This chapter describes how to configure LAN Setup, LAN Groups and Routing (Static IP) features of your ProSafe VPN Firewall 50. These features can be found under the Network Configuration menu of the router interface.

Configuring Your LAN (Local Area Network)

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the firewall LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

Using the VPN Firewall as a DHCP Server

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See the link to “Preparing a Computer for Network Access:” in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the firewall’s LAN IP address)
- Primary DNS Server (the firewall’s LAN IP address)
- WINS Server (if you entered a WINS server address in the DHCP Setup menu)
- Lease Time (date obtained and duration of lease).

The LAN Setup screen allows you to configure the LAN on your router. The default values are suitable for most users and situations.
To modify your LAN setup:

1. Select **Network Configuration** from the main menu and **LAN Setup** from the submenu. The **LAN Setup** screen will display.

![LAN Setup Screen]

2. Enter the **IP Address** of your router (factory default: 192.168.1.1). (Always make sure that the LAN Port IP address and DMZ port IP address are in different subnets.)

3. Enter the **IP Subnet Mask**. The subnet mask specifies the network number portion of an IP address. Your router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the router).

4. Check the **Enable DHCP Server** radio button. By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, providing TCP/IP configuration for all computers connected to the router's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, check the **Disable DHCP Server** radio button. Enable DHCP Server is the default. If Enabled is selected, enter the following parameters:
   
a. Enter the **Domain Name** of the router (this is optional).
b. Enter the **Starting IP Address**. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192.168.1.2 is the default start address.

c. Enter the **Ending IP Address**. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between the Starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address.

**Note:** The Starting and Ending DHCP addresses should be in the same “network” as the LAN TCP/IP address of the router (the IP Address in **LAN TCP/IP Setup** section).

d. Enter a **WINS Server** IP address. This box can specify the Windows NetBios Server IP if one is present in your network. This field is optional.

e. Enter a **Lease Time**. This specifies the duration for which IP addresses will be leased to clients.

f. Check the **Enable DNS Proxy** radio box. This is optional—the default is enabled. If enabled, the VPN firewall will provide a LAN IP Address for DNS address name resolution.

**Note:** If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address **192.168.1.1** to **10.0.0.1**, you must enter **http://10.0.0.1** in your browser to connect to the web management interface.

5. Click **Apply** to save your settings.

6. Click **Reset** to discard any changes and revert to the previous configuration.

**Note:** Once you have completed the LAN IP setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these traffic rules, refer to Chapter 4, “Firewall Protection and Content Filtering.”
Configuring Multi-Home LAN IPs

If you have computers that are using different IP address ranges in the LAN (for example, 172.16.2.0 or 10.0.0.0), then you can add “aliases” to the LAN port which give computers on those networks access to the Internet. This allows the firewall to act as a gateway to additional logical subnets on your LAN.

To add a secondary LAN IP address:

1. Select Network Configuration from the main menu and LAN Setup from the secondary menu. Click the Multi Home LAN IPs Setup link (see Figure 3-2 on page 3-4) The Secondary LAN IP Setup screen will display.

2. Enter the Secondary IP address and Subnet Mask and click Add. The Secondary IP address will be added to the Available Secondary LAN IPs table.

Note: Additional IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets must be manually configured with IP addresses, gateway IP and DNS server IP addresses.

Tip: The Secondary LAN IP address will be assigned to the LAN interface of the router and can be used as a gateway by the secondary subnet.
Managing Groups and Hosts

The Known PCs and Devices table on the Groups and Hosts screen contains a list of all known PCs and network devices, as well as hosts, that are assigned dynamic IP addresses by this router. Collectively, these entries make up the Network Database. The Network Database is created in two ways:

- **Using the DHCP Server.** The router’s DHCP server will accept and respond to DHCP client requests from PCs and other network devices. Every computer that is responded to will be added to the Network Database in the Known PCs and Devices table.

- **Scanning the Network.** The router will scan the local network periodically, using standard methods such as ARP and NetBIOS, to detect active computers or devices which are not DHCP clients. For computers that do not support the NetBIOS protocol, the name will be displayed in the known PCs and Devices table as “Unknown”.

Creating the Network Database

The Network Database offers a number of advantages:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.

