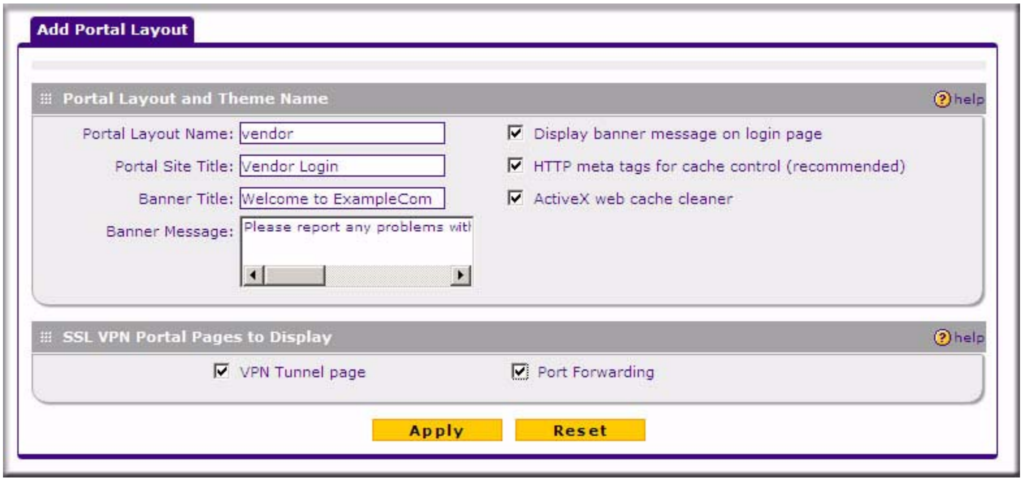


Portal Layout Name: vendor

Portal Site Title: Vendor Login

Banner Title: Welcome to ExampleCom

Banner Message: Please report any problems witl

☑ Display banner message on login page

☑ HTTP meta tags for cache control (recommended)

☑ ActiveX web cache cleaner

☑ VPN Tunnel page

☑ Port Forwarding

Figure 7-2OK

3. In the **Portal Layout and Theme Name** section of the menu, configure the following entries:

   a. Enter a descriptive name for the portal layout in the **Portal Layout Name** field. This name will be part of the path of the SSL VPN portal URL.

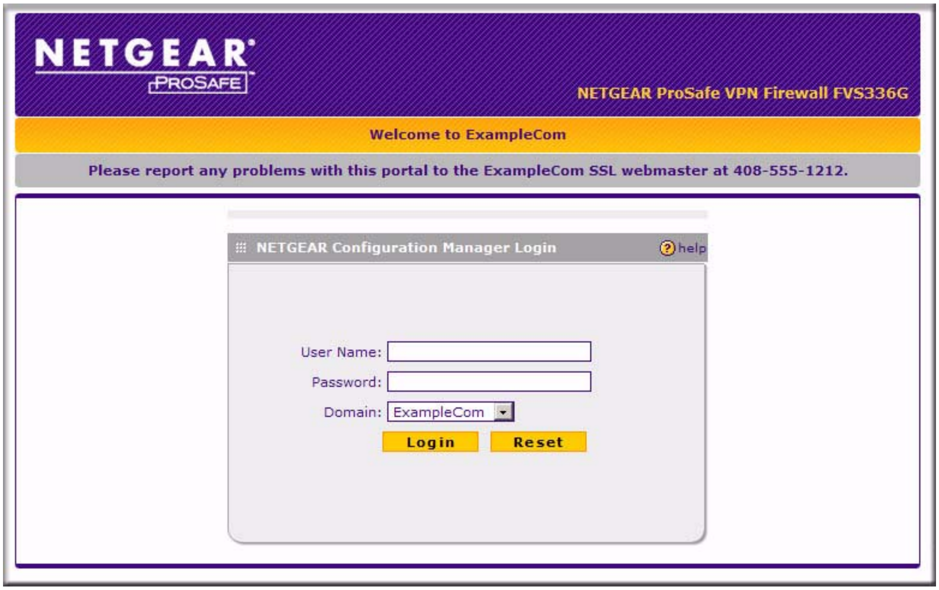
   > **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at **https://vpn.company.com**, and you created a portal layout named “sales”, then users will be able to access the sub-site at **https://vpn.company.com/portal/sales**.

   Only alphanumeric characters, hyphen (-), and underscore (_) are accepted for the Portal Layout Name. If you enter other types of characters or spaces, the layout name will be truncated before the first non-alphanumeric character. Note that unlike most other URLs, this name is case sensitive.

   b. In the **Portal Site Title** field, enter a title that will appear at the top of the user’s web browser window.

   c. To display a banner message to users before they log in to the portal, enter the banner title text in the **Banner Title** field. Also enter the banner message text in the **Banner Message** text area. Enter a plain text message or include HTML and JavaScript tags. The maximum length of the login page message is 4096 characters. Select the **Display banner message**

on login page checkbox to show the banner title and banner message text on the Login screen as shown below



Welcome to ExampleCom

Please report any problems with this portal to the ExampleCom SSL webmaster at 408-555-1212.

NETGEAR Configuration Manager Login

User Name:

Password:

Domain: ExampleCom

Figure 7-3 Need new screenshot

As shown in the figure, the banner title text is displayed in the orange header bar. The banner message text is displayed in the grey header bar.

d. Check the **Enable HTTP meta tags for cache control** checkbox to apply HTTP meta tag cache control directives to this Portal Layout. Cache control directives include:

```
<meta http-equiv=”pragma” content=”no-cache”>
<meta http-equiv=”cache-control” content=”no-cache”>
<meta http-equiv=”cache-control” content=”must-revalidate”>
```

These directives help prevent clients browsers from caching SSL VPN portal pages and other web content.

Note: NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user’s web browser cache.

e. Check the “**ActiveX web cache cleaner** checkbox to load an ActiveX cache control when users log in to the SSL VPN portal.

The web cache cleaner will prompt the user to delete all temporary Internet files, cookies and browser history when the user logs out or closes the web browser window. The ActiveX web cache control will be ignored by web browsers that don't support ActiveX.

4. In the **SSL VPN Portal Pages to Display** section, check the checkboxes for the portal pages you wish users to access. Any pages that are not selected will not be visible from the portal navigation menu. Your choices are:
   - VPN Tunnel. Provides full network connectivity.
   - Port Forwarding. Provides access to specific defined network services.
5. Click **Apply** to confirm your settings.

   The "Operation succeeded" message appears at the top of the tab. Your new layout appears in the List of Layouts table.

Configuring Domains, Groups, and Users

Remote users connecting to the SSL firewall must be authenticated before being allowed to access the network. The login window presented to the user requires three items: a User Name, a Password, and a Domain selection. The Domain determines the authentication method to be used and the portal layout that will be presented.

You must create name and password accounts for your SSL VPN users. When you create a user account, you must specify a group. Groups are used to simplify the application of access policies. When you create a group, you must specify a domain. Therefore, you should create any needed domains first, then groups, then user accounts.

To configure Domains, Groups, and Users, see "Adding Authentication Domains, Groups, and Users" on page 8-1.

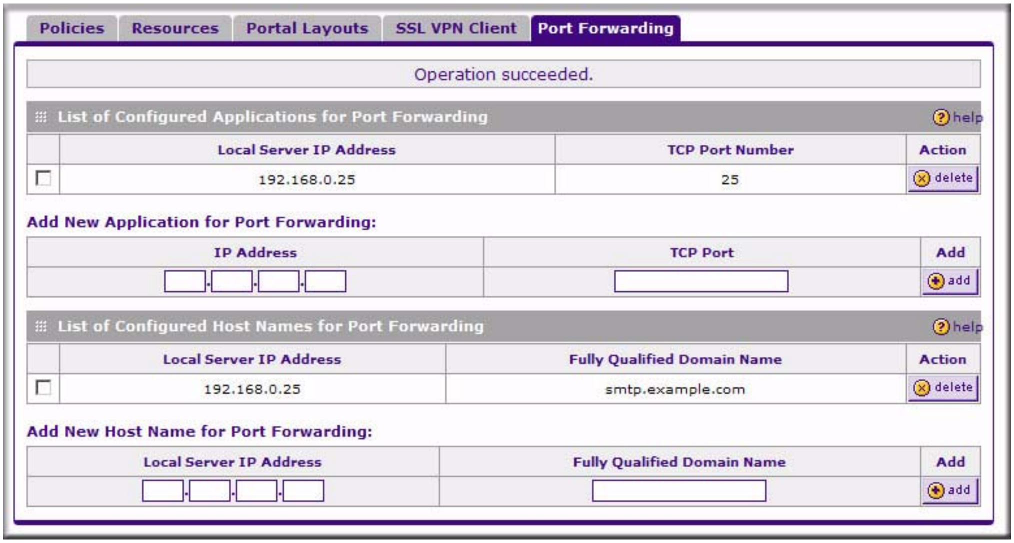
Configuring Applications for Port Forwarding

Port Forwarding provides access to specific defined network services. To define these services, you must specify the internal addresses and TCP applications (port numbers) that will be intercepted by the Port Forwarding client on the user's PC. The client will reroute this traffic to the firewall.

Adding Servers

To configure Port Forwarding, you must define the internal host machines (servers) and TCP applications available to remote users. To add servers, follow these steps:

1. Select VPN > SSL VPN from the main/submenu, and then select the Port Forwarding tab. The Port Forwarding screen display.



Operation succeeded.

List of Configured Applications for Port Forwarding

	Local Server IP Address	TCP Port Number	Action
□	192.168.0.25	25	delete

Add New Application for Port Forwarding:

IP Address	TCP Port	Add
. . .		add

List of Configured Host Names for Port Forwarding

	Local Server IP Address	Fully Qualified Domain Name	Action
□	192.168.0.25	smtp.example.com	delete

Add New Host Name for Port Forwarding:

Local Server IP Address	Fully Qualified Domain Name	Add
. . .		add

Figure 7-4OK

2. In the **Add New Application for Port Forwarding** section, enter the IP address of an internal server or host computer.

3. In the **TCP Port** field, enter the TCP port number of the application to be tunneled. The table below lists many commonly used TCP applications and port numbers.

Table 7-1. Port Forwarding Applications/TCP Port Numbers

TCP Application	Port Number
FTP Data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80

Table 7-1. Port Forwarding Applications/TCP Port Numbers (continued)

TCP Application	Port Number
POP3 (receive mail)	110
NTP (network time protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

[a] Users can specify the port number together with the host name or IP address.

4. Click **Add**.

   The “Operation succeeded” message appears at the top of the tab, and the new application entry is listed in the **List of Configured Applications**.

5. Repeat this process to add other applications for use in Port Forwarding.

Adding A New Host Name

Once the server IP address and port information has been configured, remote users will be able to access the private network servers using Port Forwarding. As a convenience for users, you can also specify host name to IP address resolution for the network servers. Host Name Resolution allows users to access TCP applications at familiar addresses such as **mail.example.com** or **ftp.example.com** rather than by IP addresses.

To add a host name for client name resolution, follow these steps:

1. Select the Port Forwarding tab, shown in Figure 7-4.
2. If the server you want to name does not appear in the **List of Configured Applications for Port Forwarding**, you must add it before you can rename it.
3. In the **Add New Host Name for Port Forwarding** section, enter the IP address of the server you want to name.
4. In the **Fully Qualified Domain Name** field, enter the full server name.
5. Click **Add**.

   The “Operation succeeded” message appears at the top of the tab, and the new entry is listed in the **List of Configured Host Names**.

Remote users can now securely access network applications once they have logged into the SSL VPN portal and launched Port Forwarding.

Configuring the SSL VPN Client

The SSL VPN Client within the SRXN3205 will assign IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the corporate subnet to the remote VPN tunnel clients.

Some additional considerations are:

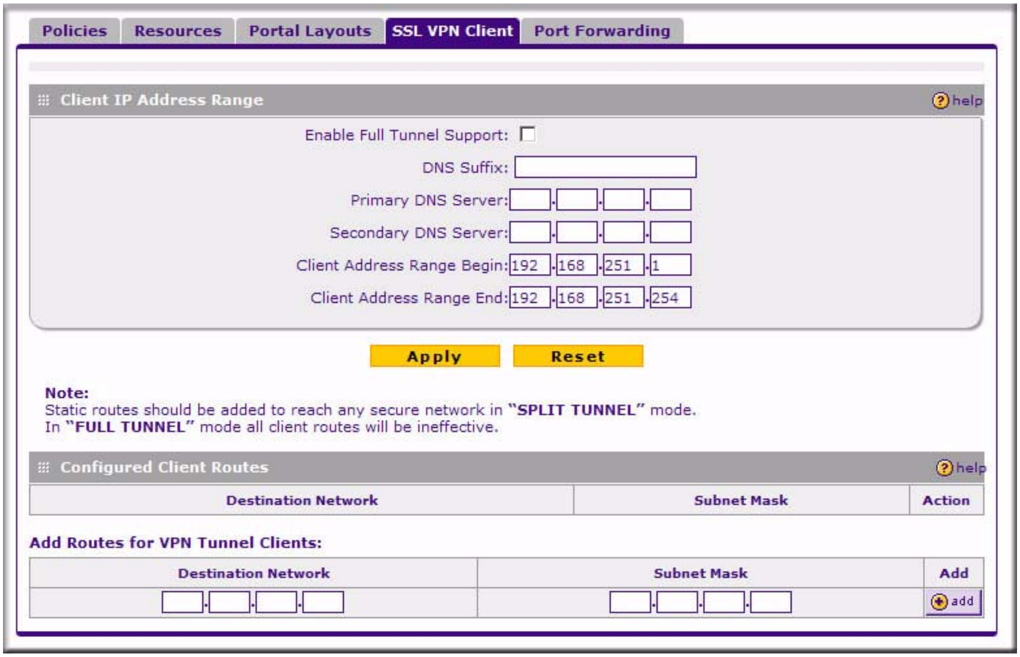
- So that the virtual (PPP) interface address of a VPN tunnel client does not conflict with addresses on the corporate network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are currently assigned to devices on your local network, then start the client address range at 192.168.1.101 or choose an entirely different subnet altogether.
- The VPN tunnel client cannot contact a server on the corporate network if the VPN tunnel client's Ethernet interface shares the same IP address as the server or the firewall (for example, if your laptop has a network interface IP address of 10.0.0.45, then you won't be able to contact a server on the remote network that also has the IP address 10.0.0.45).
- If you assign an entirely different subnet to the VPN tunnel clients than the subnet used by the corporate network, you must
  - Add a client route to configure the VPN tunnel client to connect to the corporate network using the VPN tunnel.
  - Create a static route on the corporate network's firewall to forward local traffic intended for the VPN tunnel clients to the firewall.
- Select whether you want to enable full tunnel or split tunnel support based on your bandwidth:
  - Full tunnel. Sends all of the client's traffic across the VPN tunnel.
  - Split tunnel. Sends only traffic destined for the corporate network based on the specified client routes. All other traffic is sent to the Internet. Split tunnel allows you to manage your company bandwidth by reserving the VPN tunnel for corporate traffic only.

Configuring the Client IP Address Range

Determine the address range to be assigned to VPN tunnel clients, then define the address range.

To configure the client IP address range:

1. Select **VPN** > **SSL VPN** from the main/submenu, and then select the SSL VPN Client tab. The SSL VPN Client screen displays.



Client IP Address Range

Enable Full Tunnel Support: □

DNS Suffix:

Primary DNS Server: . . .

Secondary DNS Server: . . .

Client Address Range Begin: 192 . 168 . 251 . 1

Client Address Range End: 192 . 168 . 251 . 254

Note:
Static routes should be added to reach any secure network in "**SPLIT TUNNEL**" mode.
In "**FULL TUNNEL**" mode all client routes will be ineffective.

Configured Client Routes

Destination Network	Subnet Mask	Action

Add Routes for VPN Tunnel Clients:

Destination Network	Subnet Mask	Add
. . .	. . .	add

Figure 7-5OK

2. Select **Enable Full Tunnel Support** unless you want split tunneling.
3. (Optional) Enter a **DNS Suffix** to be appended to incomplete DNS search strings.
4. Enter Primary and Secondary DNS Server IP addresses to be assigned to the VPN tunnel clients.
5. In the **Client Address Range Begin** field, enter the first IP address of the IP address range.
6. In the **Client Address Range End** field, enter the last IP address of the IP address range.
7. Click **Apply**.

   The "Operation succeeded" message appears at the top of the tab.

VPN tunnel clients are now able to connect to the firewall and receive a virtual IP address in the client address range.

Adding Routes for VPN Tunnel Clients

The VPN Tunnel Clients assume that the following networks are located across the VPN over the SSL tunnel:

- The subnet containing the client IP address (PPP interface), as determined by the class of the address (Class A, B, or C).
- Subnets specified in the Configured Client Routes table.

