Technical Document

TD VPN-GB-PIX-03

GNAT Box VPN and VPN Client

with SoftRemoteLT from SafeNet, Inc.

GTA Firewall – Cisco PIX Firewall 501

Configuring an IPSec VPN with IKE

GTA Firewall Software version 3.4
Cisco PIX 505 v 6.1(1)

Global Technology Associates, Inc.

Copyright

GTA Reporting Suite Product Guide **September 2003**

Technical Support

GTA includes 30 days installation support from the day you receive the initial shipment. 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: +1.407.482.6925 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

GNAT Box is a registered trademark of Global Technology Associates, Incorporated. RoBoX and Surf Sentinel are trademarks of Global Technology Associates, Incorporated.

GTA acknowledges all trademarks appearing in this document. This product includes software developed by the University of California, Berkeley and its contributors. Netscape Navigator is a trademark of Netscape Communications Corporation. Internet Explorer is a trademark of Microsoft Corporation. WELF and WebTrends are trademarks of NetIQ. 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
Lead Development Team: Larry Baird, Richard Briley, Jim Silas, Brad Plank.
Technical Consulting: David Brooks. **Documentation:** Mary Swanson.

Contents

Introduction

GTA Firewall – Cisco PIX 501 Firewall: Configuring an IPSec VPN is written for the administrator who has both of these systems operating on a network and requires a VPN (virtual private network) to communicate between the firewalls. It is written is with the assumption that the reader has a working knowledge of TCP/IP, Cisco PIX administration and GTA Firewall administration, including basic VPN configuration. This manual was developed using GNAT Box 3.2.5s and Cisco PIX 501 Firewall version 6.1(1).

The **GNAT Box VPN and VPN Client Feature Guide** is the main reference for GTA Firewall VPN configuration. See other documented VPN setups at www.gta.com, including interoperation with these vendors' solutions: Cisco PIX, NetScreen, WatchGuard, SonicWall and SnapGear.

VPN interoperability should be possible with any GTA Firewall that supports IKE. For the best support, the latest version of the GNAT Box Software is recommended.

GTA Firewall Example VPN Configuration

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 Network	192.168.1.0/24

Cisco PIX Example VPN Configuration

To configure the Cisco PIX, (referred to in this document as "PIX") use the Cisco PIX command line interface (CLI). This guide uses the following IP addresses as examples for a PIX configuration:

Firebox External Interface	199.120.225.90
Firebox Protected Network	10.10.11.0/24

Encryption Methods

As Phase I and Phase II VPN are not differentiated on the PIX, use the same encryption methods, hash and key group in Phase I and II of the VPN on the GTA Firewall. In addition, the policy lifetime on a Cisco PIX cannot be longer than 3600 seconds. If the SA life is greater than 3600 seconds, you MAY experience problems when the systems re-negotiate the keys.

Common Encryption Methods

GTA Firewalls have a number of encryption algorithms that do not have corresponding methods on the PIX. Use the encryption methods below, common to both firewall systems, to configure both firewalls for a VPN connection.

Mode	IKE
ESP	DES or 3DES
Hash	MD5 or SHA-1
Key Group	Diffie-Hellman group 1 or 2

GTA Firewall 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	Enable. (Uncheck).
Name	Enter a name for this object. (GTA Firewall - PIX VPN Object)
Description	Enter a description of the VPN object. (GTA Firewall - PIX IKE VPN Object)
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	MD5.
Key Group	Diffie-Hellman Group 2.
	Phase II
Encryption (ESP)	DES.
Hash	MD5.
Key Group	Diffie-Hellman Group 2.

