

Technical Document

Creating a VPN

GTA Firewall
to
WatchGuard Firebox SOHO 6



Contents

INTRODUCTION	1
Supported Encryption and Authentication Methods	1
IP Addresses Used in Examples	1
Documentation	2
Additional Documentation	2
GTA FIREWALL CONFIGURATION	4
Configuring the Encryption Objects	4
Configuring the VPN Object	5
Configuring the IPSec Tunnel	6
WATCHGUARD FIREWALL CONFIGURATION	8
Configuring General Settings	8
Configuring Phase 1	9
Configuring Phase 2	10

Introduction

This document is written for the firewall administrator who has both a GTA firewall and a WatchGuard Firebox SOHO 6 operating on a network that requires a VPN (Virtual Private Network) to utilize both firewalls. Documentation was developed using a GTA firewall running GB-OS 4.0 and a WatchGuard Firebox SOHO 6 running version 6.1.43 Boot ROM 4.14. This document is written under the assumption that the reader has a strong working knowledge of TCP/IP, GB-OS and Firebox SOHO 6 administration.



Note

The example configuration in this document assumes both firewalls have static IP addresses.

Encryption and Authentication Methods

The following methods of encryption and authentication are supported for this configuration:

Table 1.1: Supported Encryption and Authentication Methods	
<i>Field Name</i>	<i>Field Value</i>
Supported Encryption	DES or 3DES
Supported Authentication	SHA1 or MD5
Supported Key Groups	Diffie-Hellman Group 1 or 2

IP Addresses Used in Examples

The following IP addresses are used as examples in this document:

Table 1.2: IP Addresses Used in Examples	
<i>Field Name</i>	<i>Field Value</i>
GTA Firewall	
External	199.120.255.78
Protected Network	192.168.71.0/24
WatchGuard Firebox SOHO 6	
External	199.120.225.77
Protected Network	192.168.70.0/24

Documentation

A few conventions are used in this document 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

Additional Documentation

For instructions on installation, registration and setup of your GTA firewall, see the *GB-OS User's Guide*. For VPN setup and example configurations, see the *VPN Option 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. A free copy of the program can be obtained from www.adobe.com.



GTA Firewall Configuration

To configure your GTA firewall, log into the Web interface using an administrative account and follow the instructions below to setup up a GTA firewall to WatchGuard Firebox SOHO 6 VPN.

Configuring the GTA firewall requires the completion of the following steps:

1. [Configuring the Encryption Objects](#)
2. [Configuring the VPN Object](#)
3. [Configuring the IPSec Tunnel](#)



Note

GTA recommends that the NTP service be enabled on any GTA firewall using a VPN.

Configuring the Encryption Objects

To configure the encryption objects, navigate to **Configuration>System>Object Editor>Encryption Objects** and click the **New** icon. Doing so will display the EDIT ENCRYPTION OBJECT screen.

Enter the following settings to define the encryption object to be used during phase 1 of the VPN.

Disable:

Name: Phase 1 SOHO 6

Description: Phase 1 encryption object for GTA firewall to SOHO 6 VPN

Encryption Method: 3des

Hash Algorithm: hmac-sha1

Key Group: Diffie-Hellman group 1 (768 bits)

Figure 2.1: Creating the Phase 1 Encryption Object

Table 2.1: Configuring the Phase 1 Encryption Object	
Field Name	Field Value
Disable	Unchecked
Name	Phase 1 SOHO 6
Description	Phase 1 encryption object for GTA firewall to SOHO 6 VPN
Encryption Method	<3DES>
Hash Algorithm	<HMAC-SHA1>
Key Group	<Diffie-Hellman Group 1 (768 bits)>

Click **OK** to return the ENCRYPTION OBJECTS screen and click the **New** icon to create the encryption object to be used during phase 2 of the VPN.

Figure 2.2: Creating the Phase 2 Encryption Object

Table 2.2: Configuring the Phase 2 Encryption Object	
Field Name	Field Value
Disable	Unchecked
Name	Phase 2 SOHO 6
Description	Phase 2 encryption object for GTA firewall to SOHO 6 VPN
Encryption Method	<3DES>
Hash Algorithm	<HMAC-SHA1>
Key Group	<Diffie-Hellman Group 2 (1024 bits)>

Click **OK** to return to the ENCRYPTION OBJECTS screen and click the **Save** icon to save the new encryption objects to the GTA firewall's configuration.

