Technical Document

TD VPN-GB-WG-02

GNAT Box VPN and VPN Client

with SoftRemoteLT from SafeNet, Inc.

GTA Firewall – WatchGuard Firebox

Configuring an IPSec VPN with IKE

GNAT Box System Software version 3.3.2

Firebox 1000 Strong Encryption 4.6.1

Global Technology Associates, Inc.

Copyright

Disclaimer

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

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

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

Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated.
RoBoX is a trademark of Global Technology Associates, Incorporated.
SafeNet VPN client SoftRemoteLT is a trademark of SafeNet, Inc.
All other products are trademarks of their respective companies.

Version Information

SafeNet VPN client SoftRemoteLT version 8.0.2	October 2002
GNAT Box System Software version 3.3.2	November 2002

Technical Support

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

Contact Information

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

Tel	+1.407.380.0220
Fax	+1.407.380.6080
Web	http //www.gta.com
Email	info@gta.com
Support	support@gta.com

Document Information

Technical Document
GTA Firewall – WatchGuard Firebox, Configuring an IPSec VPN with IKE December 2002

Table of Contents

Introduction

Configuring an IPSec VPN with IKE for a GTA Firewall and WatchGuard Firebox is written for the administrator who has both of these systems operating on a network, and requires a virtual private network (VPN) to utilize both firewalls. This manual is written with the assumption that the reader has a strong working knowledge of TCP/IP, WatchGuard administration utilities, and the GNAT Box System Software for GTA Firewalls. This manual was developed using GNAT Box System Software version 3.3.2 and a WatchGuard Firebox 1000 Strong encryption 4.6.1.

Common Encryption Methods

A number of encryption algorithms on the GTA Firewall do not have corresponding methods on a Firebox. The following methods are common to both firewall systems; use them to configure both firewalls for a VPN connection.

Neither the encryption method nor the hash algorithm for Phase I of the VPN can be configured on a Firebox 1000. Therefore, Phase I on the GTA Firewall must use encryption method DES or 3DES, hash algorithm SHA-1, and key group Diffie-Hellman Group 1 to match the Firebox default configuration.

Note

Phase I and II are not clearly differentiated in WatchGuard Firebox 1000.

Firebox (non-configurable)

Mode	IKE
ESP	DES or 3DES (Triple DES)
Hash	SHA-1

GTA Firewall to Firebox

IPSec Key Mode	IKE
Phase I	
Exchange Mode	Main
ESP	DES
Hash	SHA-1
Key Group	Diffie-Hellman Group 1
Phase II	
ESP	DES or 3DES
Hash	SHA-1 or MD5
Key Group	Diffie-Hellman Group 1

Examples

To configure a GTA Firewall for VPN, use GBAdmin or the Web Interface. The examples given in this documentation use GBAdmin. This guide uses the following IP addresses as examples for a GTA Firewall VPN configuration:

External Interface	199.120.225.76
Protected Interface	192.168.1.1
Protected Network	192.168.1.0//24

To configure the Firebox, (referred to in this document as “FB”) use the WatchGuard Policy Manager. This guide uses the following IP addresses as examples for an FB configuration:

FB External Interface	199.120.225.90
FB Protected Interface	10.10.11.1
FB Protected Network	10.10.11.0/255.255.255.0

GTA Firewall VPN Configuration

In order to use the GTA Firewall VPN feature, four functional areas must be configured: VPN Objects, VPN Authorization, Remote Access Filters and IP Pass Through Filters. VPN objects are used as the basis for VPN authorization, forming a link between the GTA Firewall and another firewall. User Authorization allows a GTA Firewall to connect to and authenticate a mobile client user or dynamic system user.

Note

For more information and illustrations about configuring a GTA Firewall VPN, see the **GNAT Box System Software User’s Guide**.

VPN Object

Open Objects -> VPN Objects. Use the field table below as an example for entering data into the VPN Object fields.

