

GB-OS[®]

VPN Option Guide for Site-to-Site VPNs

VPNOG201003-01



**Global
Technology
Associates, Inc.**

Global Technology Associates
3505 Lake Lynda Drive Suite 109
Orlando, FL 32817

Tel: +1.407.380.0220
Fax: +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table of Contents

Introduction	1
What is a VPN?	1
About IPSec VPN on GTA Firewalls	2
The VPN Gateway (Firewall) Component	2
VPN Gateway Features	2
Installation Support	3
Support Options	3
Documentation	3
Icons	3
Additional Documentation	3
GTA Firewall UTM Appliance Setup	4
Entering Feature Codes	4
Running the IPSec Setup Wizard	5
IPSec Setup for Firewall to Firewall	6
Configuring an IPSec VPN Connection Manually	8
Authentication	8
Creating IPSec Configuration Objects	8
Which IPSec Object Should I Use?	8
Selecting the IPSec Key Mode	8
Creating a VPN Using IKE IPSec Key Mode	9
Creating a VPN Using Manual IPSec Key Mode	11
Encryption Key Length	12
Hash Key Length	12
Security Parameter Index (SPI)	12
Configuring a Custom IPSec Object	13
About Phase I	14
About Phase II	14
Configuring a Custom Encryption Object	15
Encryption Methods	15
Hash Algorithm	16
Key Group	16
Configuring VPN Policies	17
Creating Authorization	17
Creating Groups	17
Creating Users	18
Using VPN Certificates	19
How VPN Certificates Work	19
Firewall to Firewall VPNs	19
Mobile Client to Firewall VPNs	19
Generating VPN Certificates	20
Setting the Remote Administration Certificate	21
Exporting the Remote Administration VPN Certificate	21
Importing VPN Certificates	22
Reference A: VPN Concepts	23
Elements of IPSec VPN Security	23
Verifying Authorization	24
Verifying Data Integrity	24
Ensuring Data Privacy	24
Packet Structure: IPSec VPN	25
GTA Firewall VPN Packet Processing	25
Reference B: Example VPN Configurations	26
Example: Using IKE IPSec Mode and Pre-shared Secrets	26
Gateway to Gateway: Static/Static IP Addresses	26
Example VPN Configurations Using IKE IPSec Mode and VPN Certificates	28
Gateway to Gateway	28
Example VPN Configurations Using Manual IPSec Mode	30
Gateway to Gateway: Static/Static IP Addresses and Manual Key Exchange	30
Reference C: Log Messages	32



Introduction

What is a VPN?

A VPN is a Virtual Private 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.
- **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.

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

VPNs provide more secure access than standard NAT tunnels. VPN tunnels provide methods to assure authorization, data integrity and 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 and IP packet encapsulation to ensure the identity, integrity, and privacy of your data transfers over public, untrusted networks.

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) IPSec VPN connections.

GTA firewall IPSec VPNs are a security gateway version of the IPSec standard; the GTA Mobile IPSec VPN Client provides the host version.

The VPN Gateway (Firewall) Component

GTA Firewall UTM Appliances 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 **Configure>VPN>Site-to-Site**, and bound to an incoming authorization channel in either **Configure>Accounts>Users** and **Configure>Accounts>Groups** (for Mobile IPSec VPN Clients or a second VPN gateway with a dynamic IP address) or **Configure>VPN>Site-to-Site** (where both VPN gateways have a static IP address).

GTA firewalls can interoperate with either another GTA Firewall UTM Appliance (for office-to-office VPNs) or a Mobile IPSec 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/>).

VPN Gateway Features

- NAT traversal
- Easy application of security policies
- Easy creation and revision of IPSec VPNs using IPSec configuration objects
- Quickly enable and disable VPN authorizations
- AES-128, AES-192 and AES-256, 3DES, DES, Blowfish and Camellia 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
- Authentication using either VPN certificates or pre-shared secrets



Installation Support

Installation (“up and running”) support is available to registered users. See GTA’s Website for more information. If you need installation assistance, be sure to register your product and then contact the GTA Technical Support team by email at support@gta.com. Please include your serial number and a brief description of the problem in the body of the email.

Support Options

If you need support for GTA Products, a variety of support contracts are available. Contact GTA Sales staff by email at sales@gta.com for more information. Contracts range from support by the incident to full coverage for a year. Other assistance is available through the GB-Users Mailing List, GTA Firewall User Forum, or an authorized GTA Channel Partner.

Documentation

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

<i>Bold Italics</i>	Emphasis
<i>Italics</i>	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

Icons



Note

Note icons are points of interest GTA has chosen to highlight. These notes represent tips or additional information beyond standard instruction.



CAUTION

Caution icons are used to highlight important information which may affect the use of GTA products.

Additional Documentation

For instructions on installation, registration and setup of a GTA Firewall, see the *GB-OS User’s Guide*. For optional features, see the appropriate Feature Guide. Manuals and other documentation can be found on the GTA Website (www.gta.com).

Documents on the Website are either in plain text (*.txt) or Portable Document Format (*.pdf), which requires Adobe Acrobat Reader. A free copy of the program can be obtained from Adobe at www.adobe.com.

GTA Firewall UTM Appliance Setup

This chapter explains configuration steps for an IPSec Virtual Private Network (VPN) on the GTA Firewall UTM Appliance. It also provides a worksheet to help with initial configuration.

Each GTA firewall VPN requires two points: an initiator and a responder. The responder must be a GTA firewall, while the initiator can be either a second VPN gateway or a GTA Mobile IPSec VPN Client.

GTA firewall IPSec Setup requires configuration of both:

- A GTA firewall
- A GTA Mobile IPSec VPN Client or a second VPN gateway (such as another GTA Firewall UTM Appliance)

Feature activation codes are required to be entered into the GTA firewall if optional VPN features have been purchased, before using the IPSec Wizard or if the VPN connection is defined manually.

Entering Feature Codes

When a VPN option or GTA Mobile IPSec VPN Client license package has been purchased, feature activation codes are required for client-to-gateway VPNs. If you have purchased a Mobile IPSec VPN Client license package, navigate to **Configure>System>Activation Codes** to enter its feature activation code. Click **SAVE**.

The feature activation code can be retrieved from the GTA Support Center (<https://www.gta.com/support/center/>). Once logged in, click on **View Your Registered Products** and select your firewall's serial number. Your feature activation code will be displayed.

If a gateway-to-gateway VPN is not a standard feature for your GTA Firewall UTM Appliance, and you have purchased a VPN option, 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.



Running the IPSec Setup Wizard

The IPSec Setup Wizard is designed to help configure a simple Virtual Private Network (VPN). The wizard will automatically create security policies to accept connections using ESP (protocol 50) and UDP (ports 500 and 4500) protocols.

**Note**

All connections through the VPN are controlled by VPN policies, located at **Configure>Security Policies>Policy Editor>IPSec**.

To run the IPSec Wizard, navigate to **Wizards>IPSec Setup**. Before running the wizard, it may be helpful to print out and fill in the following worksheet:

Table 2.1: IPSec Wizard Worksheet		
Field	Description	Value
VPN		
Description	Enter a brief description of the VPN.	
Remote Type	Select the type of VPN being defined.	Firewall; Mobile Client
Local Network		
Gateway	Select the logical interface that acts as the gateway to the local network. Typically, this will be the external interface.	
Network	Select the address object of the configured network you wish to be able to connect to using the VPN. Select <USER DEFINED> to enter the local network's IP address manually.	...
Remote Network		
Gateway	Select <USER DEFINED> to enter the local network's IP address or FQDN if the remote firewall has a dynamic IP.	...
User Name	The user name that will be used to identify the remote network. This field is only required if the gateway is using a dynamic IP address or if setting up a Mobile Client. Enter an IP address, email address, or valid DNS resolvable host name.	
Identity	The identity for the remote network. Enter an IP address, email address, or valid DNS resolvable host name.	
Group	The user group that will be connecting to the remote network.	
Network	The destination IP address of that network that resides behind the remote firewall. Select <USER DEFINED> to enter the IP address manually.	...
Pre-shared Secret		
Pre-shared Secret Format	The format of the pre-shared secret to be used by the VPN.	ASCII Hex
Pre-shared Secret	The pre-shared secret to be used by the VPN. This same secret needs to be entered in the GTA Mobile IPSec VPN Client when configuring the security policy. This field is case sensitive.	

