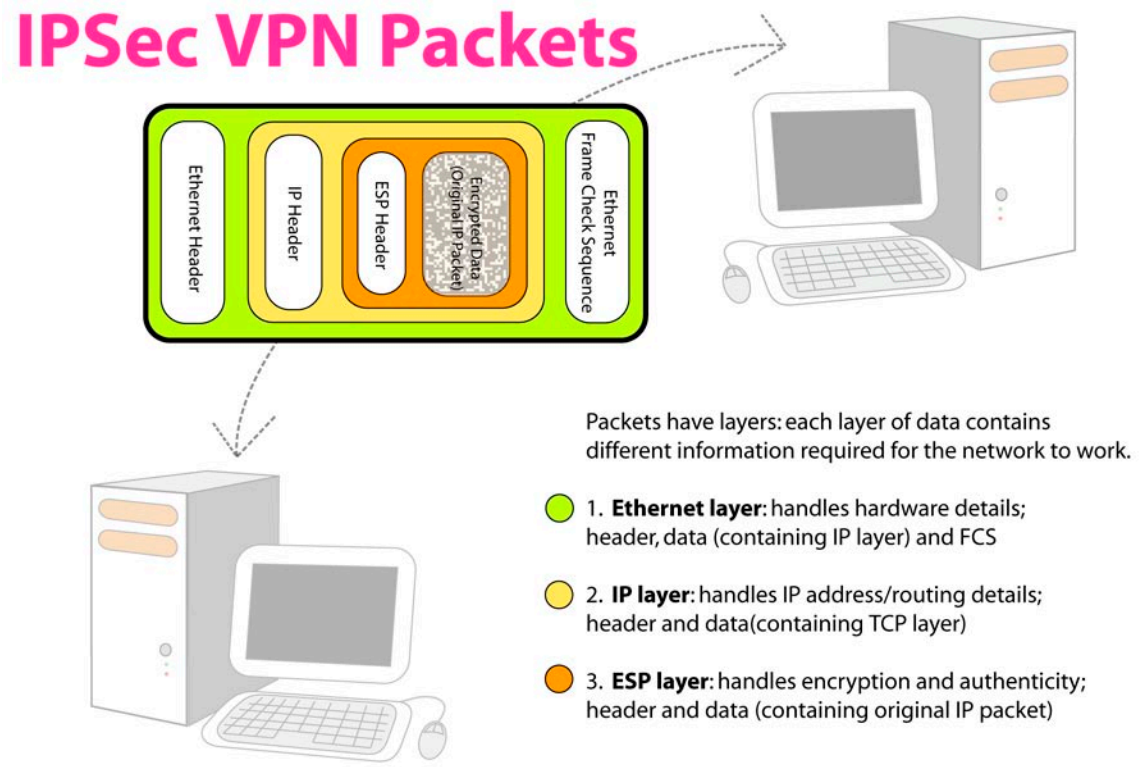
IPSec VPN provides data privacy with encryption. Encryption methods for a GTA firewall VPN connection are configured in **VPN Objects**.

Packet Structure: IPSec VPN

IPSec VPN uses encrypted, encapsulated IP packets to transfer data.

The original IP packet contents are prevented from interception and tampering by application of the ESP protocol, which applies selected encryption, hashes and authenticity checks to contents. The resulting packet is then re-wrapped in an external IP packet layer.

Only hosts containing matching IPSec information (SAs and keys) are able to decrypt the ESP-encapsulated contents.



GTA Firewall VPN Packet Processing

When a packet arrives at a GTA firewall, many evaluation sequences are performed to determine structure correctness and permissibility before a route is created to deliver the packet. These checks, plus some special additional transformations, are performed on all GTA firewall VPN packets.

Failing a check causes the packet to be denied and, by default, logged.

The generalized packet processing sequence of VPN packets includes:

1. Check for valid IP packet structure.
2. Check for spoofed packets and other network attacks.
3. Check for filters allowing, denying or transforming packet transmission (such as traffic shaping rules). For IPSec VPN packets, checks occur for a valid existing IPSec VPN SA as well as an outbound or remote access filter.
4. Check for routing instructions delivering the packet to its indicated destination. For IPSec VPN packets, checks occur for a passthrough filter.

IPSec initialization packets (packets for IKE and IPSec SA setup) are not subjected to the routing check, as the firewall is their destination; however, these initialization packets do require firewall access permission from remote access filters. Then checks are performed for authorization and VPN configuration data to create the IKE and IPSec SAs required by all further IPSec VPN packets.

Index

W

Technical Support

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's web site for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized channel partner.

Tel: +1.407.380.0220 Email: support@gta.com

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