RouteFinder™

Internet Security Appliance

IPSec VPN Client

Setup Examples

Reference Guide

MultiTech Systems

RouteFinder IPSec VPN Client
Setup Examples
PN S000397A Revision A

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

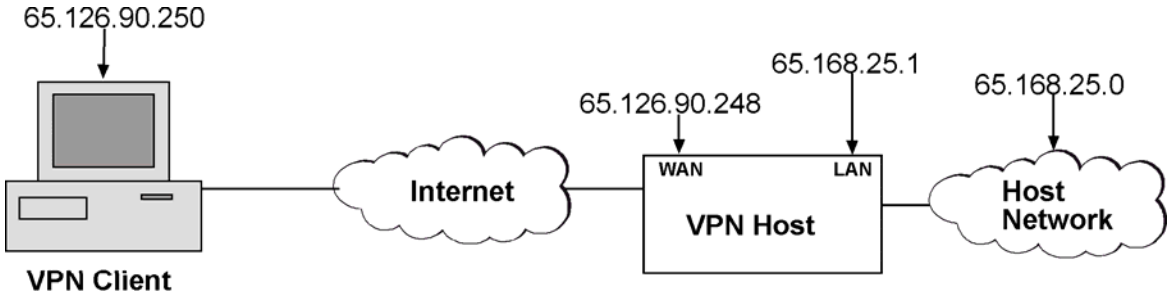
Introduction

The examples on the following pages are divided into two major catagories; 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.

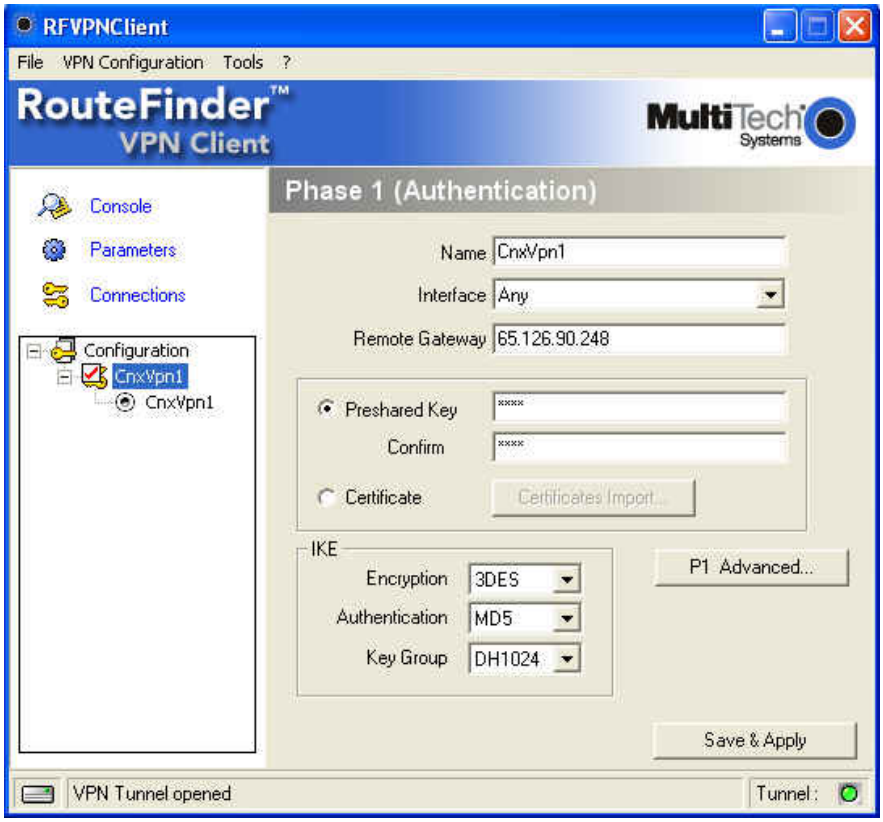
Setup for behind NAT starts out the same way with the configuration of the VPN client and then the addition of the Phase 1 Advanced for the IP addresses for the local and remote. The Behind NAT then configures the RF550 with NAT using UID, followed by the RF560 with IPSec protocol. The RouteFinder RF600,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

Setup for VPN Client (Non-NAT)



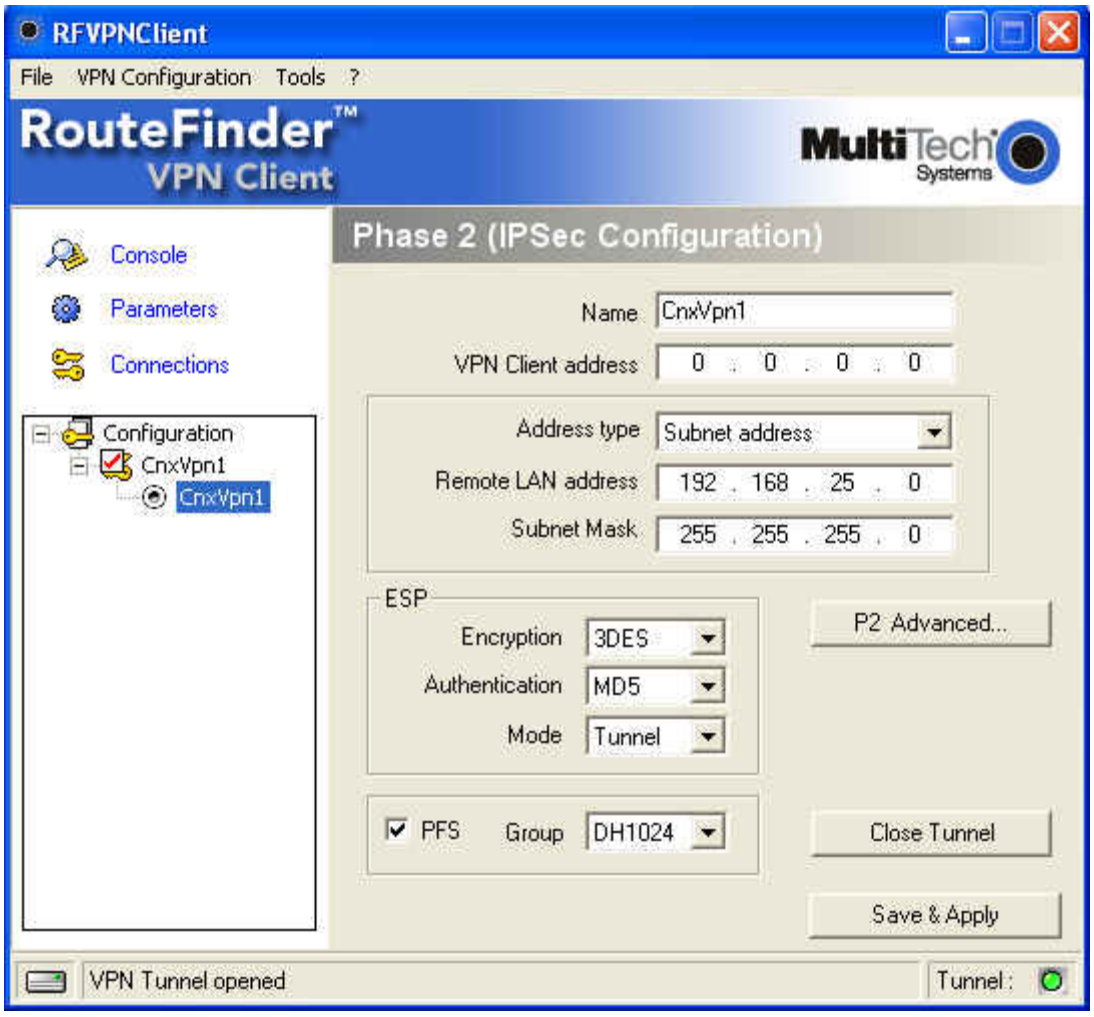
VPN client Phase 1 Setup (Non-NAT)