To run the IPsec Setup Wizard, navigate to **Wizards>IPsec Setup**.

1. The first screen of the wizard will prompt you to enter a brief description of the nature of the VPN. For example, *Orlando to New York*.
2. Select the Remote Type from the dropdown menu. Options include **Firewall** and **Mobile Client**.
3. Click the **NEXT ARROW** to continue.

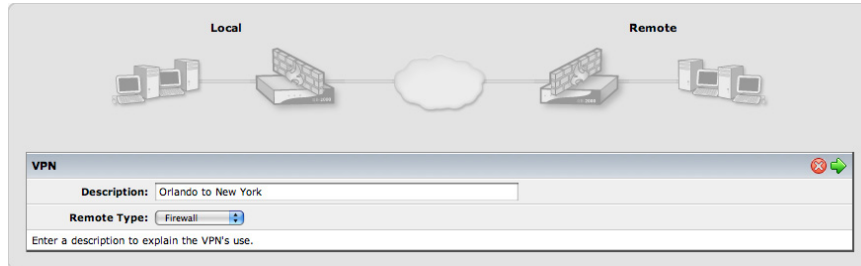


Figure 2.1: Entering the VPN's Description

Follow the instructions below according to the VPN Remote Type selected above:

- IPsec Setup for [Firewall to Firewall](#)
- IPsec Setup for a [Mobile Client](#)

IPsec Setup for Firewall to Firewall

1. If the REMOTE TYPE is a firewall, it will then be necessary to define the Local Network that will be establishing the VPN.
 - a. For the local network's Gateway, select the logical interface assigned to the external network. In most cases, this will be **<EXTERNAL>**.
 - b. For the NETWORK, select the local network that will be accessible via the VPN. If the desired local network is not listed, you may define it manually by selecting **<USER DEFINED>** and entering the network's IP address in the corresponding field.
 - c. Click the **NEXT ARROW** to continue.

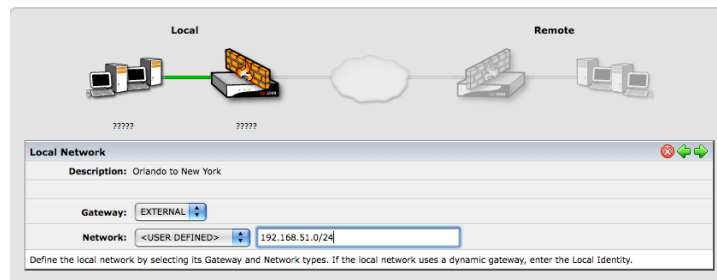


Figure 2.2: Defining the Local Network (Static Gateway)



Note

On High Availability systems, the local gateway should be HA - <Interface Name>.

2. On the next screen, define the Remote Network.
 - a. Enter the remote network's Gateway. Select **<USER DEFINED>** to enter the IP address or FQDN manually.
 - b. For the NETWORK, select the address object for the remote network. To enter the remote network manually, select **<USER DEFINED>** and enter the network's IP address in the corresponding field.
 - c. Click the **NEXT ARROW** to continue.

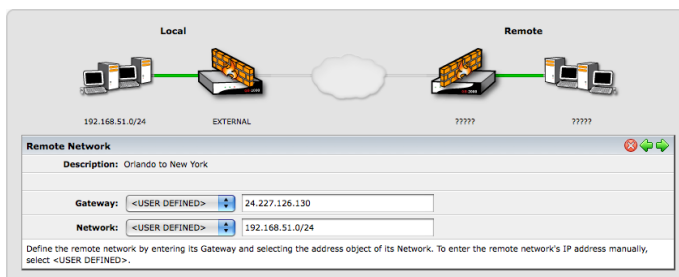


Figure 2.3: Defining the Remote Network (Static Gateway)

3. Next, enter a pre-shared secret. A pre-shared secret is used to ensure a secure, trusted connection between host computers and the internal network.
 - a. Select the character set that the pre-shared secret will be defined with; ASCII or HEX (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F). Enter the pre-shared secret in the corresponding field. The PRE-SHARED SECRET field is case sensitive.
 - b. Click the **NEXT ARROW** to continue.

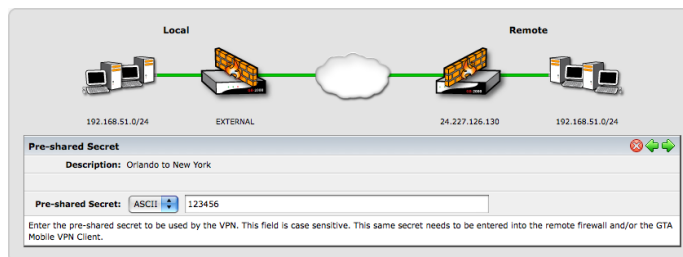


Figure 2.4: Entering the Pre-Shared Secret

4. The final screen of the IPsec Setup Wizard is a summary view of all entered settings. Please review the VPN's setup prior to committing the displayed configuration. To make changes to your basic setup, select the **BACK** button to return to the appropriate screen.

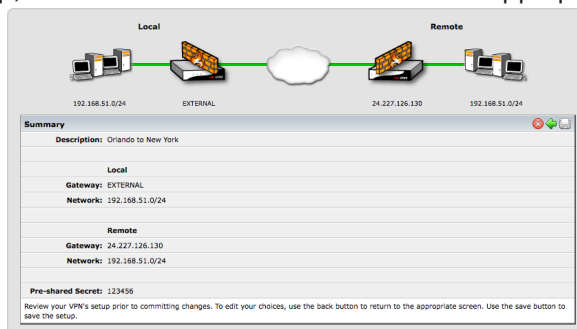


Figure 2.5: Review VPN Configuration

5. Click the **SAVE** icon to save the displayed configuration, or select the **CANCEL** icon to abort. Saving the configuration will insert a new Site-to-Site VPN.

Configuring an IPSec VPN Connection Manually

To manually configure an IPSec VPN with a GTA Firewall UTM Appliance, six aspects must be configured in order:

1. Authentication
2. IPSec Objects (optional)
3. Encryption Objects (optional)
4. Site-to-Site
5. VPN or GTA Mobile IPSec VPN Client authorization
6. VPN Policies (located at **Configure>Security Policies>Policy Editor>IPSec**)

Additionally, the second VPN gateway (GTA firewall or third-party VPN gateway) or Mobile IPSec VPN Client must be configured to reflect the same settings in order to establish the connection.

Authentication

When a VPN is being configured using IPSec key mode, authentication is performed with either pre-shared secrets or VPN certificates. GB-OS supports both methods of authentication for IPSec key mode VPNs.

A pre-shared secret is used to identify a party during the authentication phase of the VPN connection. By its definition, a pre-shared secret is shared with the other party before the VPN connection can be established.

VPN certificates, which contain a public key, can be distributed to parties that wish to connect to the VPN. During the authentication phase of the connection, the requesting party then authenticates using the VPN certificate and the private key. To create VPN certificates for authentication, see [Using VPN Certificates](#).

Creating IPSec Configuration Objects

IPSec Objects determine how incoming VPN connections will be negotiated by defining what client or VPN gateway initiation behavior should be acceptable by your GTA firewall.

Which IPSec Object Should I Use?

Depending on whether your GTA firewall has a static or dynamic (DHCP/PPP) IP address, different IPSec Objects will be used.

- **If it is a firewall to firewall IPSec VPN:**
The STANDARD STATIC IPSec Object will be used.
- **If using a Mobile IPSec VPN Client:**
The STANDARD DYNAMIC IPSec Object will be used.

Selecting the IPSec Key Mode

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

Using IKE (automatic key exchange), Phase 2 of the connection establishes an IKE security association (SA) that is later used to securely create an IPSec SA; it negotiates the VPN terms and authorizes the peer. Phase 2 establishes SAs for IPSec, providing source authentication, integrity and confidentiality.

Using manual key exchange, Phase 1 settings will be ignored by the GTA firewall.



Creating a VPN Using IKE IPsec Key Mode

Presuming default IPsec Objects are used, two screens will need to be configured. First, GB-OS must be configured to accept dynamic incoming connections. Unless VPN certificates are to be used for authentication, configuring how dynamic incoming connections is optional. Then, the Site-to-Site needs to be created to complete the VPN's configuration.

