

IPSec Interoperability between GnatBox/Robox and SnapGear for Local Area Networks

This document was created by Chris Millard. No part of it may be reproduced or published in any form without the prior written consent of the author.

Revision 1.0 - 10th April 2002
© 2002, Chris Millard - (<http://www.chrismillard.com>)

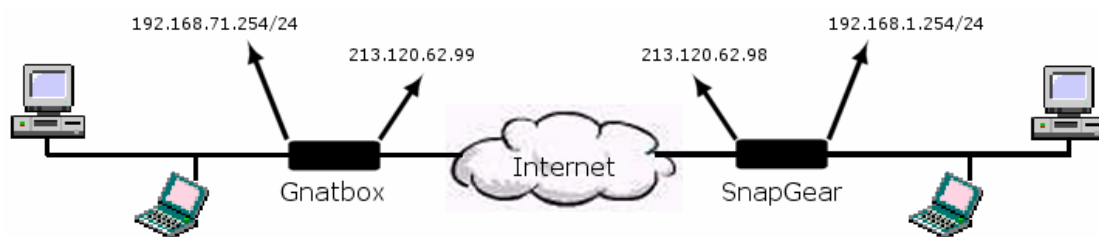
1.0 Pre-requisites

This document assumes that both the Gnatbox/Robox and SnapGear are already configured for access to the Internet.

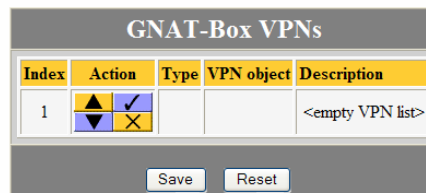
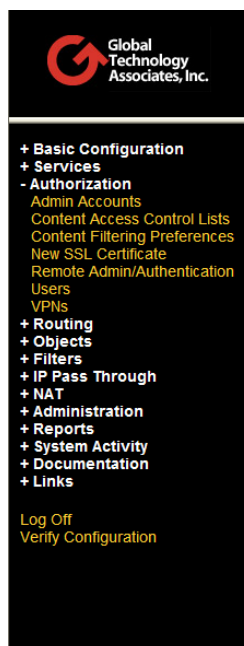
Your Robox must have firmware version 3.2.0 or , and your SnapGear product must have firmware version 1.5.4 or above (see product literature for information on determining your firmware version and for upgrading your firmware if necessary).

2.0 Introduction

This document describes the configuration needed to set up an IPSec tunnel between a Gnatbox/Robox and a SnapGear. The configuration is based on the typical topology illustrated below.



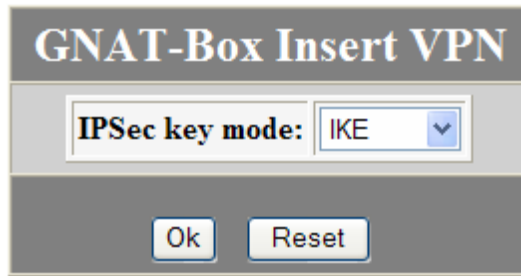
3.0 Gnatbox/Robox Configuration



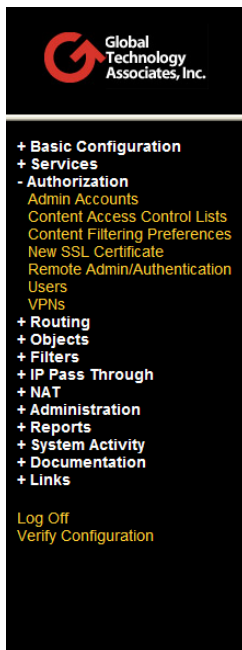
Copyright © 1996-2002 Global Technology Associates, Inc.

1. Click the "Authorization" menu.
2. Click the "VPNs" option.
3. Click on an action button to add a new VPN Object.

- When asked to select an IPSec Key Mode, select "IKE" from the drop down menu.







- Enter a description for your new VPN Object and an Identity.
- Change the VPN Object to "MANUAL"
- Set the Remote Gateway to the IP Address assigned to the "Internet" Interface of the SnapGear
- For the Remote network, leave the object as "<USE IP ADDRESS>" and set the IP address range of the Remote network (note, use CIDR format. 192.168.1.0/24 <- the 24 is the number of bits used in the subnet mask – in this case 255.255.255.0)
- Leave the Pre-shared secret as ASCII and type a phrase that is at least 24 characters long. You will use the same Pre-shared secret on your SnapGear.




