

Technical Document

Creating a VPN

GTA Firewall
to
Cisco PIX 501



Contents

INTRODUCTION	1
Encryption and Authentication Methods	1
IP Addresses Used in Examples	1
Documentation	2
Additional Documentation	2
GTA FIREWALL CONFIGURATION	4
Configuring the Encryption Object	4
Configuring the VPN Object	5
Configuring the IPSec Tunnel	6
CISCO PIX CONFIGURATION	8

Introduction

This document is written for the firewall administrator who has both a GTA firewall and a Cisco PIX 501 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 Cisco PIX 501 running firmware version 6.1(1). This document is written under the assumption that the reader has a strong working knowledge of TCP/IP, GB-OS and Cisco firewall 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
Cisco PIX 501	
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 Cisco PIX 501.

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

1. [Configuring the Encryption Object](#)
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 Object

To configure the encryption object, 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 by the VPN.

Disable:

Name: Cisco Encryption

Description: Phase 1 and 2 encryption object for GTA firewall to Linksys VPN

Encryption Method: des

Hash Algorithm: hmac-md5

Key Group: Diffie-Hellman group 2 (1024 bits)

Figure 2.1: Creating the Encryption Object

Table 2.1: Configuring the Encryption Object	
Field Name	Field Value
Disable	Unchecked
Name	Cisco Encryption
Description	Encryption object for GTA firewall to Cisco PIX VPN
Encryption Method	<DES>
Hash Algorithm	<HMAC-MD5>
Key Group	<Diffie-Hellman Group 1 (768 bits)>

Click **OK** to return to the ENCRYPTION OBJECTS screen and click the **Save** icon to save the new encryption object 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 2.2: Configuring the VPN Object

Table 2.2: Configuring the VPN Object	
Field Name	Field Value
Disable	Unchecked
Name	Cisco VPN Object
Description	VPN Object used in the GTA firewall to Cisco VPN
Phase I	
Exchange Mode	<Main>
Encryption Object	<Cisco Encryption> As defined in Configuring the Encryption Object .
Advanced	
Force Mobile Protocol	Unchecked
Force NAT-T Protocol	Unchecked
Lifetime	90 minutes
DPD Interval	30 seconds
Phase II	
Encryption Object	<Cisco Encryption> As defined in Configuring the Encryption Object .
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.

Figure 2.3: Configuring the IPsec Tunnel

Table 2.3: Configuring the IPsec Tunnel	
Field Name	Field Value
Disable	Unchecked
Description	GTA firewall to Cisco PIX 501 VPN
IPsec Mode	<IKE>
VPN Object	<Cisco VPN Object > As defined in Configuring the VPN Object .
Pre-shared Secret	adcddef123456 The pre-shared secret must match on the Cisco PIX 501.
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 This is the IP address of the Cisco PIX 501's remote gateway.
Network	<USER DEFINED>, 192.168.70.0/24 This is the IP address of the Cisco PIX 501's protected network.
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 Cisco PIX 501.

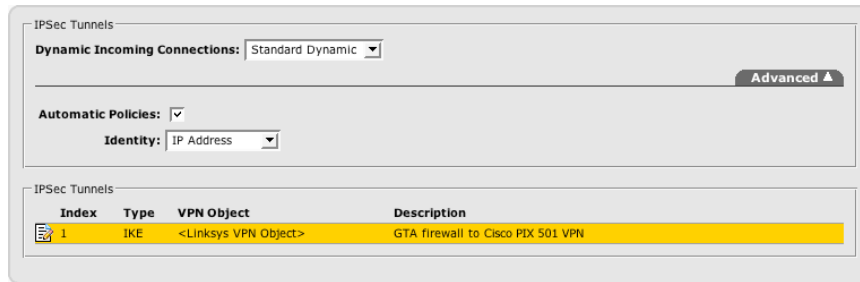


Figure 2.4: Enabling Automatic Policies

Click the **SAVE** button to apply the VPN configuration to your GTA firewall. Next, it is necessary to configure the Cisco PIX 501.

Cisco PIX Configuration

To configure your Cisco PIX 501, you will need to use the firewall's command line interface. You can either use SSH, telnet or the Command Line Interface in the Cisco PIX device manager.



Note

For more information on configuring your Cisco firewall, consult Cisco's documentation.

In the following example from the Cisco PIX Command Line Interface, lines that begin with an exclamation point (!) are commented out.

```
! Add access list to pass local traffic from local network to remote network
access-list 160 permit ip 192.168.70.0 255.255.255.0 192.168.71.0 255.255.255.0
! Disables NAT for connections bound for remote network.
nat (inside) 0 access-list 160
! Tells the PIX to trust ipsec information
sysopt connection permit-ipsec
crypto ipsec transform-set gb-set esp-des esp-md5-hmac
crypto map gb-map 1 ipsec-isakmp crypto map gb-map 1 match address 160
! Sets VPN peer to Address, external interface of the GTA firewall
crypto map gb-map 1 set peer 199.120.225.76
crypto map gb-map 1 set transform-set gb-set
! Set lifetime to a max of 3600 seconds
crypto map gb-map 1 set security-association lifetime seconds 3600
crypto map gb-map interface outside
isakmp enable outside
! Set pre-shared keys for VPN
isakmp key abcdef123456 address 199.120.225.78 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 5400
```

The Cisco PDM does not support the “nat (inside) 0 access list” command. The following dialog box will appear. This behavior is expected; click Yes to continue.



Figure 3.1: Cisco PIX Response to Unsupported Command

Your GTA firewall to Cisco PIX 501 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 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