To configure how GB-OS handles dynamic incoming connections:

1. Navigate to **Configure>VPN>Preferences**.
2. Under the **ADVANCED** tab, make sure the **AUTOMATIC POLICIES** checkbox is enabled. Automatic policies automatically configure the necessary security policies to allow inbound and outbound access on the configured VPN.
3. Navigate to **Configure>VPN>Site-to-Site**.
4. Select enable.

To configure an IKE Site-to-Site:

1. Navigate to **Configure>VPN>Site-to-Site** and select **New** to create a new Site-to-Site IPsec VPN.
2. From the **Edit Site-to-Site** screen, select the **IPSEC KEY MODE**. For this example, select **IKE** (automatic key mode)
To create a Manual VPN, see [Creating a VPN Using Manual IPsec Key Mode](#).
3. Complete the VPN settings fields as described.

Disable:

Description: Orlando to New York

IPsec Object: Standard Static

Advanced

IPsec Key Mode: IKE Manual

Notifications

Email: SMS: SNMP Trap:

Authentication

Method: Pre-shared Secret

Pre-shared Secret: Modify ASCII

Options

Failover:

Send Keep Alives: <USER DEFINED> 192.168.1.101

Advanced

Policy Compatibility:

Gateway

	Local	Remote	Identity
Primary	EXTERNAL	<USER DEFINED> 66.249.719	IP Address

Local

NAT:

Network: FW Networks - PRO

Identity: IP Address

Remote

NAT:

Network: <USER DEFINED> 192.168.1.100/2

Figure 2.13: Creating an IKE VPN

Table 2.2: Creating a VPN Using IPSec Key Mode

Field	Description
Disable	Check to disable all access for the configured Site-to-Site IPSec VPN.
Description	A description of the Site-to-Site IPSec VPN.
IPSec Object	A selection for the IPSec Object used to define this VPN. See Which IPSec Object Should I Use? for more information. To create a new IPSec Object, or to configure an existing one, see Configuring an IPSec Object .
Advanced	
IPSec Key Mode	IKE (automatic key exchange)
Notifications	
Email, SMS, SNMP Trap	Select the checkbox(es) for the desired notifications to be sent.
Authentication	
Method	A selection for the method in which the GTA firewall will authenticate during Phase 1 of the VPN connection. Options are RSA or Pre-shared Secret . See Using VPN Certificates for more information on authenticating with VPN certificates.
Pre-shared Secret	If you are authenticating using a pre-shared secret, enter the ASCII or HEX format value pre-shared secret as defined by the VPN. This same key must match the key entered by the VPN's other party.
Options	
Failover	Select the <code>FAILOVER</code> checkbox to enable VPN failover.
Send Keep Alives	To prevent the VPN connection from closing prematurely, select the <code>SEND KEEP ALIVES</code> checkbox to have GB-OS automatically send a keep alive packet every 20 seconds.
Advanced	
Policy Compatibility	A toggle for firewalls that are not compatible with unique policies.
Gateway (A Primary field will always be available. A Secondary field will be available if Failover is enabled above.)	
Local	The type of interface for the local firewall that will serve as the VPN gateway.
Remote	The IP address of the remote gateway.
Identity	A selection for the identity of the tunnel. If <code><Domain Name></code> or <code><Email Address></code> are selected, enter the appropriate value in the corresponding text field. Available if authentication method is set to Pre-shared Secret.
Local	
NAT	Select the NAT checkbox to apply network address translation to traffic originating from the GTA Firewall UTM Appliance to the VPN connection.
Network	Select the host/subnetwork that should be accessible from the VPN. Typically this is the protected network or PSN. Alternatively, select <code><USER DEFINED></code> and enter the IP address(es) in the IP ADDRESS field. If the NAT checkbox has been selected, this field will not be available since it is not required.
Identity	If GB-OS is to authenticate using pre-shared secrets, select the user IP address, domain name or email address for authentication. If you elect to use an email address or domain name but do not provide one in the accompanying text field, the firewall will use the IP address or domain name indicated in Configure>System>Information .
Remote	
NAT	When the NAT checkbox is selected, the remote network will be the same as the remote gateway.
Network	Previously defined address object, IP address or Fully Qualified Domain Name of the network that resides behind the remote firewall. This can be just the part of the network to which access is desired. (On a firewall, typically this will be the protected network, PSN or a subnet of either.) Use a subnet mask to define the class of network.



Creating a VPN Using Manual IPsec Key Mode

Presuming that default IPsec Objects are used, two screens will need to be configured. First, GB-OS must be configured to accept dynamic incoming connections. Then, the Site-to-Site needs to be created to complete the VPN's configuration.

To configure an Manual Site-to-Site:

1. Navigate to **Configure>VPN>Site-to-Site** and select **New** to create a new Site-to-Site.
2. From the **Edit Site-to-Site** screen, select the IPSEC KEY MODE. For this example, select **MANUAL**. To create a VPN using IKE IPsec Key mode, see [Creating a VPN Using IKE IPsec Key Mode](#).
3. Complete the VPN settings fields as described on the following page.

The screenshot shows the configuration page for a Manual Site-to-Site VPN. At the top, there is a 'Disable' checkbox, a 'Description' field with the value 'Orlando to New York', and an 'IPSec Object' dropdown set to 'Standard Static'. Below this is an 'Advanced' tab. Under 'IPSec Key Mode', the 'Manual' radio button is selected. The 'Gateway' section has two columns: 'Local' and 'Remote'. The 'Local' column has a 'Primary' dropdown set to 'EXTERNAL'. The 'Remote' column has a dropdown set to '<USER DEFINED>' and a text field containing '66.227.126.130'. The 'Local' section has a 'Network' dropdown set to 'FW Networks - PRO' and a 'Certificate' field with the value '<xen-vm2>'. The 'Remote' section has a 'Network' dropdown set to '<USER DEFINED>' and a text field containing '192.168.1.100/2'. The 'Manual' section has 'Encryption Key' and 'Hash Key' fields, each with a 'Modify' checkbox and a masked input field. At the bottom, the 'Security Parameter Index (SPI)' section has 'Inbound SPI' and 'Outbound SPI' fields, both set to '256'.

Figure 2.14: Creating a Manual VPN

Table 2.3: Creating a VPN Using Manual IPsec Key Mode

Field	Description
Disable	Check to disable all access for the selected VPN.
Description	A description of the VPN.
IPSec Object	A selection for the IPsec Object used to define this VPN. See Which IPsec Object Should I Use? for more information. To create a new IPsec Object, or to configure an existing one, see Configuring an IPsec Object .
Advanced	
IPSec Key Mode	Manual
Gateway	
Local	Select an IP address, alias or H ₂ A group assigned to an external network interface on the local firewall that will serve as the VPN gateway. (To the second VPN gateway or mobile client, this IP address is the remote gateway.) This is the visible, non-encapsulated, non-encrypted IP address.
Remote	The IP address of the remote end of the VPN tunnel, the gateway to the remote network. If the remote network is behind a firewall, then this will be assigned to the external network interface. This IP address will also help determine the routing of the encapsulated packet.

Table 2.3: Creating a VPN Using Manual IPsec Key Mode

Field	Description
Local	
Network	Select the host/subnetwork that should be accessible from the VPN. Typically, this is the protected network or PSN. Alternatively, select <USER DEFINED> and enter the IP address(es) in the IP Address field. If the NAT checkbox has been selected, this field will not be available since it is not required.
Remote	
Network	Previously defined address object or an IP address of the network that resides behind the remote firewall. This can be just the part of the network to which access is desired. (On a firewall, typically this will be the protected network.) Use a subnet mask to define the class of network.
Manual	
Encryption Key	Select the format for the encryption key value: ASCII or HEX .
Hash Key	ASCII or HEX format value hash algorithm for the authentication transformation.
Security Parameter Index	
Inbound SPI	Default value is 256.
Outbound SPI	Default value is 256.

Encryption Key Length

Blowfish encryption transformations use variable key lengths, while AES, DES, 3DES and Camellia use a fixed length key. If you exceed the maximum key length in these fields, you will generate an error and not be able to save the configuration until it is corrected. You may enter a shorter length key, GB-OS will pad it to the minimum key size. Higher-bit key size generally results in stronger encryption.