If the assigned client IP address range is in a different subnet than the corporate network, or the corporate network has multiple subnets, you must define Client Routes.

To add an SSL VPN Tunnel client route, follow these steps:

1. Access the SSL VPN Client tab shown in Figure 7-5.
2. In the **Add Routes** section, enter the Destination Network IP address of a local area network or subnet. For example, enter 192.168.0.0.
3. Enter the appropriate **Subnet Mask**.
4. Click **Add**.

   The “Operation succeeded” message appears at the top of the tab and the new client route is listed in the Configured Client Routes table.

Note: You must also add a static route on your corporate firewall that directs local traffic destined for the VPN tunnel client address range to the firewall.

Restart the firewall if VPN tunnel clients are currently connected. Restarting forces clients to reconnect and receive new addresses and routes.

Replacing and Deleting Client Routes

If the specifications of an existing route need to be changed, follow these steps:

1. Make a new entry with the correct specifications.
2. In the **Configured Client Routes** table, click the **Delete** button in the actions column.
3. If an existing route is no longer needed for any reason, you can delete it.

Using Network Resource Objects to Simplify Policies

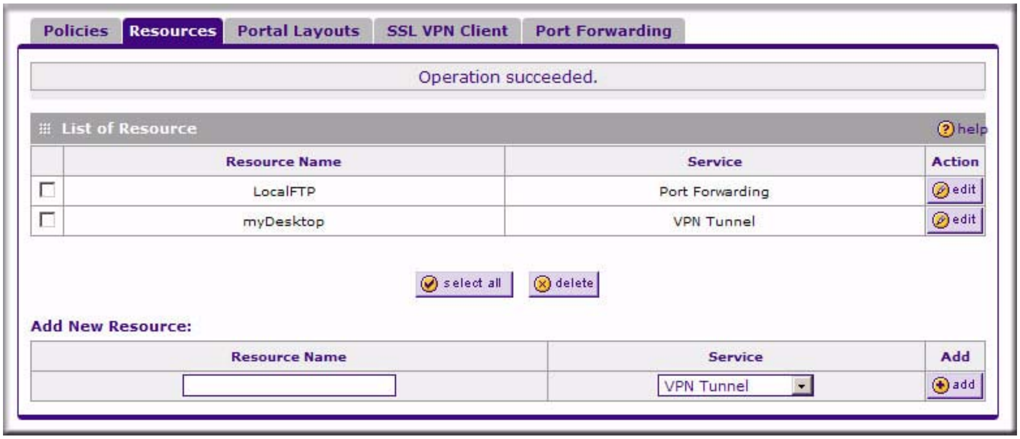
Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You will not need to redefine the same set of IP addresses or address ranges when configuring the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, we recommend that you use network resources. If your server or network configuration changes, by using network resources you can perform an update quickly instead of individually updating all of the user and group policies.

Adding New Network Resources

To define a network resource:

1. Select **VPN > SSL VPN** from the main/submenu, and then select the Resources tab. The Resources screen displays.



Operation succeeded.

List of Resource

	Resource Name	Service	Action
□	LocalFTP	Port Forwarding	edit
□	myDesktop	VPN Tunnel	edit

Add New Resource:

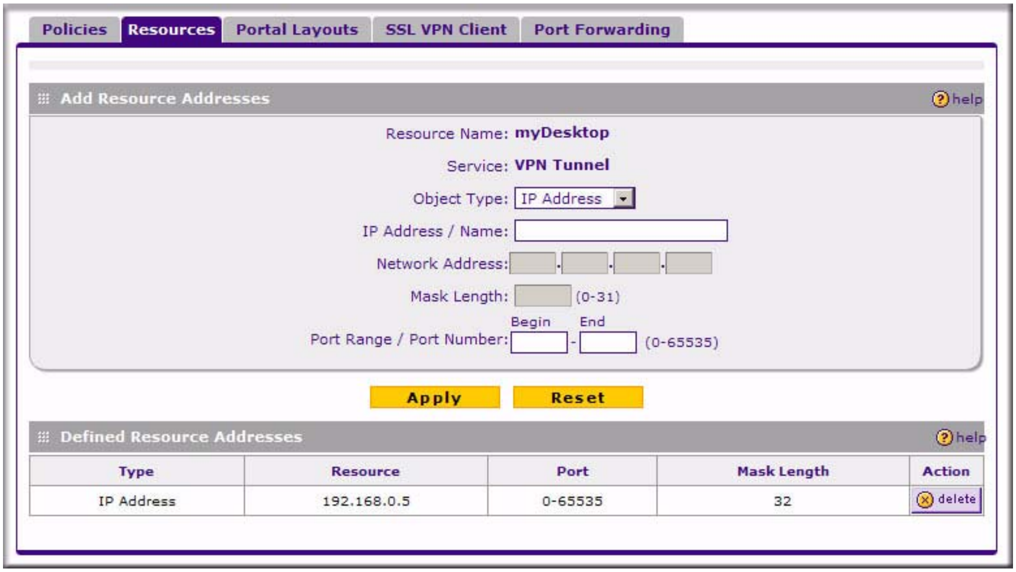
Resource Name	Service	Add
	VPN Tunnel	add

Figure 7-6OK

2. In the **Add New Resource** section, type the (qualified) resource name in the **Resource Name** field.
3. In the **Service** pull-down menu, select the type of service to apply to the resource: either VPN Tunnel or Port Forwarding.
4. Click **Add**.

The “Operation succeeded” message appears at the top of the tab, and the newly-added resource name appears on the List of Resources table.

5. Adjacent to the new resource, click the **Edit** button. The **Add Resource Addresses** screen displays.



Add Resource Addresses

Resource Name: myDesktop

Service: VPN Tunnel

Object Type: IP Address

IP Address / Name:

Network Address: . . .

Mask Length: (0-31)

Port Range / Port Number: Begin - End (0-65535)

Defined Resource Addresses

Type	Resource	Port	Mask Length	Action
IP Address	192.168.0.5	0-65535	32	delete

Figure 7-7OK

6. From the **Object Type** pull-down menu, select either IP Address or IP Network:
   - If you selected IP Address, enter an IP address or fully qualified domain name in the **IP Address/Name** field.
   - If you selected IP Network, enter the IP network address in the **Network Address** field. Enter the mask length in the **Mask Length** (0-31) field.
7. Enter the **Port Range or Port Number** for the IP Address or IP Network you selected.
8. Click **Apply** to add the IP address or IP network to the resource. The new configuration appears in the **Defined Resource Addresses** table, as shown in Figure 7-7.

Configuring User, Group, and Global Policies

An administrator can define and apply user, group and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The firewall policy hierarchy is defined as:

1. User Policies take precedence over all Group Policies.
2. Group Policies take precedence over all Global Policies.
3. If two or more user, group, or global policies are configured, *the most specific policy* takes precedence.

For example, a policy configured for a single IP address takes precedence over a policy configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy applied to all IP addresses. If two or more IP address ranges are configured, then the smallest address range takes precedence. Hostnames are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, let’s assume the following global policy configuration:

- Policy 1: A Deny rule has been configured to block all services to the IP address range 10.0.0.0 – 10.0.0.255.
- Policy 2: A Deny rule has been configured to block FTP access to 10.0.1.2 – 10.0.1.10.
- Policy 3: A Permit rule has been configured to allow FTP access to the predefined network resource, FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5 – 10.0.0.20 and ftp.company.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access:

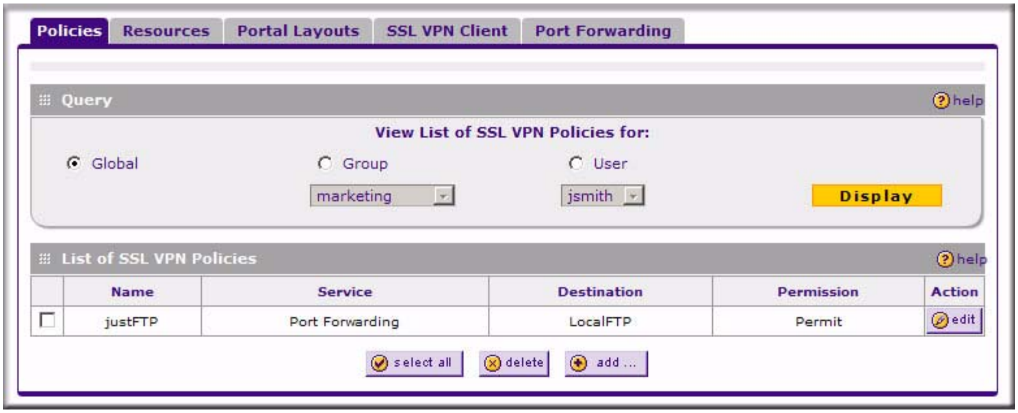
- An FTP server at 10.0.0.1, the user would be blocked by Policy 1.
- An FTP server at 10.0.1.5, the user would be blocked by Policy 2.
- An FTP server at 10.0.0.10, the user would be granted access by Policy 3. The IP address range 10.0.0.5 - 10.0.0.20 is more specific than the IP address range defined in Policy 1.
- An FTP server at ftp.company.com, the user would be granted access by Policy 3. A single host name is more specific than the IP address range configured in Policy 2.

Note: The user would not be able to access ftp.company.com using its IP address 10.0.1.3. The firewall policy engine does not perform reverse DNS lookups.

Viewing Policies

To view the existing policies, follow these steps:

1. Select **VPN** > **SSL VPN** from the main/submenu, and then select the Policies tab. The Policies screen will display.



View List of SSL VPN Policies for:

● Global ○ Group ○ User

marketing jsmith

	Name	Service	Destination	Permission	Action
□	justFTP	Port Forwarding	LocalFTP	Permit	edit

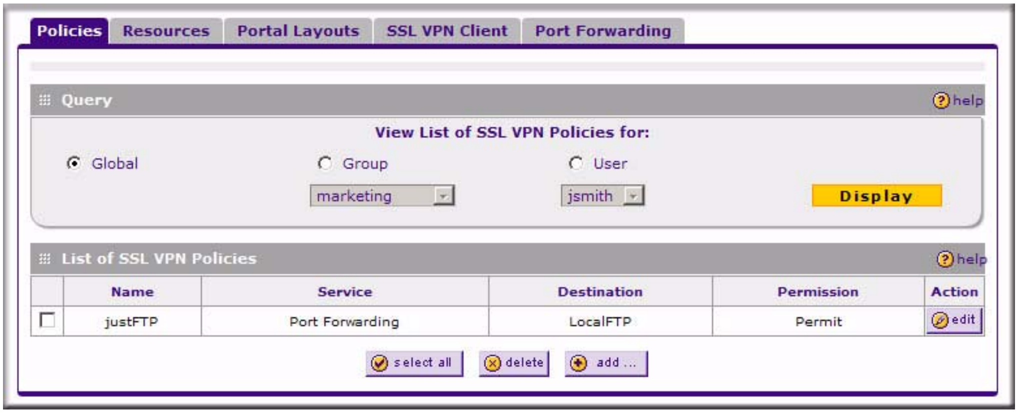
Figure 7-8OK

2. Make your selection from the following Query options:
   - Click **Global** to view all global policies.
   - Click **Group** to view group policies, and choose the relevant group's name from the pull-down menu.
   - Click **User** to view group policies, and choose the relevant user's name from the pull-down menu.
3. Click the **Display** button. The List of SSL VPN Policies will display the list for your selected Query option. Change Query selection and click display again for each of the three queries.

Adding a Policy

To add a policy, follow these steps:

1. Select **VPN** > **SSL VPN** from the main/submenu, and select the Policies tab. The Policies screen displays.



View List of SSL VPN Policies for:

● Global ○ Group ○ User

Group: marketing User: jsmith

	Name	Service	Destination	Permission	Action
□	justFTP	Port Forwarding	LocalFTP	Permit	edit

Figure 7-9OK

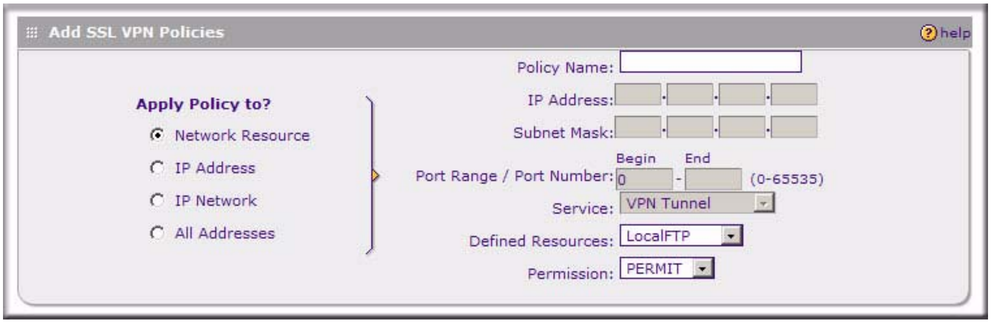
2. Make your selection from the following Query options:
   - Click **Global** if this new policy is to exclude all users and groups.
   - Click **Group** if this new policy is to be limited to a selected group.
     Open the pull-down menu and choose the relevant group’s name.
   - Click **User** if this new policy is to be limited to a selected user.
     Open the pull-down menu and choose the individual user’s name.

Note: You should have already created the needed groups or users as described in “Adding Authentication Domains, Groups, and Users” on page 8-1.

3. Click **Add**. The **Add Policies** screen appears.
4. In the **Add SSL VPN Policies** section, review the **Apply Policy To** options and click one.

   Depending upon your selection, specific options to the right are activated or inactivated as noted in the following:

   - If you choose **Network Resource**, you’ll need to enter a descriptive Policy Name, then choose a **Defined Resource** and relevant **Permission** (PERMIT or DENY) from the pull-down menus.



Add SSL VPN Policies

Apply Policy to?

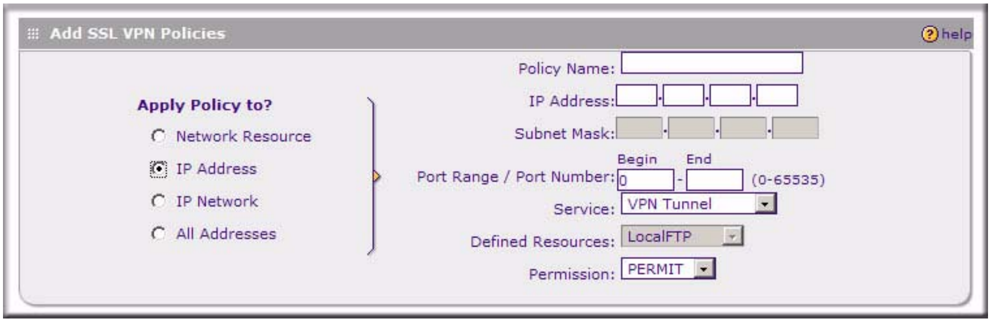
● Network Resource
○ IP Address
○ IP Network
○ All Addresses

Policy Name:
IP Address: . . .
Subnet Mask: . . .
Port Range / Port Number: Begin 0 - End (0-65535)
Service: VPN Tunnel
Defined Resources: LocalFTP
Permission: PERMIT

Figure 7-10

If a needed network resource has not been defined, you can add it before proceeding with this new policy. See "Adding New Network Resources " on page 7-13.

- If you choose **IP Address**, you'll need to enter a descriptive **Policy Name**, the specific **IP Address**, then choose the **Service** and relevant **Permission** from the pull-down menus.



Add SSL VPN Policies

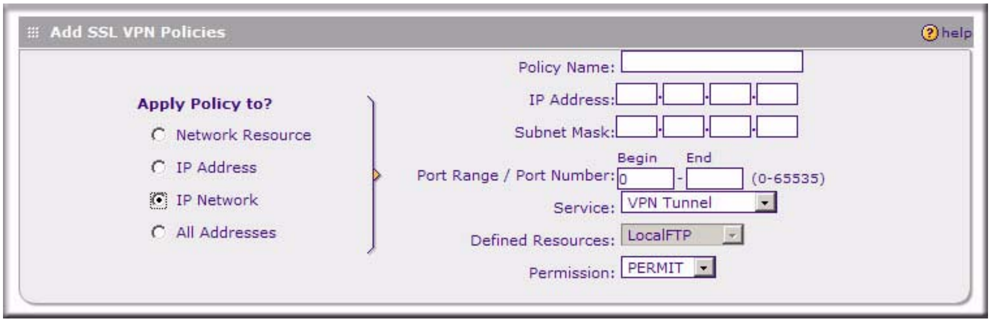
Apply Policy to?