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**.

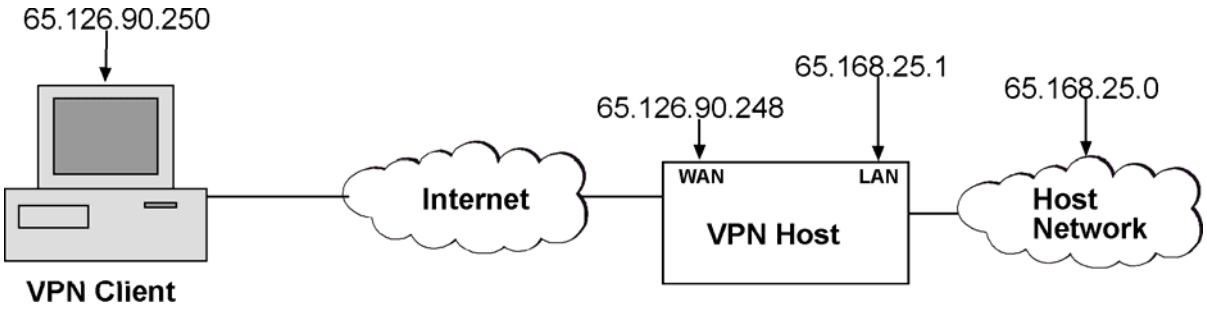


Phase 2 Setup (Non-NAT)

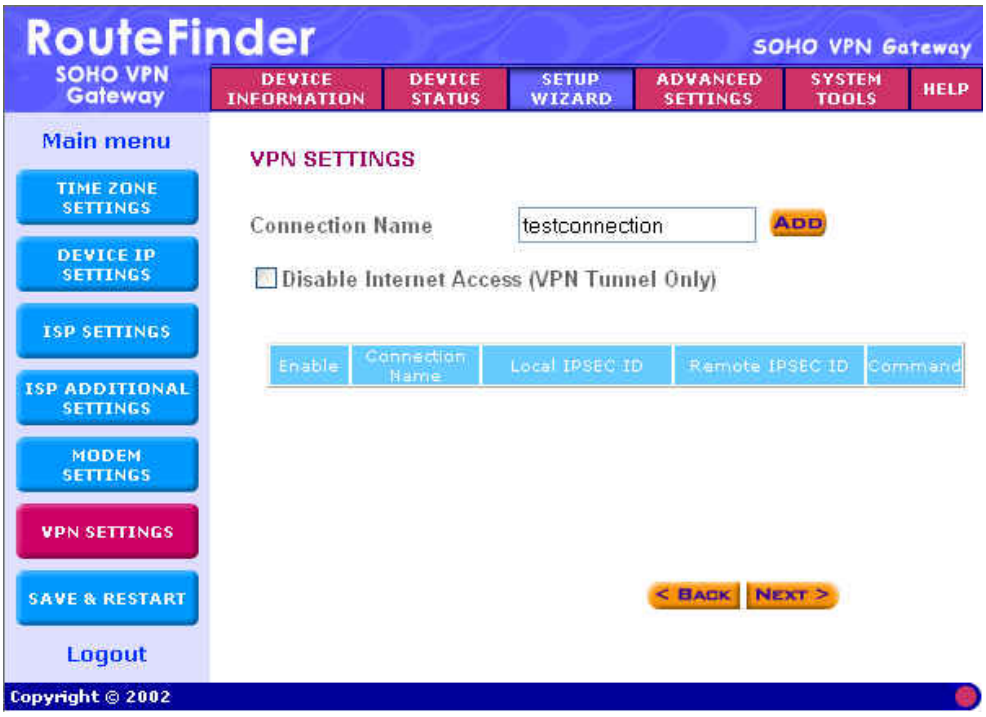
1. Start Phase 2 by right clicking on the name of your VPN Client you created in Phase 1.
2. VPN Client address will be set to 0.0.0.0 unless you have a Static IP address (e.g., 65.126.90.250).
3. Address type is the type of setup on the host side. If it's a **network**, then choose **Subnet address** 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)

