
Route**Finder**[™]

Internet Security Appliance

IPSec VPN Client

Setup Examples

Reference Guide

RouteFinder IPsec VPN Client Setup Examples PN S000397A Revision A

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2006, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents here of and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Revision	Date	Description
A	01/09/06	Initial release. This reference guide documents software version 3.00

Patents

This product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562; 5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo, and RouteFinder. Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All products or technologies are the trademarks or registered trademarks of their respective holders.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Tech Support (800) 972-2439
Internet Address: <http://www.multitech.com>

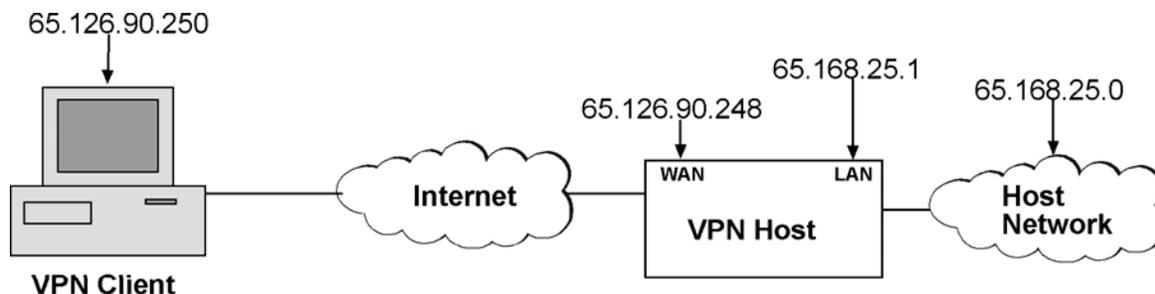
Introduction

The examples on the following pages are divided into two major categories; Non-NAT and behind NAT. With Non-NAT the VPN client is not behind a NAT device/firewall. Behind NAT(UID) the VPN client is behind a NAT device/firewall.

The setup examples start out with configuration of Non-NAT which configures the VPN client first and then sets up the VPN tunnel for the RouteFinder RF550 first. The VPN tunnel for the RF560 uses the IPSec protocol for the tunnel. The RouteFinder RF600, 660, and 760 series use IKE Connection for the tunnel.

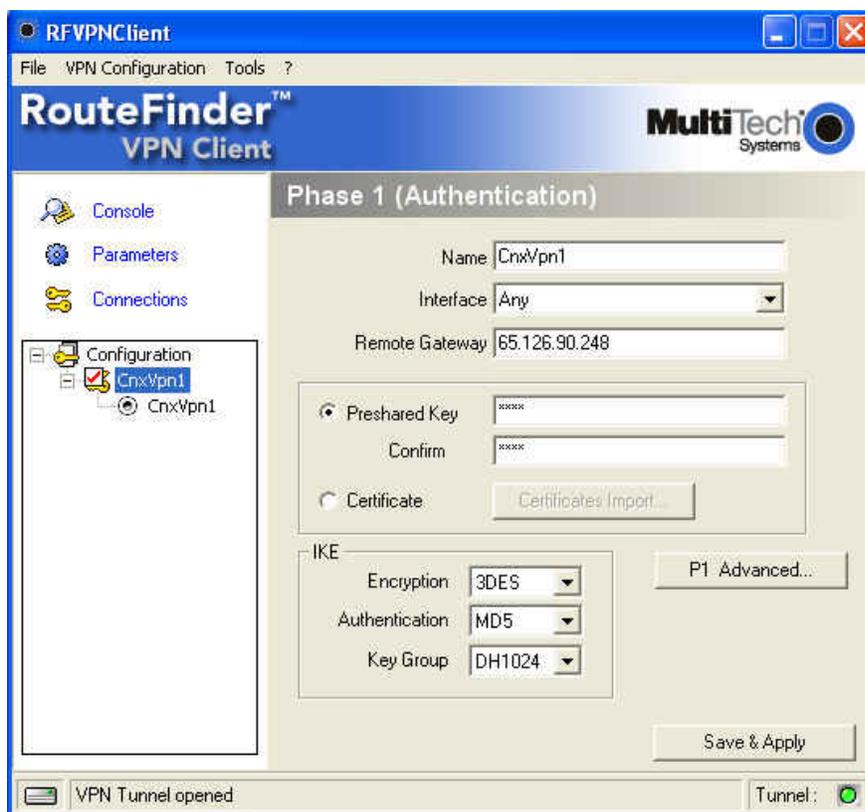
Setup for behind NAT starts out the same way with the configuration of the VPN client and then the addition of the Phase 1 Advanced for the IP addresses for the local and remote. The Behind NAT then configures the RF550 with NAT using UID, followed by the RF560 with IPSec protocol. The RouteFinder RF600, 660, and 760 series is the final configuration.

Setup for VPN Client (Non-NAT)