○ Network Resource
● IP Address
○ IP Network
○ All Addresses

Policy Name:
IP Address: . . .
Subnet Mask: . . .
Port Range / Port Number: Begin 0 - End (0-65535)
Service: VPN Tunnel
Defined Resources: LocalFTP
Permission: PERMIT

Figure 7-11

- If you choose **IP Network**, you'll need to enter a descriptive **Policy Name**, **IP Address**, **Subnet Mask**, then choose the **Service** and relevant **Permission** from the pull-down menus.



Add SSL VPN Policies

help

Apply Policy to?

○ Network Resource

○ IP Address

● IP Network

○ All Addresses

Policy Name:

IP Address: . . .

Subnet Mask: . . .

Port Range / Port Number: Begin 0 - End (0-65535)

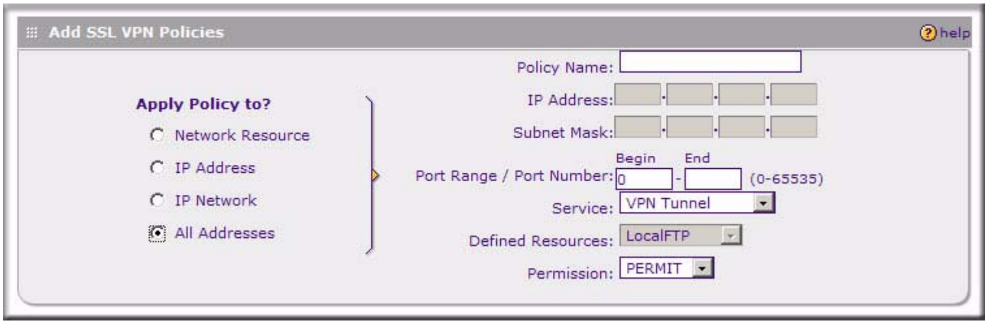
Service: VPN Tunnel

Defined Resources: LocalFTP

Permission: PERMIT

Figure 7-12

- If you choose **All Addresses**, you'll need to enter a descriptive **Policy Name**, then choose the **Service** and relevant **Permission** from the pull-down menus.



Add SSL VPN Policies

help

Apply Policy to?

○ Network Resource

○ IP Address

○ IP Network

● All Addresses

Policy Name:

IP Address: . . .

Subnet Mask: . . .

Port Range / Port Number: Begin 0 - End (0-65535)

Service: VPN Tunnel

Defined Resources: LocalFTP

Permission: PERMIT

Figure 7-13

5. When you are finished making your selections, click **Apply**. The Policies screen reappears.

Your policy goes into effect immediately and is added to the policies in the **List of SSL VPN Policies** table on this screen.

Note: In addition to configuring SSL VPN user policies, be sure that HTTPS remote management is enabled. Otherwise, all SSL VPN user connections will be disabled. See "Enabling Remote Management Access" on page 9-10.

Chapter 8
Managing Users, Authentication, and Certificates

This chapter contains the following sections:

- "Adding Authentication Domains, Groups, and Users"
- "Managing Certificates"

Adding Authentication Domains, Groups, and Users

You must create name and password accounts for all users who will connect to the firewall. This includes administrators and SSL VPN clients. Accounts for IPsec VPN clients are only needed if you have enabled Extended Authentication (XAUTH) in your IPsec VPN configuration.

Users connecting to the firewall must be authenticated before being allowed to access the firewall or the VPN-protected network. The login window presented to the user requires three items: a User Name, a Password, and a Domain selection. The Domain determines the authentication method to be used and, for SSL VPN connections, the portal layout that will be presented.

➡ **Note:** IPsec VPN users will always belong to the default domain (geardomain) and are not assigned to groups.

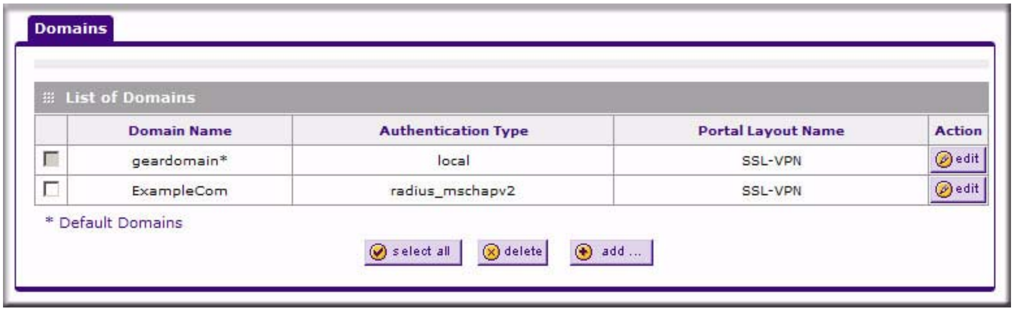
Except in the case of IPsec VPN users, when you create a user account, you must specify a group. When you create a group, you must specify a domain. Therefore, you should create any needed domains first, then groups, then user accounts.

Creating a Domain

The domain determines the authentication method to be used for associated users. For SSL VPN connections, the domain also determines the portal layout that will be presented, which in turn determines the network resources to which the associated users will have access.

To create a domain:

1. Select **Users** > **Domains** from the main/sub-menu. The Domains screen displays.

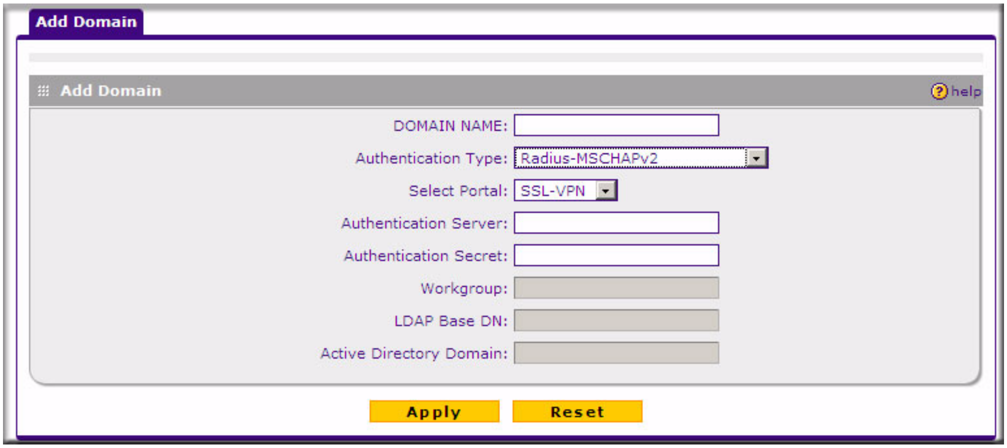


	Domain Name	Authentication Type	Portal Layout Name	Action
□	geardomain*	local	SSL-VPN	edit
□	ExampleCom	radius_mschapv2	SSL-VPN	edit

* Default Domains

Figure 8-1OK

2. Click **Add**. The Add Domain screen displays.



DOMAIN NAME:

Authentication Type: Radius-MSCHAPv2

Select Portal: SSL-VPN

Authentication Server:

Authentication Secret:

Workgroup:

LDAP Base DN:

Active Directory Domain:

Figure 8-2OK

3. Configure the following fields:

   a. Enter a descriptive name for the domain in the **Domain Name** field.

   b. Select the **Authentication Type**.

The required fields are activated in varying combinations according to your selection of Authentication Type:

Authentication Type	Required Authentication Information Fields
Local User Database	None
Radius-PAP	Authentication Server, Authentication Secret
Radius-CHAP	Authentication Server, Authentication Secret
Radius-MSCHAP	Authentication Server, Authentication Secret
Radius-MSCHAPv2	Authentication Server, Authentication Secret
NT Domain	Authentication Server, Workgroup
Active Directory	Authentication Server, Active Directory Domain
LDAP	Authentication Server, LDAP Base DN

c. **Select a portal** to which this domain will be associated.

4. Click **Apply** to save and apply your entries. The Domain screen will display a new domain row.

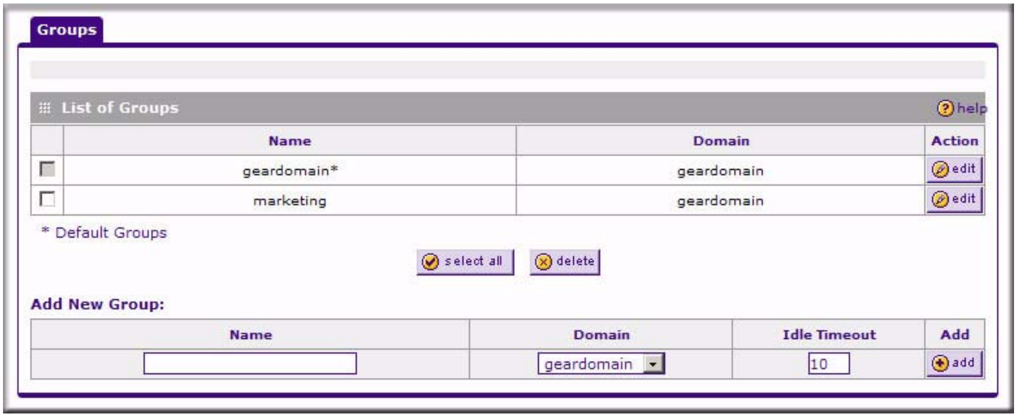
Creating a Group

The use of groups simplifies the configuration of VPN policies when different sets of users will have different restrictions and access controls.

Note: Groups that are defined in the User menu are used for setting SSL VPN policies. These groups should not be confused with LAN Groups that are defined in the Network | LAN Setup | LAN Groups tab, which are used to simplify firewall policies.

To create a group:

1. Select **Users** > **Groups** from the main/submenu and the Groups screen displays.



	Name	Domain	Action
□	geardomain*	geardomain	edit
□	marketing	geardomain	edit

* Default Groups

Add New Group:

Name	Domain	Idle Timeout	Add
	geardomain	10	add

Figure 8-3OK

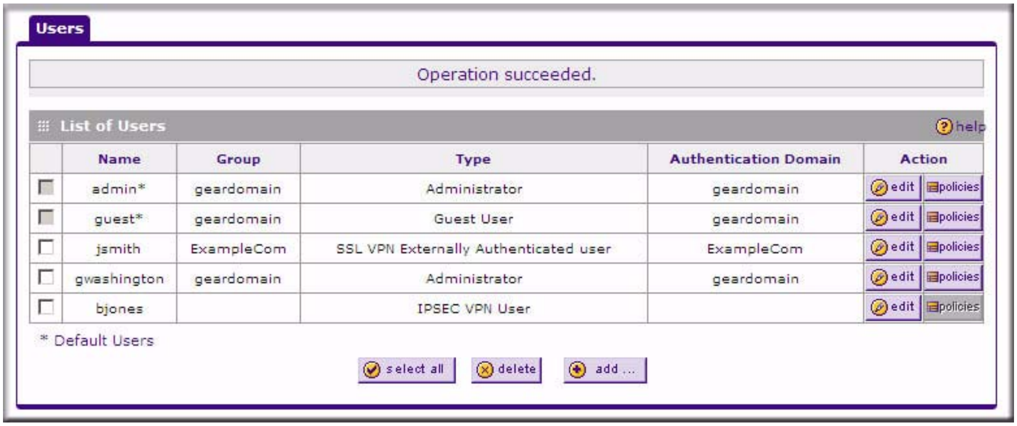
2. Configure the new group settings in the Add New Group section of the menu:
   a. **Name**. Enter a descriptive name for the group.
   b. **Domain**. Select the appropriate domain (only for Administrator or SSL VPN User).
   c. **Timeout**. For an Administrator, this is the period at which an idle user will be automatically logged out of the Web Configuration Manager
3. Click **Add**.

   The new group appears in the **List of Groups**, ready for use in user account setup.

Creating a New User Account

To add individual user accounts:

1. Select **Users > Users** from the main/submenu and the Users screen displays.



Users

Operation succeeded.

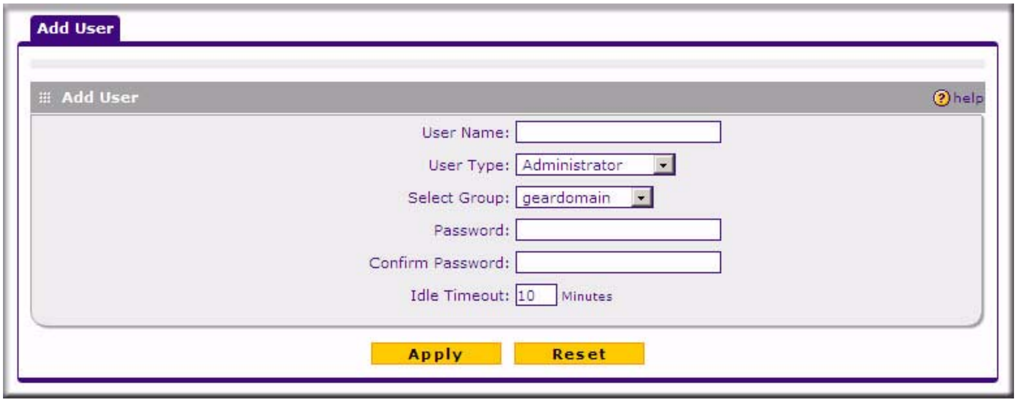
List of Users

	Name	Group	Type	Authentication Domain	Action
□	admin*	geardomain	Administrator	geardomain	edit policies
□	guest*	geardomain	Guest User	geardomain	edit policies
□	jsmith	ExampleCom	SSL VPN Externally Authenticated user	ExampleCom	edit policies
□	gwashington	geardomain	Administrator	geardomain	edit policies
□	bjones		IPSEC VPN User		edit policies

* Default Users

Figure 8-4Ok

2. Click **Add** and the Add User tab screen displays.



Add User

Add User

User Name:

User Type: Administrator

Select Group: geardomain

Password:

Confirm Password:

Idle Timeout: 10 Minutes

Figure 8-5Ok

3. Configure the following fields:
   a. **User Name**. Enter a unique identifier, using any alphanumeric characters.
   b. **User Type**. Select either Administrator, SSL VPN User, or IPsec VPN User.
   c. **Select Group**. Select from a list of configured groups. The user will be associated with the domain that is associated with that group.
   d. **Password/Confirm Password**. The password can contain alphanumeric characters, dash, and underscore.

e. **Idle Timeout**. For an Administrator, this is the period at which an idle user will be automatically logged out of the Web Configuration Manager.

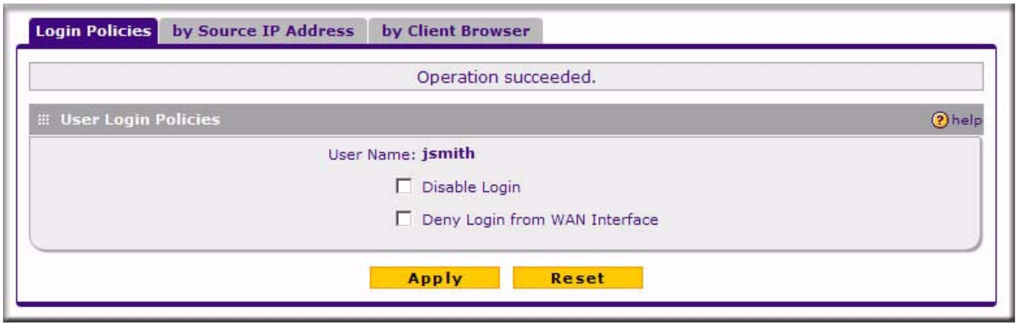
4. Click **Apply** to save and apply your entries. The new user appears in the **List of Users**.

Setting User Login Policies

You can restrict the ability of defined users to log into the Web Configuration Manager. You can also require or prohibit logging in from certain IP addresses or using particular browsers.

To configure user login policies:

1. In the **Action** column of the **List of Users** table, click **Policies** adjacent to the user policy you want to configure. The Login Policies screen displays:



Operation succeeded.

