Technical Document

TD: GB-SW-02

GTA Firewall – SonicWALL Pro

Configuring an IPSec VPN with IKE

GNAT Box System Software v3.2.3 • SonicWALL Firmware v6.1.2.0 and ROMware v 5.0.1.0

Products

GB-100
GB-1000
GB-Flash
RoBoX™

Global
Technology
Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL • 32817 USA
407.380.0220 • info@gta.com • www.gta.com

Contents

Introduction 3

Contact information 3

Required VPN Settings: GTA Firewall and SonicWALL Pro 3

Addresses used in examples 3

GTA Firewall to SonicWall Pro Configuration 4

Create a VPN Object 4

VPN Authorization 5

Create Remote Access Filters 6

Create IP Pass Through Filters 6

SonicWALL Pro to GTA Firewall VPN Configuration 7

Add/Modify IPSec Security Associations 8

Security policy 8

Destination Networks 8

Global Technology Associates, Inc.
3505 Lake Lynda Drive, Suite 109
Orlando, FL 32817 USA
Tel: +1.407.380.0220
Fax: +1.407.380.6080
Support: +1.407.482.6925
General E-mail: info@gta.com
Support E-mail: support@gta.com
Website: http://www.gta.com

1st Printing: February 2002

Introduction

Configuring a VPN for GNAT Box and SonicWall 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. It is written is with the assumption that the reader has a working knowledge of TCP/IP, SonicWall administration, and the GNAT Box systems.

To configure the GTA Firewall for VPN, use GBAdmin or the Web Interface. The examples given in this documentation use GBAdmin. To configure the SonicWall, use the SonicWall Web Admin.

Contact information

GTA's direct customers in the USA should call, fax or e-mail GTA using the contact numbers on the previous page (Contents). Other customers should contact their vendor.

Required VPN Settings: GTA Firewall and SonicWALL Pro

Mode:	IKE
ESP:	DES or 3DES
Hash:	SHA-1
Phase II Key Group:	Diffie-Hellman 1
Phase II Key Group:	ANY

Addresses used in examples

GTA Firewall IP Addresses

GTA Firewall External Interface:	199.120.225.76
GTA Firewall Protected Network:	192.168.254.0/24

SonicWall IP Addresses:

SonicWall External Interface:	199.120.225.90
SonicWall Protected Network:	10.10.5.0/24

GTA Firewall to SonicWall Pro Configuration

In order to use the GTA Firewall VPN, four functional areas must be configured. VPN creation requires setting up standard VPN Objects which can be used as the basis for VPN Authorization, forming a link between the GTA Firewall and another firewall.

- Objects>VPN Objects
- Authorization>VPN
- Remote Access Filters
- IP Pass Through Filters

Authorization>Users is currently for mobile VPNs only.

Create a VPN Object

To create a VPN Object, select Objects>VPN Objects from the menu. Insert a new VPN Object by clicking the plus ✚ icon to insert row. A new line item will appear beneath the existing VPN Objects.

Use the field table below as a quick reference for VPN Object field examples.

1. Enter a name and description.
2. Select the Interface Object for the local gateway from the dropdown menu (the name of the GTA Firewall external interface.) The default External interface is named **EXTERNAL**.
3. Enter the IP Address/Mask for the GTA Firewall's Protected Network: 192.168.254.0/24, or select the Object for the GTA Firewall's Protected Network.
4. Leave Require Mobile Authentication and Force Mobile Protocol ***unchecked***.
5. Configure Phase I by entering Exchange Mode: **Main**; Encryption (ESP): **DES**; Hash: **SHA-1**; Key Group: **Diffie-Hellman Group 1**.
6. Configure Phase II by entering Encryption (ESP): **DES**; Hash: **SHA-1**; Key Group: **ANY.**
7. Save VPN Object by clicking the single disk icon 🖫 on the toolbar to save the current section.

VPN Object Fields–Example

Disable:	Unchecked to enable this VPN Object
Name:	IKE - GB- SW VPN
Description:	GNAT Box to SonicWall VPN Object
Local Gateway:	EXTERNAL (199.120.225.76, GTA Firewall External Interface)
Local Network:	Protected Network (192.168.254.0/24, GTA Firewall)
Mobile Authentication:	Unchecked
Force Mobile Protocol:	Unchecked

Phase I

Exchange Mode:	Main	
Encryption (ESP):	DES	
Hash:	SHA-1	
Key Group:	Diffie-Hellman Group 1	

Phase II

Encryption (ESP):	DES	
Hash:	SHA-1	
Key Group:	ANY	(Select “ANY,” not a specific group)

VPN Authorization

To authorize a VPN connection, select Authorization>VPNs from the menu. Insert a new VPN by clicking the plus ✚ icon to insert row. A new line item will appear beneath any existing VPNs. Use the field table below as a quick reference for VPN field examples.

