Technical Document

TD: VPN-SDG-02

GNAT Box VPN and VPN Client

with SoftRemoteLT from SafeNet, Inc.

Connecting from a Static to a Dynamic Gateway

GNAT Box System Software version 3.3.2

Global
Technology
Associates, Inc.

Copyright

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
Support:	support@gta.com

Document Information

GNAT Box Technical Document
VPN – Connecting from a Static to a Dynamic Gateway December 2002

Table of Contents

Introduction

A static to dynamic gateway VPN is a network-to-network Virtual Private Network that links a static gateway to a dynamic gateway. The static end of the connection sees the dynamic side as a mobile user, while the dynamic end of the connection sees the static side as a normal IKE VPN.

Note

Static to Dynamic Gateway VPN is only available on systems that support an IKE VPN.

Static Gateway

A static IP address is not negotiated by the system, that is, it is defined in Network Information and does not change. A static gateway system is a firewall with a static IP address assigned to the External Network.

Dynamic Gateway

A dynamic IP address is negotiated by the system, so the IP address can, and will, change. A dynamic gateway system is a firewall with a dynamic IP address assigned to the External Network.

Use these instructions for systems using GNAT Box System Software version 3.2.2 and higher.

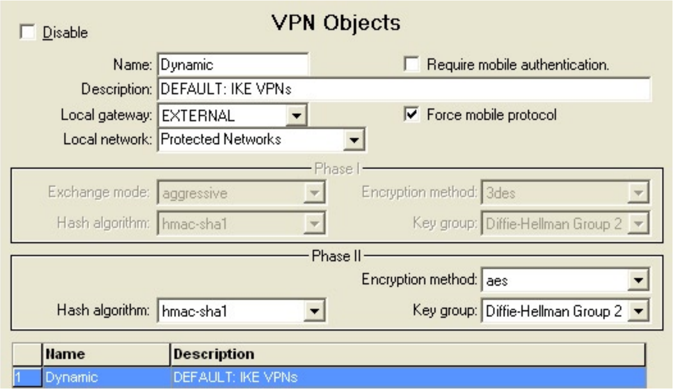
Configure the Dynamic System

The dynamic system (the firewall with the dynamic IP address) must always initiate the VPN.

The dynamic side of the connection sees the static gateway as a normal IKE VPN. To configure the dynamic system, create an IKE VPN object and a VPN Authorization, just as you would for any network-to-network VPN.

Create VPN Object

In Objects -> VPN Objects, add a new IKE VPN object or modify an existing one to create an object that defines the connection to the static system.



VPN Objects

□ Disable

Name: Dynamic

□ Require mobile authentication.

Description: DEFAULT: IKE VPNs

Local gateway: EXTERNAL

☑ Force mobile protocol

Local network: Protected Networks

Phase I

Exchange mode: aggressive

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman Group 2

Phase II

Encryption method: aes

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman Group 2

	Name	Description
1	Dynamic	DEFAULT: IKE VPNs

VPN Objects

VPN Object Fields

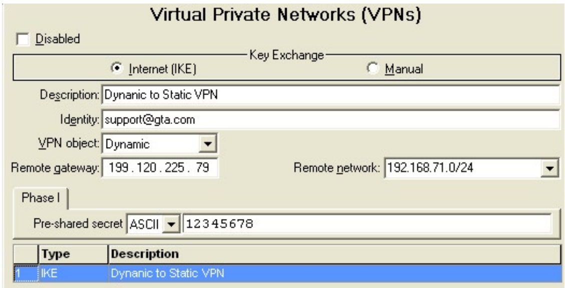
Name	Enter a name to be used for the VPN object.
Local gateway	Select the External Network interface object or an IP Alias interface object.
Local Network	Enter the IP address/mask or select an object created for the selected internal network. If you use the default, Protected Networks, verify that the correct network is defined in the object.
Require Mobile Authentication	Disable. (Leave un-checked.)
Force Mobile Protocol	Enable. (Check.)
Phase I When Force Mobile Protocol is enabled, these fields will be greyed out (uneditable).	
Phase II	
Encryption Method	Select one of the available ESP methods; None, Null, AES, Blowfish, Cast-128, DES, Twofish, 3DES, Strong.
Hash Algorithm	Select SHA-1, SHA-2 or MD5
Key Group	Select Diffie-Hellman Group 1, 2 or 5

Note

If you are not on the latest release of the GNAT Box System Software, your HASH and Encryption algorithms may be more limited.