Table 2.4: Encryption Key Length

Algorithm	Key Size	ASCII and Hexadecimal Characters
AES-128	128 bits	16 ASCII or 32 Hex
AES-192	192 bits	24 ASCII or 48 Hex
AES-256	256 bits	32 ASCII or 64 Hex
Blowfish	40-448 bits	5-56 ASCII or 10-112 Hex
DES	64 bits	8 ASCII or 16 Hex
3DES	192 bits	24 ASCII or 48 Hex
Camellia-128	128 bits	16 ASCII or 32 Hex
Camellia-192	192 bits	24 ASCII or 48 Hex
Camellia-256	256 bits	32 ASCII or 64 Hex

Hash Key Length

The key length for the MD5 transformation is 128 bits, which is 16 ASCII characters or 32 hexadecimal characters. The key length for the SHA-1 transformations is 160 bits, which is 20 ASCII (40 hexadecimal) characters; it provides 80 bits of security. The key length for the SHA-2 (SHA-256) transformations is 256 bits, which is 32 ASCII (64 hexadecimal) characters; it provides 128 bits of security against mid-transport data tampering. Generally, larger keys are more secure.

Security Parameter Index (SPI)

The Inbound and Outbound Security Parameter Index are arbitrary numbers used to uniquely identify a security association on a Manual VPN. The Inbound SPI will be the Outbound SPI on the remote side of the VPN; also, the Outbound SPI will be the Inbound SPI on the remote side of the VPN. The SPI should be unique for each SA, although the Inbound and Outbound SPI may have the same value. The minimum SPI value is 256.



Configuring a Custom IPSec Object

IPSec Objects configure how incoming IPSec VPN connections will be negotiated by defining what client or VPN gateway initiation behavior should be acceptable by your GTA firewall. Appropriate IPSec configuration objects vary with the type of IPSec VPN connection and your security policies.

Encryption objects are used to easily reference encryption settings when configuring an IPSec Object. For more information, see [Configuring an Encryption Object](#).

GTA firewalls use the IPSec VPN standard ([RFC 2401](#)) set by the IETF.

To create or configure an existing IPSec Object, navigate to **Configure>Objects>IPSec Objects**. Select **NEW** to create a new IPSec Object or select **EDIT** to modify a pre-defined IPSec Object.

The screenshot shows a configuration window for an IPSec Object. At the top, there is a 'Disable' checkbox and a 'Name' field containing 'Custom Dynamic'. Below that is a 'Description' field with the text 'Customized VPN Object for users and firewalls using dynamic gateway z'. The configuration is divided into two phases: Phase I and Phase II. Phase I includes 'Exchange Mode' (set to 'aggressive'), 'Encryption object' (set to 'AES-192,sha1,grp2'), and a 'Force Mobile Protocol' checkbox which is checked. Phase II includes an 'Encryption object' (set to 'AES-192,sha1,grp2'). An 'Advanced' section contains 'NAT-T' (set to 'Automatic'), 'Lifetime' (90 minutes), and 'DPD Interval' (30 seconds). Each section has an 'Advanced' button with a dropdown arrow.

Figure 2.15: Configuring an IPSec Object

Table 2.5: Configuring an IPSec Object	
Field Name	Description
Disable	Disables the IPSec Object for use in a VPN configuration.
Name	A unique name for the IPSec Object to reference it throughout the firewall's configuration.
Description	A brief description to describe the use of the IPSec Object.
Phase I	
Exchange Mode	Specify flexible (<main>) or forced (<aggressive>) negotiation of acceptable encryption algorithms for IKE. Aggressive mode is required if one component of the VPN has a dynamic (DHCP or PPP) IP address, such as with a dynamically-addressed VPN gateway or Mobile IPSec VPN Client.
Encryption Object	A selection for the level of encryption to be used by the IPSec Object. For more information on configuring encryption objects, see Configuring a Custom Encryption Object .
Force Mobile Protocol	A toggle used to force negotiation suited to VPNs involving dynamic IP addresses, including VPN gateways with dynamic (DHCP or PPP) IP addresses. This toggle is only available when the IPSec Object's Phase I EXCHANGE MODE has been set to <aggressive>.
Advanced	
NAT-T	A selection for the use of NAT-T (Network Address Translation - Transversal) for connections that do not require NAT-T (are not using NAT that denies VPN IKE connections). <Automatic> automatically uses NAT-T where applicable, <Disable> disables the use of NAT-T, while <Force> forces the use of NAT-T.
Lifetime	Specify the length of time in minutes before the Phase I (IKE) security associations must be renewed. Shorter times are generally more secure, but may reduce performance by adding renewal overhead time to the connection.

Table 2.5: Configuring an IPSec Object

Field Name	Description
DPD Interval	Specify the interval in seconds between checks for continued viability of the VPN connection (also known as dead peer detection). To disable DPD queries made by this firewall, set the interval to 0; the firewall will still respond to DPD signals from other VPN gateways and clients, but will not initiate any signals of its own.
Phase II	
Encryption Object	Specify the encryption algorithm that this firewall should accept for VPN data transfers (ESP). Strong encryption means that any algorithm except None and Null will be accepted from the VPN initiator. (Null provides IP encapsulation, but no encryption. None provides neither encryption nor encapsulation.). Null provides no security benefits when using NAT between firewalls. GTA firewalls initiate connections using AES-128 by default.
Advanced	
Lifetime	Specify the length of time in minutes before the Phase II security associations must be renewed. The entered value must be smaller than the Phase I Lifetime. Shorter times are generally more secure, but may reduce performance by adding renewal overhead time to the connection.

About Phase I

Phase I establishes VPN peer identities (keys) that can be tested for authenticity and establish initial security associations (SAs) that correlate hosts to encryption methods, securing further VPN negotiation/setup communications, and not actual transfers of user data.

During Phase I, the Diffie-Hellman cryptographic technique uses random and prime numbers to generate a secondary number. These secondary numbers are then exchanged, and each host uses a combination of these secondary numbers as keys. Because predicting random numbers and determining prime numbers are both computationally difficult, knowledge of the random and prime numbers behind the generation of a key can be used to prove host authenticity. Increased computational power means that a key may eventually be computed, which is why key-based security such as VPN phases must be periodically regenerated to guarantee authenticity of a packet's source.

Once Diffie-Hellman key exchanges have been performed, (automatically with IKE or manually), these temporary keys are used to prove authenticity of hosts requesting encryption and hash methods to be used during Phase II negotiations.

Automatic key exchange (IKE) uses Phase I settings during its automatic negotiations. Manual key exchange does not use Phase I settings, because the firewall does not provide automatic negotiations in manual mode.

About Phase II

Phase II uses the host authenticity and agreed initial hash and encryption established in Phase I to protect secondary negotiations for authenticity, data integrity and confidentiality settings. These secondary settings are used in the actual transfer of user data.

Using the temporary protection mechanisms devised during Phase I, Phase II again performs negotiations for keys, hashes and encryption that will be used to protect the transfer of actual user data.



Configuring a Custom Encryption Object

Encryption objects are used to easily reference encryption settings when configuring an IPSec Object. By default, GB-OS ships with five built-in encryption objects that are pre-configured with varying levels of encryption. They can be viewed and duplicated, but cannot be edited or deleted. Multiple encryption objects may also be combined.

To create or configure an existing encryption object, navigate to **Configure>System>Objects>Encryption Objects**.

Figure 2.16: Configuring a Custom Encryption Object

Table 2.6: Configuring a Custom Encryption Object

Field	Description
Disable	Disables the configured encryption object.
Name	A unique name for the encryption object to reference it throughout the firewall's configuration.
Description	A brief description to describe the use of the encryption object.
Encryption Method	Select the encryption algorithm that the firewall should accept for VPN data transfers. Default is <AES-192> . For more information on what encryption method to select, see Encryption Method .
Hash Algorithm	Select the hash algorithm that should be used to provide checks for packet tampering. Default is <HMAC-SHA1> . For more information on what hash algorithm to select, see Hash Algorithm .
Key Group	Select the Diffie-Hellman key group (bit size of the key) to use in authenticity keys. Default is <Diffie-Hellman Group 2> . For more information on what key group to select, see Key Group .
Description	Enter a short description of the encryption object.

