

# Technical Document

**TD: VPN-DS-02**

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

*with SoftRemoteLT from SafeNet, Inc.*

---

### **Connecting to Discontiguous Subnets**

GNAT Box System Software version 3.3.2

# 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. All other products are trademarks of their respective companies.

## Version Information

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

GNAT Box Technical Document  
VPN – Connecting to Discontiguous Subnets

December 2002

---

# Table of Contents

<b>Introduction</b> .....	1
Example IP Addresses.....	1
<b>GTA Firewall</b> .....	1
Address Object .....	2
IP Aliases .....	2
VPN Object .....	2
Remote Access Filters .....	3
User Authorization .....	4
IP Pass Through Filters .....	5
<b>GNAT Box VPN Client</b> .....	5
Add Connections .....	6



---

# Introduction

Discontiguous subnets are two or more networks that cannot be logically combined with a subnet mask, such as 192.168.71.0/24 and 10.254.254.0/24. Using multiple discontiguous subnets, the VPN setup on the firewall and mobile client requires some additional configuration.

To create a VPN from a mobile client to a network with discontiguous subnets, follow these steps:

1. Create an address object that references all the desired internal subnets.
2. Create an IP alias to be used as the secure gateway for each internal subnet after the first.
3. Create a VPN object to reference the address object containing the internal subnets.
4. Create Remote Access Filters to accept connections on both the External Interface and on the aliases to which VPN connections will be made.
5. Create a connection on the VPN Client for each internal subnet that cannot be grouped together using a subnet mask.

## Example IP Addresses

External IP Address:	199.120.225.79
External IP Alias:	199.120.225.78
Protected Network #1:	10.254.254.0/24
Protected Network #2:	192.168.71.0/24

---

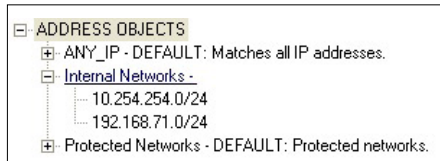
## GTA Firewall

The following sections describe how to customize the standard VPN setup on the GTA Firewall to accommodate a connection to Discontiguous Subnets.

- Create an address object for the internal subnets.
- IP aliases for each subnet after the first.
- VPN object that references the address object.
- Remote Access Filters for IKE and ESP.
- User Authorization for the mobile user.
- IP Pass Through Filters to allow inbound traffic for the subnets.

## Address Object

Open Objects -> Address Objects. Add a new address object and name it **Internal Networks**. Next, add the IP addresses of the discontiguous internal subnets, in the example, Protected Network 10.254.254.0/24 and Protected Network 192.168.71.0/24. For more information on creating objects, please refer to the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**.



*Address Object*

## IP Aliases

Open NAT -> Aliases. For each additional internal subnet, create an IP alias to be used as the gateway (default route) for that subnet. In the example, the IP alias 199.120.225.78 (**Alias1**) will be used on the External Network interface as the gateway for the second subnet, 192.168.70.0/24. For more information on creating aliases, please refer to the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**.

Address Aliases			
	Name	Interface	IP Address
1	Alias1	EXTERNAL	199.120.225.78

*IP Alias*

## VPN Object

Open Objects -> VPN Objects. Create a VPN object that references the **Internal Subnets** address object, or modify an existing VPN object. For more information on creating or editing VPN objects, please refer to the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**.

In the example below, the default mobile VPN object has been copied, then modified to use the Internal Subnets address object.

### Note

The Local Gateway uses the External Interface Object.

Disable

### VPN Objects

Name:   Require mobile authentication.

Description:

Local gateway:   Force mobile protocol

Local network:

---

Phase I

Exchange mode:  Encryption method:

Hash algorithm:  Key group:

---

Phase II

Hash algorithm:  Encryption method:

Key group:

	Name	Description
1	IKE	DEFAULT: IKE VPNs
2	MANUAL	DEFAULT: MANUAL VPNs
3	MOBILE	DEFAULT: MOBILE VPNs

*VPN Object*

## Remote Access Filters

Open Filters -> Remote Access. Create Remote Access Filters that accept connections on the External Network interface and on the IP alias, or modify an existing object. In the example below, the Remote Access Filters will accept IKE and ESP connections on **Alias1**, the External Network interface IP address, and any other IP addresses assigned to the firewall.

### **Note**

To narrow the scope of the filter, you may wish to use an address object in the DESTINATION field that refers to only the External Network interface and the IP alias.