User Name: jsmith

□ Disable Login

□ Deny Login from WAN Interface

Figure 8-6ok

2. To prohibit this user from logging in to the firewall, select the **Disable Login** checkbox.

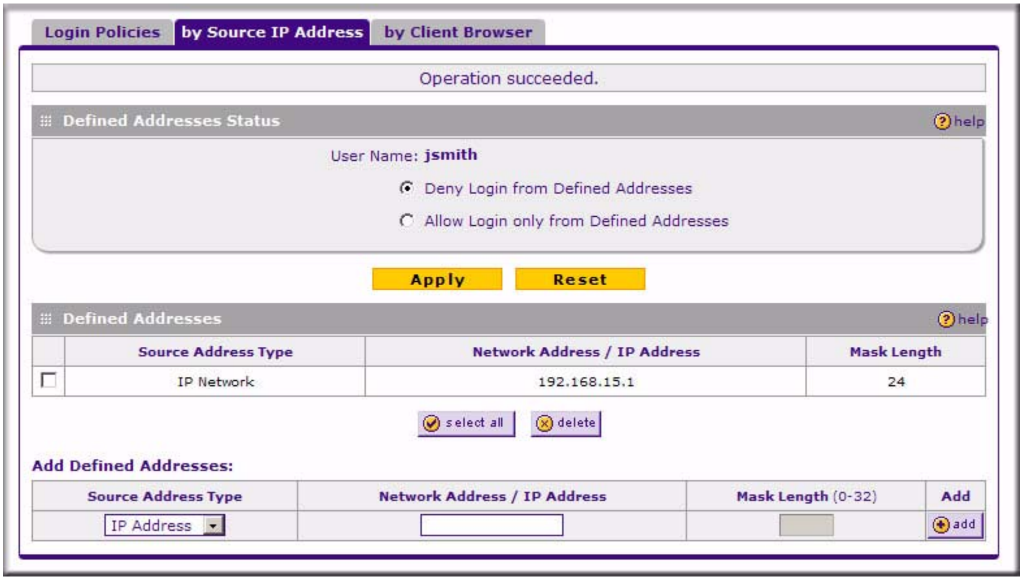
3. To prohibit this user from logging in from the WAN interface, select the **Deny Login from WAN Interface** checkbox. In this case, the user can log in only from the LAN interface.

Note: For security reasons, **Deny Login from WAN Interface** is checked by default for admin and guest.

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

To restrict logging in based on IP address:

1. Select the **by Source IP Address** tab and the by Source IP Address screen displays.



Operation succeeded.

Defined Addresses Status

User Name: **jsmith**

● Deny Login from Defined Addresses

○ Allow Login only from Defined Addresses

Defined Addresses

	Source Address Type	Network Address / IP Address	Mask Length
□	IP Network	192.168.15.1	24

Add Defined Addresses:

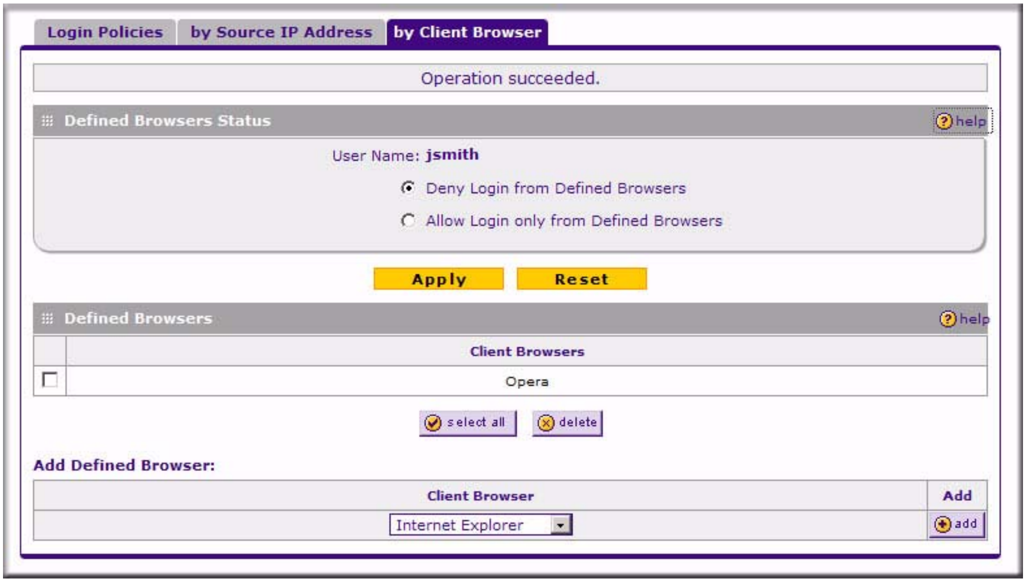
Source Address Type	Network Address / IP Address	Mask Length (0-32)	Add
IP Address			add

Figure 8-7ok

2. In the **Defined Addresses Status** section, select:
   - the **Deny Login from Defined Addresses** to deny logging in from the IP addresses that you will specify
   - the **Allow Login only from Defined Addresses** to allow logging in from the IP addresses that you will specify.
3. Click **Apply.**
4. To specify a single IP address, select **IP Address** from the **Source Address Type** pull-down menu and enter the IP address in the **Network Address/IP address** field.
5. To specify a subnet of IP addresses, select **IP Network** from the **Source Address Type** pull-down menu. Enter the network address and netmask length in the **Network Address/IP address** field.
6. Click **Add** to move the defined address to the **Defined Addresses** table.
7. Repeat these steps to add additional addresses or subnets.

To restrict logging in based on the user's browser:

1. Select the **by Client Browser** tab. The by Client Browser screen will display.



Operation succeeded.

User Name: jsmith

● Deny Login from Defined Browsers

○ Allow Login only from Defined Browsers

	Client Browsers
□	Opera

Add Defined Browser:

Client Browser	Add
Internet Explorer	add

Figure 8-8ok

2. In the **Defined Browsers Status** section, select:
   - the **Deny Login from Defined Browsers** to deny logging in from browsers that you will specify.
   - the **Allow Login only from Defined Browsers** to allow logging in from browsers that you will specify.
3. From the **Add Defined Browser** selection, select a browser from the **Client Browser** pull-down menu and click **Add** to move the defined browser to the **Defined Browsers** table.
4. Repeat these steps to add additional browsers, then click **Apply** to save your changes.

Managing Certificates

The firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A certificate that authenticates a server, for example, is a file that contains:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified absolutely.

You can obtain a certificate from a well-known commercial Certificate Authority (CA) such as Verisign or Thawte, or you can generate and sign your own certificate. Because a commercial CA takes steps to verify the identity of an applicant, a certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate will trigger a warning from most browsers as it provides no protection against identity theft of the server.

Your firewall contains a self-signed certificate from NETGEAR. We recommend that you replace this certificate prior to deploying the firewall in your network.

From the **VPN > Certificates** main menu/submenu, you can view the currently loaded certificates, upload a new certificate and generate a Certificate Signing Request (CSR). Your firewall will typically hold two types of certificates:

- CA certificate. Each CA issues its own CA identity certificate in order to validate communication with the CA and to verify the validity of certificates signed by the CA.
- Self certificate. The certificate issued to you by a CA identifying your device.

Viewing and Loading CA Certificates

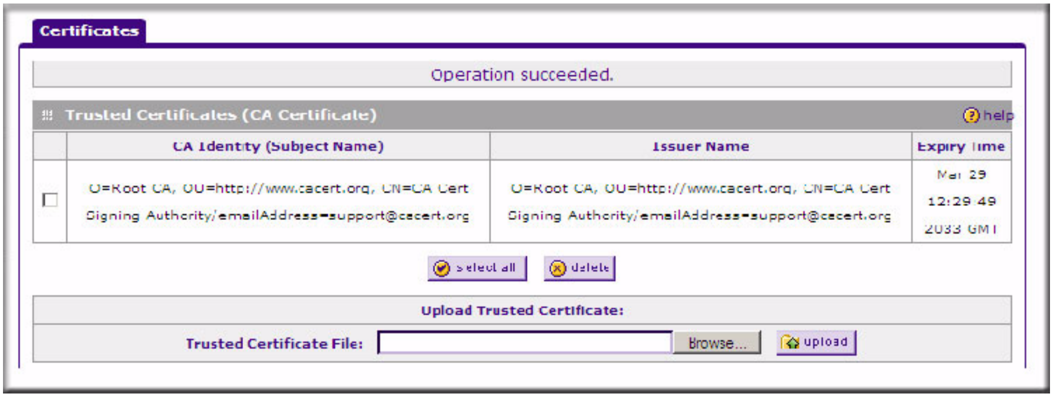
The Trusted Certificates (CA Certificates) table lists the certificates of CAs and contains the following data:

- **CA Identity (Subject Name)**. The organization or person to whom the certificate is issued.
- **Issuer Name**. The name of the CA that issued the certificate.
- **Expiry Time**. The date after which the certificate becomes invalid.

To view the VPN Certificates:

Select **VPN** > **Certificates** from the main/sub-menu and the Certificates screen displays.

The top section of the Certificates screen displays the **Trusted Certificates (CA Certificates)**.



Operation succeeded.

Trusted Certificates (CA Certificate)

	CA Identity (Subject Name)	Issuer Name	Expiry Time
□	O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing Authority/emailAddress=support@cacert.org	O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing Authority/emailAddress=support@cacert.org	Mar 29 12:29:49 2033 GMT

Upload Trusted Certificate:

Trusted Certificate File:

Figure 8-9 Maybe OK??

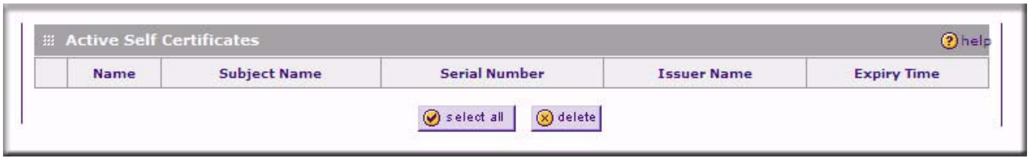
When you obtain a self certificate from a CA, you will also receive the CA certificate. In addition, many CAs make their certificates available on their websites.

To load a CA certificate into your firewall:

1. Store the CA certificate file on your computer.
2. Under **Upload Trusted Certificates** in the Certificates menu, click Browse and locate the CA certificate file.
3. Click **Upload**. The CA Certificate will appear in the **Trusted Certificates (CA Certificates) table**.

Viewing Active Self Certificates

The Active Self Certificates table in the Certificates screen shows the certificates issued to you by a CA and available for use.



Active Self Certificates

	Name	Subject Name	Serial Number	Issuer Name	Expiry Time

Figure 8-10OK

For each self certificate, the following data is listed:

- **Name**. The name you used to identify this certificate.
- **Subject Name**. This is the name that other organizations will see as the holder (owner) of this certificate. This should be your registered business name or official company name. Generally, all of your certificates should have the same value in the Subject field.
- **Serial Number**. This is a serial number maintained by the CA. It is used to identify the certificate with in the CA.
- **Issuer Name**. The name of the CA that issued the certificate.
- **Expiry Time**. The date on which the certificate expires. You should renew the certificate before it expires.

Obtaining a Self Certificate from a Certificate Authority

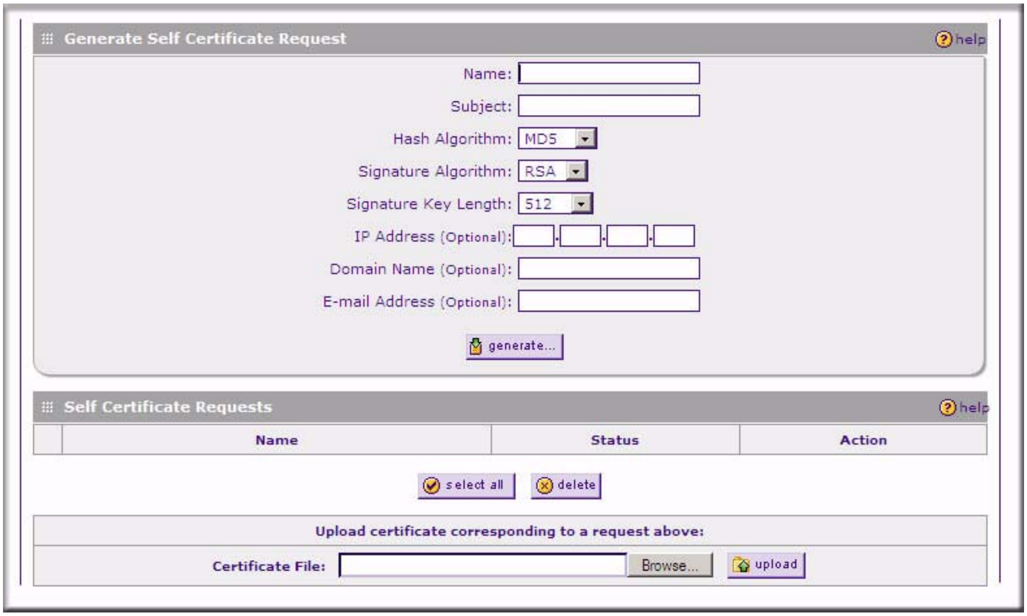
To use a self certificate, you must first request the certificate from the CA, then download and activate the certificate on your system. To request a self certificate from a CA, you must generate a Certificate Signing Request (CSR) for your firewall. The CSR is a file containing information about your company and about the device that will hold the certificate. Refer to the CA for guidelines on the information you include in your CSR.

To generate a new Certificate Signing Request (CSR) file:

1. Locate the **Generate Self Certificate Request** section of the Certificates screen.
2. Configure the following fields:
   - **Name** – Enter a descriptive name that will identify this certificate.
   - **Subject** – This is the name which other organizations will see as the holder (owner) of the certificate. Since this name will be seen by other organizations, you should use your registered business name or official company name. (Using the same name, or a derivation of the name, in the Title field would be useful.)
   - From the pull-down menus, choose the following values:
     – Hash Algorithm: MD5 or SHA2.

     – Signature Algorithm: RSA.

     – Signature Key Length: 512, 1024, 2048. (Larger key sizes may improve security, but may also decrease performance.)



Generate Self Certificate Request

Name:

Subject:

Hash Algorithm: MD5

Signature Algorithm: RSA

Signature Key Length: 512

IP Address (Optional): . . .

Domain Name (Optional):

E-mail Address (Optional):

Self Certificate Requests

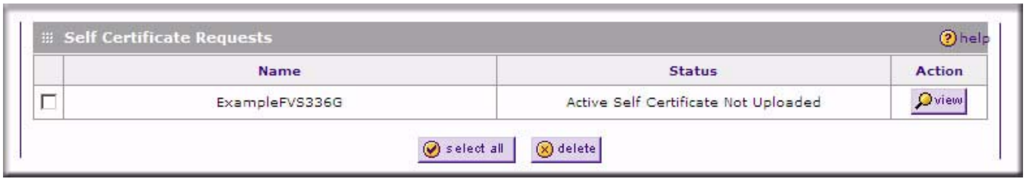
	Name	Status	Action

Upload certificate corresponding to a request above:

Certificate File:

Figure 8-11OK

3. Complete the **Optional** fields, if desired, with the following information:
   - **IP Address** – If you have a fixed IP address, you may enter it here. Otherwise, you should leave this field blank.
   - **Domain Name** – If you have an Internet domain name, you can enter it here. Otherwise, you should leave this field blank.
   - **E-mail Address** – Enter the e-mail address of a technical contact in your organization.
4. Click **Generate**. A new certificate request is created and added to the **Self Certificate Requests** table.

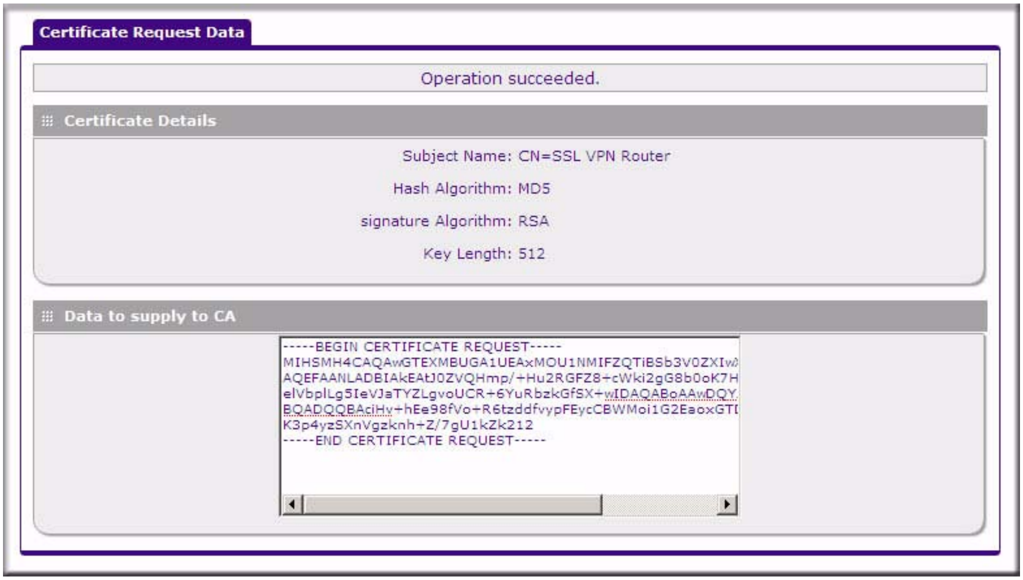


Self Certificate Requests

	Name	Status	Action
□	ExampleFVS336G	Active Self Certificate Not Uploaded	view

Figure 8-12 Need new screenshot

5. In the **Self Certificate Requests** table, click **View** under the Action column to view the request.



Operation succeeded.