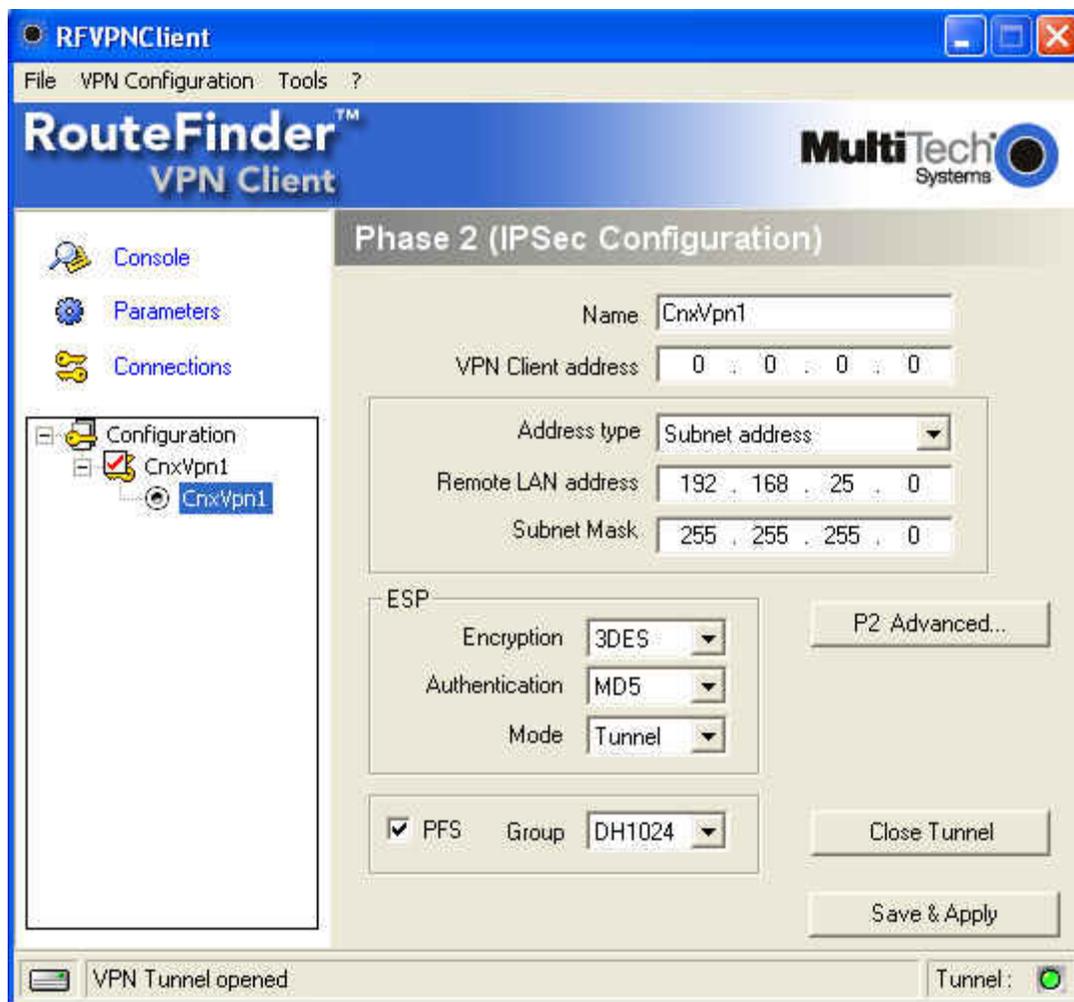
VPN client Phase 1 Setup (Non-NAT)

1. Right click on RouteFinder Client **VPN Configuration** and select **New Phase 1**.
2. Enter the name of your connection in **Name**.
3. Choose **Any** for the client Interface if your IP address is dynamic or the IP address provided by your ISP if Static (e.g., 65.126.90.250).
4. Enter the IP address of the VPN WAN for your **Remote Gateway** (e.g., 65.126.90.248).
5. Enter the Shared Secret in **Preshared Key** for your network (has to match on both ends) and **confirm** the shared secret.
6. Choose **IKE Authentication** of **MD5**.

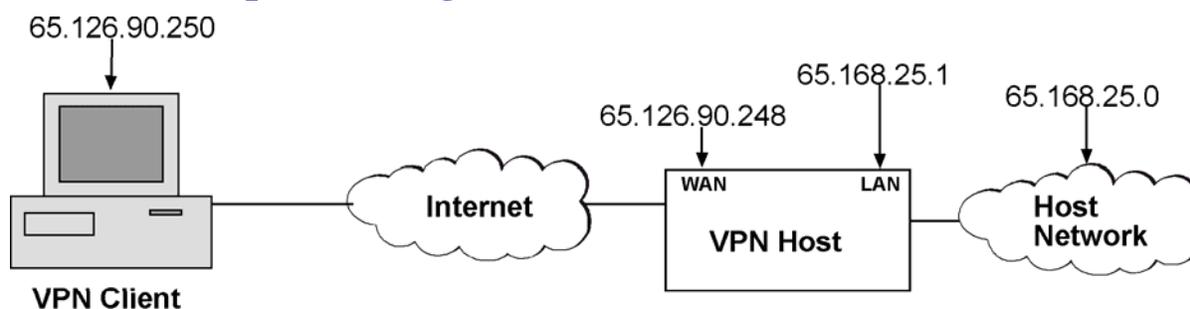


Phase 2 Setup (Non-NAT)

1. Start Phase 2 by right clicking on the name of your VPN Client you created in Phase 1.
2. VPN Client address will be set to 0.0.0.0 unless you have a Static IP address (e.g., 65.126.90.250).
3. Address type is the type of setup on the host side. If it's a **network**, then choose **Subnet address** and enter in the Remote LAN address (e.g., 192.168.25.0) and Subnet Mask (e.g., 255.255.255.0). If it's a **single IP address** change it to that address.
4. Choose **ESP Authentication** of **MD5**.



RF550VPN Setup: Enabling VPN (Non-NAT)



1. In the RouteFinder RF550VPN, VPN Settings menu, enter the name of your VPN tunnel in the **Connection Name** field.
2. Click the **ADD** button to add the tunnel and the VPN Settings menu is displayed.

The screenshot shows the 'VPN SETTINGS' page in the RouteFinder web interface. The page title is 'RouteFinder SOHO VPN Gateway'. The main menu on the left includes options like TIME ZONE SETTINGS, DEVICE IP SETTINGS, ISP SETTINGS, ISP ADDITIONAL SETTINGS, MODEM SETTINGS, VPN SETTINGS (highlighted), SAVE & RESTART, and Logout. The VPN SETTINGS section shows a 'Connection Name' field with 'testconnection' and an 'ADD' button. There is also a checkbox for 'Disable Internet Access (VPN Tunnel Only)'. Below is a table with columns: Enable, Connection Name, Local IPSEC ID, Remote IPSEC ID, and Command. At the bottom are '< BACK' and 'NEXT >' buttons.