Encryption Methods

Different encryption methods use proprietary methods for generating keys used to verify VPN data transfers. GTA firewalls support the following encryption methods:

Table 2.7: Encryption Methods

Field	Description
None	<None> provides neither encryption nor encapsulation when establishing a VPN connection.
Null	<Null> provides IP encapsulation, but no encryption. There are no security benefits when <Null> is selected, but it is useful to transport non-IP protocols when using NAT between firewalls.
AES 128-256	Advanced Encryption Standard; AES has become the new United States federal standard for encrypting commercial and government data. AES, with a key strength of 192 bits, is the default encryption level used by GB-OS encryption objects.
Blowfish	Blowfish is fast, supports long keys and is widely recognized throughout the security industry. Blowfish has been known to perform nearly twenty times faster than DES encryption.
DES	Data Encryption Standard; an algorithm used for encryption which had been the official algorithm of the United States Government.
3DES	3DES, often referred to as Triple DES, is three rounds of DES encryption. Each round uses a different permutation of your key. 3DES is a secure algorithm, yet can impact performance.
Strong	Selecting allows use of any encryption algorithm, a suitable selection when the IPSec Object's Phase 2 EXCHANGE MODE is set to <Main> .

Table 2.7: Encryption Methods

Field	Description
Camellia	Camellia has a block size of 128 bits, and can use 128-bit, 192-bit or 256-bit keys. Camellia can be implemented at high performance by software on various platforms and has many similarities to AES.

Hash Algorithm

The encryption object's **HASH ALGORITHM** is used to perform packet tampering checks in the Phase I and Phase II authentication headers. GTA firewalls support the following hash algorithms:

Table 2.8: Hash Algorithms

Field	Description
None	<None> provides no authenticity checks on the connection.
HMAC-MD5	A one-way hash function that creates a 16-byte (128-bit) hash or message digest to authenticate packet data.
HMAC-SHA1	A one-way hash function that creates a 20-byte (160-bit) hash or message digest to authenticate packet data. SHA1 is more resistant to attacks than MD5, but takes longer to compute.
HMAC-SHA2	Since the inception of SHA1, four more variants have been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512; collectively referred to as SHA-2.
All	<All> allows for the use of any hash algorithm.

Key Group

The encryption object's **KEY GROUP** is used to exchange the VPN's pre-shared secret using a Diffie-Hellman exchange. In a Diffie-Hellman exchange, two parties independently generate random public and private values. Each sends their public value to the other (using authentication to foil man-in-the-middle attacks); the private values remain secret. Each then combines the public key received with their own private key. The resulting key is the pre-shared secret and it is identical for both sides.

When selecting the bit size Diffie-Hellman group, keep in mind that while a larger bit size is generally more secure, it can significantly increase the amount of time it takes to decrypt content. GB-OS encryption objects default to **<Diffie-Hellman Group 2 (1024 bits)>**.



Note

For Phase II, Diffie-Hellman is sometimes referred to as Perfect Forward Secrecy (PFS).



Configuring VPN Policies

By default, GB-OS will automatically configure the necessary security policies to allow inbound and outbound access for all configured VPNs. If this has been disabled (the **AUTOMATIC POLICIES** setting is available under the **ADVANCED** tab located at **Configure>VPN>Site-to-Site**) it is necessary to manually define remote access and pass through policies to allow VPN traffic.



Note

It is recommended to have automatic policies enabled on the **Configure>VPN>Site-to-Site** screen to simplify the VPN configuration process.

To define the necessary remote access policies, navigate to **Configure>Security Policies>Policy Editor>Remote Access**. Create a new remote access policy of type Accept that allows VPN traffic (ESP (protocol 50) and UDP (ports 500 and 4500)).

To define the necessary pass through policies, navigate to **Configure>Security Policies>Policy Editor>Pass Through**. If an Site-to-Site has already been defined, click the **DEFAULT** button have GB-OS auto-configure a set of pass through policies.

Creating Authorization

If the configured VPN is to be used by GTA Mobile IPSec VPN Client users, it is necessary to define how the mobile users will be authenticating with the firewall.

After configuring a VPN connection, navigate to the **Configure>Accounts** section to configure mobile users by assigning them to groups and defining their user accounts. User groups are used to assign users to an IPSec Object and local network. User accounts, pooled in user groups, define the identity and password to be entered when authenticating with the firewall.

Creating Groups

Groups are used to define the IPSec Object and local network that GTA Mobile IPSec VPN Client users will be using.

When defining a group, additional groups can also be added to the group being defined to pool additional users. This can be useful if a policy is being defined that is required to affect multiple groups.

Groups are configured under **Configure>Accounts>Groups**.

Table 2.9: Creating Groups

Field Name	Description
Disable	Disables the group.
Name	The name for the group.
Description	A short description to identify the purpose of the group.
Mobile IPSec	
Enable	Enables VPN access for the user group.
Authentication Required	A toggle for whether or not users configured under the group should be required to authenticate with the firewall using the GTA Mobile IPSec VPN Client.
IPSec Object	The IPSec Object to be used by the user group.
Local Network	The local network on which the user organized within the configured user group can access. This will override configuration settings defined under Configure>VPN>Remote Access>IPSec .
Groups	
Sub Group	Select a previously defined group to reference additional groups.
Description	A short description to explain why this group is included.

Creating Users

User accounts define the identity and password to be entered when mobile users authenticate with the firewall. By default, the Mobile IPsec VPN section of the user's configuration settings are disabled. The MOBILE IPSEC VPN section must be enabled to allow the connection of mobile users.

Table 2.10: Creating User Accounts

Field Name	Description
Disable	Disables the account.
Identity	Used for authentication purposes, this is typically the user's email address.
Full Name	The name for the account.
Description	A short description to identify the use of the account.
Group	A selection for the user's user group. Selecting ??? means no user group has been selected. See Creating Groups for more information.
Authentication	
Method	Select the method for authentication. This field is used for GBAuth authentication with the GTA Firewall UTM Appliance, and is not necessary for the configuration of a GTA Mobile IPsec VPN Client user.
Password	The password for GBAuth authentication.
Mobile IPsec	
Enable	Enables VPN access for the account.
Remote Network	The IP address or address object of the remote network. If <USER DEFINED> is selected to identify the REMOTE NETWORK, then enter the IP address here.
Authentication	Select the method the mobile user will use to authenticate with the GTA Firewall UTM Appliance. Options are either Certificates or Pre-shared Secret .
Certificate	If the AUTHENTICATION method is set to CERTIFICATE , then select the VPN certificate that identifies the remote user. For more information on VPN Certificates, see Using VPN Certificates .
Pre-shared Secret	If PRE-SHARED SECRET is selected for the method for authentication, enter the ASCII or HEX value pre-shared secret.



Using VPN Certificates

VPN certificates are based on public-key cryptography, a method of authentication in which one party verifies another party's identity using a pair of keys (private and public). The public key is embedded in the VPN certificate, and is used to authenticate parties that have the corresponding private key.

GB-OS administrators have the choice to create either a self-signed certificate or a Certificate Signing Request (CSR). A CSR is an unsigned certificate that is meant to be submitted to a Certificate Authority (CA), which is a reputable third party that verifies the identity of the certificate holder. Upon receiving the CSR, the CA will then contact the administrator to verify their identity. Once the CA has verified that the administrator is who they claim to be, the CA will generate a certificate using data provided in the CSR and encrypt it using the CA's own private key.

A VPN certificate generated by GB-OS contains, at a minimum:

- A name
- An email address
- A country of origin
- An organization
- The duration until the certificate expires
- A public key

To define, import and export VPN certificates, navigate to **Configure>VPN>Certificates**.

How VPN Certificates Work

VPN certificates can be used for firewall to firewall or mobile client to firewall VPN connections.

Firewall to Firewall VPNs

To create a secure firewall to firewall VPN connection using VPN certificates for authentication, two GTA Firewall UTM Appliance administrators define certificates for their firewalls and assign them as the local certificate. The local certificate is used to identify their GTA Firewall UTM Appliance during Phase 1 of the VPN connection.

After the two administrators have set the local certificate on their firewalls, they then export their certificate and send it to the administrator of the other firewall. Next, each administrator then imports the other administrator's exported certificate into their own configuration.