Subject Name: CN=SSL VPN Router

Hash Algorithm: MD5

signature Algorithm: RSA

Key Length: 512

```
-----BEGIN CERTIFICATE REQUEST-----
MIHSMH4CAQAwGTEXMBUGA1UEAxMOU1NMIFZQTiBSb3V0ZXIw
AQEFAANLADBIAkEAtJ0ZVQHmp/+Hu2RGFZ8+cWki2gG8b0oK7H
elVbplLg5IeVJaTYZLgvoUCR+6YuRbzkGfSX+wIDAQABoAAwDQY
BQADQQBAciHv+hEe98fVo+R6tzddfvypFEycCBWMoi1G2EaoxGT
K3p4yzSXnVgzknh+Z/7gU1kZk212
-----END CERTIFICATE REQUEST-----
```

Figure 8-13OK

6. Copy the contents of the **Data to supply to CA** text box into a text file, including all of the data contained from “----BEGIN CERTIFICATE REQUEST---” to “---END CERTIFICATE REQUEST---”.

7. Submit your certificate request to a CA:

   a. Connect to the website of the CA.

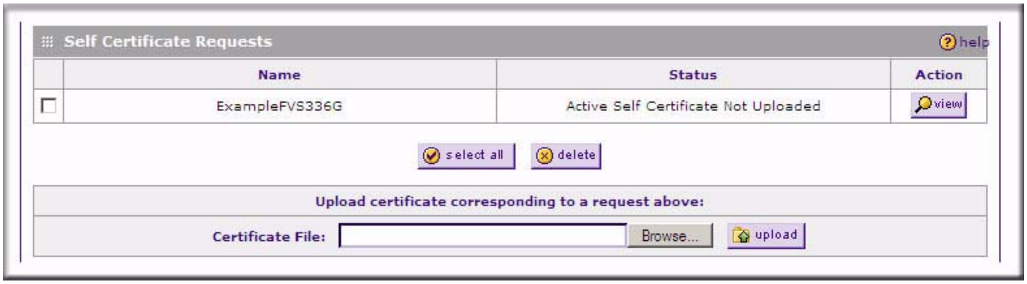
   b. Start the Self Certificate request procedure.

   c. When prompted for the requested data, copy the data from your saved text file (including “----BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST”).

   d. Submit the CA form. If no problems occur, the certificate will be issued.

8. Store the certificate file from the CA on your computer and backup the certificate file from the CA in another location.

9. Return to the Certificates screen and locate the **Self Certificate Requests** section..



Self Certificate Requests

	Name	Status	Action
□	ExampleFVS336G	Active Self Certificate Not Uploaded	view

Upload certificate corresponding to a request above:

Certificate File:

Figure 8-14need new screenshot

10. Select the checkbox next to the certificate request, then click **Browse** and locate the certificate file on your PC.

11. Click **Upload**. The certificate file will be uploaded to this device and will appear in the **Active Self Certificates** list.

If you have not already uploaded the CA certificate, do so now, as described in "The top section of the Certificates screen displays the Trusted Certificates (CA Certificates)." on page 8-10. You should also periodically check your CA's Certificate Revocation List, as described in "Managing your Certificate Revocation List (CRL)" on page 8-14.

Managing your Certificate Revocation List (CRL)

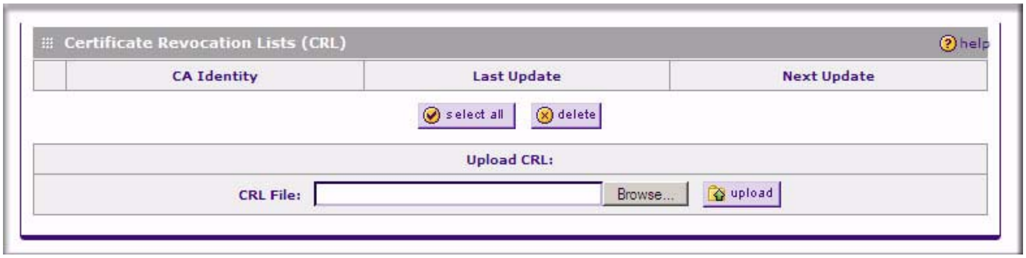
A CRL file shows certificates that have been revoked and are no longer valid. Each CA issues their own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

In the Certificates menu, you can view your currently-loaded CRLs and upload a new CRL.

To view and upload CRLs:

1. Select **VPN** > **Certificates** from the main/submenu.

   The Certificates menu will display showing the **Certificate Revocation Lists (CRL)** table at the bottom of the screen.



Certificate Revocation Lists (CRL)

	CA Identity	Last Update	Next Update

Upload CRL:

CRL File:

Figure 8-15OK

The CRL table lists your active CAs and their critical release dates:

- **CA Identify –** The official name of the CA which issued this CRL.
- **Last Update –** The date when this CRL was released.
- **Next Update –** The date when the next CRL will be released.

2. Click **Browse** and locate the CRL file you previously downloaded from a CA.
3. Click **Upload.** The CRL file will be uploaded and the CA Identity will appear in the **Certificate Revocation Lists (CRL)** table. If you had a previous CA Identity from the same CA, it will be deleted.

Chapter 9
Firewall and Network Management

This chapter describes how to use the network management features of your ProSafe Wireless-N VPN Firewall. These features can be found by clicking on the appropriate heading in the Main Menu of the browser interface.

The ProSafe Wireless-N VPN Firewall offers many tools for managing the network traffic to optimize its performance. You can also control administrator access, be alerted to important events requiring prompt action, monitor the firewall status, perform diagnostics, and manage the firewall configuration file.

This chapter contains the following sections:

- "Performance Management"
- "Changing Passwords and Administrator Settings"
- "Enabling Remote Management Access"
- "Using an SNMP Manager"
- "Settings Backup and Firmware Upgrade"
- "Configuring Time Zone Settings"

Performance Management

Performance management consists of controlling the traffic through the firewall so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the firewall in each direction is as follows:

- LAN side: 5000 Mbps (five LAN ports at 1000 Mbps each)

- WAN side: 1000 Mbps (one WAN port at 1000 Mbps)

In practice, the WAN side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. As a result and depending on the traffic being carried, the WAN side of the firewall will be the limiting factor to throughput for most installations.

Features that Reduce Traffic

Features of the VPN firewall that can be called upon to decrease WAN-side loading are as follows:

- Service blocking
- Block sites
- Source MAC filtering

Service Blocking

You can control specific outbound traffic (from LAN to WAN). Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.

⚠ **Warning:** This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

As you define your firewall rules, you can further refine the application according to the following criteria:

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired options:
  - Any**.** All PCs and devices on your LAN.
  - Single address**.** The rule will be applied to the address of a particular PC.
  - Address range**.** The rule is applied to a range of addresses.

  - Groups**.** The rule is applied to a Group (see “Managing Groups and Hosts (LAN Groups)” on page 3-5 to assign PCs to a Group using the LAN Groups Database).

- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on the IP address.
  - Any**.** The rule applies to all Internet IP address.
  - Single address**.** The rule applies to a single Internet IP address.
  - Address range**.** The rule is applied to a range of Internet IP addresses.
- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “Services-Based Rules” on page 5-2 and “Adding Customized Services” on page 5-17).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see “Setting Schedules to Block or Allow Traffic” on page 5-20).

See “Using Rules & Services to Block or Allow Traffic” on page 5-2 for the procedure on how to use this feature.

Services

The Rules menu contains a list of predefined Services for creating firewall rules. If a service does not appear in the predefined Services list, you can define the service. The new service will then appear in the Rules menu's Services list.

See “Services-Based Rules” on page 5-2 for the procedure on how to use this feature.

Groups and Hosts

You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The LAN Groups Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

- **DHCP Client Request.** By default, the DHCP server in this firewall is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the LAN Groups Database. Because of this, leaving the DHCP server feature (on the LAN screen) enabled is strongly recommended.
- **Scanning the Network.** The local network is scanned using ARP. requests. The ARP scan will detect active devices that are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will appear in the database as Unknown.
- **Manual Entry**. You can manually enter information about a device.

See "Managing Groups and Hosts (LAN Groups)" on page 3-5 for the procedure on how to use this feature.

Schedule

If you have set firewall rules on the Rules screen, you can configure three different schedules (for example, schedule 1, schedule 2, and schedule 3) for when a rule is to be applied. Once a schedule is configured, it affects all Rules that use this schedule. You specify the days of the week and time of day for each schedule.

See "Setting Schedules to Block or Allow Traffic" on page 5-20 for the procedure on how to use this feature.

Block Sites

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall's filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed.

- **Keyword (and Domain Name) Blocking.** You can specify up to 32 words that, should they appear in the Web site name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

  You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

  You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains on this list by PCs even in the groups for which keyword blocking has been enabled will still be allowed without any blocking.

- **Web Component blocking.** You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Sites on the Trusted Domains list are still subject to Web component blocking when the blocking of a particular Web component has been enabled.

See "Setting Block Sites (Content Filtering)" on page 5-21 for the procedure on how to use this feature.

Source MAC Filtering

If you want to reduce outgoing traffic to prevent Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed.

See "Enabling Source MAC Filtering (Address Filter)" on page 5-24 for the procedure on how to use this feature.

Features that Increase Traffic

Features that tend to increase WAN-side loading are as follows:

- Port forwarding
- Port triggering
- Exposed hosts
- VPN tunnels

Port Forwarding

The firewall always blocks DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it (i.e., the service is unavailable). You can also create additional firewall rules that are customized to block or allow specific traffic.

⚠	**Warning:** This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

You can control specific inbound traffic (from WAN to LAN). Inbound Services lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- ALLOW always
- BLOCK by schedule, otherwise allow
- ALLOW by schedule, otherwise block

You can also enable a check on special rules:

- **VPN Passthrough.** Passes the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.
- **Drop fragmented IP packets.** Drops any fragmented IP packets.
- **UDP Flooding.** Limits the number of UDP sessions created from one LAN machine.
- **TCP Flooding.** Protects the firewall from SYN flood attack.

- **Enable DNS Proxy.** Allows the firewall to handle DNS queries from the LAN.
- **Enable Stealth Mode.** Prevents the firewall from responding to incoming requests for unsupported services.

As you define your firewall rules, you can further refine the application according to the following criteria:

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired IP Address in this field.
- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on the IP address.
  - Any: The rule applies to all Internet IP address.
  - Single address: The rule applies to a single Internet IP address.
  - Address range: The rule is applied to a range of Internet IP addresses.
- **Destination Address.** These settings determine the destination IP address for this rule which will be applicable to incoming traffic. This rule will be applied only when the destination IP address of the incoming packet matches the IP address of the WAN interface. Selecting ANY enables the rule for any LAN IP destination.
- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 5-17).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Setting Schedules to Block or Allow Traffic" on page 5-20).

See "Using Rules & Services to Block or Allow Traffic" on page 5-2 for the procedure on how to use this feature.

Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the application.

Once configured, port triggering operates as follows:

- A PC makes an outgoing connection using a port number defined in the Port Triggering table.
- This firewall records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.

- The remote system receives the PCs request and responds using the different port numbers that you have now opened.
- This firewall matches the response to the previous request and forwards the response to the PC. Without port triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules.
  - Only one PC can use a port triggering application at any time.
  - After a PC has finished using a port triggering application, there is a time-out period before the application can be used by another PC. This is required because the firewall cannot be sure when the application has terminated.

See “Enabling Port Triggering” on page 5-28 for the procedure on how to use this feature.

VPN Tunnels

The VPN firewall permits up to 5 IPsec VPN tunnels and 3 SSL VPN tunnels not to exceed 8 total tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See Chapter 6, “Virtual Private Networking Using IPsec” for the procedures on how to use IPsec VPN, and Chapter 7, “Virtual Private Networking Using SSL for the procedures on how to use SSL VPN.

Using QoS to Shift the Traffic Mix

The QoS priority settings determine the priority and, in turn, the quality of service for the traffic passing through the firewall. The QoS is set individually for each service.

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

The QoS priority settings conform to the IEEE 802.1D-1998 (formerly 802.1p) standard for class of service tag.

You will not change the WAN bandwidth used by changing any QoS priority settings. But you will change the mix of traffic through the WAN port by granting some services a higher priority than others. The quality of a service is impacted by its QoS setting, however.

See “Setting Quality of Service (QoS) Priorities” on page 5-19 for the procedure on how to use this feature.

Tools for Traffic Management

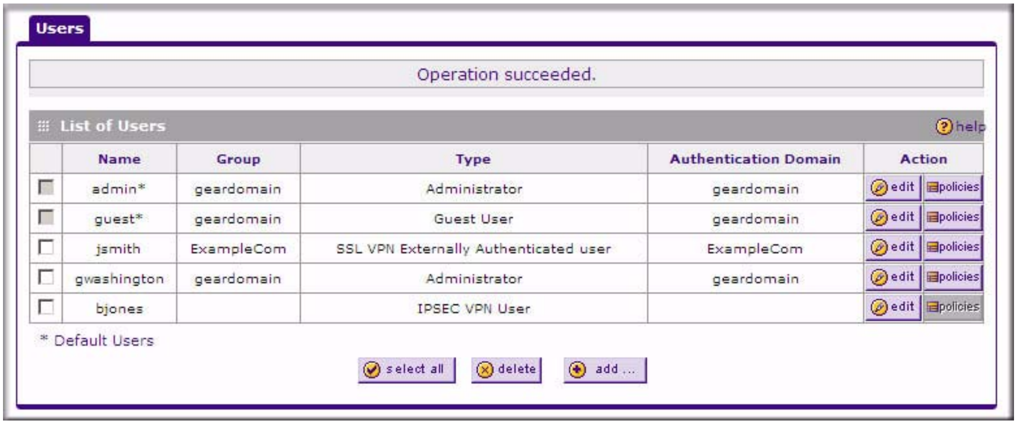
The ProSafe Wireless-N VPN Firewall includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic each individual is allowed to have. See “Monitoring System Performance” on page 11-1 for a discussion of the tools.

Changing Passwords and Administrator Settings

The default administrator and guest password for the Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password. You can also configure a separate password for the guest account.

To modify the Administrator user account settings, including password:

1. Select **Users > Users** from the main/submenu and the List of Users screen displays.



Operation succeeded.

List of Users

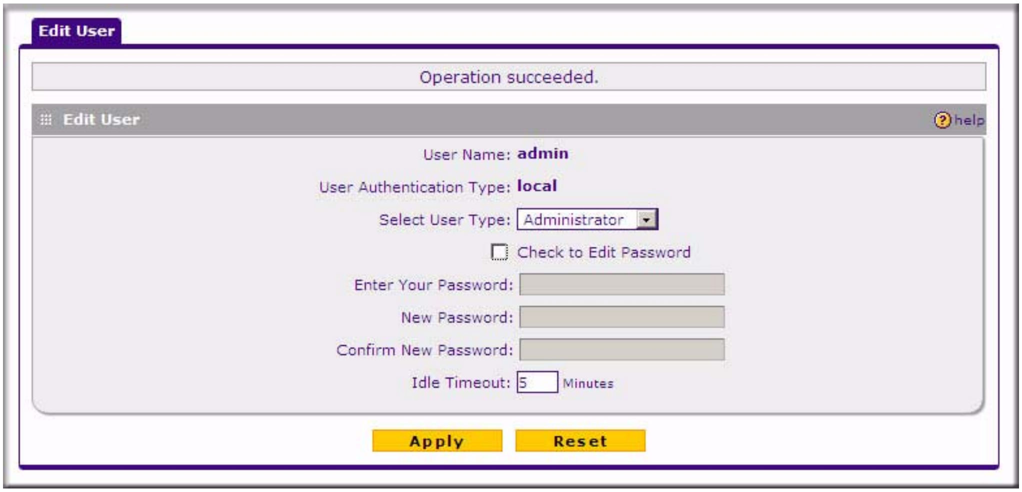
	Name	Group	Type	Authentication Domain	Action
□	admin*	geardomain	Administrator	geardomain	edit policies
□	guest*	geardomain	Guest User	geardomain	edit policies
□	jsmith	ExampleCom	SSL VPN Externally Authenticated user	ExampleCom	edit policies
□	gwashington	geardomain	Administrator	geardomain	edit policies
□	bjones		IPSEC VPN User		edit policies

* Default Users

Figure 9-1OK

2. Select the checkbox adjacent to admin in the **Name** column, then click **Edit** in the **Action** column.

The Edit User screen is displayed, with the current settings for Administrator displayed in the **Select User Type** pull-down menu.



Operation succeeded.