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command

RF550VPN VPN tunnel Setup (Non-NAT)

1. Check **Enabled Keep Alive** to keep the tunnel up constantly.
2. Click on **LAN** option in Remote Site (Default).
3. In **Remote Gateway IP/FQDN** option, the IP address of 0.0.0.0 if a Dynamic address is being used or if a static address (e.g., 65.126.90. 250) is provided by your ISP.
4. In the **Secure Association** option, the default of **Main Mode** is OK and in **Perfect Forward Secure**, the default of **Enabled** is OK.
5. The **Encryption Protocol** has to match on each end of the tunnel; **3Des** is the most common setting.
6. In the **PreShared Key**, the shared secret has to match on both ends of the tunnel.
7. In **Key Life**, default of **28800** and **IKE Life Time**, default of **3600** can be left at their defaults, unless there is a problem with the tunnel once its activated.
8. Click the **SAVE** button to save your new tunnel information.
9. Once the tunnel information is saved you can click the **Next** button to continue. The save and restart menus displayed. This reboots the RouteFinder software and applies the new tunnel configuration.

RouteFinder
SOHO VPN Gateway

SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP

Main menu

TIME ZONE SETTINGS

DEVICE IP SETTINGS

ISP SETTINGS

ISP ADDITIONAL SETTINGS

MODEM SETTINGS

VPN SETTINGS

SAVE & RESTART

Logout

VPN SETTINGS

Connection Name:

Enable UID (Unique Identifier String)
 Disable UID

Local IPSEC Identifier:

Remote IPSEC Identifier:

Enabled Keep Alive
 Enabled NetBIOS Broadcast

Remote Site: Single User LAN

Remote IP Network:

Remote IP Netmask:

Remote Gateway IP/FQDN:

Network Interface:

Secure Association: IKE Manual

Perfect Forward Secure: Enabled Disabled

Encryption Protocol:

PreShared Key:

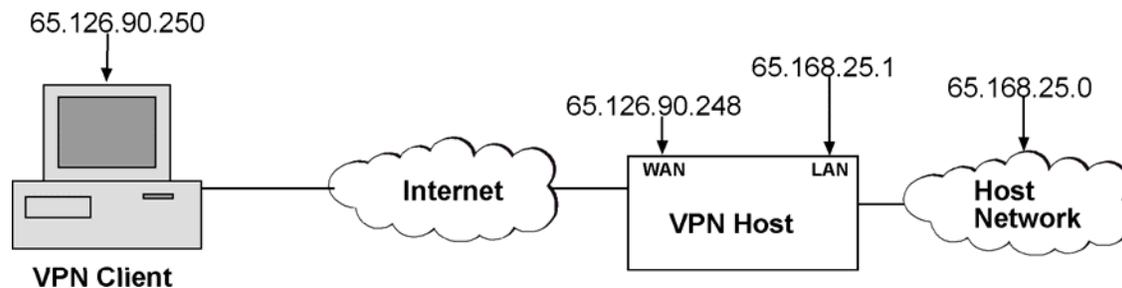
Key Life: Seconds

IKE Life Time: Seconds

SAVE

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input checked="" type="checkbox"/>	testconnection			<input type="button" value="Edit"/> <input type="button" value="Del"/>

RF560VPN Setup: Enabling VPN (Non-NAT)



1. In the RouteFinder RF560VPN, VPN Settings – IPSec menu, check the box to **Enable IPSec Function**.
2. In the **Connection Name** window, enter the name of your VPN client.
3. Click the **Add** button to add the tunnel and the **VPN Settings – IPSec** menu is displayed.

The screenshot shows the **RouteFinder** web interface for the **SOHO VPN Gateway**. The main navigation bar includes **DEVICE INFORMATION**, **DEVICE STATUS**, **SETUP WIZARD**, **ADVANCED SETTINGS**, **SYSTEM TOOLS**, and **HELP**. The current page is **VPN SETTINGS - IPSec**. The **Enable IPSec Function** checkbox is checked. The **Connection Name** field contains **Testconnection**, and the **Add** button is highlighted. Below the form is a table with the following structure:

Enable	Connection Name	Local IPSec ID	Remote IPSec ID	Command

At the bottom of the page, there are **< BACK** and **NEXT >** buttons, and a **Copyright © 2003** notice.

RF560VPN VPN Tunnel Setup (Non-NAT)

1. Check **Enabled Keep Alive** to keep the tunnel up constantly.
2. Click on **LAN** option in Remote Site (Default).
3. In **Remote Gateway IP/FQDN** option, the IP address of 0.0.0.0 if a Dynamic address is being used or if a static address (e.g., 65.126.90. 250) is provided by your ISP.
4. In the **Secure Association** option, the default of **Main Mode** is OK and in **Perfect Forward Secure**, the default of **Enabled** is OK.
5. The **Encryption Protocol** has to match on each end of the tunnel; **3Des** is the most common setting.
6. In the **PreShared Key**, the shared secret has to match on both ends of the tunnel.
7. In **Key Life**, default of **28800** and **IKE Life Time**, default of **3600** can be left at their defaults, unless there is a problem with the tunnel once its activated.
8. Click the **SAVE** button to save your new tunnel information.
9. Once the tunnel information is saved you can click the **Next** button to continue to the save and restart menu. This reboots the RouteFinder software and applies the new tunnel configuration.

RouteFinder
SOHO VPN Gateway

SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP

Back

IPSec SETTINGS

PPTP SETTINGS

Logout

VPN SETTINGS - IPSec

Connection Name

Enable UID (Unique Identifier String) Disable UID

Local IPSec Identifier

Remote IPSec Identifier

Enabled Keep Alive Enabled NetBIOS Broadcast

Remote Site Single User LAN

Remote IP Network

Remote IP Netmask

Remote Gateway IP/FQDN

Network Interface

Secure Association Main Mode Aggressive Manual

Perfect Forward Secure Enabled Disabled

Encryption Protocol

PreShared Key

Key Life Seconds

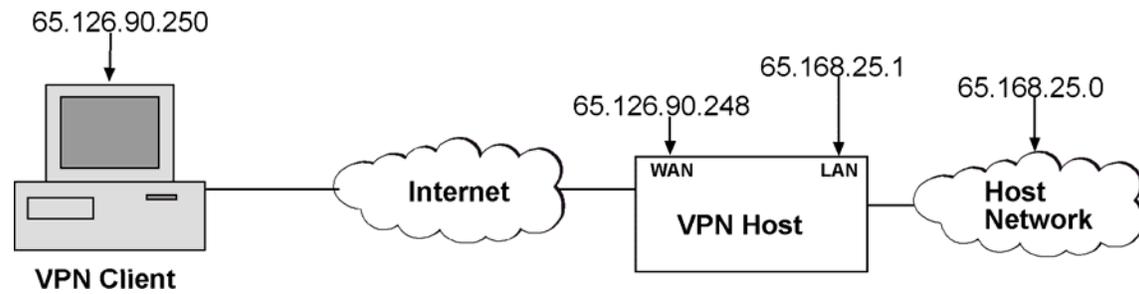
IKE Life Time Seconds

SAVE

Enable	Connection Name	Local IPSec ID	Remote IPSec ID	Command
<input checked="" type="checkbox"/>	testconnection			<input type="button" value="Edit"/> <input type="button" value="Del"/>