1. Select the IKE key exchange type.
2. Enter a description.
3. Leave the Identity field **blank**.
4. Select the VPN Object created in the previous section.
5. Enter the IP Address of the remote gateway (**199.120.225.90**) (SonicWALL external interface).
6. Enter the IP Address/Mask or Object that contains the network behind the SonicWALL Pro firewall in the Remote Network field (10.10.5.0/24).
7. Enter the pre-shared secret (pre-shared key must be the same on both systems).
8. Save VPN by clicking the single disk icon 🖫 on the toolbar to save the current section.

VPN Fields–Example

Disable:	Unchecked to enable this VPN	
Key exchange:	IKE	
Description:	GNAT Box to Sonic Wall VPN	
Identity:	***Leave blank***	
VPN Object:	IKE - GB- SW VPN	
Remote Gateway:	199.120.225.90	(SonicWALL Pro External Interface)
Remote Network:	10.10.5.0/24	(SonicWALL Pro Protected Network)

Phase I*

Preshared Secret:	A preshared secret key identical to that on the SonicWALL Pro

* Note that Phase II was fully configured in VPN Objects and does not appear in VPN Authorization.

Create Remote Access Filters

When using IKE, create two Remote Access filters; one for the ESP Tunnel (IP protocol 50) and one for IKE access on UDP/500. These filters can be created automatically by defaulting the Remote Access Filters. Be aware that using the default filters option will overwrite existing filters.

```
1. Description: VPN: Allow ESP connections From GNAT Box to SonicWall IKE VPN.
   Type: Accept Interface: ANY Protocol: 50
   Source IP: 199.120.225.90/32
     Port––Blank or 0
   Destination IP: 199.120.225.76/32
     Port––Blank or 0
2. Description: VPN: Allow IKE connections From GNAT Box to FW1 IKE VPN.
   Type: Accept Interface: ANY Protocol: UDP
   Source IP: 199.120.225.90/32
     Port––Blank or 0
   Destination IP: 199.120.225.76/32
     Port––500
```

> ***Note:*** *Wherever an IP address is used, an appropriate object can be selected from the dropdown menu. Objects may be created by default or by the user.*

Create IP Pass Through Filters

The example filters below allow all access between the SonicWALL and GTA Firewall networks. Typically, single inbound and outbound IP Pass Through filters are created for a VPN, but multiple filters may be required to conform to the local security policy.

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 local host outbound access to any remote host for any protocol at any time, or as narrow as allowing only a specific local host outbound access to a specific remote host for a given protocol at a specific time.

Generally, an inbound IP Pass Through filter is also created to allow the remote side of the VPN access to the local protected network. This filter does not have to be the same as an outbound filter.

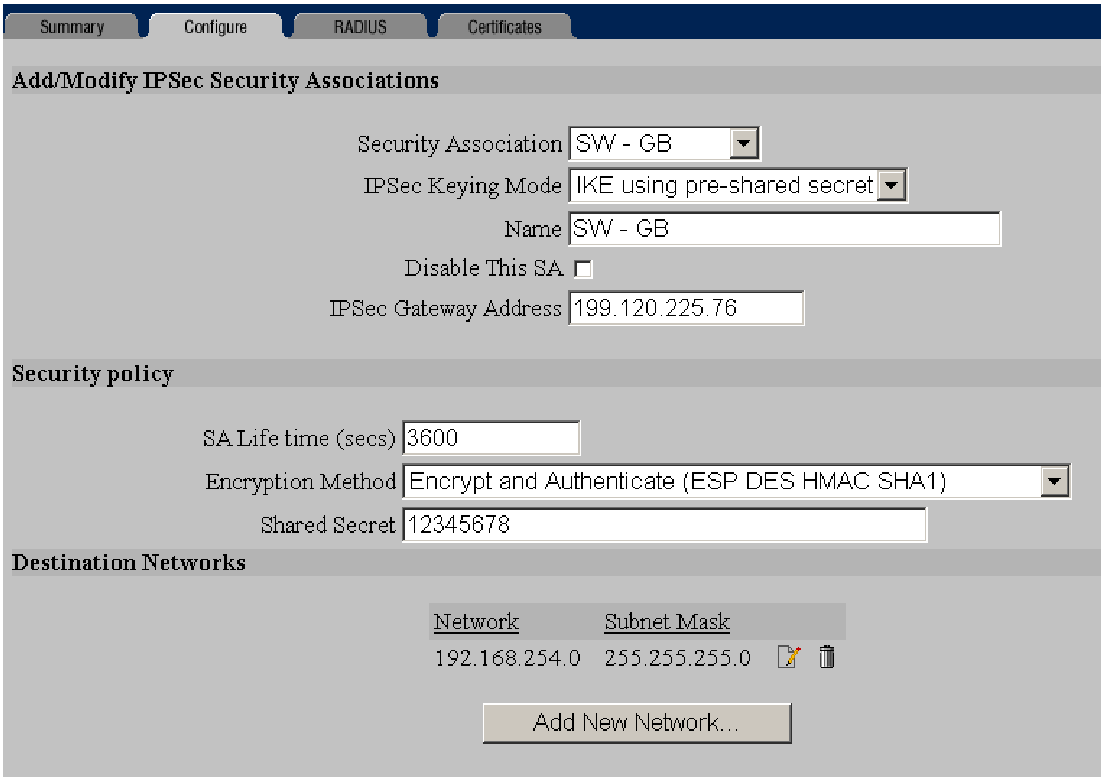
```
1. Description: VPN, inbound connections (GNAT Box to SonicWall VPN).
   Type: Accept Interface: “EXTERNAL” Protocol: ALL
   Source IP: 10.10.5.0/24
     Port––Blank or 0
   Destination IP: 192.168.254.0/24
     Port––Blank or 0
```

```
2. Description: VPN, Outbound connections (GNAT Box to SonicWall VPN).
   Type: Accept Interface: “PROTECTED” Protocol: ALL
   Source IP: 192.168.254.0/24
     Port--Blank or 0
   Destination IP: 192.168.254.0/24
     Port--Blank or 0
```