Next, the VPN object must be configured.

Configuring the VPN Object

To configure the VPN object to be used by the connection, navigate to **Configuration>System>Object Editor>VPN Objects** and click the **New** icon. Doing so will display the EDIT VPN OBJECT screen.

Figure 2.3: Configuring the VPN Object

Table 2.3: Configuring the VPN Object	
Field Name	Field Value
Disable	Unchecked
Name	SOHO 6 VPN Object
Description	VPN Object used in the GTA firewall to SOHO 6 VPN
Phase I	
Exchange Mode	<Main>
Encryption Object	<Phase 1 SOHO 6> As defined in Configuring the Encryption Objects .
Advanced	
Force Mobile Protocol	Unchecked
Force NAT-T Protocol	Unchecked
Lifetime	120 minutes
DPD Interval	30 seconds
Phase II	
Encryption Object	<Phase 2 SOHO 6> As defined in Configuring the Encryption Objects .
Advanced	
Lifetime	60 minutes

Click **OK** to return to the VPN OBJECTS screen and click the **SAVE** icon to save the new VPN object to the GTA firewall's configuration.

Next, the IPSec tunnel must be configured.

Configuring the IPSec Tunnel

To configure the IPSec tunnel, which will be utilizing the configured encryption and VPN objects, navigate to **Configuration>VPN>IPSec Tunnels** and click the **New** icon. Doing so will display the EDIT IPSEC TUNNEL screen.

The screenshot shows the 'EDIT IPSEC TUNNEL' configuration interface. At the top, there is a 'Disable' checkbox which is unchecked. Below it is a 'Description' field. The 'IPSec Key Mode' is set to 'IKE' with radio buttons for 'IKE' and 'Manual'. The 'VPN Object' is set to 'SOHO 6 VPN Object' via a dropdown menu. The 'Pre-shared Secret' is set to 'ASCII' and 'abcdef123456'. The 'Local' section has a 'Gateway' dropdown set to 'EXTERNAL' and a 'Network' dropdown set to 'Protected Networks'. The 'Remote' section has a 'Gateway' text field with '199.120.225.77' and a 'Network' dropdown set to '<USER DEFINED>' with a text field containing '192.168.70.0/24'. Both the Local and Remote sections have an 'Advanced' button with a dropdown arrow.

Figure 2.4: Configuring the IPSec Tunnel

Table 2.4: Configuring the IPSec Tunnel	
Field Name	Field Value
Disable	Unchecked
Description	GTA firewall to WatchGuard Firebox SOHO 6 VPN
IPSec Mode	<IKE>
VPN Object	<SOHO 6 VPN Object > As defined in Configuring the VPN Object .
Pre-shared Secret	adcdef123456 The pre-shared secret must match on the WatchGuard SOHO 6 firewall.
Local	
Gateway	<External> This is the external network's logical interface.
Network	<Protected Networks> This is the protected network's logical interface.
Advanced	
Identity	<IP Address>
Remote	
Gateway	199.120.225.77
Network	<USER DEFINED>, 192.168.70.0/24
Advanced	
Identity	<IP Address>

Click **OK** to return to the IPSEC TUNNELS screen. Under the **ADVANCED** tab, ensure that the **AUTOMATIC POLICIES** checkbox is enabled. By enabling automatic policies, the GTA firewall will generate the necessary VPN policies to allow traffic between the GTA firewall and the WatchGuard Firebox SOHO 6.

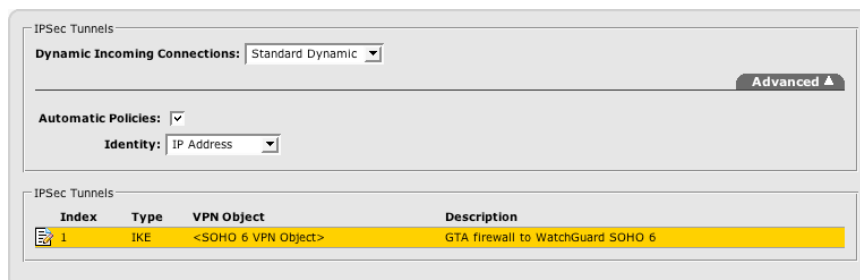


Figure 2.5: Enabling Automatic Policies

Click the **SAVE** button to apply the VPN configuration to your GTA firewall. Next, it is necessary to configure the WatchGuard Firebox SOHO 6.