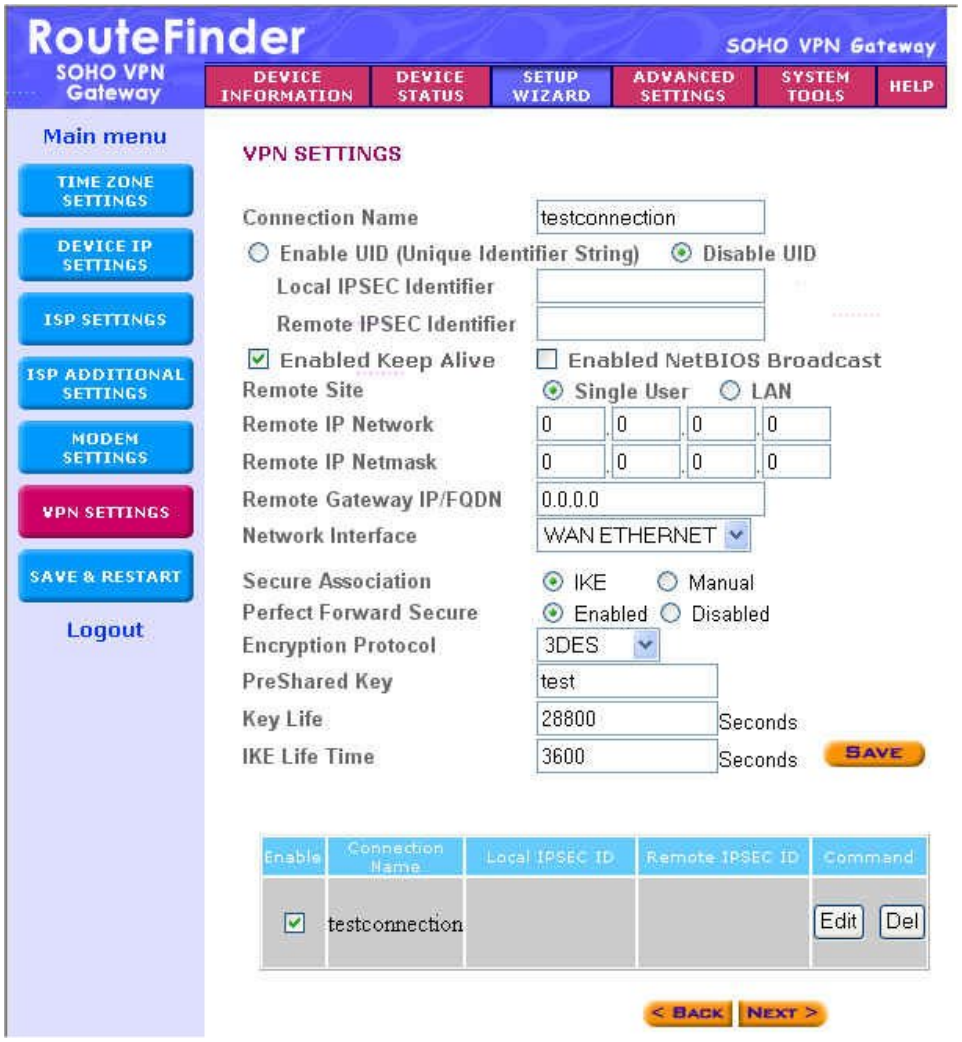


1. In the RouteFinder RF550VPN, VPN Settings menu, enter the name of your VPN tunnel in the **Connection Name** field.
2. Click the **ADD** button to add the tunnel and the VPN Settings menu is displayed.

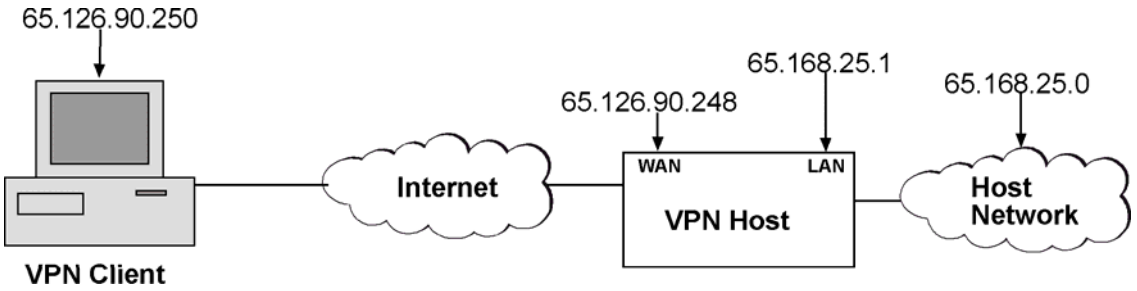


RF550VPN VPN tunnel Setup (Non-NAT)

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 shave your new tunnel information.
9. Once the tunnel information is saved you can click the **Next** button to continue. The save and restart menuis displayed. This reboots the RouteFinder software and applies the new tunnel configuration.



RF560VPN Setup: Enabling VPN (Non-NAT)

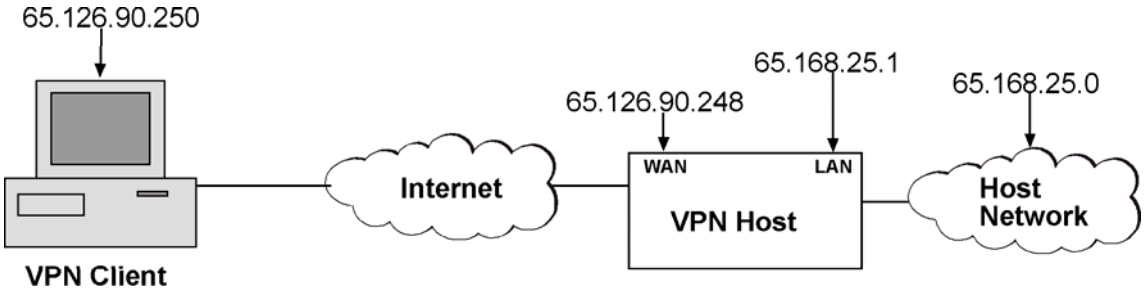


1. In the RouteFinder RF560VPN, VPN Settings – IPSec menu, check the box to **Enable IPSec Function**.
2. In the **Connection Name** window, enter the name of your VPN client.
3. Click the **Add** button to add the tunnel and the **VPN Settings – IPSec** menu is displayed.

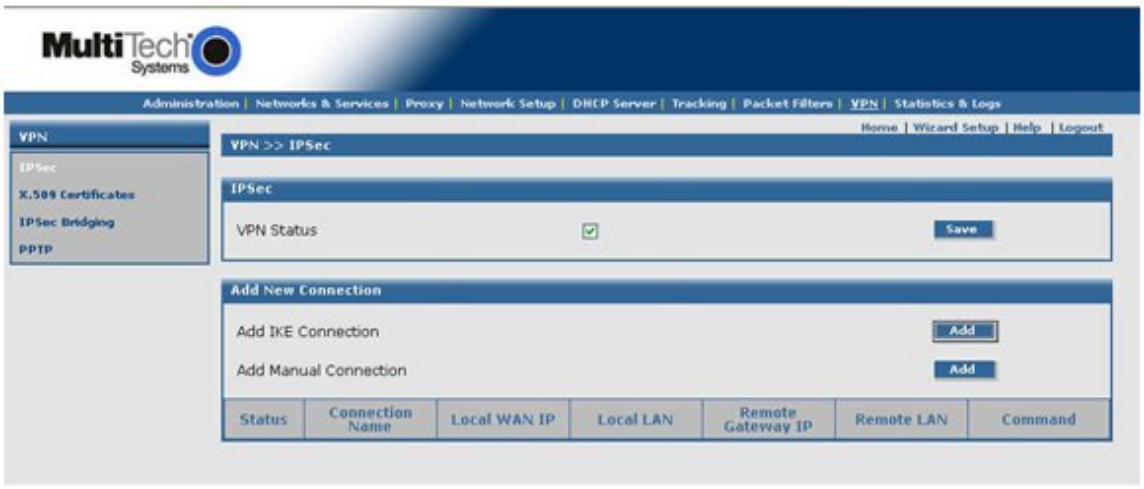
RF560VPN VPN Tunnel Setup (Non-NAT)

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.