Now that each administrator has both created and imported VPN certificates, they can create a secure VPN connection using VPN certificates for authentication.

Mobile Client to Firewall VPNs

To create a secure VPN connection between a GTA Firewall UTM Appliance and a mobile user running the GTA Mobile IPsec VPN Client using VPN certificates, the GTA Firewall UTM Appliance administrator must define two certificates. The first certificate is to be used as the local certificate, which identifies the GTA Firewall UTM Appliance during Phase 1 of the VPN connection. The second certificate is to identify the mobile user.

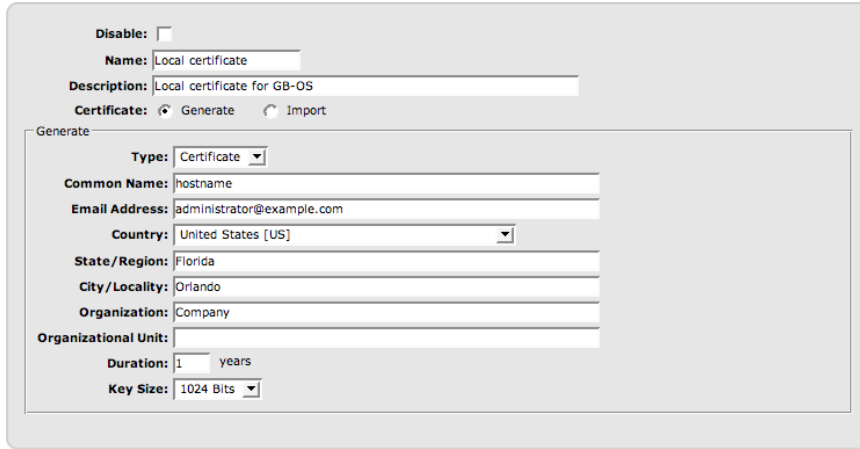
After the administrator has defined and set the firewall's local certificate, the firewall administrator must also define a VPN certificate for the user of the GTA Mobile IPsec VPN Client. After the certificates have been created, they must be exported along with the private key for the GTA Mobile IPsec VPN Client and then imported into the client's configuration.

After the administrator has both created the certificates for the GTA Firewall UTM Appliance and the mobile user, the local certificate as well as the mobile user's certificate and private key must be exported and imported it into the GTA Mobile IPsec VPN Client. Now the GTA Firewall UTM Appliance administrator and the mobile user can create a secure VPN connection using VPN certificates for authentication.

Generating VPN Certificates

To use VPN certificates for authentication, a local certificate must be created to identify the GTA Firewall UTM Appliance during the authentication phase of the VPN connection.

To generate a VPN certificate, navigate to **Configure>VPN>Certificates** and select the **New** icon. The **Edit Certificate** screen will then be displayed. Enter settings as described below:



The screenshot shows a web-based configuration interface for generating a VPN certificate. At the top, there is a 'Disable' checkbox. Below it are fields for 'Name' (containing 'Local certificate') and 'Description' (containing 'Local certificate for GB-OS'). A 'Certificate' section has radio buttons for 'Generate' (selected) and 'Import'. A 'Generate' section contains a 'Type' dropdown menu set to 'Certificate'. Below this are several text input fields: 'Common Name' (hostname), 'Email Address' (administrator@example.com), 'Country' (United States [US]), 'State/Region' (Florida), 'City/Locality' (Orlando), 'Organization' (Company), and 'Organizational Unit'. At the bottom of the generate section are 'Duration' (1 years) and 'Key Size' (1024 Bits) dropdown menus.

Figure 2.17: Generating VPN Certificates

Table 2.11: Generating VPN Certificates	
Field	Description
Disable	A toggle to disable the configured VPN certificate.
Name	A unique name used to identify the VPN certificate.
Description	A brief description to describe the function of the VPN certificate.
Certificate	Generate.
Generate	
Type	A selection for the VPN certificate's type. Select CERTIFICATE to generate a self-signed certificate, or CSR to generate a certificate signing requesting for a Certificate Authority.
Common Name	Typically, this is the firewall's or mobile user's host name.
Email Address	The email address of the firewall administrator or mobile user.
Country	The country where the firewall or mobile user is physically located.
State/Region	The state or region where the firewall or mobile user is physically located.
City/Locality	The city or locality where the firewall or mobile user is physically located.
Organization	The organization or company that the firewall or mobile user belongs.
Organizational Unit	The organizational unit that the firewall or mobile user belongs.
Duration	The amount of time, in years, that the certificate is valid for until it expires.
Key Size	A selection for the key size of the VPN certificate. A larger key size is generally more secure, but is more processor intensive.



Setting the Remote Administration Certificate

The remote administration certificate is used to locally identify the firewall and defines the firewall's SSL certificate. To set the remote administration certificate, navigate to **Configure>VPN>Certificates** and select the previously defined VPN certificate for the GTA Firewall UTM Appliance from the REMOTE ADMINISTRATION pull down.

If the REMOTE ADMINISTRATION field has not been set, and no certificates have been defined, clicking **DEFAULT** will cause GB-OS to generate and assign a remote administration certificate for the firewall using the firewall's host name and data entered in the **Configure>System>Contact Information** screen.



Note

Changing the remote administration certificate used by your firewall will cause it to automatically generate a new SSL certificate using data from the remote administration certificate. Once a new SSL certificate has been generated, the firewall will prompt the user to re-approve the certificate.

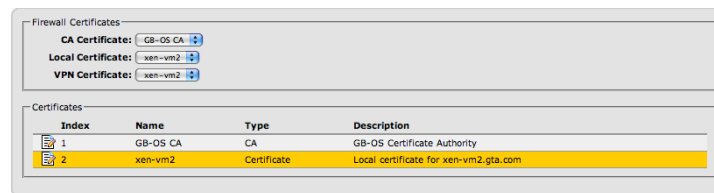


Figure 2.18: Setting the Local VPN Certificate

Exporting the Remote Administration VPN Certificate

In order to send the remote administration VPN certificate to the administrator of the VPN's endpoint, the certificate must be exported. When exporting VPN certificates from the configuration, the following file formats are available:

- **PEM:** The VPN certificate and its private key are exported as separate PEM files. VPN certificates have a .crt file extension and private keys have a .key file extension.
- **DER:** The VPN certificate and its private key are exported as separate DER files. VPN certificates have a .der file extension and private keys have a .key file extension.
- **PKCS#12:** The VPN certificate and its private key, along with the certificate chain used are exported as a single PKCS#12 file. PKCS#12 files have a .p12 file extension.



Note

GTA recommends exporting VPN certificates using the PKCS#12 file format. Both the VPN certificate and its private key are stored in one file, which allows for simplified certificate management.

PEM and DER file formats require that certificates and private keys are downloaded separately.

To export the remote administration VPN certificate, navigate to **Configure>VPN>Certificates**, select the previously defined VPN certificate that is being used as the GTA Firewall UTM Appliance's certificate in **Configure>VPN>Site-to-Site** and click the **Edit** button to bring up the **Edit Certificate** screen. Then, select the desired file formats for the VPN certificate and its private key and click the **DOWNLOAD** buttons to export the files.

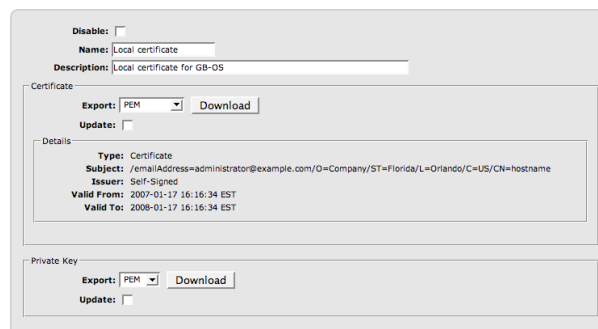


Figure 2.19: Exporting the Local VPN Certificate

Table 2.12 : Exporting the Remote Administration VPN Certificate	
Field	Description
Disable	A toggle to disable the configured VPN certificate.
Name	A unique name used to identify the configured VPN certificate.
Description	A brief description to describe the function of the configured VPN certificate.
Certificate	
Export	Select the file format for the VPN certificate. Click the DOWNLOAD button to export the file.
Update	Toggle the UPDATE checkbox if you wish to update the VPN certificate's definition with an existing VPN certificate, or generate a new VPN certificate.
PKCS#12 Password	If the VPN certificate is to be exported as a PKCS#12 file, an optional password can be set to secure the certificate. The PKCS#12 PASSWORD field is case sensitive.
Private Key	
Export	Select the file format for the private key. Click the DOWNLOAD button to export the file. If the VPN certificate is to be exported as a PKCS#12 file, this field will not be available.
Update	Toggle the UPDATE checkbox if you wish to update the private key with an existing private key.