WatchGuard Firewall Configuration

To configure your WatchGuard Firebox SOHO 6, log into the web interface using an administrative account and follow the instructions below to setup up a GTA firewall to WatchGuard Firebox SOHO 6 VPN.

Once logged into the firewall, navigate to **VPN>Manual VPN** and click **Add**. Doing so will display the **ADD GATEWAY** screen.

Configuring General Settings

General settings for the **ADD GATEWAY** screen consist of the name for the VPN connection and the shared key (pre-shared secret). The shared key must match the defined pre-shared secret on the GTA firewall.

Table 3.1: Configuring General Settings	
Field Name	Field Value
Name	GTA This is the user defined name for the VPN.
Shared Key	abcdef123456 This field must match the pre-shared secret entered when configuring the GTA firewall's IPSec tunnel.



VPN > Manual VPN
Edit Gateway

Name

Shared Key

Figure 3.1: Configuring General Settings

Configuring Phase 1

Under the PHASE 1 SETTINGS section of the screen, enter the following information:

Table 3.2: Configuring Phase 1 Settings	
Field Name	Field Value
Mode	<Main Mode>
Local ID	199.120.225.77 The WatchGuard Firebox SOHO 6's external IP address. Set the TYPE to <IP Address>.
Remote ID	199.120.225.78 The GTA firewall's external IP address. Set the TYPE to <IP Address>.
Authenticaton Algorithm	<SHA1-HMAC> or <MD5>
Negotiation Expiration in Kilobytes	0
Negotiation Expiration in Hours	2 Value should be less than or equal to the GTA firewall's PHASE 1 LIFETIME.
Diffie-Hellman Group	<1>
Enable Perfect Forward Secrecy	Checked
Generate IKE Keep Alive Messages	Unchecked

Phase 1 Settings

Mode: Main Mode

Local ID: 199.120.225.77 Type: IP Address

Remote ID: 199.120.225.78 Type: IP Address

Authentication Algorithm: SHA1-HMAC

Encryption Algorithm: 3DES-CBC

Negotiation expiration in kilobytes: 0

Negotiation expiration in hours: 2

Diffie-Hellman Group: 1

Enable Perfect Forward Secrecy

Generate IKE Keep Alive Messages

Figure 3.2: Configuring Phase 1

Configuring Phase 2

Under the Phase 2 Settings section of the screen, enter the following information:

Table 3.3: Configuring Phase 1 Settings	
Field Name	Field Value
Authentication Method	<SHA1-HMAC>
Encryption Algorithm	<3DES-CBC>
Negotiation Expiration in Kilobytes	0
Negotiation Expiration in Hours	1 Value should be less than or equal to the GTA firewall's PHASE 2 LIFETIME.
Configure Local and Remote Network	
Local Network	192.168.70.0/24 The IP address of the WatchGuard Firebox SOHO 6's protected network.
Remote Network	192.168.71.0/24 The IP address of the GTA firewall's protected network.

Figure 3.3: Configuring Phase 2

Once all the necessary information has been entered, click **SUBMIT** to commit the configuration. Your GTA firewall to WatchGuard Firebox SOHO 6 VPN is now complete. You can test the VPN's functionality by pinging from a host on one protected network to a host on the other firewall's protected network.

Copyright

© 1996-2006, 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 GTA authorized 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

GNAT Box, GB Commander and Surf Sentinel are registered trademarks of Global Technology Associates, Incorporated. GB-OS, RoBoX, GB-Ware and Firewall Control Center are trademarks of Global Technology Associates, Incorporated. Global Technology Associates and GTA are registered service marks of Global Technology Associates, Incorporated.

The GTA Mobile VPN Client is licensed from TheGreenBow.

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 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/>.

SurfControl is a registered trademark of SurfControl plc. Some products contain technology licensed from SurfControl plc.

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

Kaspersky Lab and Kaspersky Anti-Virus is licensed from Kaspersky Lab Int. Some products contain technology licensed from Kaspersky Lab Int.

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