> ***Note:*** *For more information about configuring a GTA Firewall VPN, see the* GNAT Box User’s Guide.

SonicWALL Pro to GTA Firewall Configuration

Follow these steps to establish an IKE VPN between a SonicWALL Pro and a GTA Firewall. Log onto SonicWALL Web Administration. Select the **VPN** section., and click on the **Configure** tab. Most SonicWALL VPN configuration is completed on this screen.



Add/Modify IPSec Security Associations

Security Association: SW - GB
IPSec Keying Mode: IKE using pre-shared secret
Name: SW - GB
Disable This SA: □
IPSec Gateway Address: 199.120.225.76

Security policy

SA Life time (secs): 3600
Encryption Method: Encrypt and Authenticate (ESP DES HMAC SHA1)
Shared Secret: 12345678

Destination Networks

Network	Subnet Mask
192.168.254.0	255.255.255.0

Configure Tab in SonicWALL Web Administration

Add/Modify IPSec Security Associations

1. For Security Association, select **“Add New SA**.” In the resulting field, enter the name used to identify the VPN.
2. Select “IKE using preshared secret” for the IPSec Keying Mode.
3. In the IPSEC Gateway field, enter the IP Address of the External Interface of the GTA Firewall.

Security policy

1. Enter 3600 for the “SA Life time (secs).” (The maximum SA life for a GTA Firewall VPN is 3600 seconds in Phase II.)
2. Select “Encrypt and Authenticate” for Encryption Method. (ESP, DES, and HMAC SHA-1)
3. Enter the pre-shared secret (pre-shared key must be the same on both systems).

Configuration Tab Fields

Add/Modify IPSec Security Associations

Security Association:	Add New SA
IPSec Keying Mode:	IKE using preshared secret
Name:	SW-GB VPN
Disable this SA:	Leave unchecked
IPSec Gateway:	199.120.225.76 (External Interface of the GNAT Box system.)

Security Policy

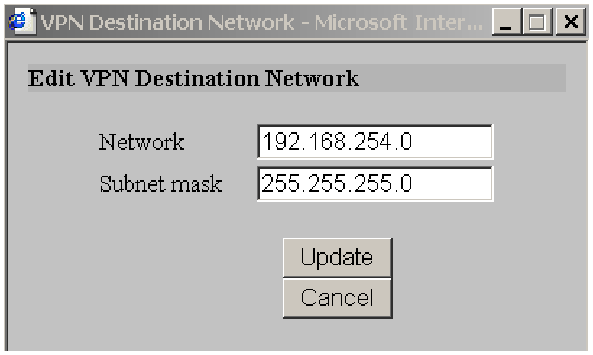
SA Lifetime (secs):	3600
Encryption Method:	Encrypt and Authenticate (ESP DES HMAC SHA-1)
Shared secret:	A preshared secret key identical to that on the GTA Firewall

Destination Networks

(Add New Network button)

Destination Networks

1. Click on the **Add New Network** button. Enter the IP Address of the network behind the GTA Firewall in the **Network** field. In our example this is 192.168.254.0.
2. Enter the appropriate Subnet Mask. In our example this is 255.255.255.0. (Comparable to GNAT Box /24 suffix)



Edit VPN Destination Network

Network: 192.168.254.0

Subnet mask: 255.255.255.0

VPN Destination Network dialog box

VPN Destination Network Dialog Box Fields

Edit VPN Destination Network

Network:	192.168.254.0	(The network behind the GTA Firewall)
Subnet Mask:	255.255.255.0	(Comparable to GNAT Box /24 suffix)

Once the information is entered, click **Update**. This will bring up the previous screen, the **Configure** tab. Here again, click **UPDATE**, located in the lower left hand corner below the illustrated screen.

This completes the GTA Firewall to SonicWALL Pro VPN connection.