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

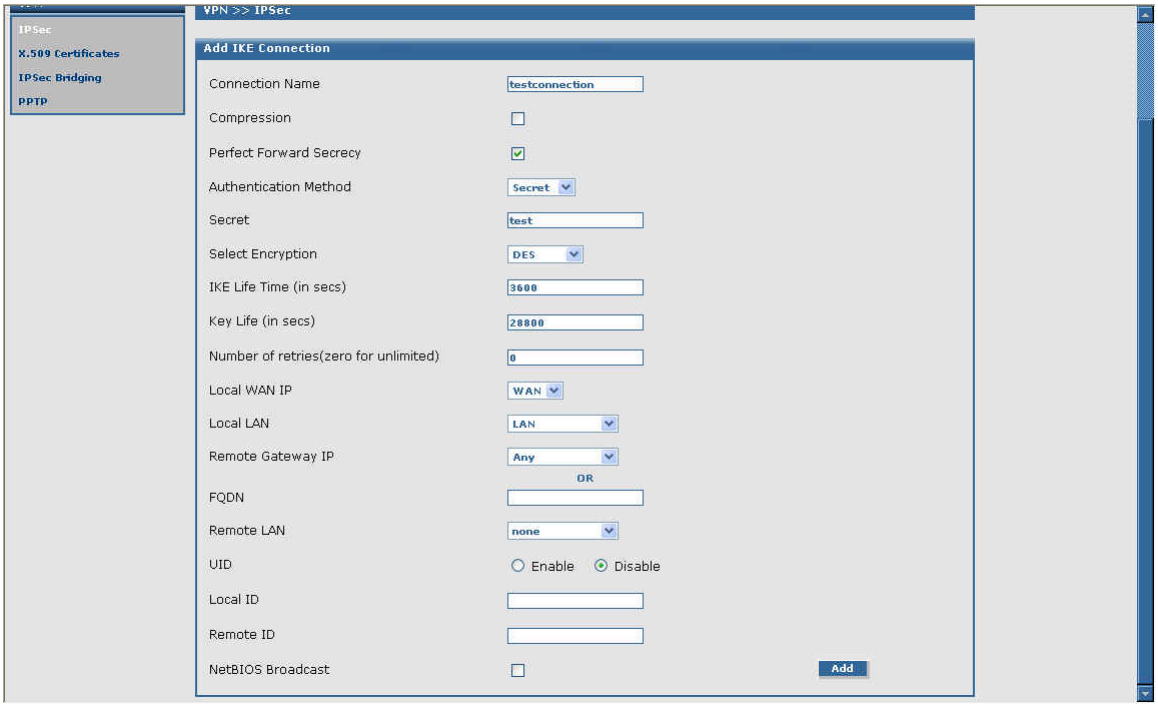


1. In the RouteFinder RF600,660,760VPN software, click the **VPN Status** check box.
2. Click the **Save** button to save the setting.
3. In the **Add IKE Connection**, click on the Add button. The **Add IKE Connection** screen is displayed.



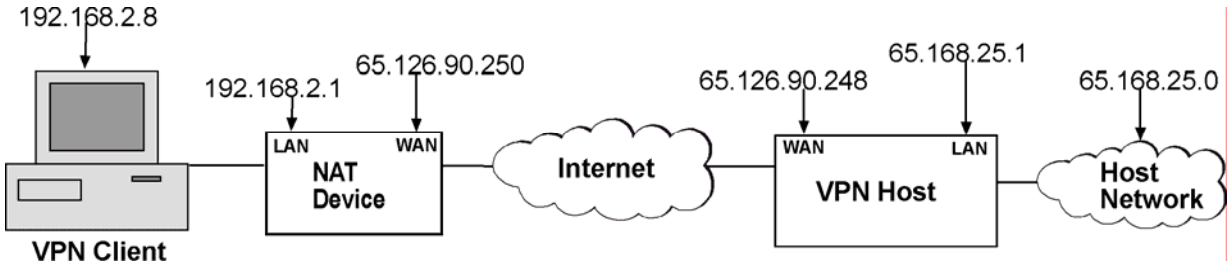
RF600,660,760VPN - VPN Tunnel Setup (Non-NAT)

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



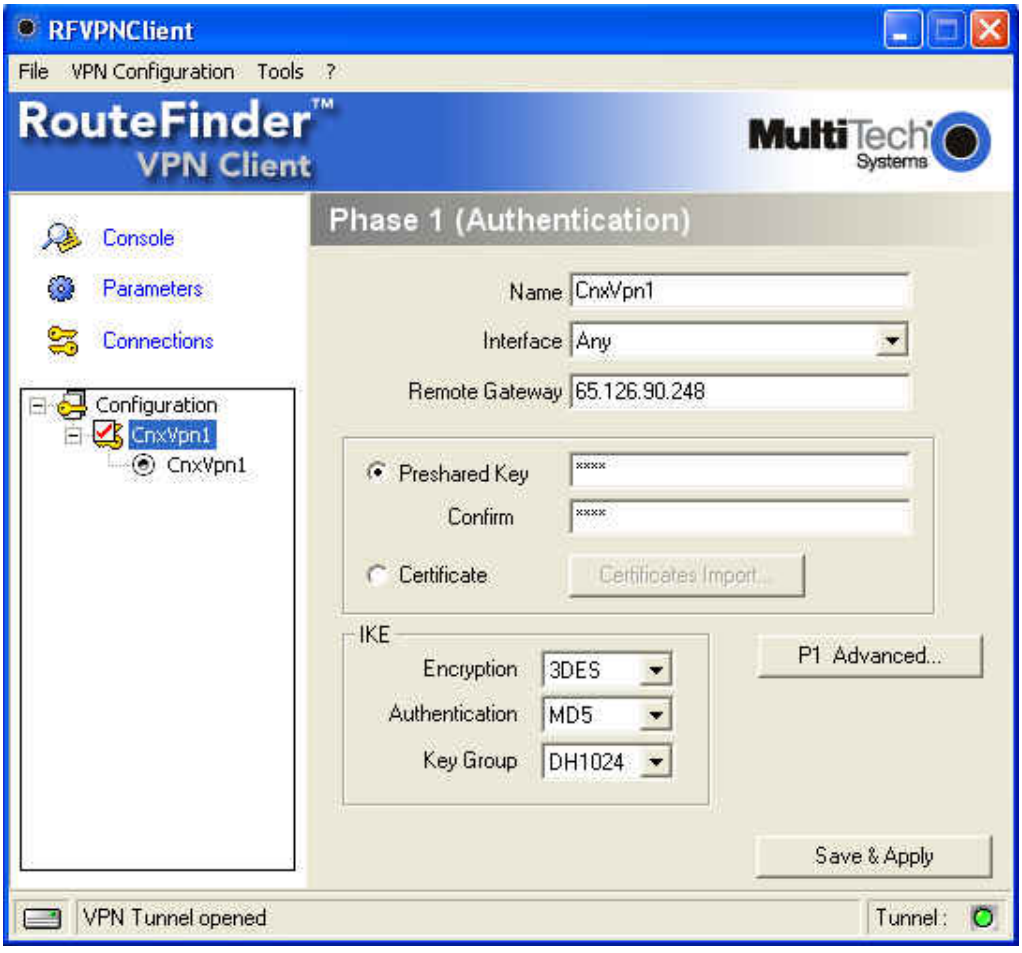
2. **Compression**, **Perfect forward secrecy**, and **Authentication Method** options can be left at their default.
3. In **Secret**, enter the shared secret which has to match on both ends of the tunnel.
4. **IKE life Time** & **Key life** options can be left at their defaults, unless there are problems 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)