Importing VPN Certificates

To import a VPN certificate into GB-OS for use in a VPN's configuration or user account definition, navigate to **Configure>VPN>Certificates** and select the **New** icon. The **Edit Certificate** screen will then be displayed. Select the **Import** toggle in the **CERTIFICATE** field to import a VPN certificate.

When importing a VPN certificate that is a PKCS#12 file, all certificates used in the certificate chain as well as the VPN certificate's private key are imported into the configuration.

Figure 2.20: Importing VPN Certificates

Table 2.13 : Importing VPN Certificates	
Field	Description
Disable	A toggle to disable the configured VPN certificate.
Name	A unique name used to identify the VPN certificate.
Description	A brief description for the function of the VPN certificate.
Certificate	Import
Certificate	
File	Select the BROWSE button to locate the certificate file.
Private Key	
File	Select the BROWSE button to locate the associated private key.



Reference A: VPN Concepts

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 Site-to-Sites (VPNs) cause the original IP packet to be:

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

A GTA Firewall UTM Appliance’s VPN is essentially a tunnel and a security processing service for IP traffic, both tunneling and securing packet contents. All GTA Firewall UTM Appliance VPN-secured traffic receives encapsulation by a secondary IP packet layer after it is secured.

All IP protocols can be secured with a 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 pre-shared keys or VPN certificates.
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 be tamper-proof (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 2 (IKE) part of VPN initialization. **The GTA firewall implementation of IPSec VPN requires authorization; VPNs will not activate without an authorization that references an IPSec configuration object.**

The source of the authorization can be provided in two separate areas 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 2 and Phase 2 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 **Configure>System>Objects>IPSec 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. 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 typically 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 2 and Phase 2 of VPN creation using encryption algorithms. Separate encryption methods may be selected for either phase.

IPSec VPNs provide data privacy with encryption. Encryption methods for a GTA firewall VPN connection are configured in **Configure>System>Objects>IPSec Objects**.



Packet Structure: IPSec VPN

IPSec VPNs use encrypted, encapsulated IP packets to transfer data.

The original IP packet's 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.

IPSec VPN Packets

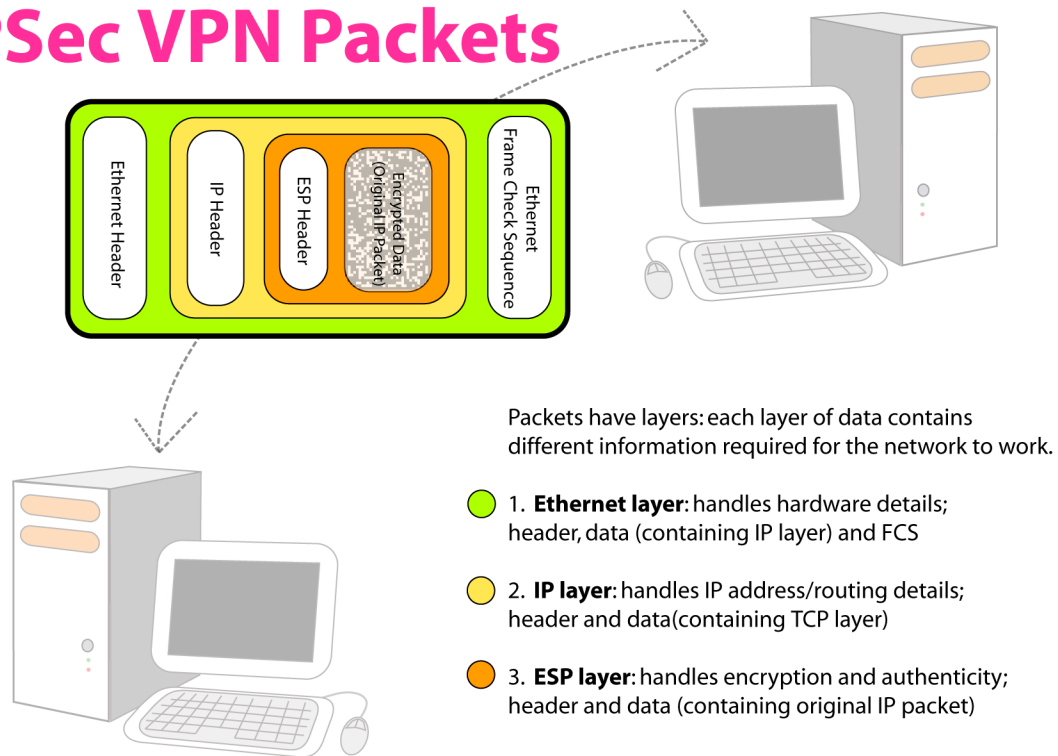


Figure B.1: IPSec VPN Packets

GTA Firewall VPN Packet Processing

When a packet arrives at a GTA Firewall UTM Appliance, 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 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 security policies 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.

Reference B: Example VPN Configurations

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

- Do both initiator and responder have static IP addresses?
- Is key exchange manual or automatic (IKE)?
- If the IKE key exchange is used, is authentication handled using pre-shared secrets or VPN certificates?

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.

This reference is divided into three sections:

1. [Example: Using IKE IPsec Mode and Pre-shared Secrets](#)
2. [Example: Using IKE IPsec Mode and VPN Certificates](#)
3. [Example: VPN Configurations Using Manual IPsec Mode](#)



Note

It is assumed that automatic policies are enabled on the **Configure>VPN>Site-to-Site** screen. Automatic policies allow all VPN traffic by default. If disabled, it is necessary to create security policies that allow ESP protocol 50 and UDP ports 500/4500.

For information on manually defining security policies, see the *GB-OS User's Guide*.



Note

Example configurations contain fictional descriptions, IP addresses and subnet masks. 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.*.* as an example. In your implementation, those settings may contain 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

Before manually configuring a VPN, consider running the IPsec Setup Wizard, located at **Wizards>IPsec Setup**. The IPsec Setup Wizard is designed to help configure a simple VPN quickly and easily.

Example: Using IKE IPsec Mode and Pre-shared Secrets

Gateway to Gateway: Static/Static IP Addresses

The identifying characteristics of this type of VPN include:

- Static external IP addresses on **both** firewalls, as set in **Configure>Network>Settings**
- Default or edited IKE **IPsec Objects** selected in **VPNs**
- LOCAL IDENTITY is not necessary, since static IP addresses serve as a constant element for identity
- Authentication using pre-shared secrets

Table B.1: Gateway to Gateway: Static/Static IP Addresses & IKE

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 System>Objects>Address Objects:		
Disable	Unchecked	Unchecked
Name	Protected Networks	Protected Networks



Table B.1: Gateway to Gateway: Static/Static IP Addresses & IKE

Field Name	Initiator: GTA firewall with static IP address	Responder: GTA firewall with static IP address
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	All	All
Object	<USER DEFINED>	<USER DEFINED>
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 VPN>Site-to-Sites:		
Disable	Unchecked	Unchecked
Description	IKE VPN	IKE VPN
IPSec Key Mode	IKE	IKE
IPSec Object	Standard Static (default object)	Standard Static (default object)
Authentication		
Method	Pre-shared Secret	Pre-shared Secret
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)
Options		
Send Keep Alives	Unchecked	Unchecked
Local		
Gateway	<EXTERNAL>	<EXTERNAL>
NAT	Unchecked	Unchecked
Network	Protected Networks (or the address object as defined above)	Protected Networks (or the address object as defined above)
Identity	<IP Address>	<IP Address>
Remote		
Gateway	200.200.200.200 (the external IP address of the other VPN gateway)	100.100.100.100 (the external IP address or FQDN of the other VPN gateway)
NAT	Unchecked	Unchecked
Network	<USER DEFINED> 192.168.1.0/24 (the attached hosts on the other VPN gateway)	<USER DEFINED> 192.168.2.0/24 (the attached hosts on the other VPN gateway)
Advanced		
Identity	<IP Address>	<IP Address>

