

# Technical Document

**TD VPN-GB-CP-02**

## **GNAT *Box* VPN and VPN Client**

*with SoftRemoteLT from SafeNet, Inc.*

### **GTA Firewall – Check Point Firewall-1**

Configuring an IPSec VPN with IKE

---

GNAT Box System Software version 3.3.2

Firewall-1 v 4.1



# Copyright

© 1996-2002, Global Technology Associates, Incorporated (GTA). All rights reserved.

GTA acknowledges all trademarks appearing in this document. This product includes software developed by the University of California, Berkeley, and its contributors. 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.

## 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](mailto:info@gta.com)  
Support [support@gta.com](mailto:support@gta.com)

## Document Information

Technical Document

GTA Firewall – Check Point Firewall-1, Configuring an IPSec VPN with IKE December 2002

# Table of Contents

<b>Introduction</b>	1
GTA Firewall Example VPN Configuration	1
Firewall-1 Example VPN Configuration	1
Common Encryption Methods	1
<b>GTA Firewall Configuration</b>	2
VPN Object	2
VPN Authorization	3
Remote Access Filters	3
IP Pass Through Filters	4
<b>Firewall-1 Configuration</b>	5
Objects	5
CP-Protected_Network	6
CP-External_Interface	7
GB-Protected_Network	8
GB-External_Interface	8
Preshared Secrets	9
Rules	10
External Interfaces	10
Source	11
Destination	11
Action	12
Track	12
Install On	13
Allow and Encrypt Connections Rule	13
Source	14
Destination	14
Action (Phase II of VPN negotiation corresponds to steps 3 through 5.)	14
Track	15
Install On	15
Corporate Policy Rules	15
Default Rule	15
NAT Rule	15
Install New Policy	16
<b>Index</b>	19



---

# Introduction

**GTA FIREWALL – CHECK POINT FIREWALL-1: 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 with the assumption that the reader has a working knowledge of TCP/IP, Firewall-1 administration utilities and GTA Firewall administration, including basic VPN configuration.

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](http://www.gta.com), including interoperation with these vendors' solutions: Cisco PIX, NetScreen, WatchGuard, SonicWall and SnapGear.

## GTA Firewall Example VPN Configuration

To configure a GTA Firewall for VPN, use GBAAdmin or the Web Interface. The examples given in this documentation use GBAAdmin. 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

## Firewall-1 Example VPN Configuration

To configure the Firewall-1, (referred to in this document as "FW-1") use the Check Point Policy Editor. This guide uses the following IP addresses as examples for a FW-1 configuration:

External Interface	199.120.225.90
Protected Interface	199.170.225.1
Protected Network	199.170.225.0/24

## Common Encryption Methods

GTA Firewalls have a number of encryption algorithms that do not have corresponding methods on Firewall-1. The following encryption methods are common to both firewall systems. Use the encryption methods below to configure both firewalls for a VPN connection.

Mode	IKE
ESP	DES or 3DES
Hash	MD5 or SHA-1

# 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 - FW-1 VPN Object)
Description	Enter a description of the VPN object. (GTA Firewall - FW-1 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.
<b>Phase I</b>	
Exchange Mode	Main.
Encryption (ESP)	DES.
Hash	HMAC-MD5.
Key Group	Diffie-Hellman Group 2.
<b>Phase II</b>	

Encryption (ESP)	DES.
Hash	HMAC-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 - FW-1 VPN Authorization)
Identity	Leave blank.
VPN Object	Select the VPN object created previously. (GTA Firewall - FW-1 IKE VPN)
Remote Gateway	Select the IP address or object that references the FW-1 External Network interface. (199.120.225.90)
Remote Network	Select the IP Address or object that references the FW-1 Protected Network. (199.170.225.0/24)
Preshared Secret	Preshared secret/key entered on the FW-1 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 FW-1 IKE VPN.
	Type	Accept
	Interface	ANY
	Protocol	50
	Log	Default
	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 FW-1 IKE VPN.
	Type	Accept
	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 Firewall-1 and 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	Description	VPN: Allow inbound connections from GTA Firewall to FW-1 IKE VPN.
	Type	Accept
	Interface	External
	Protocol	ALL
	Log	Default
	Source	199.170.225.0/24
	Source Port	Blank
	Destination	192.168.1.0/24
	Destination Port	Blank
2	Description	VPN: Allow outbound connections GTA Firewall to FW-1 IKE VPN.
	Type	Accept



Interface	Protected
Protocol	ALL
Source	192.168.1.0/24
Source Port	Blank
Destination	199.170.225.0/24
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.