< BACK
NEXT >

RF600,660,760VPN Setup: Enabling VPN (Non-NAT)



1. In the RouteFinder RF600,660,760VPN software, click the **VPN Status** check box.
2. Click the **Save** button to save the setting.
3. In the **Add IKE Connection**, click on the Add button. The **Add IKE Connection** screen is displayed.



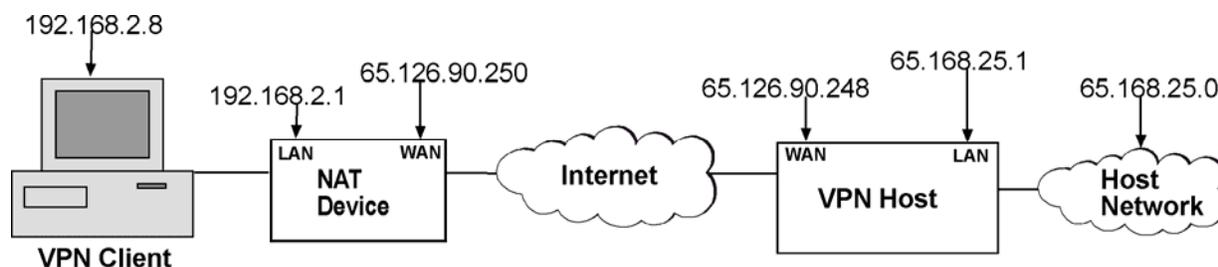
RF600,660,760VPN - VPN Tunnel Setup (Non-NAT)

1. In the RouteFinder RF600,660,760, **Add IKE Connection** menu, enter the name of your VPN tunnel in the **Connection Name** field.

The screenshot shows the 'Add IKE Connection' configuration window. The 'Connection Name' field is set to 'testconnection'. The 'Perfect Forward Secrecy' checkbox is checked. The 'Authentication Method' is set to 'Secret' and the 'Secret' field contains 'test'. The 'Select Encryption' is set to 'DES'. The 'IKE Life Time (in secs)' is 3600 and 'Key Life (in secs)' is 28800. The 'Number of retries(zero for unlimited)' is 0. The 'Local WAN IP' is set to 'WAN', 'Local LAN' is 'LAN', and 'Remote Gateway IP' is 'Any'. The 'Remote LAN' is set to 'none'. The 'UID' is set to 'Disable'. The 'Add' button is at the bottom right.

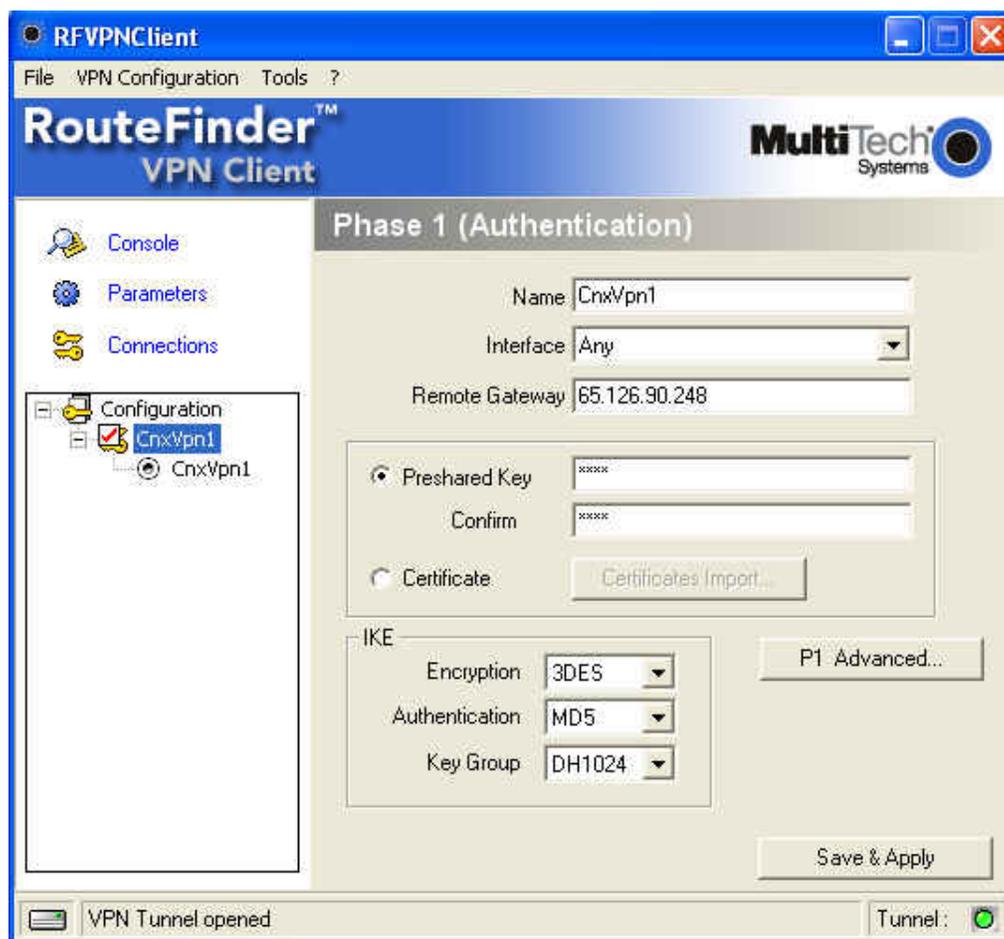
2. **Compression**, **Perfect forward secrecy**, and **Authentication Method** options can be left at their default.
3. In **Secret**, enter the shared secret which has to match on both ends of the tunnel.
4. **IKE life Time & Key life** options can be left at their defaults, unless there are problems with the tunnel once activated.
5. **Number of retries**(zero for unlimited) should be **0**.
6. In **Local WAN IP**, choose **WAN** which was setup in the network and services tab (e.g., 65.126.90.248).
7. In **Local LAN**, choose **LAN** which was setup in the network and services tab (e.g., 65.168.25.1).
8. **Remote Gateway IP** can be set to **Any** if the IP address is dynamic or the static IP of the remote if there is one (e.g., 65.126.90.250).
9. **Remote LAN** is the network you created in network and services for this client (e.g., 65.126.90.250) or you can select none if the IP address is Dynamic.
10. Click the **Add** button to save these settings for your new tunnel.