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 - PIX VPN Authorization)
Identity	Leave blank.
VPN Object	Select the VPN object created previously. (GTA Firewall - PIX IKE VPN)
Remote Gateway	Select the IP address or object that references the PIX External Network interface. (199.120.225.90)
Remote Network	Select the IP Address or object that references the PIX Protected Network. (199.170.225.0/24)
Preshared Secret	Preshared secret/key entered on the PIX 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	Description	VPN: Allow ESP connections from GTA Firewall to PIX VPN.
	Type	Accept

	Priority	Notice
	Interface	ANY
	Protocol	50 (ESP)
	Source	199.120.225.90
	Source Port	Blank
	Destination	External interface object (199.120.225.76)
	Destination Port	Blank
2	Description	VPN: Allow IKE connections from GTA Firewall to PIX VPN.
	Type	Accept
	Priority	Notice
	Interface	ANY
	Protocol	UDP
	Log	Default
	Source	199.120.225.90
	Source Port	Blank
	Destination	External interface object (199.120.225.76)
	Destination Port	500

IP Pass Through Filters

Example filters below allow all access between the PIX and GTA Firewall networks. Set these filters according to your corporate 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 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	Description	VPN: Allow inbound connections from GTA Firewall to PIX VPN.
	Type	Accept
	Priority	Notice
	Interface	External

	Protocol	ANY
	Source	10.10.11.0/24
	Source Port	Blank
	Destination	192.168.1.0/24
	Destination Port	Blank
2	Description	VPN: Allow outbound connections GTA Firewall to PIX VPN.
	Type	Accept
	Priority	Notice
	Interface	Protected
	Protocol	ANY
	Source	192.168.1.0/24
	Source Port	Blank
	Destination	10.10.11.0/24
	Destination Port	Blank

Note

Wherever an IP address is used in the filters, you can substitute an appropriate address object selected from the dropdown menu.

Cisco PIX Configuration

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

For more information on Cisco PIX VPN set up please see Cisco PIX support.

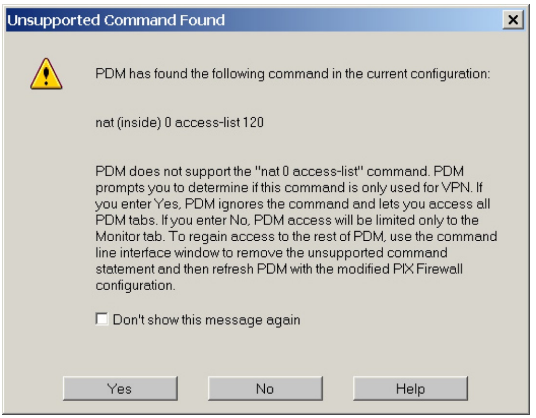
In the following example from the Cisco PIX CLI, the lines that begin with an exclamation point symbol "!" are commented out.

```
! Add access list to pass local traffic from local network to
remote network

access-list 160 permit ip 10.10.11.0 255.255.255.0 192.168.1.0
255.255.255.0

!

! Disables NAT for connections bound for remote network. Matches
same accesslist as

! vpn, vpn WILL NOT WORK without this

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 3600

crypto map gb-map interface outside

!

isakmp enable outside
```

```
! set pre-shared keys for VPN

isakmp key 12345678 address 199.120.225.76 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 3600
```

Note

The Cisco PDM does not support the “Nat (inside) 0 access-list” Command. You will see the following dialog box appear. Just select “Yes” to continue using the PDM.



PIX response to “NAT (inside) 0 access-list” command

Example Script

Below is an editable script that can be used to set up a GTA Firewall to PIX VPN. Lines that begin with an exclamation point symbol “!” are commented out. You can substitute the IP Address for your VPN configuration.

```
! access list to pass local traffic (xxx.111.xxx.xxx to remote vpn

! network, xxx.222.xxx.xxx)

access-list 160 permit ip XXX.111.XXX.XXX 255.255.255.0
XXX.222.XXX.XXX 255.255.255.0

!
```

```
! disables NAT for connections bound for VPN. matches same
accesslist as
! vpn, vpn WILL NOT WORK without this
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 xxx.xxx.xxx.xxx
crypto map gb-map 1 set peer XXX.XXX.XXX.XXX
Crypto map gb-map 1 set transform-set gb-set
crypto map gb-map 1 set security-association lifetime 3600
crypto map gb-map interface outside
!
isakmp enable outside
! using preshared keys, sets key ******** for peer xxx.xxx.xxx.xxx
isakmp key ******** address XXX.XXX.XXX.XXX 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 3600
```