---

## Firewall-1 Configuration

The Firewall-1 configuration is based on the use of Objects. Once an object is defined, you apply rules to the firewall or the VPN. In order to establish an IKE VPN between a Firewall-1 and a GTA Firewall System, you will need to create at least four Objects. Then apply the appropriate rules as directed by your corporate security policy.

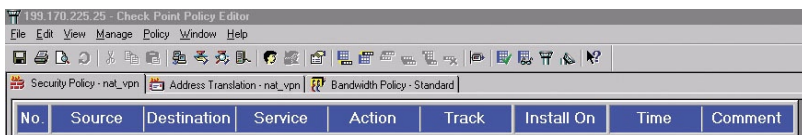
Below are the steps to perform on the Firewall-1 in order to create the appropriate Objects and rules for a GTA Firewall to Firewall-1 VPN.

### Objects

Listed below are examples of the Objects need for the VPN.

- CP-External\_Interface – IP address assigned to the External NIC the Firewall-1.
- CP-Protected\_Network – Internal FW-1 network or host to use the VPN.
- GB-External\_Interface – IP address assigned to the External NIC of the GTA Firewall system.
- GB-Protected\_Network – Internal GTA Firewall network or host to use the VPN.

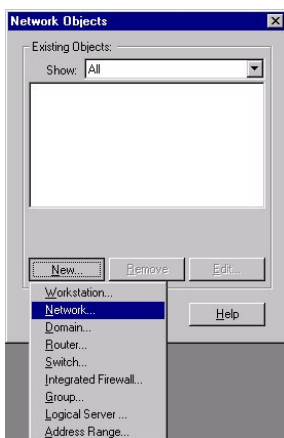
In addition to the four Objects, you will need to create at least three rules, and if you are using Address Translation (Network Address Translation or NAT), four rules. The fourth rule is used in the Address Translation section.



*Firewall-1 Menu Bar, Tabs and Security Policy Window header*

## CP-Protected\_Network

On the Menu Bar under the Manage menu, select Network Objects. The Network Objects Box will appear. Click New, and select Network.



*Network Objects screen and menu*

Define your Firewall-1 Internal Network Object as:

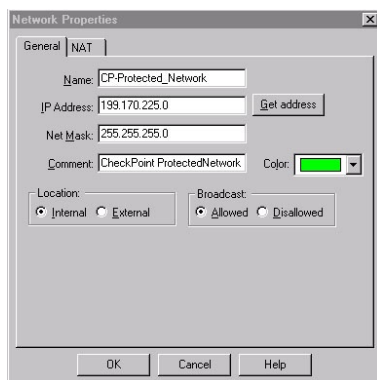
Name CP-Protected\_Network

IP Address 199.170.225.0

Mask 255.255.255.0

Location Internal

Broadcast Allowed



*Define Firewall-1 Protected Network*

## CP-External\_Interface

Return the focus to the Network Objects screen. Click New, and select Workstation.

1. Define the Firewall-1 External Interface Object as:

Name CP-External\_Interface

IP Address 199.120.225.90

Type Gateway

Modules Installed VPN-1 & Firewall-1

Location Internal

2. Click on the VPN tab under Workstation Properties and select IKE.

Encryption Scheme defined – Select IKE

Domain – Select CP-Protected\_Network

3. Phase I of VPN negotiation.

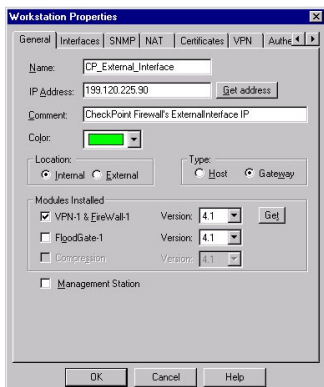
On the VPN tab under the Encryption schemes defined click Edit.