- No need to reserve an IP address for a PC in the DHCP Server. All IP address assignments made by the DHCP Server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.

- No need to use a Fixed IP on PCs. Because the address allocated by the DHCP Server will never change, you don't need to assign a fixed IP to a PC to ensure it always has the same IP address.

- MAC-level Control over PCs. The Network Database uses the MAC address to identify each PC or device. So changing a PC's IP address does not affect any restrictions on that PC.

- Group and Individual Control over PCs
  - You can assign PCs to Groups and apply restrictions to each Group using the Firewall Rules screen (see “Services-Based Rules” on page 4-2).
  - You can also select the Groups to be covered by the Block Sites feature (see “Setting Block Sites (Content Filtering)” on page 4-21).
  - If necessary, you can also create Firewall Rules to apply to a single PC (see “Enabling Source MAC Filtering” on page 4-23). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.
• A computer is identified by its MAC address—not its IP address. Hence, changing a computer’s IP address does not affect any restrictions applied to that PC.

This **Known PCs and Devices** table lists entries in the Network Database. For each computer or device, the following fields are displayed:

• **Name**: The name of the PC or device. For computers that do not support the NetBIOS protocol, this will be listed as “Unknown” (you can edit the entry manually to add a meaningful name). If the computer was assigned an IP address by the DHCP server, then the Name will be appended by an asterisk.

• **IP Address**: The current IP address of the computer. For DHCP clients of the router, this IP address will not change. If a computer is assigned a static IP addresses, you will need to update this entry manually if the IP address on the computer has been changed.

• **MAC Address**: The MAC address of the PC’s network interface.

• **Group**: Each PC or device can be assigned to a single group. By default, a computer is assigned to Group 1, unless a different group is selected from the Group pull-down menu.

• **Action**: Allows modification of the selected entry by clicking Edit.

To add computers to the network database manually:

1. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. The **Groups and Hosts** screen will display.

2. In the **Add Known PCs and Devices** table, enter the name of the PC or device.

3. Enter the **IP Address Type**. Select **Reserved (DHCP Client)** to direct the router to reserve the IP address for allocation by the DHCP server. Select **Fixed (Set on PC)** if the IP address is statically assigned on the computer.

4. Enter the **IP Address** that this computer or device is assigned. If the IP Address Type is Reserved (DHCP Client), the router will reserve the IP address for the associated MAC address.

5. Enter the **MAC Address** of the computer. The MAC address should be in the form: xx:xx:xx:xx:xx:xx (for example: 00:80:48:2a:8b:c0)

6. From the **Group** pull-down menu, select the group to which the computer will be assigned.

7. Click **Add** to add the new entry to the network database in the **Known PCs and Devices** table.

---

**Note:** When specifying a Reserved IP address, make sure that you select an IP address outside of the DHCP Server pool of addresses.
To edit an entry in the **Known PCs and Devices** table:

1. Click **Edit** adjacent to the entry you want to modify. The **Edit Known PCs and Devices** screen will display. Make your modifications to the entry.
2. Click **Apply** to save your settings. The changes will appear in the **Known PCs and Devices** table.

To edit a Group Name in the Network Database:

1. On the **Groups and Hosts** screen, click the **Edit Group Names** link.
2. Check the radio button by the group name you want to modify and type in a suitable name.
3. Click **Apply** to save the settings.
Setting Up Address Reservation

When you specify a reserved IP address for a device on the LAN (based on the MAC address of the device), that computer or device will always receive the same IP address each time it accesses the firewall’s DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP settings. The Reserved IP address that you select must be outside of the DHCP Server pool.

To reserve an IP address, use the Groups and Hosts screen under the Network Configuration menu, LAN Groups submenu (see “Creating the Network Database” on page 3-5).

Note: The reserved address will not be assigned until the next time the PC contacts the firewall's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

Configuring Static Routes

Static Routes provide additional routing information to your firewall. Under normal circumstances, the firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

To add or edit a Static Route:

1. Select Network Configuration from the main menu and Routing from the submenu. The Routing screen will display.
2. Click Add. The Add Static Route screen will display.
3. Enter a name for the static route in the Route Name field (for identification purpose only).
4. Determine whether the route is

   • Active or Inactive. A route can be added to the table and made inactive, if not needed. This allows routes to be used as needed without deleting the entry and re-adding it. An inactive route is not broadcast if RIP is enabled. Select the Active radio box to make this route effective.