User Name: admin

User Authentication Type: local

Select User Type: Administrator

□ Check to Edit Password

Enter Your Password:

New Password:

Confirm New Password:

Idle Timeout: 5 Minutes

Figure 9-2OK

3. Select the **Check to Edit Password** checkbox. The password fields become active.
4. Enter the old password, then enter the new password twice.
5. (Optional) To change the idle timeout for an administrator login session, enter a new number of minutes in the **Idle Timeout** field.
6. Click **Apply** to save your settings or **Reset** to return to your previous settings.

Note: If the administrator login timeout value is too large, you may have to wait a long time before you are able to log back into the firewall if your previous login was disrupted (for example, if you did not click **Logout** on the Main Menu bar to log out).

Note: After a factory default reset, the password and timeout value will be changed back to **password** and **5** minutes, respectively.

Enabling Remote Management Access

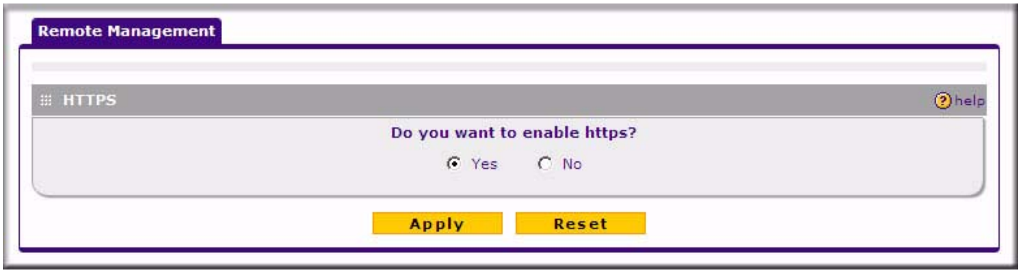
Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your firewall. You must be logged in locally to enable remote management (see "Logging into the Security Router" on page 2-2).

> **Note:** Be sure to change the default configuration password of the firewall to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See "Changing Passwords and Administrator Settings" on page 9-8 for the procedure on how to do this.

To configure your firewall for Remote Management:

1. Select **Administration** > **Remote Management** from the main/submenu.

   The Remote Management screen displays.



Remote Management

HTTPS

Do you want to enable https?

● Yes ○ No

Figure 9-3OK

2. Click the **Yes** radio box to enable HTTPS remote management (enabled by default).

> **Note:** For enhanced security, restrict access to as few external IP addresses as practical. See "Setting User Login Policies" on page 8-6 for instructions on restricting administrator access. Be sure to use strong passwords.

3. Click **Apply** to have your changes take effect.

   When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* (not *http://*) and type your firewall's WAN IP address into your browser.

   For example, if your WAN IP address is 172.16.0.123, type the following in your browser:

https://172.16.0.123

The firewall's remote login URL is **https://<*IP_address*>** or **https://<*FullyQualifiedDomainName*>**..

Note: To maintain security, the SRXN3205 will reject a login that uses *http://address* rather than the SSL *https://address*.

Note: The first time you remotely connect to the SRXN3205 with a browser via SSL, you may get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate.

Note: If you are unable to remotely connect to the SRXN3205 after enabling HTTPS remote management, check whether other user policies, such as the default user policy, are preventing access.

Note: If you disable HTTPS remote management, all SSL VPN user connections will also be disabled.

Tip: If you are using a dynamic DNS service such as TZO, you can identify the WAN IP address of your SRXN3205 by running `tracert` from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert SRXN3205.mynetgear.net`**, and the WAN IP address that your ISP assigned to the SRXN3205 is displayed.

Using an SNMP Manager

Simple Network Management Protocol (SNMP) lets you monitor and manage your firewall from an SNMP Manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

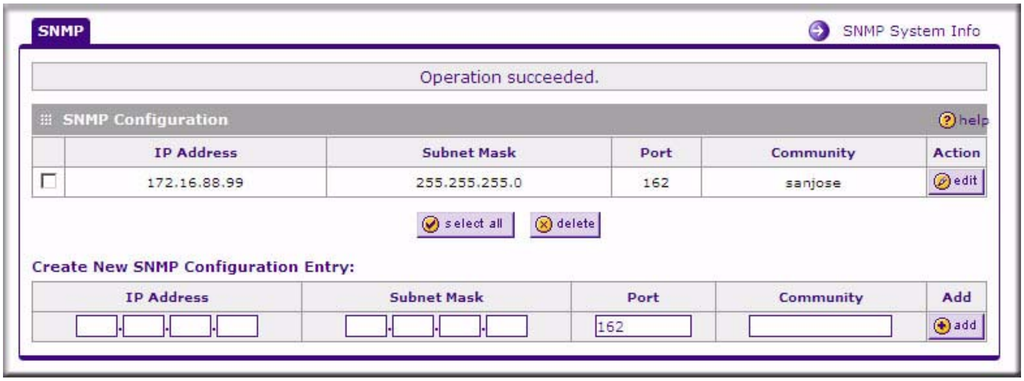
The SNMP Configuration table lists the SNMP configurations by:

- **IP Address**. The IP address of the SNMP manager.

- **Port**. The trap port of the configuration.
- **Community**. The trap community string of the configuration.

To create a new SNMP configuration entry:

1. Select **Administration > SNMP** from the main/submenu and the **SNMP** screen displays.



Operation succeeded.

SNMP Configuration

	IP Address	Subnet Mask	Port	Community	Action
□	172.16.88.99	255.255.255.0	162	sanjose	edit

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	Community	Add
		162		add

Figure 9-4OK

2. Configure the following fields in the **Create New SNMP Configuration Entry** section:
   - Enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.
     – If you want to allow only the host address to access the VPN firewall and receive traps, enter an IP Address of, for example, 192.168.1.101 with a Subnet Mask of 255.255.255.**255**.
     – If you want to allow a subnet access to the VPN firewall through SNMP, enter an IP address of, for example,192.168.1.101 with a Subnet Mask of 255.255.255.**0**. The traps will still be received on 192.168.1.101, but the entire subnet will have access through the community string.
     – If you want to make the VPN firewall globally accessible using the community string, but still receive traps on the host, enter 0.0.0.0 as the Subnet Mask and an IP Address for where the traps will be received.
   - Enter the trap port number of the configuration in the **Port** field. The default is 162.
   - Enter the trap community string of the configuration in the **Community** field.
3. Click **Add** to create the new configuration. The entry is displayed in the **SNMP Configuration** table.

The **SNMP System Info** link, located in the upper right of the screen, opens the **SNMP SysConfiguration** screen. This screen displays the VPN firewall identification information available to the SNMP manager: System Contact, System Location, and System name. You can edit these values.

Settings Backup and Firmware Upgrade

Once you have installed the VPN firewall and have it working properly, you should back up a copy of your settings, in case something gets corrupted. When you backup the settings, these are saved as a file on your computer. You can then restore the VPN firewall settings from this file. The **Settings Backup and Firmware Upgrade** screen allows you to:

- Back up and save a copy of your current settings
- Restore saved settings from the backed-up file.
- Revert to the factory default settings.
- Upgrade the VPN firewall firmware from a saved file on your hard disk to use a different firmware version.

Backup and Restore Settings

To backup settings:

1. Select **Administration** > **Settings Backup and Firmware Upgrade** from the main/submenu.

   The Settings Backup and Firmware Upgrade screen displays.

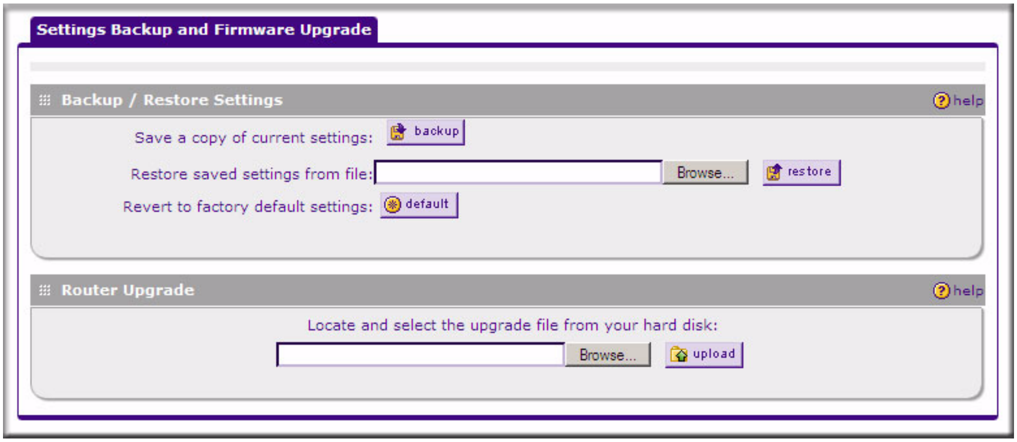

Settings Backup and Firmware Upgrade
Backup / Restore Settings
help
Save a copy of current settings:
backup
Restore saved settings from file:
Browse...
restore
Revert to factory default settings:
default
Router Upgrade
help
Locate and select the upgrade file from your hard disk:
Browse...
upload

Figure 9-5OK

2. Click **Backup** to save a copy of your current settings.
   - If your browser isn't set up to save downloaded files automatically, locate where you want to save the file, specify file name, and click Save.
   - If you have your browser set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk.

⚠	**Warning:** Once you start restoring settings or erasing the firewall, do NOT interrupt the process. Do not try to go online, turn off the firewall, shut down the computer or do anything else to the firewall until it finishes restarting!

To restore settings from a backup file:

1. Next to **Restore save settings from file**, click the **Browse** button.
2. Locate and select the previously saved backup file (by default, netgear.cfg).
3. When you have located the file, click the **Restore** button.

   An Alert page will appear indicating the status of the restore operation. You must manually restart the VPN firewall for the restored settings to take effect.

To reset the firewall to the original factory default settings, click the **Default** button.

You must manually restart the VPN firewall before the default settings to take effect. After rebooting, the firewall's password will be **password** and the LAN IP address will be **192.168.1.1.** The VPN firewall will act as a DHCP server on the LAN, to the wireless clients, and act as a DHCP client to the Internet.

⚠	**Warning:** When you click **default,** your firewall settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Please backup your settings or all your settings will be lost!

Router Upgrade

You can install a different version of the VPN firewall firmware from the **Settings Backup and Firmware Upgrade** menu. To view the current version of the firmware that your VPN firewall is running, choose **Monitoring** from the main menu. The **Router Status** screen is displayed, showing all of the VPN firewall router statistics, including the firmware version. When you upgrade your firmware, the new firmware version will be displayed.

To download a firmware version:

1. Go to the NETGEAR Web site at *http://www.netgear.com/support* and click **Downloads.**

2. From the **Product Selection** pull-down menu, choose the SRXN3205. Select the software version and follow the **To Install** steps to download your software.

   After downloading an upgrade file, you may need to unzip (uncompress) it before upgrading the firewall. If release notes are included in the download, read them before continuing.

To upgrade the router software:

1. Select **Administration** > **Settings Backup and Firmware Upgrade** from the main/submenu.
2. In the **Router Upgrade** section, click **Browse.**
3. Locate the downloaded file and click **Upload.** This will start the software upgrade to your VPN firewall. This may take some time. At the conclusion of the upgrade, your firewall will reboot.

⚠	**Warning:** Do not try to go online, turn off the firewall, shutdown the computer or do anything else to the firewall until the firewall finishes the upgrade! When the Test light turns off, wait a few more seconds before doing anything.

4. After the VPN firewall has rebooted, click **Monitoring** and confirm the new firmware version to verify that your firewall now has the new software installed.

➡	**Note:** In some cases, such as a major upgrade, it may be necessary to erase the configuration and manually reconfigure your firewall after upgrading it. Refer to the release notes included with the software to find out if this is required.

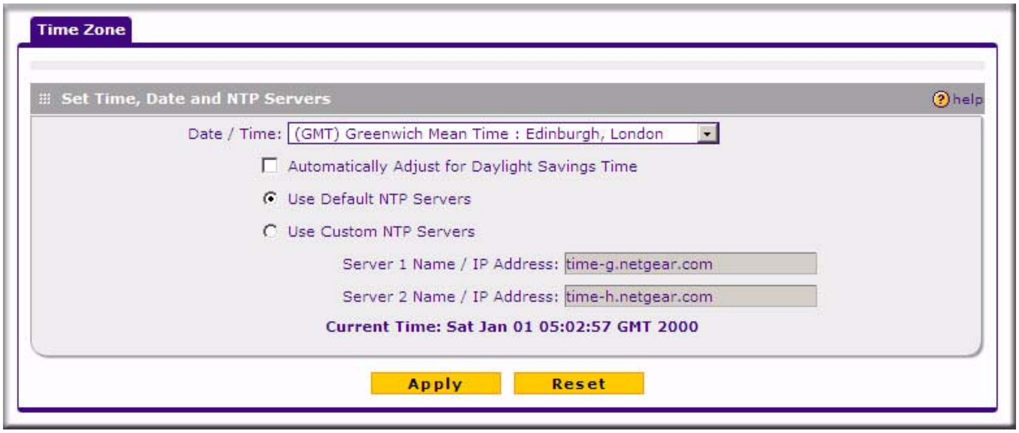
Configuring Time Zone Settings

The **Time Zone** screen provides settings for Date, Time and NTP server designations. The Network Time Protocol (NTP) is used to synchronize computer clock times in a network of computers.

To set Time, Date and NTP servers:

1. Select **Administration** > **Time Zone** from the main/submenu.

   The Time Zone screen displays.



Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London

□ Automatically Adjust for Daylight Savings Time

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-g.netgear.com

Server 2 Name / IP Address: time-h.netgear.com

Current Time: Sat Jan 01 05:02:57 GMT 2000

Figure 9-6Need new screen shot

2. From the **Date/Time** pull-down menu, choose the Local Time Zone.

   This is required for scheduling work correctly. The VPN firewall includes a real-time clock (RTC), which it uses for scheduling.

3. If supported in your region, click **Automatically Adjust for Daylight Savings Time**.

4. Select an NTP Server option:

   - **Use Default NTP Servers**. The RTC is updated regularly by contacting a Netgear NTP server on the Internet. A primary and secondary (backup) server are preloaded.
   - **Use Custom NTP Servers**. If you prefer to use a particular NTP server, enter the name or IP address of the NTP Server in the **Server 1 Name/IP Address** field. You can enter the address of a backup NTP server in the **Server 2 Name/IP Address** field. If you select this option and leave either the Server 1 or Server 2 fields empty, they will be set to the default Netgear NTP servers.

> **Note:** If you select the default NTP servers or if you enter a custom server FQDN, the firewall must determine the IP address of the NTP server by a DNS lookup. You must configure a DNS server address in the Network menu before the firewall can perform this lookup.

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

Chapter 11
Monitoring System Performance

This chapter describes the full set of system monitoring features of your ProSafe Wireless-N Security Router. You can be alerted to important events such as {{WAN port rollover}}, WAN traffic limits reached, and login failures and attacks. You can also view status information about the firewall, WAN port, LAN ports, and VPN tunnels.

This chapter contains the following sections:

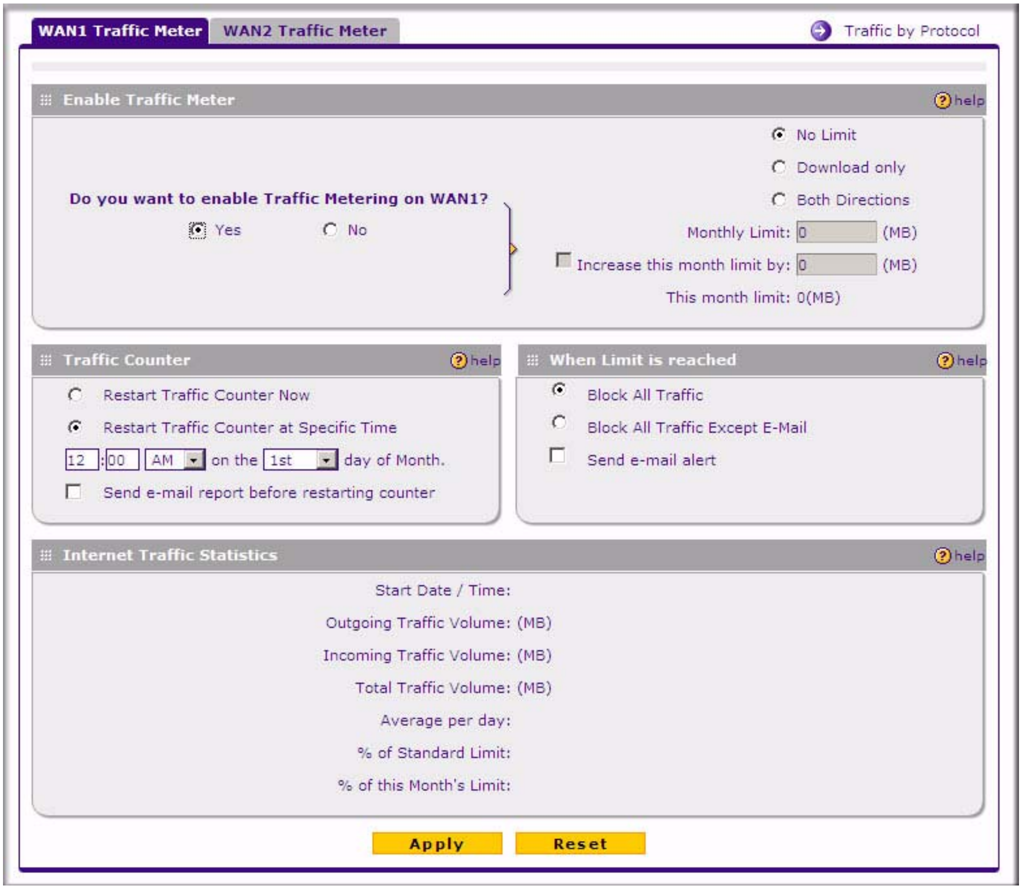
Enabling the Traffic Meter

If your ISP charges by traffic volume over a given period of time, or if you want to study traffic types over a period of time, you can activate the Traffic Meter for the WAN port.