Support key exchange encryption with – Select DES

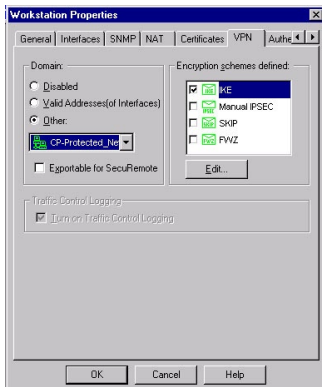
Support Data Integrity with – Select MD5

Support Authentication methods – Select Preshared Secret.

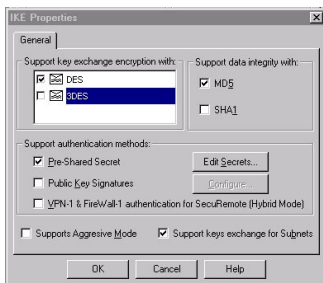
Check key exchange for Subnets.



Firewall-1 External Interface



Firewall-1 External Interface



Firewall-1 External Interface–Encryption scheme defined Edit

## GB-Protected\_Network

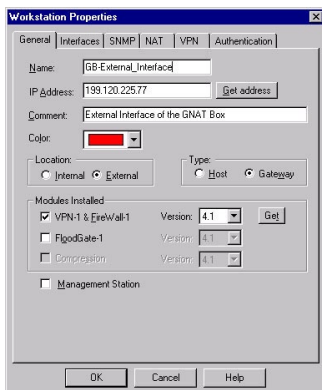
Return the focus to the Network Objects screen. Click New, and select Network. Define the GTA Firewall Internal Network Object:

Name	GB-Protected_Network
IP Address	192.168.1.0
Mask	255.255.255.0
Location	External
Broadcast	Allowed

## GB-External\_Interface

Return the focus to the Network Objects Box. Click New, and select Workstation.

1. Define the GTA Firewall External Interface Object as  
Name GB-External\_Interface  
IP Address 199.120.225.76  
Type Gateway  
Modules Installed VPN-1 & Firewall-1  
Location External
2. Click on the VPN tab under Workstation Properties and select IKE.  
Encryption Scheme defined – Select IKE  
Domain – Select GB-Protected\_Network
3. Phase I of VPN negotiation  
Under Encryption Scheme defined click Edit.  
Support key exchange encryption with – Select DES  
Support Data Integrity with – Select MD5  
Support Authentication methods – Select Preshared Secret.  
Check key exchange for Subnets.



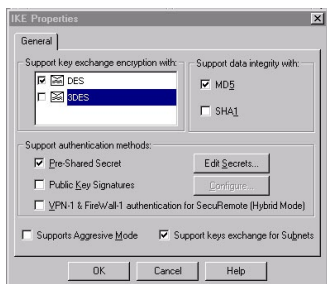
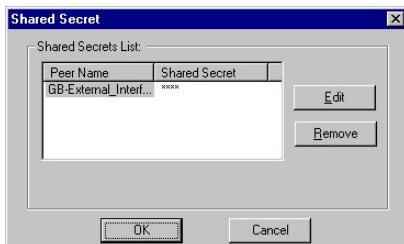
*GTA Firewall External Interface*

## Preshared Secrets

Preshared Secrets must be edited after the two gateways have been defined, as in the previous sections. This is part of Phase I of VPN negotiation.

1. Go back to the Network Objects screen by going to Menu Bar/Manage/Network Objects.
2. Select the gateway you wish to edit, either CP-External\_Interface or GB-External\_Interface, and click Edit. (You can use the Show drop down box to select only gateways.)
3. Click the VPN tab.

4. Under the Encryption schemes defined click Edit. This will take you to the IKE Properties screen. You have already selected Preshared Secret.
5. Click Edit Secrets.
6. Enter the number of the Preshared Secret and click Set. Then click OK to return to the previous screen.
7. Repeat for the other gateway.

*IKE Properties screen**Shared Secret screen*

## Note

You cannot edit the preshared secrets until you have defined at least the two gateways previously defined for the Firewall-1 and GTA Firewall interface.

## Rules

Add rules to connect Firewall-1 and GTA Firewall to using the External Interfaces; allow and encrypt connections between the Firewall-1 Protected Network and the GTA Firewall's Protected Network; any rules required by your corporate security policy; and then add the default rule. The Network Address Translation rule is created only if you are using NAT.