   • Private: Determine whether the route can be shared with other routers when RIP is enabled. If Yes, then the route will not be shared in a RIP broadcast or multicast. Check the Private radio box if you want to limit access to the LAN only. The static route will not be advertised in RIP.
5. Type the **Destination IP Address** or network of the route’s final destination.

6. Enter the **IP Subnet Mask** for this destination. If the destination is a single host, enter 255.255.255.255.

7. From the **Interface** pull-down menu, select the physical network interface (Broadband, Dialup, or LAN) through which this route is accessible.

8. Enter the **Gateway IP Address** (which must be a firewall on the same LAN segment as the firewall) of the gateway through which the destination host or network can be reached.

9. Enter the **Metric** value that determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

10. Click **Apply** to save the static route to the **Static Routes** table.

### Static Route Example

For example, a static route is needed if:

- Your primary Internet access is through a cable modem to an ISP.
• You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall’s address on your LAN is 192.168.1.100.

• Your company’s network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company’s firewall.

In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN firewall at 192.168.1.100.

In this example:
• The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
• The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.1.100.
• A Metric value of 1 will work since the ISDN firewall is on the LAN.
• Private is selected only as a precautionary security measure in case RIP is activated.

**RIP Configuration**

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) and is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network. RIP is disabled by default.
To enable RIP:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The **Routing** screen will display.

2. Click the **RIP Configuration** link. The **RIP Configuration** screen will display.

3. From the **RIP Direction** pull-down menu, select the direction for the router to send and receive RIP packets:
   - **Both** — the router broadcasts its routing table and also processes RIP information received from other routers.
   - **Out Only** — the router broadcasts its routing table periodically but does not accept RIP information from other routers.
   - **In Only** — the router accepts RIP information from other routers, but does not broadcast its routing table.
• **None** – the router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.

4. Select the **RIP Version** from the pull-down menu:
   - **RIP-1** – classful routing and does not include subnet information. This is the most commonly supported version.
   - **RIP-2** – supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format:
     - **RIP-2B** – uses subnet broadcasting.
     - **RIP-2M** – uses multicasting (see Note below).

5. RIP authentication is disabled by default. To enable authentication for RIP-2B or RIP-2M,
   - a. Check the **Yes** radio button.
   - b. Input MD5 keys and effective and end dates for the **First Key Parameters** and **Second Key Parameters** for MD5 based authentication between routers.

6. Click **Apply** to save your settings.

---

**Note:** Multicasting can reduce the load on non-router machines because they do not listen to the RIP multicast address and will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting. For RIP-2B and RIP-2M you can select the type of authentication as **NONE** or **MD5**. If you select MD5 then you need to enter additional parameters.

---

**Enabling Trend Micro Antivirus Enforcement**

If you have installed the Trend Micro Client/Server Messaging Suite for SMB on your local network, the firewall can enforce antivirus scanning. When Antivirus Enforcement is selected, local PCs will not be allowed web access unless they have the Trend Micro OfficeScan client installed and updated with the latest virus definitions.

To enable Trend Micro Antivirus Enforcement:

1. Select **Security** from the main menu and **Trend Micro** from the submenu. The **Trend Micro** screen will display.

2. Check the **Yes** radio box for **Do you want to enable antivirus Enforcement?**.
3. Enter the IP address of the **OfficeScan Server** on your local network.

4. Enter the 5-digit port number used for communications between the OfficeScan clients and the server.

5. Click **Apply** to enable Trend Micro.

The Host Exclusion List table lists PCs that are allowed to access the WAN without OfficeScan client.

| Note: The OfficeScan Server must appear in the exclusion list. |

To allow a PC to access the web without the OfficeScan client:

Enter the IP address of the PC in the **Host** field in the **Add Host** section and click **Add**. The address will be added to the **Host Exclusion List** table.

![Figure 3-6](image)

| Note: Follow the instructions in the Trend Micro documentation to complete the installation and configuration of the Trend Micro OfficeScan Server. |