To monitor traffic limits on the WAN port:

1. Select **Monitoring** > **Traffic Meter** from the main/submenu, and then the WAN Traffic Meter tab.

   The WAN Traffic Meter screen will display.



Enable Traffic Meter

Do you want to enable Traffic Metering on WAN1?

● Yes ○ No

● No Limit
○ Download only
○ Both Directions

Monthly Limit: 0 (MB)

□ Increase this month limit by: 0 (MB)

This month limit: 0(MB)

Traffic Counter

○ Restart Traffic Counter Now
● Restart Traffic Counter at Specific Time

12 :00 AM on the 1st day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block All Traffic
○ Block All Traffic Except E-Mail
□ Send e-mail alert

Internet Traffic Statistics

Start Date / Time:
Outgoing Traffic Volume: (MB)
Incoming Traffic Volume: (MB)
Total Traffic Volume: (MB)
Average per day:
% of Standard Limit:
% of this Month's Limit:

Figure 11-1 Need New Screenshot

2. Enable the traffic meter by clicking the **Yes** radio box under **Do you want to enable Traffic Metering on WAN?** The traffic meter will record the volume of Internet traffic passing through the WAN. Select the following options:
   - **No Limit.** Any specified restrictions will not be applied when traffic limit is reached.
   - **Download only.** The specified restrictions will be applied to the incoming traffic only
   - **Both Directions.** The specified restrictions will be applied to both incoming and outgoing traffic only
   - **Monthly Limit**. Enter the monthly volume limit and select the desired behavior when the limit is reached.

Note: Both incoming and outgoing traffic are included in the limit

- **Increase this month limit by**. Temporarily increase the Traffic Limit if you have reached the monthly limit, but need to continue accessing the Internet. Select the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so that the increase is only applied once.)
- **This month limit**. Displays the limit for the current month.

3. In the **Traffic Counter** section, make your traffic counter selections:
   - **Restart Traffic Counter Now**. Select this option and click Apply to restart the Traffic Counter immediately.
   - **Restart Traffic Counter at Specific Time**. Restart the Traffic Counter at a specific time and day of the month. Fill in the time fields and choose AM or PM and the day of the month from the pull-down menus.
   - **Send e-mail report before restarting counter**. An E-mail report will be sent immediately before restarting the counter. You must configure the E-mail screen in order for this function to work (see "E-Mail Notifications of Event Logs and Alerts" on page 5-33).
4. In the **When limit is reached** section, make the following choice:
   - **Block all traffic**. All access to and from the Internet will be blocked.
   - **Block all traffic except E-mail**. Only E-mail traffic will be allowed. All other traffic will be blocked.
   - **Send E-mail alert.** You must configure the E-mail screen in order for this function to work. Go to the Firewall Logs and & E-mail Tab to set this up.
5. Click **Apply** to save your settings.

   The **Internet Traffic Statistics** section displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.
6. Click the **Traffic by Protocol** link, in the upper right header, to see a report of the Internet traffic by type. The volume of traffic for each protocol will be displayed in a popup window. Traffic counters are updated in MBytes scale; the counter starts only when traffic passed is at least 1MB.

Activating Notification of Events and Alerts

The Firewall Logs can be configured to log and then e-mail denial of access, general attack information, and other information to a specified e-mail address. For example, your security router will log security-related events such as: accepted and dropped packets on different segments of your LAN; denied incoming and outgoing service requests; hacker probes and login attempts; and other general information based on the settings you input on the **Firewall Logs & E-mail** menu. In addition, if you have set up Content Filtering on the Block Sites screen (see "Setting Block Sites (Content Filtering)" on page 5-21), a log will be generated when someone on your network tries to access a blocked site.

You must have e-mail notification enabled to receive the logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs by clicking the **View Logs** option arrow to the right of the tab. Selecting all events will increase the size of the log, so it is good practice to select only those events which are required

To configure logging and notifications:

1. Select Monitoring from the main menu and Firewall Logs & E-mail from the submenu.

   The Firewall Logs & E-mail screen displays.

2. Enter the name of the log in the **Log Identifier** field.

   Log Identifier is a mandatory field used to identify which device sent the log messages. The identifier is appended to log messages.

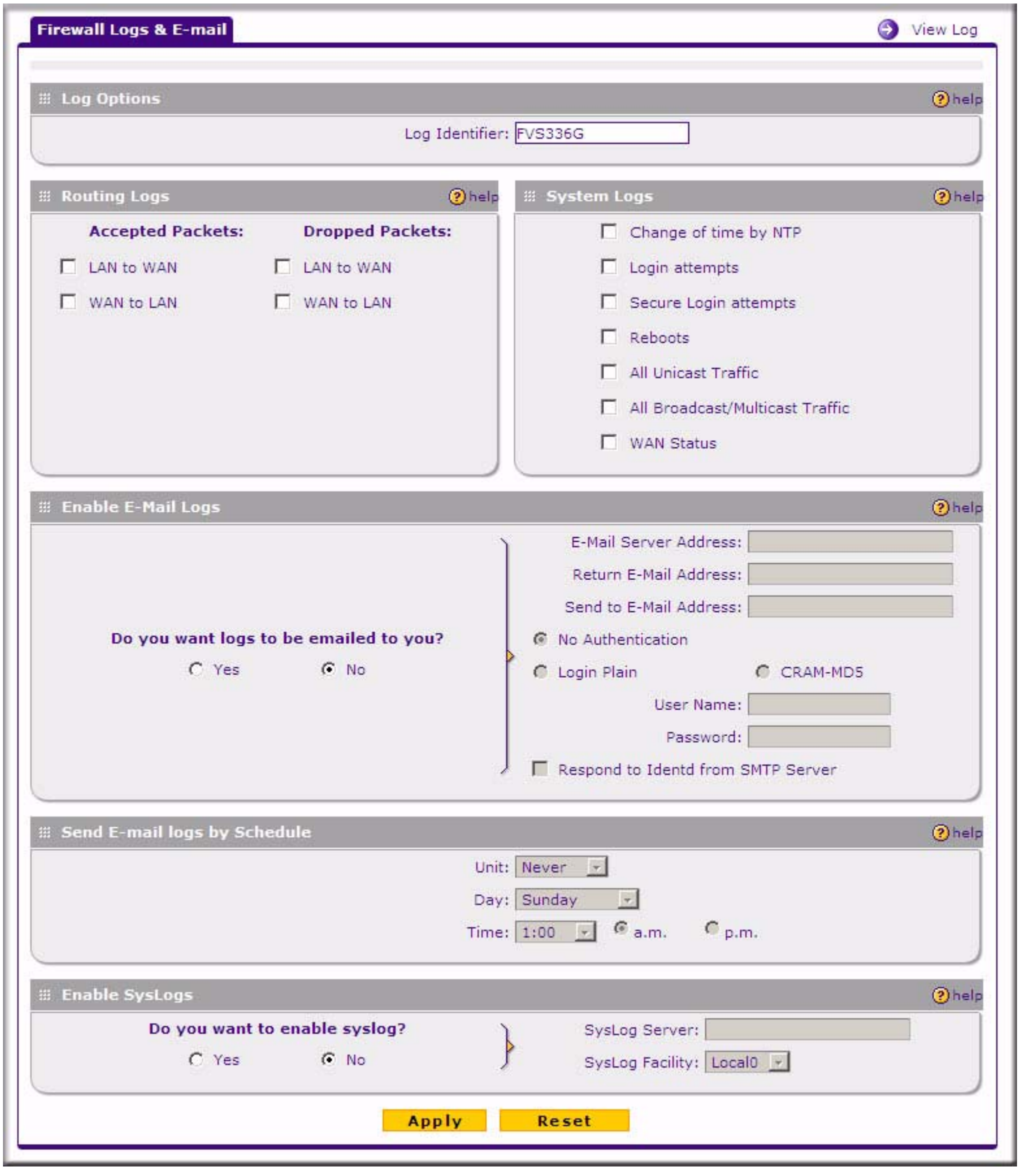
3. In the **Routing Logs** section, select the network segments for which you would like logs to be sent (for example, LAN to WAN under Dropped Packets).
4. In the **System Logs** section, select the type of system events to be logged.
5. Check **Yes** to enable E-mail Logs. Then enter:

   a. **E-mail Server address**. Enter either the IP address or Internet name of your ISP's outgoing E-mail SMTP server. If you leave this box blank, no logs will be sent to you.

   b. **Return E-mail Address**. Enter an e-mail address to appear as the sender.

   c. **Send To E-mail Address**. Enter the e-mail address where the logs and alerts should be sent. You must use the full e-mail address (for example, jsmith@example.com).

6. **No Authentication** is selected by default. If your SMTP server requires user authentication, select the required authentication type—either **Login Plain** or **CRAM-MD5**. Then enter the user name and password to be used for authentication.



Firewall Logs & E-mail

View Log

Log Options

Log Identifier: FVS336G

Routing Logs

Accepted Packets:	Dropped Packets:
□ LAN to WAN	□ LAN to WAN
□ WAN to LAN	□ WAN to LAN

System Logs

□ Change of time by NTP

□ Login attempts

□ Secure Login attempts

□ Reboots

□ All Unicast Traffic

□ All Broadcast/Multicast Traffic

□ WAN Status

Enable E-Mail Logs

Do you want logs to be emailed to you?

○ Yes ● No

E-Mail Server Address:

Return E-Mail Address:

Send to E-Mail Address:

● No Authentication

○ Login Plain ○ CRAM-MD5

User Name:

Password:

□ Respond to Identd from SMTP Server

Send E-mail logs by Schedule

Unit: Never

Day: Sunday

Time: 1:00 ● a.m. ○ p.m.

Enable SysLogs

Do you want to enable syslog?

○ Yes ● No

SysLog Server:

SysLog Facility: Local0

Figure 11-2 Need new screenshot more option in this one

7. To respond to IDENT protocol messages, check the **Respond to Identd from SMTP Server** radio box. The Ident Protocol is a weak scheme to verify the sender of e-mail (a common daemon program for providing the ident service is identd).

8. Enter a **Schedule** for sending the logs. From the **Unit** pull-down menu, choose: Never, Hourly, Daily, or Weekly. Then set the Day and Time fields that correspond to your selection.
9. You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Click **Yes** to enable SysLogs and send messages to the syslog server, then:
   - **a.** Enter your **SysLog Server** IP address
   - **b.** Select the appropriate syslog facility from the **SysLog Facility** pull-down menu. The SysLog Facility levels of severity are described in the table below.
10. Click **Apply** to save your settings.

Numerical Code	Severity
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions
5	Notice: Normal but significant conditions
6	Informational: Informational messages
7	Debug: Debug level messages

Viewing Firewall Logs

To view the Firewall logs:

1. Select Monitoring from the main menu and Firewall Logs & E-mail in the submenu.

   The Firewall Logs & E-mail screen displays
2. Click the **View Log** link in the upper right-hand section of the screen.

   The **Logs** screen is displayed.
3. If the E-mail Logs options as been enabled, you can send a copy of the log by clicking **Send Log.**
4. Click **Refresh Log** to retrieve the latest update; click **Clear Log** to delete all entries.

Log entries are described in Table 11-1.

Table 11-1. Firewall Logs Field Descriptions

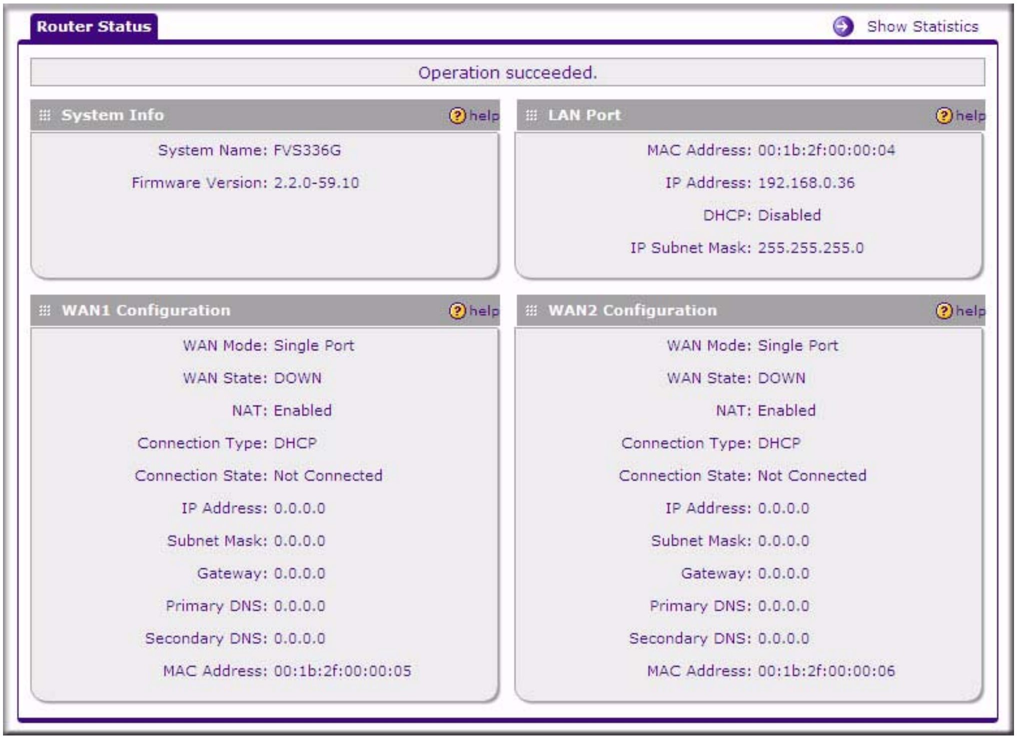
Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN or WAN.

Viewing Router Configuration and System Status

The **Router Status** screen provides status and usage information. To view the router configuration and system status:

1. Select Monitoring from the main menu and Router Status in the submenu.

   The Router Status screen is displayed.



Operation succeeded.

System Info

System Name: FVS336G
Firmware Version: 2.2.0-59.10

LAN Port

MAC Address: 00:1b:2f:00:00:04
IP Address: 192.168.0.36
DHCP: Disabled
IP Subnet Mask: 255.255.255.0

WAN1 Configuration

WAN Mode: Single Port
WAN State: DOWN
NAT: Enabled
Connection Type: DHCP
Connection State: Not Connected
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
MAC Address: 00:1b:2f:00:00:05

WAN2 Configuration

WAN Mode: Single Port
WAN State: DOWN
NAT: Enabled
Connection Type: DHCP
Connection State: Not Connected
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
MAC Address: 00:1b:2f:00:00:06

Figure 11-3 Need New screenshot

The following information is displayed:

Item	Description
System Name	This is the Account Name that you entered in the Basic Settings page.
Firmware Version	This is the current software the router is using. This will change if you upgrade your router.

Item	Description
LAN Port	Displays the current settings for MAC address, IP address, DHCP role and IP Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.
WAN Configuration	Indicates whether the WAN Mode is Single, Dual, or Rollover, and whether the WAN State is UP or DOWN. It also is displayed if: • NAT is Enabled or Disabled. • Connection Type: DHCP enabled or disabled. • Connection State • WAN IP Address • Subnet Mask • Gateway Address • Primary and Secondary DNS Server Addresses • MAC Address.

Note: The **Router Status** screen displays current settings and statistics for your router. As this information is read-only, any changes must be made on other pages.