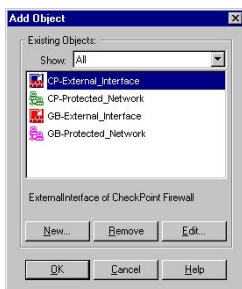
## External Interfaces

Add a new rule to allow Firewall-1 and GTA Firewall to connect using the External Interfaces by right-clicking on the Security Policy Window under the Security Policy tab. A blank rule will be created.

*Blank rule*

## Source

1. Right-click within Source cell to add a new target. Select CP-External\_Interface from the list of objects.



*List of Objects*

2. Repeat procedure to add GB-External\_Interface in the same cell under CP-External\_Interface.

### Note

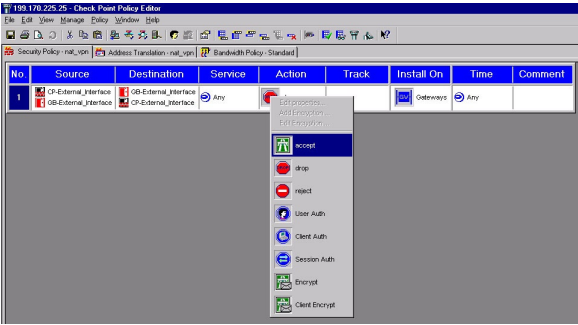
CP-External\_Interface must be above GB-External\_Interface. See example below.

## Destination

1. Right-click within Destination cell to add a new target. Select GB-External\_Interface from the list of objects.
2. Repeat procedure to add CP-External\_Interface in the same cell under GB-External\_Interface.

### Note

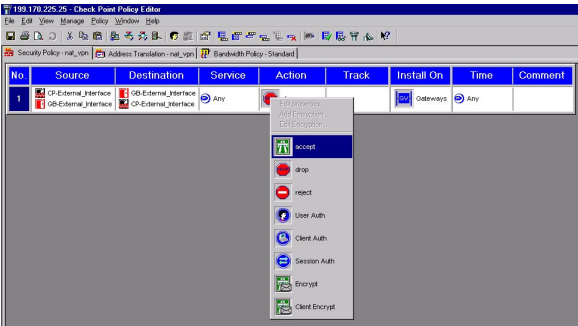
GB-External\_Interface must be above CP-External\_Interface. See example below.



*Source and Destination targets added to rule.*

**Action**

Right-click within Action cell and choose Accept.

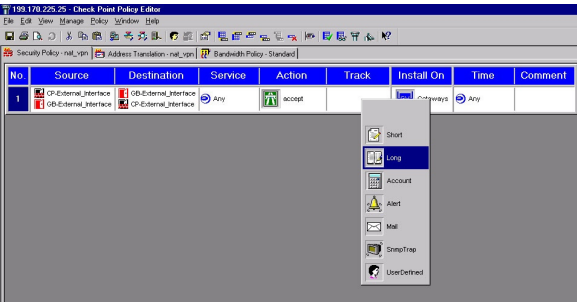


*Action cell menu*

**Track**

Right-click within Track cell and choose Long.

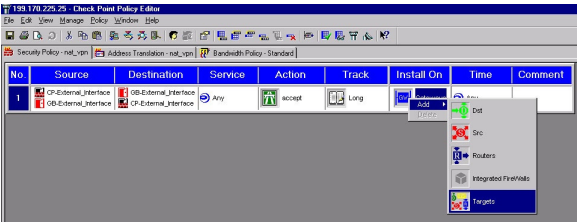




Track cell menu

Install On

- 1. Right-click within Install On cell, then select Add>Targets.



Install On menu

- 2. In the Select Target box select CP-External\_Interface.



Select Target Box

Allow and Encrypt Connections Rule

Add a rule to allow and encrypt connections between the Firewall-1 Protected Network and the GTA Firewall systems Protected Network.

## Source

1. Right-click within Source cell to add a new target CP-Protected\_Network.
2. Repeat procedure to add GB-Protected\_Network in the same cell under CP-Protected\_Network.

### Note

CP-Protected\_Network must be above GB-Protected\_Network.

---

## Destination

1. Right-click within Destination cell to add a new target GB- Protected\_Net-  
work.
2. Repeat procedure to add CP-Protected\_Network in the same cell under  
GB- Protected\_Network.

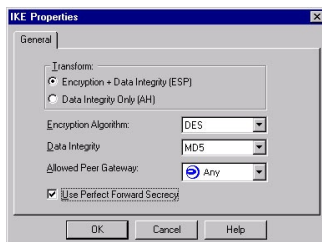
### Note

GB-Protected\_Network must be above CP-Protected\_Network.