GNAT-Box Insert VPN	
Disable:	<input type="checkbox"/>
IPSec key mode:	IKE
Description:	VPN to SnapGear
VPN object:	MANUAL
Identity:	My VPN Tunnel
Gateways	
Remote gateway:	213.120.62.98
Remote Network	
Object:	<USE IP ADDRESS>
IP Address:	192.168.1.0/24
Phase I	
Pre-shared secret:	ASCII Chris Millard's VPN Solutions
<input type="button" value="Back"/> <input type="button" value="Copy"/> <input type="button" value="Ok"/> <input type="button" value="Reset"/>	

Copyright © 1996-2002 Global Technology Associates, Inc.

- Once you have entered this information, click on "Ok".









































GNAT-Box VPNs				
Index	Action	Type	VPN object	Description
1	   	IKE	MANUAL	VPN to SnapGear

11. Click on "Save"
12. From the main menu in the left-hand pane, select "Filters"
13. Click on "Remote Access"
14. Click on the "Default" button at the bottom of the list of Remote Access filters. (Note defaulting this list will remove any custom filters that you have added, so ensure you have a copy of them to hand so that you can re-enter them after).
You should now have two new filters at the top of your list for the VPN Object you have just created.
15. Click on the "Save" button at the bottom of the list.

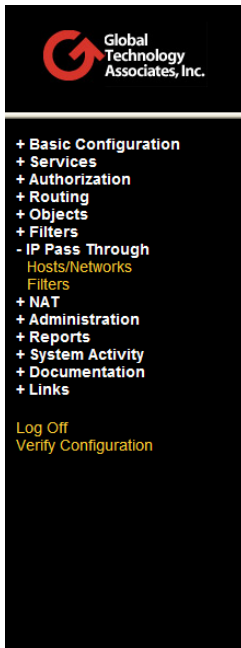


- + Basic Configuration
- + Services
- + Authorization
- + Routing
- + Objects
- Filters
 - Outbound
 - Preferences
 - Protocols
 - Remote Access
 - Time Groups
- + IP Pass Through
- + NAT
- + Administration
- + Reports
- + System Activity
- + Documentation
- + Links

[Log Off](#)
[Verify Configuration](#)

GNAT-Box Remote Access Filters		
Index	Action	Description
1	   	DEFAULT: VPN: Allow ESP connections (test). Accept notice ANY 50 from 213.120.62.98/32 to EXTERNAL
2	   	DEFAULT: VPN: Allow access to IKE (test). Accept notice ANY UDP from 213.120.62.98/32 500 to EXTERNAL 500
3	   	DEFAULT: Allow protected network access to remote admin services. Accept notice "PROTECTED" TCP from ANY_IP to ANY_IP 443 77
4	   	DEFAULT: DNS: Allow protected network access to DNS server. DISABLED - Accept notice "PROTECTED" UDP from ANY_IP to ANY_IP 53
5	   	DEFAULT: Allow access to user authentication server. DISABLED - Accept notice ANY TCP from ANY_IP to ANY_IP 76
6	   	DEFAULT: DNS: Allow all DNS replies. DISABLED - Accept notice ANY UDP from ANY_IP 53 to ANY_IP 1024:65535
7	   	DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy. DISABLED - Accept notice "PROTECTED" TCP from ANY_IP to 0.0.0.0/0 2784
8	   	DEFAULT EMAIL PROXY: Allow connections to email proxy. DISABLED - Accept notice "EXTERNAL" TCP from ANY_IP to ANY_IP 25
9	   	DEFAULT: Block/nolog discard bootp, netbios, snmp, and rwho. Deny warning ANY UDP nolog from ANY_IP to ANY_IP 9 67 68 137 138 161 513
10	   	DEFAULT NO RIP: Block/nolog rip. Deny warning ANY UDP nolog from ANY_IP to ANY_IP 520
Index	Action	Description

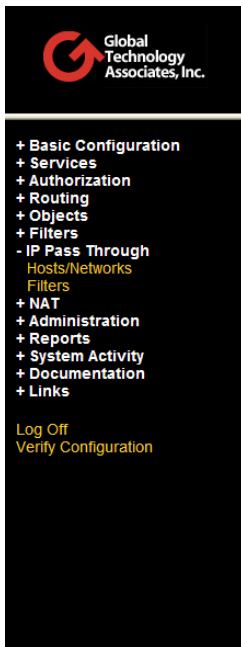
16. From the main menu in the left-hand pane, select "IP Pass Through"
17. Click on "Filters"



GNAT-Box IP Pass Through Filters		
Index	Action	Description
1	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<empty filter list>

Copyright © 1996-2002 Global Technology Associates, Inc.