Setup for VPN Client (Behind NAT)



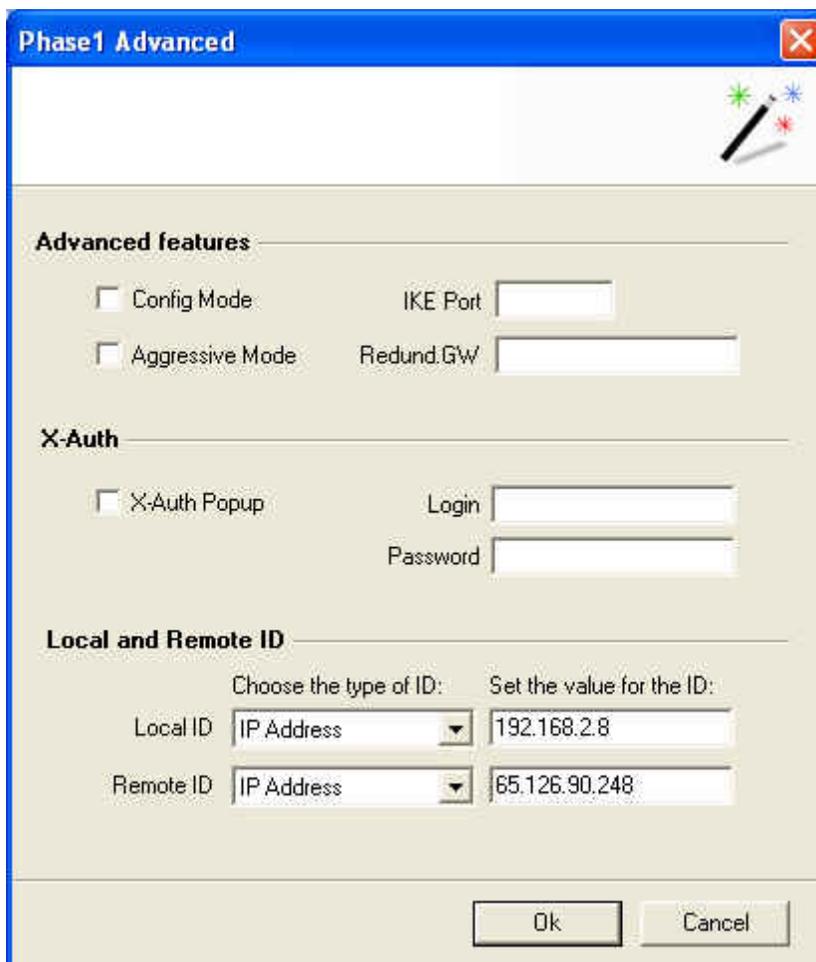
Client Phase 1 Setup (Behind NAT)

1. Right click on RouteFinder Client **VPN Configuration** and select **New Phase 1**.
2. Enter the name of your connection in **Name**.
3. Enter in **Any** for client Interface if your IP address is dynamic or the IP address provided by your ISP if static (e.g., 192.168.2.8).
4. Enter the IP address of your WAN in **Remote Gateway** (e.g., 65.126.90.248).
5. Enter the Shared Secret in **Preshared Key** for your network (has to match on both ends) and **confirm** the shared secret.
6. Choose **IKE authentication** of **MD5**.



Client Phase 1 Advanced Setup (Behind NAT)