VPN Object Fields	
Disable	(Uncheck).
Name	Enter a name for the object: (GTA Firewall - FB VPN)
Description	Enter a description: (GTA Firewall - FB IKE VPN)

Local Gateway	Select the interface object or enter the IP address for the GTA Firewall External Interface. (199.120.225.76)
Local Network	Select the interface object for the GTA Firewall Protected Interface. (192.168.1.0/24)
Require Mobile Authentication	Uncheck.
Force Mobile Protocol	Uncheck.
Phase I	
Exchange Mode	Main.
Encryption (ESP)	DES.
Hash	SHA-1.
Key Group	Diffie-Hellman Group 2.
Phase II	
Encryption (ESP)	DES.
Hash	SHA-1.
Key Group	Diffie-Hellman Group 1.

VPN Authorization

Open Authorization -> VPNs and add a new VPN. In the Key Exchange Type dialog, select IKE. Select OK, then enter the information in the VPN Authorization fields.

VPN Object Fields–Example	
Disable	Enable. (Uncheck.)
Key Exchange	IKE (Uneditable. Selected in the previous dialog.)
Description	Enter a description of the VPN object. (GTA Firewall - FB VPN Authorization)
Identity	Leave blank.
VPN Object	Select the VPN object created previously. (GTA Firewall - FB IKE VPN)
Remote Gateway	Select the IP address or object that references the FB External Network interface. (199.120.225.90)
Remote Network	Select the IP Address or object that references the FB Protected Network. (10.10.11.0/24)
Preshared Secret	Preshared secret/key entered on the FB system. (Preshared keys must be the same on both systems.)

Remote Access Filters

When using IKE, two Remote Access filter are necessary; one for the ESP Tunnel (IP protocol 50) and the other to allow access for IKE on UDP/500.

1. Allow ESP connections (GNAT Box FB IKE VPN).

Type	Accept
Interface	ANY
Protocol	50 (ESP)
Source	199.120.225.90/32
Port	Blank
Destination	199.120.225.76/32
Port	Blank

2. Allow IKE connections (GNAT Box FB IKE VPN).

Type	Accept
Interface	ANY
Protocol	UDP
Source	199.120.225.90 /32
Port	Blank
Destination	199.120.225.76/32
Port	500

IP Pass Through Filters

The example filters below allow all access between the Firebox and the GTA Firewall networks.

At a minimum, an IP Pass Through filter must be created that allows outbound access on the defined VPN. Depending on your security policy, the filter can be as simple as allowing any host on the local network outbound access to any remote host for any protocol at any time, or as narrow as limiting a specific local host outbound access to a specific remote host for a given protocol at a specific time.

Generally, in addition, an inbound IP Pass Through filter is created that allows the remote side of the VPN access to the local Protected Network. This filter does not have to be symmetrical to the outbound IP Pass through filter, but rather should be created to meet the local security policy.

Typically, single inbound and outbound IP Pass Through filters are created for a VPN, but multiple filters may be required to make access conform to the local security policy.

1. VPN, inbound connections (GNAT Box FB IKE VPN)

Type	Accept
Interface	External
Protocol	ANY
Source	10.10.11.0/32
Port	Blank
Source	192.168.1.0/32
Port	Blank

2. VPN, outbound connections (GNAT Box FB IKE VPN)

Type	Accept
Interface	Protected
Protocol	ANY
Source	192.168.1.0/32
Port	Blank
Source	10.10.11.0/32
Port	Blank

Firebox VPN Configuration

Open the WatchGuard Policy Manager and follow the instructions below to set up a GTA Firewall to Firebox 1000 VPN. In the example, select screens are shown to illustrate the configuration process.

Note

This example allows all access between the Firebox networks and the GTA Firewall networks. Consult your corporate security policy for specific filtering rules.