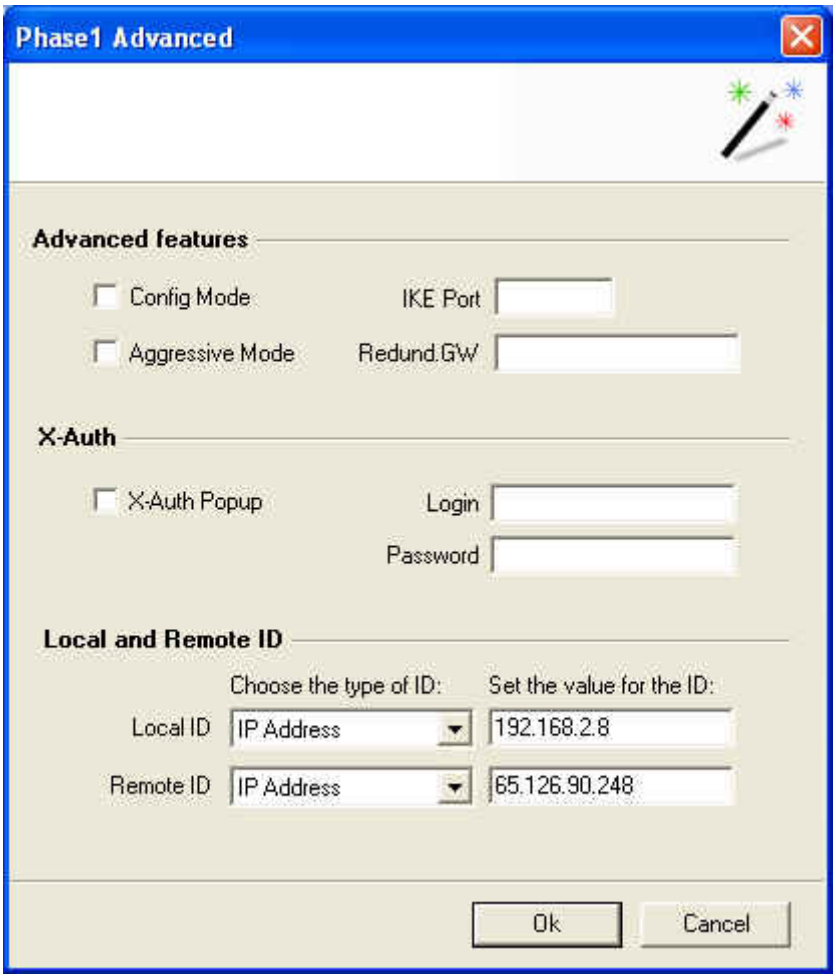
Client Phase 1 Setup (Behind NAT)

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)

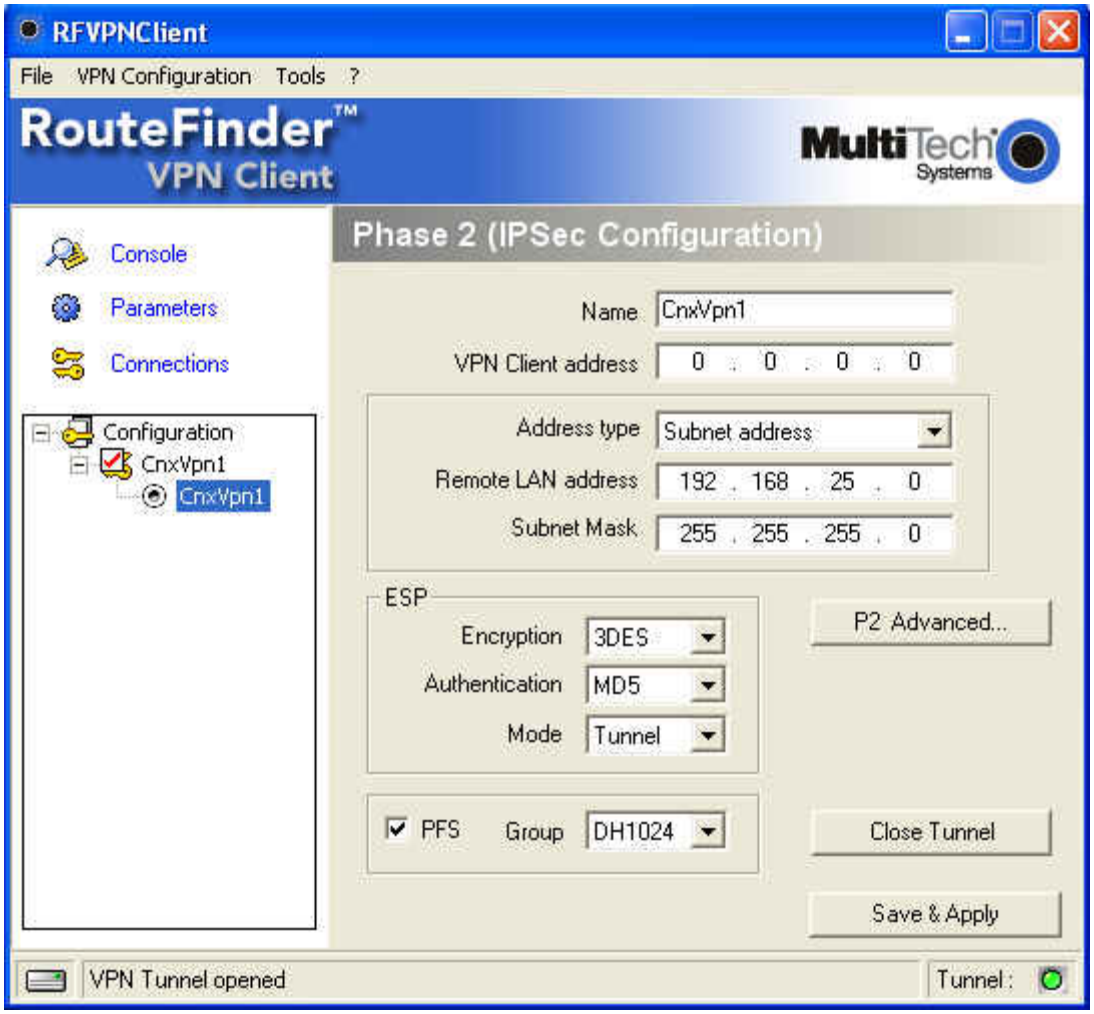
1. Click on the **P1 Advanced** button in the Phase 1 (Authentication) menu. The Phase1 Advanced menu is displayed.