1. Click on the **P1 Advanced** button in the Phase 1 (Authentication) menu. The Phase1 Advanced menu is displayed.

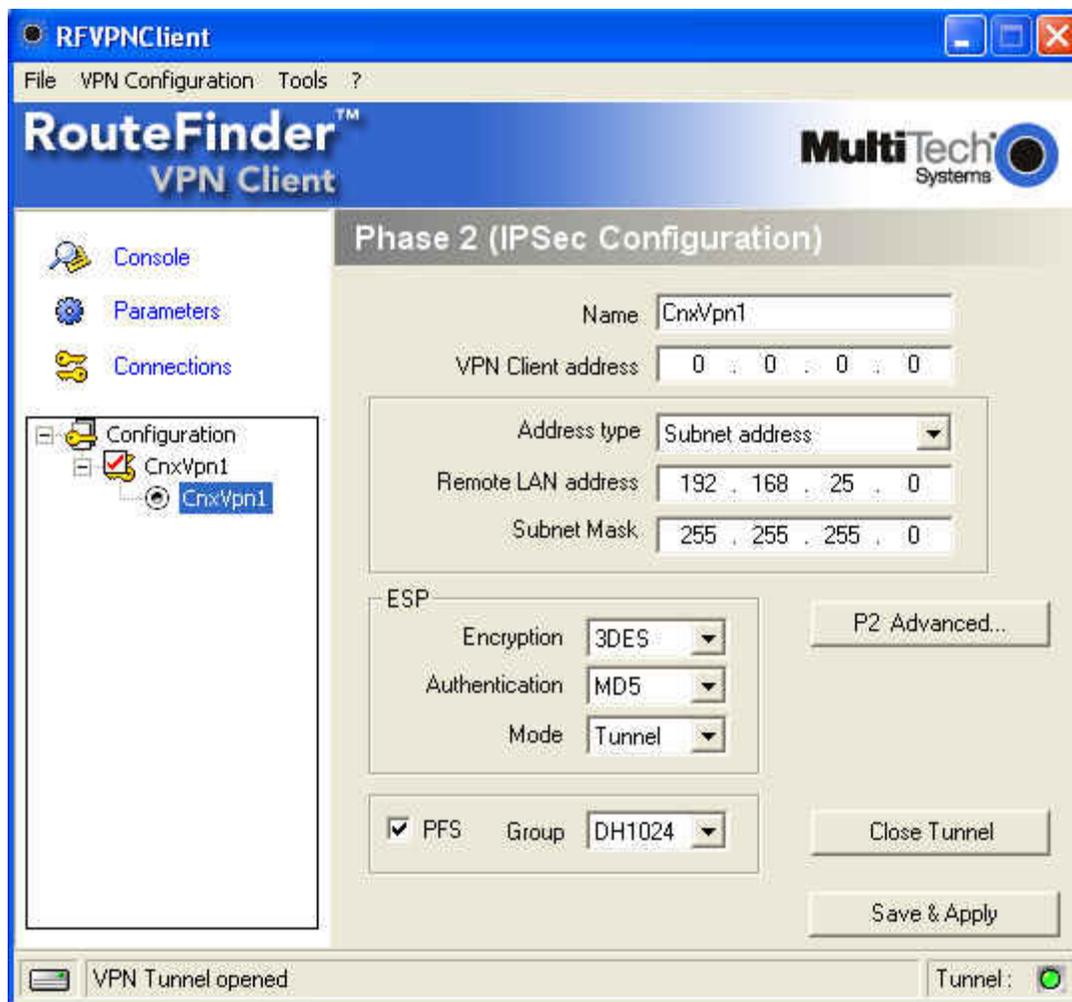


The screenshot shows the 'Phase1 Advanced' configuration window. It has a blue title bar with the text 'Phase1 Advanced' and a close button. The window is divided into three sections: 'Advanced features', 'X-Auth', and 'Local and Remote ID'. In the 'Advanced features' section, there are two checkboxes: 'Config Mode' and 'Aggressive Mode', both of which are unchecked. To the right of these are two text input fields: 'IKE Port' and 'Redund.GW'. In the 'X-Auth' section, there is a checkbox for 'X-Auth Popup' which is unchecked, and two text input fields for 'Login' and 'Password'. In the 'Local and Remote ID' section, there are two rows. The first row is for 'Local ID' and the second is for 'Remote ID'. Each row has a dropdown menu for 'Choose the type of ID:' and a text input field for 'Set the value for the ID:'. For 'Local ID', the dropdown is set to 'IP Address' and the value is '192.168.2.8'. For 'Remote ID', the dropdown is set to 'IP Address' and the value is '65.126.90.248'. At the bottom right of the window are 'Ok' and 'Cancel' buttons.

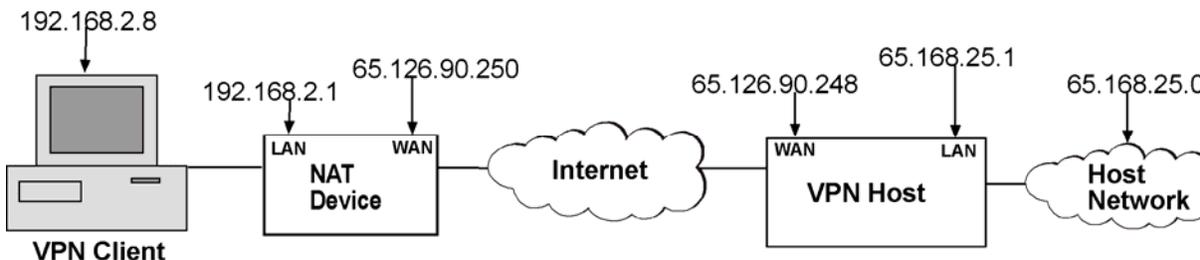
2. Choose **IP Address** for **Local ID** and **Remote ID**.
3. Enter the IP address of the VPN Client in Set the value for the ID: **local ID** (e.g., 192.168.2.8).
4. Enter the IP address of the RouteFinder in Set the value for the ID: **Remote ID** (e.g., 65.126.90.248).
5. Click **OK**.

Client Phase 2 Setup (Behind NAT)

1. Start Phase 2 by Right clicking on the name of your VPN Client you created in Phase 1.
2. **VPN Client address** will be set to 0.0.0.0, unless you have a Static IP address (e.g., 192.168.2.8)
3. Address type is the type of setup on the host side. If it's a **network**, then choose **Subnet address** and enter in the **Remote LAN** address (e.g., 192.168.25.0) and Subnet Mask (e.g., 255.255.255.0). If it's a single IP address, change it to that address.
4. Choose **ESP Authentication** of **MD5**.



RF550VPN Setup: Enabling VPN (NAT using UID)



1. In the RouteFinder RF550VPN, VPN Settings menu, enter the name of your VPN tunnel in the **Connection Name** field.
2. Click the **ADD** button to add the tunnel and VPN Settings menu is displayed.