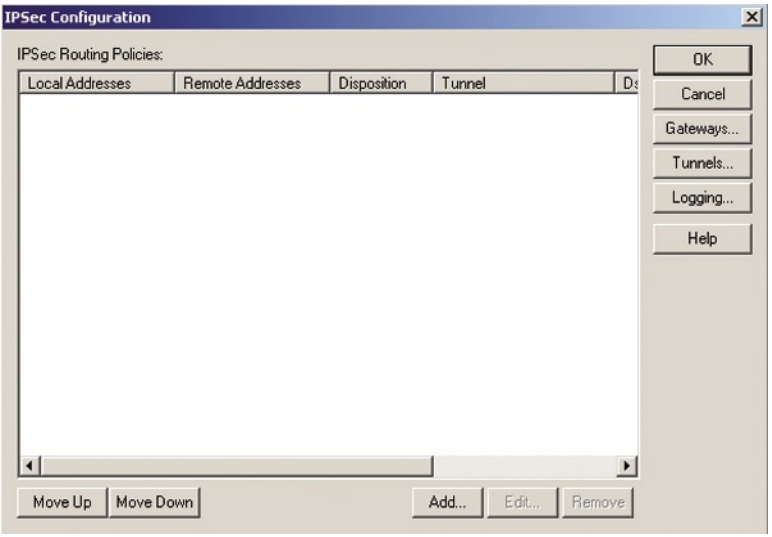
Define the VPN

Define a gateway

This step defines the External Interface of the GTA Firewall. From the Main Menu, Select Network Branch Office VPN IPSec.

Network Menu

This brings up the IPSec Configuration screen. Click Gateways.



IPSec Configuration screen

This brings up the Configure Gateways screen. Click ADD. The IPSec Gateway dialog box will appear.

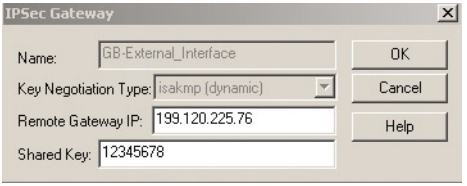
In the Name field, enter the name that will be used to identify the Firebox remote gateway to the GTA Firewall. In the Key Negotiation Type field, select isakmp (dynamic). In the Remote Gateway IP field, enter the External IP Address of the GTA Firewall. In the Shared key field, enter the same shared key as the one entered in the GNAT Box system's Pre-shared Secret field.

Note

The shared key must be identical to the pre-shared secret on the GNAT Box system.

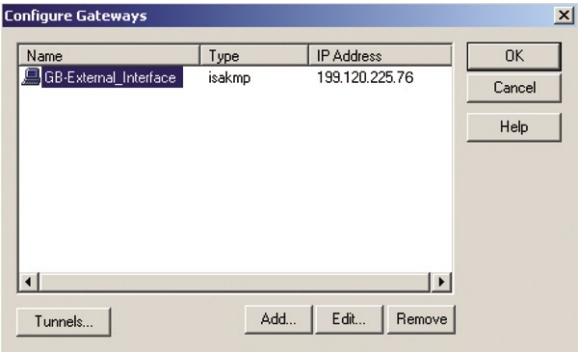
Enter information into each field, or select it from the drop-down box, as in the following example:

IPSec Gateway Fields	
Name	GB-External_Interface
Key Negotiation Type	isakmp (dynamic)
Remote Gateway	199.120.225.76
Shared key	12345678



IPSec Gateway dialog box–completed

Click OK to save this gateway and return to the Configure Gateways screen. The new gateway will appear in the list.

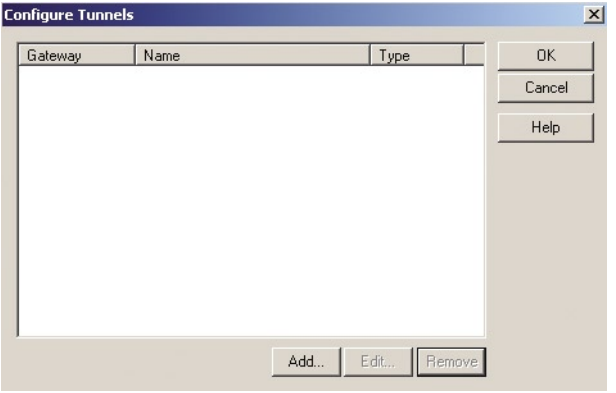


Configure Gateways screen

Define a tunnel

The tunnel encapsulates packets between the GTA Firewall and the Firebox 1000. It also specifies the tunnel's encryption types, authentication methods and end points.