---

## Action (Phase II of VPN negotiation corresponds to steps 3 through 5.)

1. Right-click within Action cell and choose Encrypt.
2. Right-click within Action cell and choose Edit.
3. At Encryption Properties General choose IKE.
4. Click Edit.
5. Under IKE Properties select the following
  - Encryption + Data Integrity (ESP)
  - Encryption Algorithm DES
  - Data Integrity MD5
  - Allow Peer Gateway ANY
  - Use Perfect Forward Secrecy



*IKE Properties*

## Track

Right-click within Track cell and choose Long.

## Install On

1. Right-click within Install On cell, then select Add Target.
2. In the Select Target box select CP-External\_Interface.

## Corporate Policy Rules

Add other rules according to your corporate security policy (if any) after the two VPN rules.

## Default Rule

Add the default rule at the bottom of the list of rules. This step is required for proper function of the firewalls.

### Note

Rule order is important. The two VPN-related rules specified in this document must be first in the list, and the last rule must be a default rule, which excludes all other traffic. All other rules may be placed between the GTA Firewall<->Firewall-1 rules and the default rule.

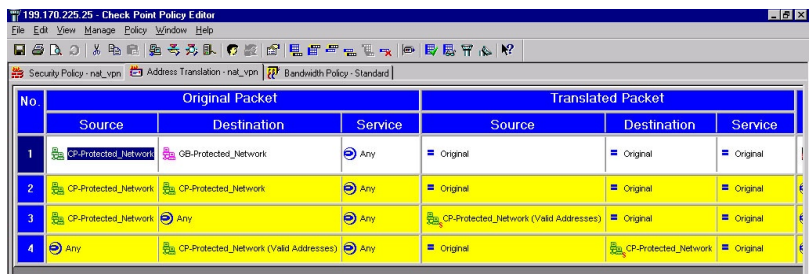
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	CP-External_Interface GB-External_Interface	GB-External_Interface CP-External_Interface	Any	accept	Long	CP-External_Interface	Any	Allow Check Point and QNAT Box to connect using external interface
2	CP-Protected_Network GB-Protected_Network	GB-Protected_Network CP-Protected_Network	Any	Encrypt	Long	CP-External_Interface	Any	Allow and encrypt internal VPN network connections
3	Any	Any	Any	drop	Long	CP-External_Interface	Any	

*Two defined rules and final default rule*

## NAT Rule

If you are using Network Address Translation you will need to add a rule in the Firewall-1 Address Translation section (second tab) not to NAT packets between the Firewall-1 Protected Network and the GTA Firewall Protected Network. This rule should be located at the top of your Address Translation Rule Set.

1. Select the second tab in the Security Policy Window.
2. Right-click within Source cell to add a new target CP-Protected\_Network.
3. Right-click within Destination cell to add a new target GB- Protected\_Network.



199.170.225.25 - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - nat\_vpn | Address Translation - nat\_vpn | Bandwidth Policy - Standard

No	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	CP-Protected_Network	GB-Protected_Network	Any	Original	Original	Original
2	CP-Protected_Network	CP-Protected_Network	Any	Original	Original	Original
3	CP-Protected_Network	Any	Any	CP-Protected_Network (Valid Addresses)	Original	Original
4	Any	CP-Protected_Network (Valid Addresses)	Any	Original	CP-Protected_Network	Original

*NAT rule in the Address Translation rule set*

**Install New Policy**

Using the Policy menu or toolbar button, install the new policy. Follow the onscreen instructions. Your GTA Firewall and Firewall-1 VPN is now in place.





# Index

## Symbols

3DES 1

## C

Copyright ii

## D

DES 1

Diffie-Hellman 2

## E

email support ii

external interface 7

## F

filter

Remote Access 3

## G

gateway 9

local 2

remote 3

GBAdmin 1

GNAT Box System Software ii

## I

IKE 1, 5

## K

key

group 2

## M

MD5 1

## N

NAT 5

## O

objects 5

## P

Phase I 7, 9

Phase II 14

policy

install 16

security 5, 10, 15

Protected Network 6, 8

## S

SHA-1 1

support ii

## T

Telephone ii

trademark ii

## V

version ii

VPN 1

## W

Web Interface 1