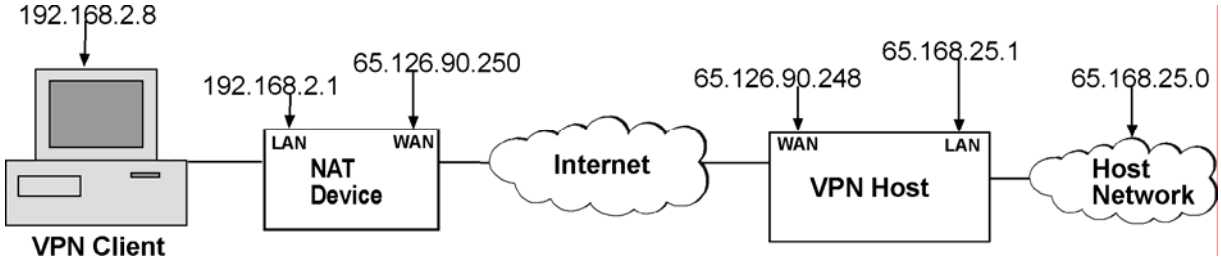
2. Choose **IP Address** for **Local ID** and **Remote ID**.
3. Enter the IP address of the VPN Client in Set the value for the ID: **local ID** (e.g., 192.168.2.8).
4. Enter the IP address of the RouteFinder in Set the value for the ID: **Remote ID** (e.g., 65.126.90.248).
5. Click **OK**.

Client Phase 2 Setup (Behind NAT)

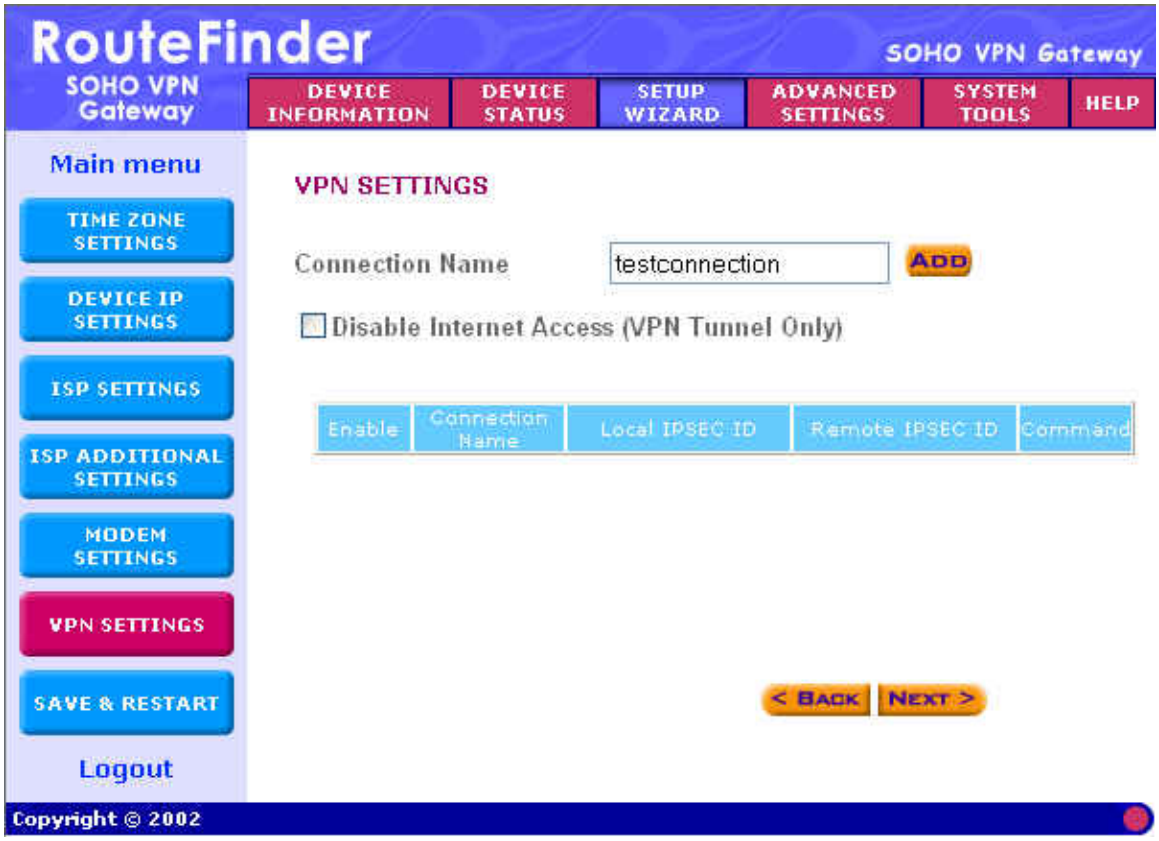
1. Start Phase 2 by Right clicking on the name of your VPN Client you created in Phase 1.
2. **VPN Client address** will be set to 0.0.0.0, unless you have a Static IP address (e.g., 192.168.2.8)
3. Address type is the type of setup on the host side. If it's a **network**, then choose **Subnet address** 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*)