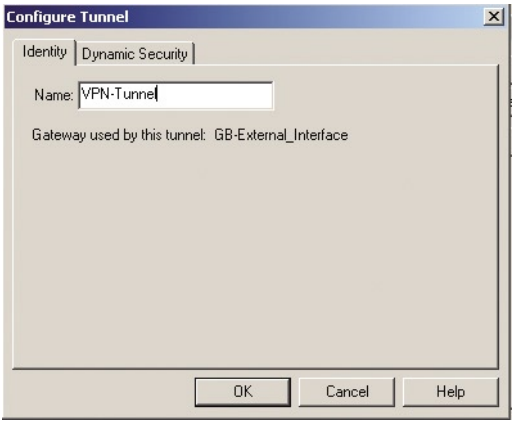
From the Configure Gateways screen, click Tunnels. This will bring up the Configure Tunnels screen.



Configure Tunnels screen

Click ADD to add a new tunnel. This brings up the Select Gateway dialog box. Select GB-External_Interface, the gateway created in the first step, then click OK. The Configure Tunnel dialog box will appear.

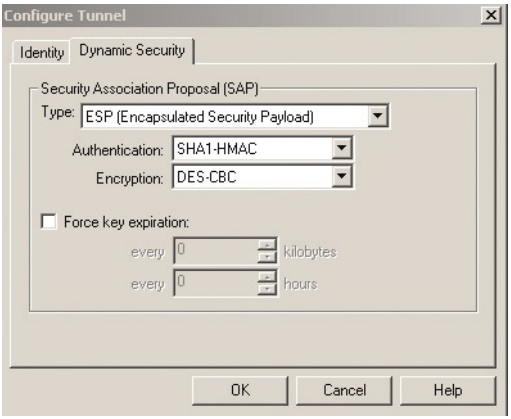
In the Identity tab, give the tunnel a name by entering VPN-Tunnel



Configure Tunnel dialog box–Identity tab

Click the Dynamic Security tab. Enter, or select from the drop-down box, the required information as in the following example:

Configure Tunnel Fields	
Type	ESP (Encapsulated Security Payload).
Authentication	SHA1-HMAC.
Encryption	DES or 3DES.
Force key expiration	(Uncheck.)



Configure Tunnel dialog box–Dynamic Security tab

Note

GTA recommends that the user disable (uncheck) FORCE KEY EXPIRATION in the Firebox side of the VPN configuration. This will allow the GTA Firewall to renegotiate the key at default intervals. If ***Force key expiration*** is enabled on the Firebox, key renegotiation may not work properly. In a GTA Firewall, the default for Phase I key renegotiation is 90 minutes and the default for Phase II is 60 minutes.

To save this tunnel configuration, click OK. The Configure Tunnels screen will reappear. Click OK again to return to the IPSec Configuration screen.

Add an IPSec (Routing) Policy for the VPN

In a Firebox system, the term “policy” refers to a set of rules that define how IPSec traffic is routed thorugh a tunnel. An IPSec policy is defined by the end points of the VPN, which can be either hosts or networks connecting through the VPN. For this example, we will use network end points.

In the IPSec Configuration screen, click ADD. This brings up the Add Routing Policy screen. Enter, or select from the drop-down box, the required information as in the following example:

Local <Network> **10.10.11.0/24**	
Remote <Network>	**192.168.100.0/24**
Disposition	**secure**
Tunnel	**VPN-Tunnel** (Tunnel created in step 2)

Click **OK** to finish adding the new policy. Click **OK** again to close the **IPSec Configuration** Screen.

Create a Service

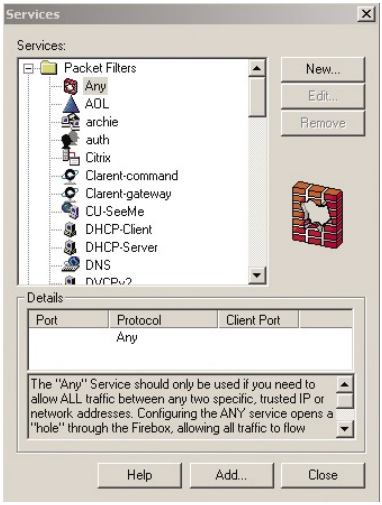
In a Firebox system, the term service refers to the set of rules set up to allow certain services through the VPN tunnel. (Some call this a “policy.”)

This step allows the user to select what services are allowed through the VPN tunnel. The Firebox must be configured to allow GTA Firewall traffic through the VPN tunnel.