- |   |  |  |  |
|---|--|--|--|
| 1 |  | Description: #VPN: Allow ESP connections (Mobile VPN). |  |
|   |  | Type: Accept   |  |
|   |  | Interface: ANY   |  |
|   |  | Protocol: ESP  |  |
|   |  | Source: ANY_IP   |  |
|   |  | Source Port: Blank                                     |  |
|   |  | Destination: ANY_IP                                    |  |
|   |  | Destination Port: Blank                                |  |
|   |  |  |  |
| 2 |  | Description: #VPN: Allow access to IKE (Mobile VPN)    |  |
|   |  | Type: Accept   |  |
|   |  | Interface: ANY   |  |
|   |  | Protocol: UDP  |  |
|   |  | Source: ANY_IP   |  |
|   |  | Source Port: 500 or Blank                              |  |

Destination: ANY\_IP  
 Destination Port: 500

## User Authorization

Open Authorization -> Users. To define a user on the GTA Firewall, follow the standard method for creating users for the mobile VPN. Enter the email address that was used in the My Identity section of the VPN Client policy. Enter the preshared key entered in the policy definition. The IDENTITY and PASSWORD fields are required by GBAuth User Authentication.

The Remote Network is the internal network IP address entered in the My Identity section of the GNAT Box VPN Client policy definition. The subnet mask should always be /32 or 255.255.255.255 (specifying a single host).

GNAT-Box Edit User	
Disable:	<input type="checkbox"/>
Name:	Jane User
Description:	Test User
Identity:	janeuser@gta.com
Authentication	
Method:	Password
Password:	janeuser
Mobile VPN	
Disable:	<input type="checkbox"/>
VPN object:	MOBILE
Remote Network:	
Pre-shared secret:	ASCII   12345678
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>	

*User Authorization*

### User Authorization Fields

Disable	Check to disable all access for the selected user.
Name	Enter full name of the user.
Description	Enter description of user.
Identity	Enter user email address for user authentication.
Authentication	
Method	Password method.
Password	Enter password for user authentication.

---

### Mobile VPN

Disable	Check to disable VPN access for the selected user.
VPN Object	Select a previously defined VPN object.
Remote Network	Enter IP address of the remote network.
Preshared secret	Select ASCII or HEX value. Enter preshared secret as defined in VPN in ASCII or HEX format.

## IP Pass Through Filters

Open IP Pass Through -> Filters. Create IP Pass Through Filters that allow connections to the **Internal Networks**. The filters in the examples below will allow all access inbound to networks defined in the **Internal Networks** object.

- Description : VPN, allow inbound (Mobile VPN).  
 Type: Accept  
 Interface: EXTERNAL  
 Protocol: ALL  
 Source: 192.168.100.1  
 Source Port: Blank  
 Destination: Internal Networks  
 Destination Port: Blank
- Description: VPN, allow outbound (Mobile VPN).  
 Type: Accept  
 Interface: PROTECTED  
 Protocol: ALL  
 Source: Internal Networks  
 Source Port: Blank  
 Destination: 192.168.100.1  
 Destination Port: Blank

---

## GNAT Box VPN Client

Create two or more connections (security policies) on the VPN mobile client, one for each subnet on the internal network side of the firewall to which you wish to establish a VPN.

Generally, follow the mobile client setup for VPN Client, illustrated in **GNAT BOX VPN AND VPN CLIENT FEATURE GUIDE**. Use the following section to modify the mobile client setup for discontinuous networks.

## Add Connections

Add one connection for each subnet you are using on the firewall. The Remote Party Identity and Addressing section will be different for each subnet connection.

- In each connection, reference the selected internal subnet in the **SUBNET** and **MASK** fields.
- In the first connection, refer to the IP address of the first subnet connection. Then, for each additional connection, refer to the appropriate IP alias defined on the firewall for that subnet.

The example below illustrates how to set up a connection on the mobile client that will reach the 10.254.254.0/24 subnet. The IP Address of the gateway (referred to in the **CONNECT USING SECURE GATEWAY TUNNEL** field) is the External IP address of the firewall, 199.120.225.79.

The screenshot shows the 'Remote Party Identity and Addressing' configuration window. The 'ID Type' is set to 'IP Subnet'. The 'Subnet' field contains '10.254.254.0' and the 'Mask' field contains '255.255.255.0'. The 'Port' is set to 'All' and the 'Protocol' is set to 'All'. The 'Connect using' dropdown is checked and set to 'Secure Gateway Tunnel'. Below this, the 'ID Type' is set to 'IP Address' and the field contains '199.120.225.79'.

*Add connection – 10.254.254.0/24 Network*

The next example illustrates how to set up a connection on the mobile client that will reach the 192.168.71.0/24 subnet. The IP Address of the gateway is the IP alias, 199.120.225.78 (Alias1), the alias of 199.120.225.79, the firewall's External IP address.

The screenshot shows the 'Remote Party Identity and Addressing' configuration window. The 'ID Type' is set to 'IP Subnet'. The 'Subnet' field contains '192.168.71.0' and the 'Mask' field contains '255.255.255.0'. The 'Port' is set to 'All' and the 'Protocol' is set to 'All'. The 'Connect using' dropdown is checked and set to 'Secure Gateway Tunnel'. Below this, the 'ID Type' is set to 'IP Address' and the field contains '199.120.225.78'.

*Add connection – 192.168.71.0/24 Network*