Create VPN Authorization

In Authorization -> VPNs, add a new VPN authorization or modify an existing one that allows a connection to the static system.



Virtual Private Networks (VPNs)

□ Disabled

Key Exchange: ● Internet (IKE) ○ Manual

Description: Dynanic to Static VPN

Identity: support@gta.com

VPN object: Dynamic

Remote gateway: 199 . 120 . 225 . 79

Remote network: 192.168.71.0/24

Phase I

Pre-shared secret: ASCII 12345678

	Type	Description
1	IKE	Dynanic to Static VPN

Dynamic to Static VPN

VPN Authorization Fields	
Use IKE protocol	Yes.
Description	Enter a description to be used for the VPN.
VPN object	Select the VPN object created in the previous step.
Identity	Enter the email address of the authorized person or organization that will access this VPN. (e.g.: support@gta.com)
Gateways	
Remote Gateway	Enter the External IP address of the static system (the remote network).
Remote Network	
Object	Select the object that defines the remote network (the static system), or select USE IP ADDRESS.
IP Address	If you selected USE IP ADDRESS, enter the IP address that defines the remote network (the static system).
Phase I	
Preshared secret	Select ASCII or HEX, and then enter the preshared key, which must be the same on both systems.

Remote Access Filters

Define Remote Access Filters to accept IKE and ESP connections. Below are example Remote Access Filters.

1	Description:	#DEFAULT: VPN: Allow ESP connections (VPN to Static Gateway).
	Type:	Accept
	Interface:	ANY
	Protocol:	ESP
	Source:	199.120.225.79
	Source Port:	Blank
	Destination:	EXTERNAL
	Destination Port:	Blank

2	Description:	#DEFAULT: VPN: Allow access to IKE (VPN to Static Gateway).
	Type:	Accept
	Interface:	ANY
	Protocol:	UDP
	Source:	199.120.225.79
	Source Port:	500 or Blank
	Destination:	EXTERNAL
	Destination Port:	500

IP Pass Through Filters

Create IP Pass Through Filters in accordance with your corporate security policy. Below are example IP Pass Through Filters.

Description:	VPN, allow inbound (VPN to Static Gateway).
Type:	Accept
Interface:	EXTERNAL
Protocol:	ALL
Source:	192.168.71.0/24
Source Port:	Blank
Destination:	Protected Networks
Destination Port:	Blank

Description:	VPN, allow outbound (VPN to Static Gateway).
Type:	Accept
Interface:	PROTECTED
Protocol:	ALL
Source:	Protected Networks
Source Port:	Blank
Destination:	192.168.71.0/24
Destination Port:	Blank

Configure the Static System

The static end of a VPN connection sees the dynamic side as a mobile user. To configure the static system, create a VPN object, then set up the dynamic system as a user, just as you would define any mobile client user.

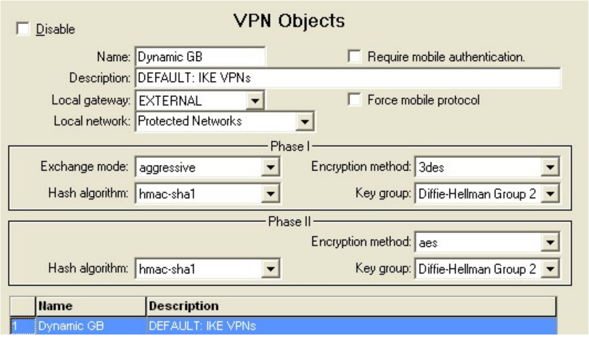
Note

Remember that in the static to dynamic gateway setup, the firewall with the dynamic External IP address must always initiate the VPN.

Create VPN Object

Open Objects -> VPN Objects.

You may either edit a default object directly, or select the default object and copy it using the Insert key or the Add (+) icon. The copy will retain all the settings of the default, but leave the name and description blank.



VPN Objects

□ Disable

Name: Dynamic GB

□ Require mobile authentication.