Note

This example creates a VPN service with the same rules as the Firebox Any service, which allows all traffic through any port. You should consult your own security policy before implementing the VPN Tunnel as described.

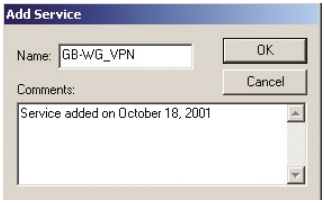
Create a new service by selecting Edit Add Service from the Main Window. This brings up the Services window.



Services window

In the Services window, expand Packet Filters. Select Any from the list and click Add (at the bottom of the window).

This brings up the Add Service dialog box. Give the service a name by entering: GB-WG_VPN. Click OK.



Add Service dialog box

This brings up the Properties dialog box for the new service with the Incoming tab selected.

Define Incoming service

On the Incoming tab, select Enabled and Allowed from the drop-down list.

In the top portion of the dialog box, under the From list, click ADD. This brings up the Add Address dialog box.

Click Add Other. This brings up the Add Member dialog box. Enter the following:

Choose Type	Network IP Address
Value	192.168.1.0/24 (The IP address of the network behind the GTA Firewall.)

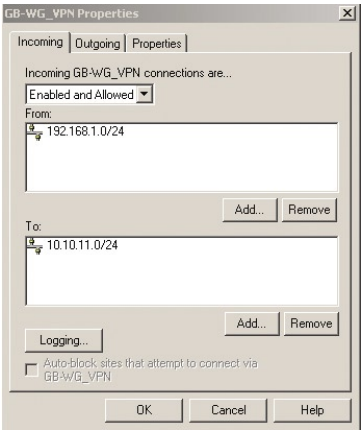
Click OK. This returns the user to the Add Address dialog box. Click OK to save the address to the From list and return to the service's Properties box.

In the bottom portion of the dialog box, under the To list, click ADD. This brings up the Add Address dialog box.

Click Add Other. This will bring up the Add Member dialog box. Enter the following:

Choose Type	Network IP Address
Value	10.10.11.0/24 (The IP address of the network behind the Firebox.)

Click OK. This returns the user to the Add Address dialog box. Click OK to save the address to the To list and return to the service's Properties dialog box.



Properties dialog box, Incoming tab, complete

Define Outgoing service

This process is simply the inverse of that in the Incoming tab.

Select the Outgoing tab. Select Enabled and Allowed from the drop-down list.

In the top portion of the dialog box, under the From list, click ADD. This brings up the Add Address dialog box.

Click Add Other. This will bring up the Add Member dialog box. Enter the following:

Choose Type	Network IP Address
Value	10.10.11.0/24 (The IP address of the network behind the Firebox.)

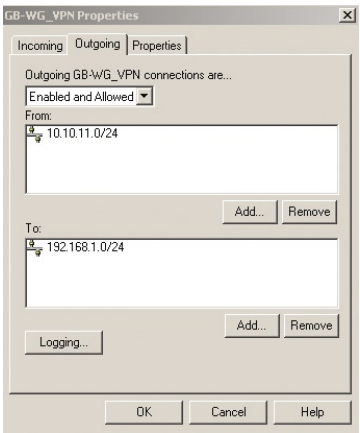
Click OK. This returns the user to the Add Address dialog box. Click OK to save the address to the From list and return to the service's Properties dialog box.

In the bottom portion of the dialog box, under the To list, click ADD. This brings up the Add Address dialog box.

Click Add Other. This will bring up the Add Member dialog box. Enter the following:

Choose Type	Network IP Address
Value	192.168.1.0/24 (The IP address of the network behind the GTA Firewall.)

Click OK. This returns the user to the Add Address dialog box. Click OK to save the address to the From list and return to the service's Properties dialog box.



Any Properties dialog box, Outgoing tab, complete

Click OK in the Properties dialog box to close it and save the new service and its properties.

Save the configuration

To save the new gateway, tunnel, IPSec policy and service to the Firebox:

- Select File>Save to Firebox.

- Select your Firebox from the drop-down list.
- Enter the configuration read/write pass phrase (password). Click OK.
- Reboot the Firebox to enable the new VPN.

Your GTA Firewall and Firebox VPN is now in place.

Index