Example VPN Configurations Using IKE IPsec Mode and VPN Certificates

Gateway to Gateway

The identifying characteristics of this type of VPN include:

- Static external IP addresses on **both** firewalls, as set in **Configure>Network>Settings**
- Default or edited IKE **IPsec Objects** selected in **VPNs**
- LOCAL IDENTITY is not necessary, since static IP addresses serve as a constant element for identity
- Authentication using VPN certificates

Table B.2: Gateway to Gateway

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 Configure>VPN>Certificates>Edit Certificate		
Disable	Unchecked	Unchecked
Name	Firewall 1	Firewall 2
Description	Firewall 1 local certificate	Firewall 2 local certificate
Certificate	Generate	Generate
Generate		
Type	Certificate	Certificate
Common Name	firewall1.example.com The host name of the firewall.	firewall2.example.com The host name of the firewall.
Email Address	fwadmin1@example.com The email address belonging to the firewall administrator.	fwadmin2@example.com The email address belonging to the firewall administrator.
Country	The country the remote user is located.	The country the remote user is located.
State/Region	The state the remote user is located.	The state the remote user is located.
City/Locality	The city or location the remote user is located.	The city or location the remote user is located.
Organization	The remote user's organization.	The remote user's organizational.
Organizational Unit	The remote user's organizational unit.	The remote user's organizational unit.
Duration	1	1
Key Size	<1024> Bits	<1024> Bits
In Configure>VPN>Certificates		
Firewall Certificates		
VPN Certificate	Firewall 1	Firewall 2
In Configure>VPN>Certificates>Edit Certificate		
Disable	Unchecked	Unchecked
Name	Leave blank	Leave blank
Description	Leave blank	Leave blank
Certificate	Import	Import



Table B.2: Gateway to Gateway

Field Name	Initiator: GTA firewall with static IP address	Responder: GTA firewall with static IP address
Certificate		
File [Type]	PKCS #12 For this example, PKCS #12 certificates will be used.	PKCS #12 For this example, PKCS #12 certificates will be used.
File {Browse}	Select the VPN certificate exported from Firewall 2.	Select the VPN certificate exported from Firewall 1.
PKCS #12 Password	Enter the PKCS #12 password for Firewall 2's certificate, if any.	Enter the PKCS #12 password for Firewall 1's certificate, if any.
Private Key		
File	n/a	n/a
In System>Objects>Address Objects:		
Disable	Unchecked	Unchecked
Name	Protected Networks	Protected Networks
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	All	All
Object	<USER DEFINED>	<USER DEFINED>
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 Configure>VPN>Site-to-Site:		
VPN Certificate	Firewall 1	Firewall 2
Advanced		
Automatic Policies	Checked	Checked
Dynamic Incoming Connections		
Authentication	Certificates	Certificates
IPSec Object	Standard Dynamic (default object)	Standard Dynamic (default object)
In VPN>Site-to-Sites>Edit Site-to-Site		
Disable	Unchecked	Unchecked
Description	IKE VPN	IKE VPN
IPSec Key Mode	IKE	IKE
IPSec Object	Standard Static (default object)	Standard Static (default object)
Authentication		
Method	Certificates	Certificates
Options		
Send Keep Alives	Unchecked	Unchecked
Gateway		
Local	<EXTERNAL>	<EXTERNAL>
Remote	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)
Certificate	Firewall 2 Select the VPN certificate imported from the other firewall	Firewall 1 Select the VPN certificate imported from the other firewall

Table B.2: Gateway to Gateway		
Field Name	Initiator: GTA firewall with static IP address	Responder: GTA firewall with static IP address
Local		
NAT	Unchecked	Unchecked
Network	Protected Networks	Protected Networks
Remote		
NAT	Unchecked	Unchecked
Network	<USER DEFINED> 192.168.2.0/24 (the attached hosts on the other VPN gateway)	<USER DEFINED> 192.168.1.0/24 (the attached hosts on the other VPN gateway)

Example VPN Configurations Using Manual IPsec Mode

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 **IPsec Objects** selected in **VPNs**
- **Only Phase 2 settings of the manual IPsec Object are used** (Phase 1 may be entered, but it is not used; instead, Phase 2 from the IPsec Object is used)
- LOCAL IDENTITY is not necessary, since static IP addresses serve as a constant element for identity

Table B.3: Gateway to Gateway: Static/Static IP Addresses & Manual Key Exchange		
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 System>Objects>Address Objects:		
Disable	Unchecked	Unchecked
Name	Protected Networks	Protected Networks
Description	DEFAULT: Protected networks	DEFAULT: Protected networks
Type	All	All
Object	<USER DEFINED>	<USER DEFINED>
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 System>Objects>IPsec Objects:		
Disable	Unchecked	Unchecked
Name	Manual	Manual
Description	IKE IPsec Object	IKE IPsec Object
Phase 1		
Exchange Mode	n/a	n/a
Encryption Object	n/a	n/a
Advanced		
Force Mobile Protocol	n/a	n/a
NAT-T	n/a	n/a



Table B.3: Gateway to Gateway: Static/Static IP Addresses & Manual Key Exchange		
Field Name	Initiator: GTA firewall with static IP address	Responder: GTA firewall with static IP address
Lifetime	n/a	n/a
DPD Interval	n/a	n/a
Phase 2		
Encryption Object	<AES-192, sha1, grp2> (default)	<AES-192, sha1, grp2> (default)
Advanced		
Lifetime	n/a	n/a
In VPN>Site-to-Sites:		
Disable	Unchecked	Unchecked
Description	Office-to-office VPN	Office-to-office VPN
IPSec Mode	Manual	Manual
IPSec Object	Manual (the VPN configuration object, as previously defined)	Manual (the VPN configuration object, as previously defined)
Local		
Gateway	<EXTERNAL>	<EXTERNAL>
NAT	Unchecked	Unchecked
Network	Protected Networks (or the address object as defined above)	Protected Networks (or the address object as defined above)
Identity	<IP Address>	<IP Address>
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)
NAT	Unchecked	Unchecked
Network	<USER DEFINED> 192.168.2.0/24 (the attached hosts on the other VPN gateway)	<USER DEFINED> 192.168.1.0/24 (the attached hosts on the other VPN gateway)
Manual		
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)
Security Parameter Index (SPI)		
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)

Reference C: Log Messages

GTA Firewall

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 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 a 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 acquire license, access for 'user@example.com' denied." type=mgmt,vpn src=200.200.200.200 dst=100.100.100.100
```

GTA Mobile IPsec VPN Client

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 **IPsec 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 **IPsec 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 2 Settings

An incorrect Phase 2 (IKE) setting was used. These settings should match the GTA firewall's dynamic **IPSec Objects** PHASE 2 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 2 Settings

An incorrect encryption, authentication or key group was used in Phase 2 settings. These settings should match the GTA firewall's mobile **IPSec Objects** PHASE 2 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 2 Authentication Settings

An incorrect value was used for Phase 2 authentication (hash) settings. This value should match the GTA firewall's mobile **IPSec Objects** PHASE 2 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 2 Key Group Settings

An incorrect value was used for Phase 2 key group (Diffie-Hellman) settings. This value should match the GTA firewall's mobile **IPSec Objects** PHASE 2 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
```

Incorrect Filter Configuration

A misconfigured or missing filter for UDP port 4500 on the GTA firewall. Add a remote access filter that accepts UDP port 4500 on the GTA firewall.

```
Description 130059 Default message_recv: bad message length
130059 Default dropped message from 216.9.84.83 due to notification type
UNEQUAL_PAYLOAD_LENGTHS
130059 Default SEND Informational [NOTIFY] with UNEQUAL_PAYLOAD_LENGTHS
error
130059 Default (SA GBPhase1-GBPhase2-P2) SEND phase 2 Quick Mode [HASH]
```



Copyright

© 1996-2010, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

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 Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

GB-OS, Surf Sentinel, Mail Sentinel and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. GB Commander is a trademark of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

Some products include software developed by the OpenSSL Project (<http://www.openssl.org/>).

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • **Fax:** +1.407.380.6080 • **Web:** <http://www.gta.com> • **Email:** info@gta.com