18. Click on "Default". (Note as with Remote Access Filters, defaulting this list will remove any custom filters that you have added, so ensure you have a copy of them to hand so that you can re-enter them after).
19. Click on "Save".



GNAT-Box IP Pass Through Filters		
Index	Action	Description
1	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	DEFAULT: VPN, allow inbound (VPN to SnapGear). Accept notice "EXTERNAL" ALL from 192.168.1.0/24 to Protected Networks
2	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	DEFAULT: VPN, allow outbound (VPN to SnapGear). Accept notice "PROTECTED" ALL from Protected Networks to 192.168.1.0/24

Copyright © 1996-2002 Global Technology Associates, Inc.

19. Your Gnatbox/Robox is now ready to communicate to your SnapGear

4.0 SnapGear Configuration

The screenshot shows the SnapGear web interface for IPsec VPN Setup. On the left is a navigation menu with categories: NETWORKING, FIREWALL, VPN, and SYSTEM. The VPN section is selected, showing options for PPTP VPN Client, PPTP VPN Server, and IPsec. The main content area is titled 'IPsec VPN Setup' and contains three sections: 'IPsec Setup', 'IPsec Interfaces', and 'Add New IPsec Connection'. In the 'IPsec Setup' section, 'Enable IPsec:' is checked and a 'Submit' button is present. The 'IPsec Interfaces' section has 'Default route' selected, 'Restart IPsec with new configuration:' is checked, and another 'Submit' button is present. The 'Add New IPsec Connection' section has an 'Add' button.

SNAPgear

IPsec VPN Setup

IPsec Setup

IPsec allows you to connect two or more remote networks via an encrypted tunnel. Please refer to the Quick Install Guide and User Manual for steps to setting up an IPsec tunnel. For the latest Interoperability documentation with other IPsec vendors please visit the Knowledge Base at www.snapgear.com.

Enable IPsec:

IPsec Interfaces

Specify which interfaces IPsec is to be used on. A maximum of 4 interfaces can be used.

Default route - brought up when connected to a modem. Ensure the *Connect to Internet* settings allow for this.

Specific routes:

eth1

Restart IPsec with new configuration:

Add New IPsec Connection

NETWORKING

- [Connect to Internet](#)
- [Dial In Setup](#)
- [IP Configuration](#)
- [DHCP Server](#)
- [Advanced Networking](#)

FIREWALL

- [Incoming Access](#)
- [Outgoing Access](#)
- [Rules](#)
- [Intrusion Detection](#)

VPN

- [PPTP VPN Client](#)
- [PPTP VPN Server](#)
- [IPsec](#)

SYSTEM

- [Time Server](#)
- [Password](#)
- [Diagnostics](#)
- [Advanced](#)

1. From the main menu in the left-hand pane, select "IPsec"
2. In the "IPsec Setup" section, place a tick in "Enable IPsec:" and click on "Submit".
3. In the "IPsec Interfaces" section, select "Default Route" and place a tick in "Restart IPsec with new configuration:" and click on "Submit".
4. Click "Add" to add a new IPsec Connection
5. Enter a name for the VPN Connection (Note you cannot use spaces or quotes within the name, and it cannot start with a number).
6. Your "Local Gateway" details should already be entered for you, but if not, enter the IP address of your Local network and the subnet mask.
7. In the "Remote Gateway" section, enter the IP address and subnet mask of the Remote network, and in the External IP field, enter the IP address assigned to the EXTERNAL interface of your Gnatbox/Robox.
8. Select "Using a Pre-Shared Secret key"
9. Click on "Add"



NETWORKING

- [Connect to Internet](#)
- [Dial In Setup](#)
- [IP Configuration](#)
- [DHCP Server](#)
- [Advanced Networking](#)

FIREWALL

- [Incoming Access](#)
- [Outgoing Access](#)
- [Rules](#)
- [Intrusion Detection](#)

VPN

- [PPTP VPN Client](#)
- [PPTP VPN Server](#)
- [IPSec](#)

SYSTEM

- [Time Server](#)
- [Password](#)
- [Diagnostics](#)
- [Advanced](#)

Add New IPSec Connection

[Return to the main IPSec setup page.](#)

General Setup

Please fill in the name for the IPSec connection. The name must not start with numbers or contain quotes or spaces.