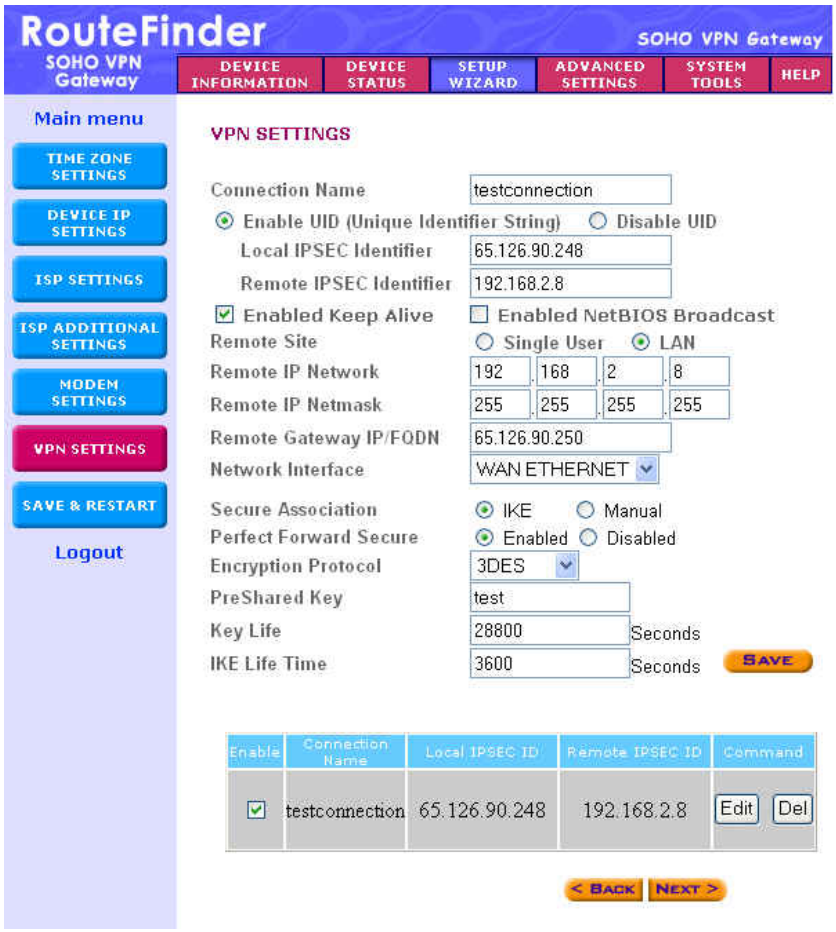


1. In the RouteFinder RF550VPN, VPN Settings menu, enter the name of your VPN tunnel in the **Connection Name** field.
2. Click the **ADD** button to add the tunnel and VPN Settings menu is displayed.



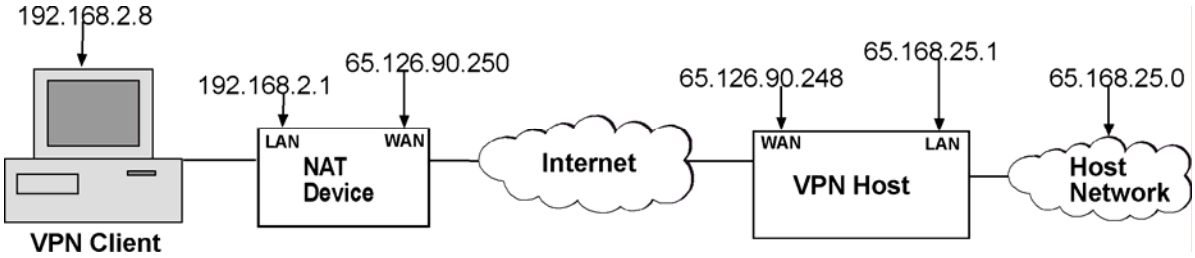
RF550VPN VPN Tunnel Setup (NAT using *UID*)

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



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.

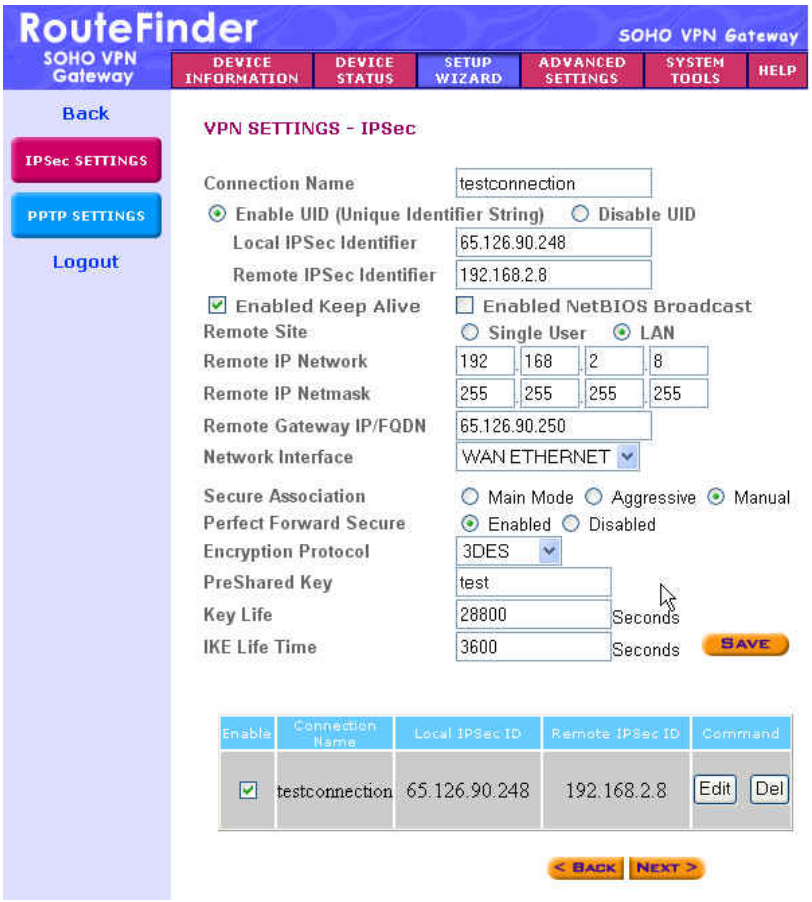
RF560VPN Setup: Enabling VPN (NAT using *UID*)



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.