Description: DEFAULT: IKE VPNs

Local gateway: EXTERNAL

□ Force mobile protocol

Local network: Protected Networks

Phase I

Exchange mode: aggressive

Encryption method: 3des

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman Group 2

Phase II

Encryption method: aes

Hash algorithm: hmac-sha1

Key group: Diffie-Hellman Group 2

	Name	Description
1	Dynamic GB	DEFAULT: IKE VPNs

Dynamic VPN Object

VPN Object Fields (configured on the static system)

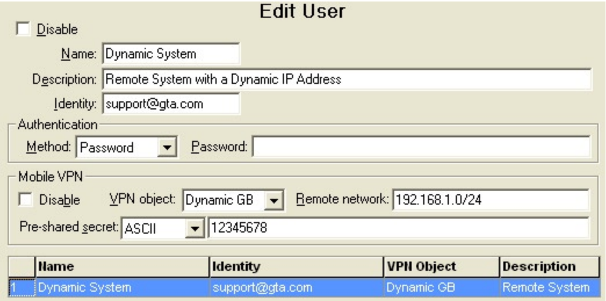
Name	Enter a name for the VPN object.
Description	Enter a description of this dynamic system VPN object.
Local gateway	Select the External Interface name or IP alias name.
Local Network	Enter the IP address/mask, or select an address object created for the selected internal network. If you choose to use the default Protected Networks address object, verify that the correct network is defined in the object.
Require Mobile Authentication	Disable (Uncheck).
Force Mobile Protocol	Disable (Uncheck). Optional: Enable (check) Force Mobile Protocol. This selection will set Phase I automatically.
Phase I	
Mode	Select Aggressive. (Main, Aggressive).
Encryption Method	Select 3DES. (AES, Blowfish, DES, 3DES, Strong).
Hash Algorithm	Select SHA-1. (SHA-1, SHA-2, MD-5, All).
Key Group	Select Diffie-Hellman Group 2. (Any, Diffie-Hellman Group 1, 2, 5).
Phase II See the previous table for more about encryption methods in Phase II.	
Encryption Method	Select ESP method.
Hash Algorithm	Select SHA-1, SHA-2 or MD5.
Key Group	Select Diffie-Hellman Group 1, 2 or 5.

Note

If you are not on the latest release of the GNAT Box System Software, your HASH and Encryption algorithms may be more limited.

Create User Authorization

Open Authorization -> Users. The Remote Network is the internal network IP address entered in the My Identity section of the GNAT Box VPN Client policy definition. The netmask should always be /32 or 255.255.255.255 (specifying a single host). Enter the email address that you used in the My Identity section of the policy. Enter the policy definition preshared key.



Edit User

□ Disable

Name: Dynamic System

Description: Remote System with a Dynamic IP Address

Identity: support@gta.com

Authentication

Method: Password

Password:

Mobile VPN

□ Disable

VPN object: Dynamic GB

Remote network: 192.168.1.0/24

Pre-shared secret: ASCII 12345678

	Name	Identity	VPN Object	Description
1	Dynamic System	support@gta.com	Dynamic GB	Remote System

Dynamic Remote System User

User Authorization Fields (configured on the static system)

Name	Enter a name for the VPN user (system).
Description	Enter a description of the VPN user (system).
Identity	Enter an email address to identify the user (system).
Password	Leave blank.
VPN Object	Select the mobile VPN object previously created.
Remote Network	Enter the IP address of remote network.
Preshared secret	Preshared secret or key for the remote firewall.

Remote Access Filters

Define Remote Access Filters to accept IKE and ESP connections. Below are examples of Remote Access Filters for IKE and ESP.

1	Description	#DEFAULT: VPN: Allow ESP connections (VPN to Dynamic System).
	Type:	Accept
	Interface:	ANY
	Protocol:	ESP
	Source:	Object <ANY_IP>
	Source Port:	Port: 0 or Blank
	Destination:	EXTERNAL
	Destination Port:	Blank

2	Description	#DEFAULT: VPN: Allow access to IKE (VPN to Dynamic System).
	Type:	Accept
	Interface:	ANY
	Protocol:	UDP
	Source:	ANY_IP
	Port:	500 or Blank
	Destination:	EXTERNAL
	Port:	500

IP Pass Through Filters

Open IP Pass Through -> Filters. Create IP Pass Through Filters according to your corporate security policy. Below are examples of appropriate IP Pass Through Filters.

1	Description	#DEFAULT: VPN, allow inbound (VPN to Static Gateway).
	Type:	Accept
	Interface:	EXTERNAL
	Protocol:	ALL
	Source:	192.168.1.0/24
	Source Port:	Port: 0 or Blank
	Destination:	Protected Networks
	Destination Port:	Blank

2	Description	#DEFAULT: VPN, allow outbound (VPN to Static Gateway).
	Type:	Accept
	Interface:	PROTECTED
	Protocol:	ALL
	Source:	Protected Networks
	Port:	Blank
	Destination:	192.168.1.0/24
	Destination Port:	Blank