Connection Name:

Use Aggressive Mode:

Local Gateway

Please fill in the configuration for your local network. The *Internal subnet/netmask* refers to the private network behind the SnapGearSOHO+. The *External IP* refers to the public network interface that the SnapGearSOHO+ will use for IPSec. This can be an IP address or a DNS hostname address. The *Authentication Identifier* is required when using Aggressive Mode or using RSA key signatures for multiple Road Warriors and is used to identify the other participant for authentication. For all other scenarios, this field should be left blank and it will default to the *External IP*.

Internal subnet/netmask: /

External IP:

Authentication Identifier:

Remote Gateway

Please fill in the configuration for your remote network. To connect a remote machine that has a dynamic public IP address, enter an *External IP* of *0.0.0.0*.

Internal subnet/netmask: /

External IP:

Authentication Identifier:

Authentication Method for Automatic Keying (IKE)

Please choose the authentication method to be used.

- Using a Pre-Shared Secret - (recommended)
- Using RSA Digital Signatures - (allow a few seconds to generate)

10. Place a tick in the "Automatically enable connection when IPsec is started:" box.
11. Select "ESP Encryption"
12. In the "Authentication" section, enter the Pre-Shared secret EXACTLY as it was entered on the Gnatbox/Robox.
13. Leave the "Key Lifetime" at 1 hour
14. Place a tick in "Enable Perfect Forward of Secrecy keys"
15. Select "Never Give Up" under "Negotiate Connection Attempts:"
16. Place a tick in "Restart IPsec tunnel with the new configuration:"
17. Click "Add"

SNAPgear

Automatic Keying (IKE) Setup

[Return to the main IPsec setup page.](#)

Automatic Startup

Automatically enable connection when IPsec is started:

Authorisation

Please choose the authorisation method.

ESP Encryption - Encapsulating Security Payload. Encrypts and authenticates data - (recommended)

AH Protocol - Authentication Header. Provides a packet authentication service only. *No* encryption is provided.

Authentication

The Pre-Shared Secret should be at least 24 characters long. The pre-shared secret is a highly sensitive piece of information. It is essential to keep this information secret. Communications over the IPsec tunnel may be compromised if this information is divulged.

Key Configuration

Key Lifetime (hr):

Enable Perfect Forward Secrecy of keys:

Negotiate Connection Attempts:

Never give up (recommended)

Restart IPsec tunnel with new configuration:

NETWORKING

- [Connect to Internet](#)
- [Dial In Setup](#)
- [IP Configuration](#)
- [DHCP Server](#)
- [Advanced Networking](#)

FIREWALL

- [Incoming Access](#)
- [Outgoing Access](#)
- [Rules](#)
- [Intrusion Detection](#)

VPN

- [PPTP VPN Client](#)
- [PPTP VPN Server](#)
- [IPsec](#)

SYSTEM

- [Time Server](#)
- [Password](#)
- [Diagnostics](#)
- [Advanced](#)

18. Your SnapGear is now ready to communicate with your Gnatbox/Robox
(Note – you “may” need to soft-reboot your SnapGear first”.

SNAPgear

NETWORKING

- [Connect to Internet](#)
- [Dial In Setup](#)
- [IP Configuration](#)
- [DHCP Server](#)
- [Advanced Networking](#)

FIREWALL

- [Incoming Access](#)
- [Outgoing Access](#)
- [Rules](#)
- [Intrusion Detection](#)

VPN

- [PPTP VPN Client](#)
- [PPTP VPN Server](#)
- [IPSec](#)

SYSTEM

- [Time Server](#)
- [Password](#)
- [Diagnostics](#)
- [Advanced](#)

IPSec VPN Setup

IPSec Setup

IPSec allows you to connect two or more remote networks via an encrypted tunnel. Please refer to the Quick Install Guide and User Manual for steps to setting up an IPSec tunnel. For the latest Interoperability documentation with other IPSec vendors please visit the Knowledge Base at www.snapgear.com.

Enable IPSec:

Tunnels

Connection	Enable/Disable
My_VPN_Tunnel	<input type="button" value="Disable"/> <input type="button" value="Modify"/> <input type="button" value="Remove"/>

IPSec Interfaces

Specify which interfaces IPSec is to be used on. A maximum of 4 interfaces can be used.

- Default route - brought up when connected to a modem. Ensure the *Connect to Internet* settings allow for this.
- Specific routes:
 - eth1

Restart IPSec with new configuration:

Add New IPsec Connection