RouteFinder SOHO VPN Gateway

SOHO VPN Gateway

DEVICE INFORMATION | DEVICE STATUS | SETUP WIZARD | ADVANCED SETTINGS | SYSTEM TOOLS | HELP

Main menu

TIME ZONE SETTINGS

DEVICE IP SETTINGS

ISP SETTINGS

ISP ADDITIONAL SETTINGS

MODEM SETTINGS

VPN SETTINGS

SAVE & RESTART

Logout

Copyright © 2002

VPN SETTINGS

Connection Name: testconnection **ADD**

Disable Internet Access (VPN Tunnel Only)

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input type="checkbox"/>				

< BACK | NEXT >

RF550VPN VPN Tunnel Setup (NAT using UID)

1. Click **Enable UID (Unique Identifier String)**.
2. Check **Enabled Keep Alive** to keep the tunnel up constantly.

RouteFinder SOHO VPN Gateway

DEVICE INFORMATION | DEVICE STATUS | SETUP WIZARD | ADVANCED SETTINGS | SYSTEM TOOLS | HELP

Main menu

TIME ZONE SETTINGS

DEVICE IP SETTINGS

ISP SETTINGS

ISP ADDITIONAL SETTINGS

MODEM SETTINGS

VPN SETTINGS

SAVE & RESTART

Logout

VPN SETTINGS

Connection Name: testconnection

Enable UID (Unique Identifier String) Disable UID

Local IPSEC Identifier: 65.126.90.248

Remote IPSEC Identifier: 192.168.2.8

Enabled Keep Alive Enabled NetBIOS Broadcast

Remote Site: Single User LAN

Remote IP Network: 192.168.2.8

Remote IP Netmask: 255.255.255.255

Remote Gateway IP/FQDN: 65.126.90.250

Network Interface: WAN ETHERNET

Secure Association: IKE Manual

Perfect Forward Secure: Enabled Disabled

Encryption Protocol: 3DES

PreShared Key: test

Key Life: 28800 Seconds

IKE Life Time: 3600 Seconds

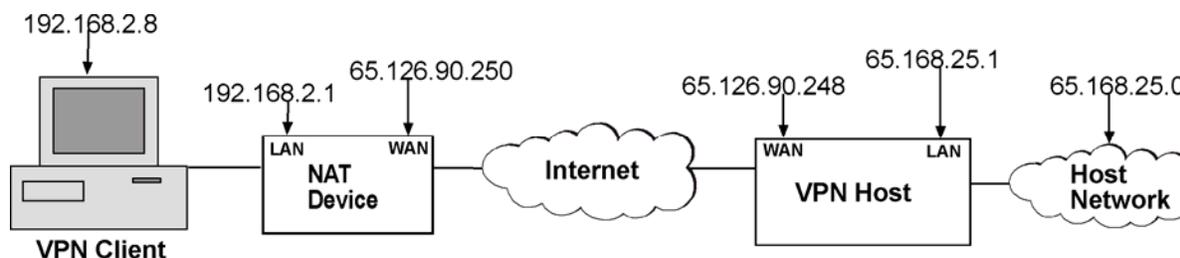
SAVE

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input checked="" type="checkbox"/>	testconnection	65.126.90.248	192.168.2.8	Edit Del

< BACK NEXT >

3. Enter the RouteFinder IP address in the **Local IPsec Identifier** (e.g., 65.126.90.248)
4. Enter VPN Client address in the **Remote IPsec Identifier** (e.g., 192.168.2.8)
5. **Remote Site** by default is set to **LAN**.
6. Enter in the **Remote IP Network** address, the IP address of the VPN client (e.g., 192.168.2.8)
7. Enter in the **Remote IP Netmask**, the netmask of (e.g., 255.255.255.255)
8. Enter in the **Remote Gateway IP/FQDN**, the IP address provided by your ISP for the client (e.g., 65.126.90.250) or 0.0.0.0 for dynamic.
9. In the **Secure Association** option, the default of **IKE** is OK and in **Perfect Forward Secure**, the default of **Enabled** is OK.
10. The **Encryption Protocol** has to match on each end of the tunnel; **3Des** is the most common setting.
11. In the **Preshared Key**, the Shared Secret has to match on both ends of the tunnel
12. In **Key Life**, default of **28800** and **IKE Life Time**, default of **3600** can be left at default unless there is a problem with the tunnel once its activated.
13. Click the **SAVE** button to save your new tunnel Information.
14. Once the tunnel information is saved you can click the **Next** button to continue. The save and restart window is displayed. This reboots the RouteFinder software and applies the new tunnel configuration.

RF560VPN Setup: Enabling VPN (NAT using *UID*)



1. In the RouteFinder RF560VPN, VPN Setting – IPsec menu, check the **Enable IPsec Function**.
2. In the **Connection Name** window, enter the name of your VPN client.
3. Click the **Add** button to add the tunnel and the **VPN Settings – IPsec** menu is displayed.

The screenshot shows the **RouteFinder** web interface for a **SOHO VPN Gateway**. The navigation menu includes **DEVICE INFORMATION**, **DEVICE STATUS**, **SETUP WIZARD**, **ADVANCED SETTINGS**, **SYSTEM TOOLS**, and **HELP**. The current page is **VPN SETTINGS - IPsec**. It features a sidebar with **Back**, **IPsec SETTINGS**, **PPTP SETTINGS**, and **Logout**. The main content area shows the **Enable IPsec Function** checkbox checked. Below it, the **Connection Name** field contains "Testconnection" and an **Add** button. There is also an unchecked checkbox for **Disable Internet Access (IPsec Tunnel Only)**. At the bottom, there is a table with columns: **Enable**, **Connection Name**, **Local IPsec ID**, **Remote IPsec ID**, and **Command**. Navigation buttons **< BACK** and **NEXT >** are located at the bottom of the page. The footer indicates **Copyright © 2003**.

RF560VPN VPN Tunnel Setup (NAT using UID)