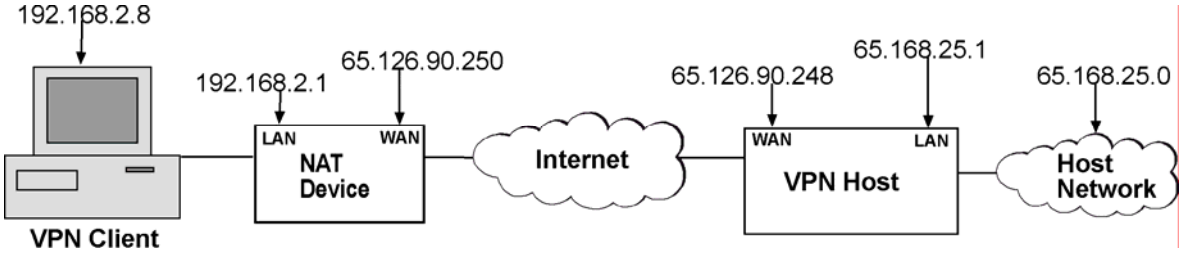
RF560VPN VPN Tunnel Setup (NAT using UID)

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

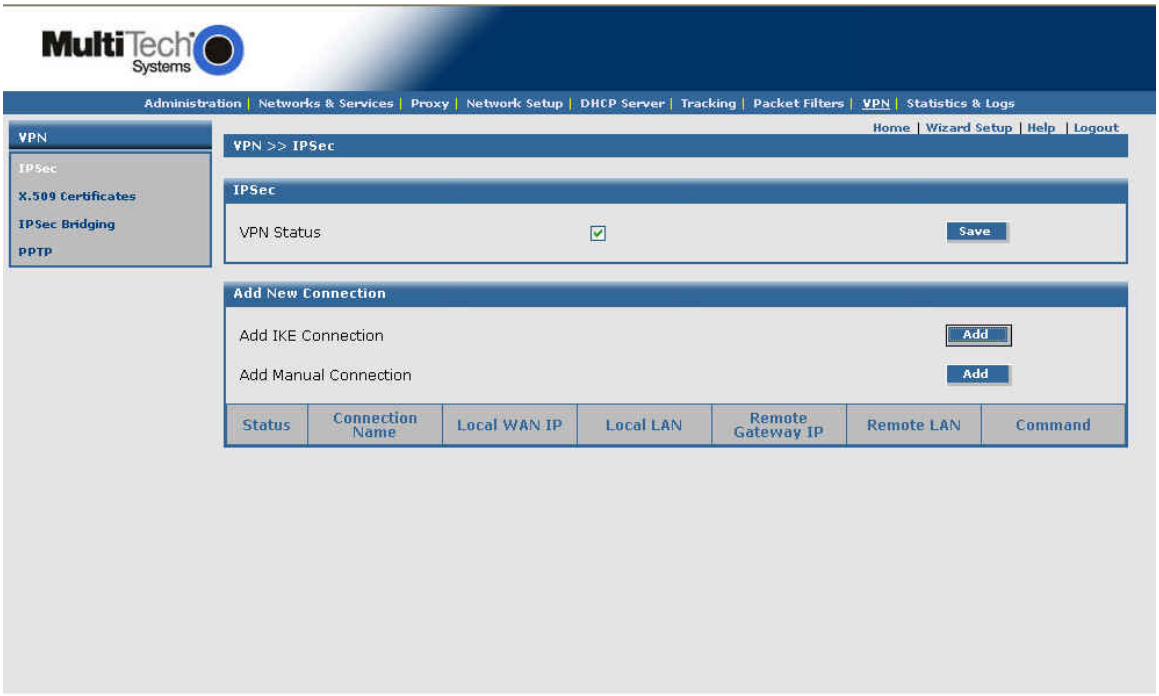


3. Enter the RouteFinder IP address in the **Local IPSec Identifier** (e.g., 65.126.90.248).
4. Enter the VPN Client address in the **Remote IPSec Identifier** (e.g., 192.168.2.8).
5. **Remote Site** by default is set to **LAN**.
6. Enter in the **Remote IP address**, the IP address of the VPN client (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*)

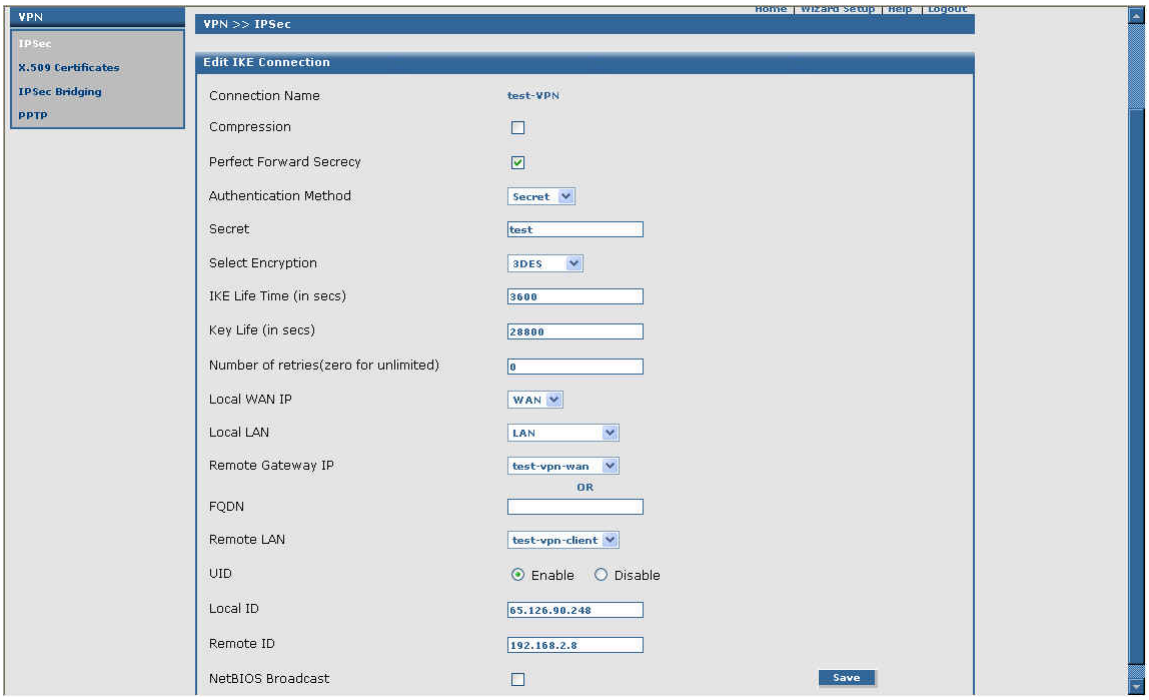


1. In the RouteFinder RF600,660,760VPN software, check the **VPN status** box.
2. Click the **Save** button to save this setting.
3. In the **Add IKE Connection**, click the Add button. The **Add IKE Connection** screen is displayed.



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.



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.