1. Click **Enable UID (Unique Identifier String)**.
2. Check **Enabled Keep Alive** to keep the tunnel up constantly.

RouteFinder SOHO VPN Gateway

DEVICE INFORMATION | DEVICE STATUS | SETUP WIZARD | ADVANCED SETTINGS | SYSTEM TOOLS | HELP

Back

IPSec SETTINGS

PPTP SETTINGS

Logout

VPN SETTINGS - IPSec

Connection Name: testconnection

Enable UID (Unique Identifier String) Disable UID

Local IPsec Identifier: 65.126.90.248

Remote IPsec Identifier: 192.168.2.8

Enabled Keep Alive Enabled NetBIOS Broadcast

Remote Site: Single User LAN

Remote IP Network: 192 | 168 | 2 | 8

Remote IP Netmask: 255 | 255 | 255 | 255

Remote Gateway IP/FQDN: 65.126.90.250

Network Interface: WAN ETHERNET

Secure Association: Main Mode Aggressive Manual

Perfect Forward Secure: Enabled Disabled

Encryption Protocol: 3DES

PreShared Key: test

Key Life: 28800 Seconds

IKE Life Time: 3600 Seconds

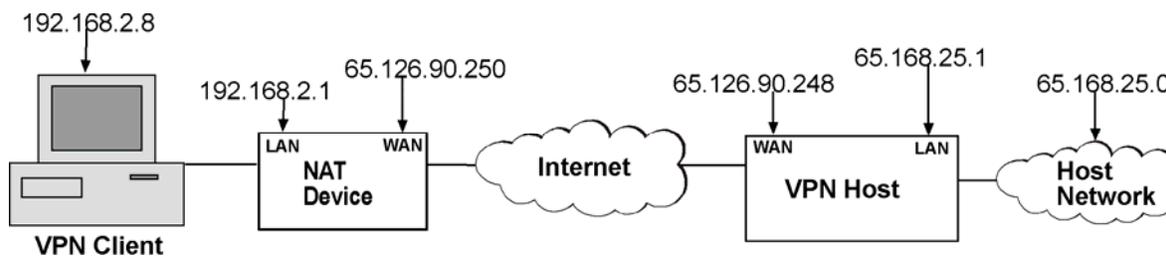
SAVE

Enable	Connection Name	Local IPsec ID	Remote IPsec ID	Command
<input checked="" type="checkbox"/>	testconnection	65.126.90.248	192.168.2.8	Edit Del

< BACK NEXT >

3. Enter the RouteFinder IP address in the **Local IPsec Identifier** (e.g., 65.126.90.248).
4. Enter the VPN Client address in the **Remote IPsec Identifier** (e.g., 192.168.2.8).
5. **Remote Site** by default is set to **LAN**.
6. Enter in the **Remote IP address**, the IP address of the VPN client (e.g., 192.168.2.8).
7. Enter in the **Remote IP netmask**, the netmask of (e.g., 255.255.255.255).
8. In the **Remote Gateway IP/FQDN**, the IP address provided by your ISP for the client (e.g., 65.126.90.250) or 0.0.0.0 for dynamic.
9. In the **Secure Association** option, the default of **Manual** is OK and in **Perfect Forward Secure**, the default of **Enabled** is OK.
10. The **Encryption Protocol** has to match on each end of the tunnel; **3Des** is the most common setting.
11. In the **Preshared Key**, Shared Secret has to match on both ends of the tunnel
12. In **Key Life**, the default of **28800** and in **IKE Life Time**, the default of **3600** can be left at default unless there is a problem with the tunnel once its activated.
13. Click the **SAVE** to save your new tunnel information.
14. Once the tunnel information is saved, you can click the **Next** button to continue. The save and restart window is displayed. This reboots the RouteFinder software and applies the new tunnel configuration.

RF600,660,760VPN Setup:Enabling VPN (NAT using *UID*)



1. In the RouteFinder RF600,660,760VPN software, check the **VPN status** box.
2. Click the **Save** button to save this setting.
3. In the **Add IKE Connection**, click the Add button. The **Add IKE Connection** screen is displayed.

The screenshot shows the MultiTech Systems VPN configuration interface. The top navigation bar includes: Administration | Networks & Services | Proxy | Network Setup | DHCP Server | Tracking | Packet Filters | **VPN** | Statistics & Logs. The left sidebar shows: VPN, IPsec, X.509 Certificates, IPsec Bridging, and PPTP. The main content area is titled "VPN >> IPsec" and includes a "Home | Wizard Setup | Help | Logout" link. The "IPsec" section shows "VPN Status" with a checked checkbox and a "Save" button. Below this is the "Add New Connection" section, which includes "Add IKE Connection" and "Add Manual Connection" buttons. At the bottom, there is a table with the following columns: Status, Connection Name, Local WAN IP, Local LAN, Remote Gateway IP, Remote LAN, and Command.

Status	Connection Name	Local WAN IP	Local LAN	Remote Gateway IP	Remote LAN	Command

RF600,660,760VPN - VPN Tunnel Setup (NAT using UID)

1. In the RouteFinder RF600,660,760VPN, **Add IKE Connection** menu, enter the name of your VPN tunnel in the **Connection Name** field.

The screenshot shows the 'Edit IKE Connection' configuration page. The settings are as follows:

Field	Value
Connection Name	test-VPN
Compression	<input type="checkbox"/>
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Authentication Method	Secret
Secret	test
Select Encryption	3DES
IKE Life Time (in secs)	3600
Key Life (in secs)	28800
Number of retries(zero for unlimited)	0
Local WAN IP	WAN
Local LAN	LAN
Remote Gateway IP	test-vpn-wan
OR	
FQDN	
Remote LAN	test-vpn-client
UID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local ID	65.126.90.248
Remote ID	192.168.2.8
NetBIOS Broadcast	<input type="checkbox"/>

A 'Save' button is located at the bottom right of the form.

2. **Compression**, **Perfect forward secrecy**, and **Authentication Method** options can be left at their default.
3. In **Secret**, enter the shared secret which has to match on both ends of the tunnel.
4. **IKE life time** & **Key life** options can be left at default unless there are problems with the tunnel once its activated.
5. **Number of retries** should be set to **0**.
6. In **Local WAN IP** choose **WAN** which was setup in the network and services tab (e.g., 65.126.90.248).
7. In **Local LAN** choose **LAN** which was setup in the network and services tab (e.g., 65.168.25.1).
8. **Remote Gateway** can be set to **Any** if the IP address is dynamic or the static IP of the remote gateway if there is one (e.g., 65.126.90.250).
9. **Remote LAN** is the network you created in network and services for this client (e.g., 192.168.2.8) or you can select none if the IP address is dynamic.
10. Click on **Enable** for the UID option.
11. Enter the IP address of the Local VPN host in the **local ID** (e.g., 65.126.90.248).
12. Enter the IP address of the remote VPN client in the **Remote ID** (e.g., 192.168.2.8).
13. Click the **Save** button to save these settings for your new tunnel.