Monitoring the WAN Port Status

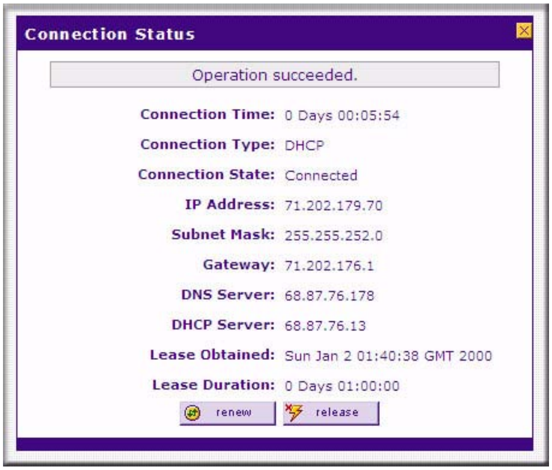
You can monitor the status of the WAN connection, the Dynamic DNS Server connection, and the DHCP Server connection. To monitor the status of the WAN port:

1. Select Network Configuration from the main menu and WAN Settings in the submenu.

The **WAN ISP Settings** screen is displayed.

2. Click the **WAN Status** link in the upper right-hand section of the screen.

The **Connection Status** popup window displays a status report on the WAN port. See figure 12-4.



Connection Status

Operation succeeded.

Connection Time: 0 Days 00:05:54

Connection Type: DHCP

Connection State: Connected

IP Address: 71.202.179.70

Subnet Mask: 255.255.252.0

Gateway: 71.202.176.1

DNS Server: 68.87.76.178

DHCP Server: 68.87.76.13

Lease Obtained: Sun Jan 2 01:40:38 GMT 2000

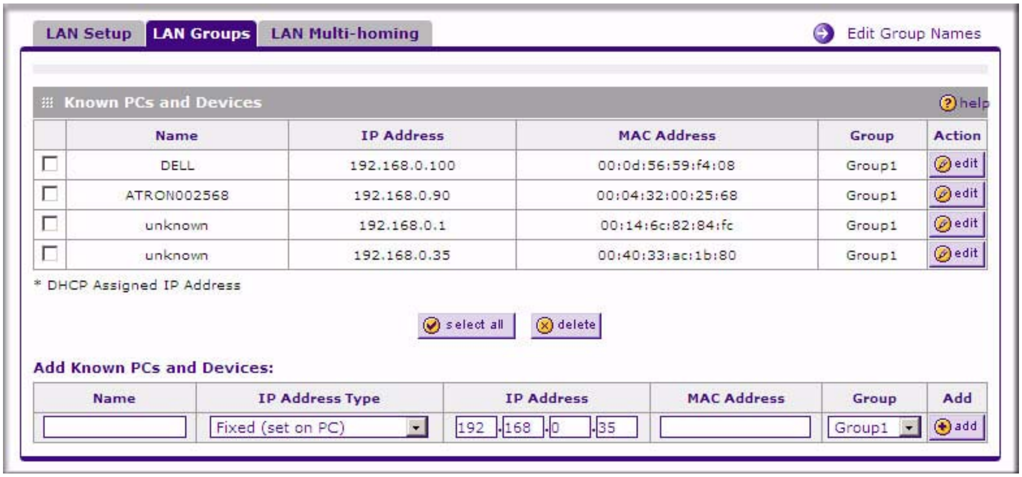
Lease Duration: 0 Days 01:00:00

Figure 11-4 Need new screenshot

Monitoring Attached Devices

The **LAN Groups** screen contains a table of all IP devices that the security router has discovered on the local network. To view the LAN Groups screen:

1. Select Network Configuration from the main menu and LAN Settings in the submenu.
2. Then select the LAN Groups tab and the LAN Groups screen displays.
3. The **Known PCs and Devices** database is an automatically-maintained list of LAN-attached devices. PCs and other LAN devices become known by the following methods:
   - **DHCP Client Requests**. By default, the DHCP server in the router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the database. Because of this, leaving the DHCP Server feature enabled (in the LAN Setup menu) is strongly recommended.
   - **Scanning the Network**. The local network is scanned using standard methods such as ARP. The scan will detect active devices that are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined and will be shown as unknown.
   - **Manually Adding Devices**. You can enter information in the **Add Known PCs and Devices** section and click **Add** to manually add a device to the database.



Known PCs and Devices

	Name	IP Address	MAC Address	Group	Action
□	DELL	192.168.0.100	00:0d:56:59:f4:08	Group1	edit
□	ATRON002568	192.168.0.90	00:04:32:00:25:68	Group1	edit
□	unknown	192.168.0.1	00:14:6c:82:84:fc	Group1	edit
□	unknown	192.168.0.35	00:40:33:ac:1b:80	Group1	edit

* DHCP Assigned IP Address

select all   delete

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Add
	Fixed (set on PC)	192.168.0.35		Group1	add

Figure 11-5OK

The **Known PCs and Devices** table lists all current entries in the LAN Groups database. For each PC or device, the following data is displayed

Table 11-2. Known PCs and Devices options

Item	Description
Name	The name of the PC or device. Sometimes, this can not be determined, and will be listed as Unknown. In this case, you can edit the entry to add a meaningful name.
IP Address	The current IP address. For DHCP clients, where the IP address is allocated by the DHCP Server in this device, this IP address will not change. Where the IP address is set on the PC (as a fixed IP address), you may need to update this entry manually if the IP address on the PC is changed.
MAC Address	The MAC address of the PC. The MAC address is a low-level network identifier which is fixed at manufacture.
Group	Each PC or device must be in a single group. The Group column indicates which group each entry is in. By default, all entries are in the Group1.

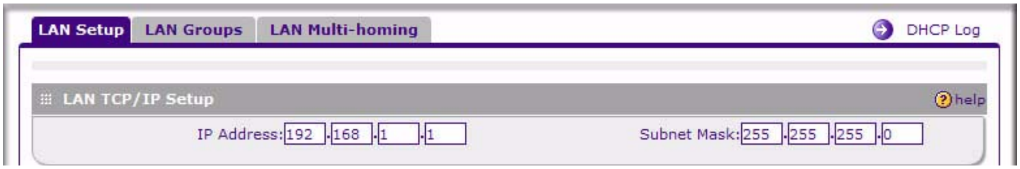
Note: If the security router is rebooted, the table data is lost until the security router rediscovers the devices.

Reviewing the DHCP Log

To review the most recent entries in the DHCP log:

1. Select **Network Configuration** > **LAN Setup** from the main/submenu, and then click the LAN Setup tab.

   The LAN Setup screen displays.

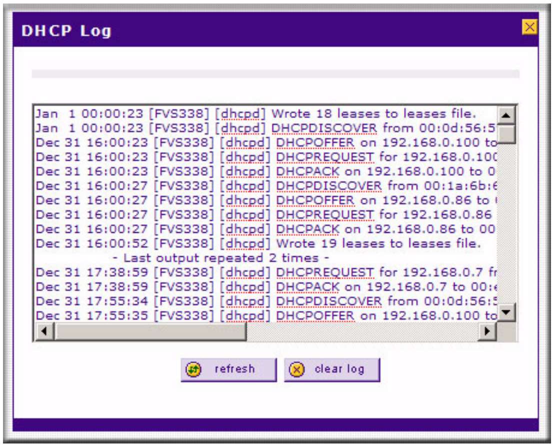


IP Address: 192 .168 .1 .1

Subnet Mask: 255 .255 .255 .0

Figure 11-6OK

2. Click the **DHCP Log** link to the right of the tabs. The **DHCP Log** appears in a popup window.



```
Jan  1 00:00:23 [FVS338] [dhcpd] Wrote 18 leases to leases file.
Jan  1 00:00:23 [FVS338] [dhcpd] DHCPDISCOVER from 00:0d:56:5
Dec 31 16:00:23 [FVS338] [dhcpd] DHCPOFFER on 192.168.0.100 to
Dec 31 16:00:23 [FVS338] [dhcpd] DHCPREQUEST for 192.168.0.10
Dec 31 16:00:23 [FVS338] [dhcpd] DHCPACK on 192.168.0.100 to 0
Dec 31 16:00:27 [FVS338] [dhcpd] DHCPDISCOVER from 00:1a:6b:
Dec 31 16:00:27 [FVS338] [dhcpd] DHCPOFFER on 192.168.0.86 to
Dec 31 16:00:27 [FVS338] [dhcpd] DHCPREQUEST for 192.168.0.86
Dec 31 16:00:27 [FVS338] [dhcpd] DHCPACK on 192.168.0.86 to 00
Dec 31 16:00:52 [FVS338] [dhcpd] Wrote 19 leases to leases file.
              - Last output repeated 2 times -
Dec 31 17:38:59 [FVS338] [dhcpd] DHCPREQUEST for 192.168.0.7 fr
Dec 31 17:38:59 [FVS338] [dhcpd] DHCPACK on 192.168.0.7 to 00:
Dec 31 17:55:34 [FVS338] [dhcpd] DHCPDISCOVER from 00:0d:56:
Dec 31 17:55:35 [FVS338] [dhcpd] DHCPOFFER on 192.168.0.100 to
```

Figure 11-7OK

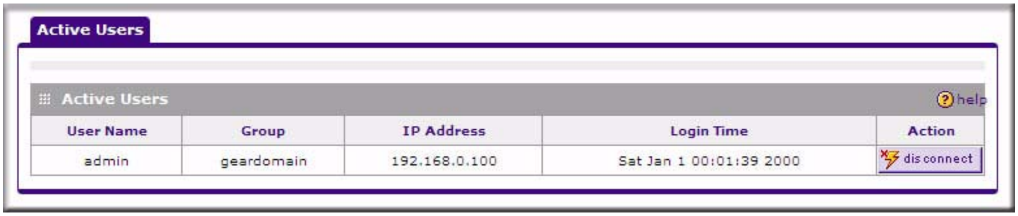
3. To view the most recent entries, click **refresh**. To delete all the existing log entries, click **clear log**.

Monitoring Active Users

The Active Users menu screen displays a list of administrators and SSL VPN users currently logged into the device.

To display the list of active users:

1. Select **Monitoring** > **Active Users** from the main/submenu. The Active Users screen is displayed.



User Name	Group	IP Address	Login Time	Action
admin	geardomain	192.168.0.100	Sat Jan 1 00:01:39 2000	disconnect

Figure 11-8 Need new screenshot

The active user’s username, group, and IP address are listed in the table with a timestamp indicating the time and date that the user logged in.

2. You can disconnect an active user by clicking **Disconnect** to the right of the user’s list entry.

Viewing Port Triggering Status

To view the status of Port Triggering:

1. Select **Security** > **Port Triggering** from the main/submenu.

   The Port Triggering screen displays.

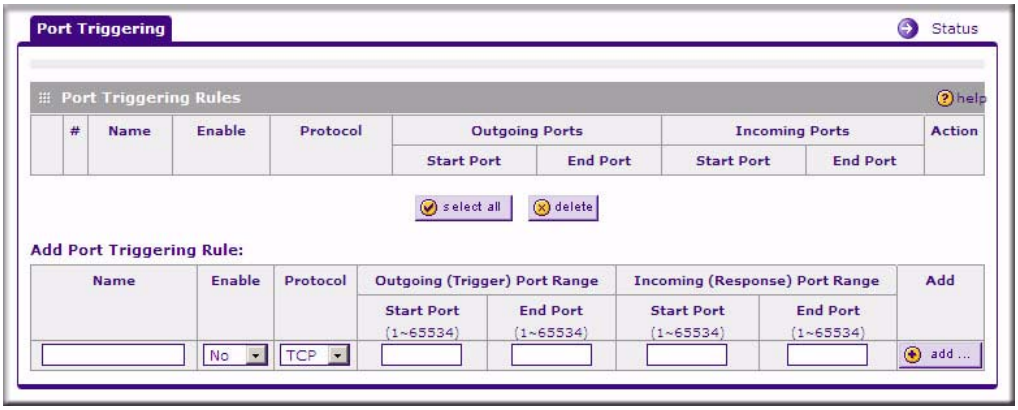


Figure 11-9OK

2. When the **Port Triggering** screen is displayed, click the **Status** link to the right of the tab to display the **Port Triggering Status**.

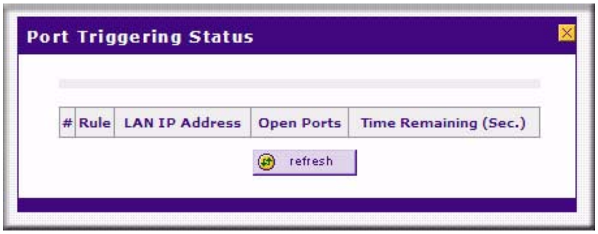


Figure 11-10OK

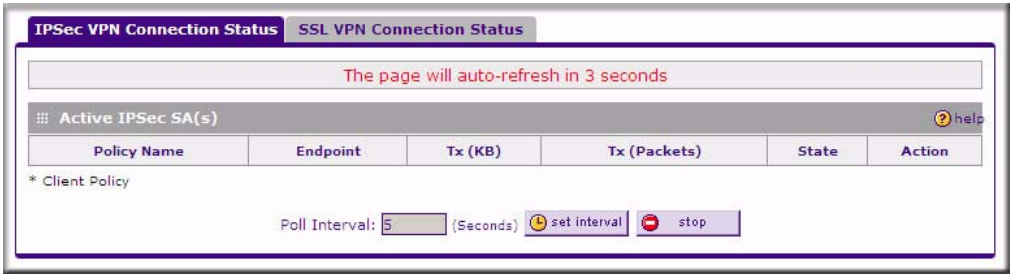
The status window displays the following information:

Item	Description
Rule	The name of the port triggering rule associated with this entry.
LAN IP Address	The IP address of the PC currently using this rule.
Open Ports	The Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above.
Time Remaining	The time remaining before this rule is released and made available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Monitoring VPN Tunnel Connection Status

To review the status of current VPN tunnels:

1. Select **VPN > Connection Status** from the main/submenu, and then select the IPsec VPN Connection Status tab. The IPsec Connection Status screen displays.



The page will auto-refresh in 3 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action

* Client Policy

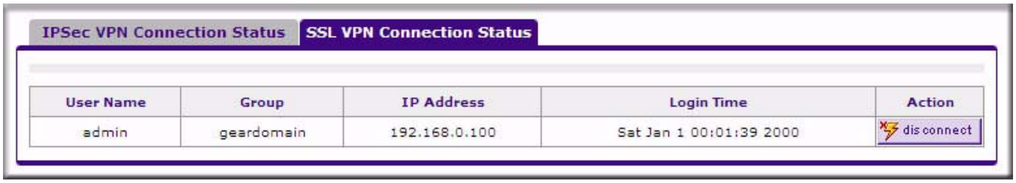
Poll Interval: 5 (Seconds)

Figure 11-11OK

The Active IPsec SAs table lists each active connection with the following information.

Item	Description
Policy Name	The name of the VPN policy associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data transmitted over this SA.
Tx (Packets)	The number of IP packets transmitted over this SA.
State	The current status of the SA. Phase 1 is Authentication phase and Phase 2 is Key Exchange phase.
Action	Use this button to terminate/build the SA (connection) if required.

2. Select the **SSL VPN Connection Status** tab and the SLL VPN Connection Status screen displays.



User Name	Group	IP Address	Login Time	Action
admin	geardomain	192.168.0.100	Sat Jan 1 00:01:39 2000	dis connect

Figure 11-12 Need new screenshot

The active SSL VPN user's username, group, and IP address are listed in the table with a timestamp indicating the time and date that the user connected.

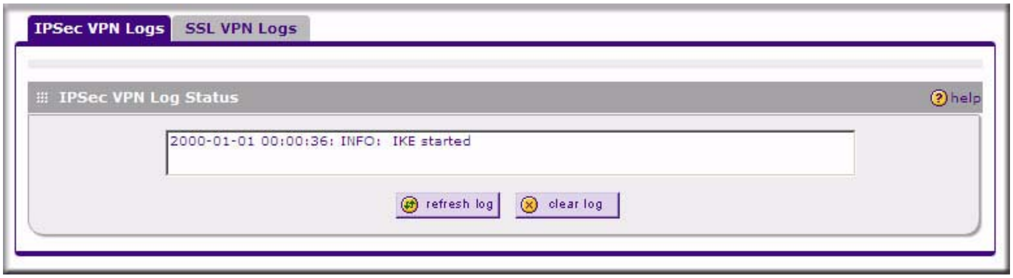
3. You can disconnect an active SSL VPN user by clicking **Disconnect** to the right of the user's list entry.

Reviewing the VPN Logs

The **VPN Logs** screen gives log details for recent VPN activity.

1. Select **Monitoring** > **VPN Logs** from the main/submenu, and select the IPsec VPN Logs tab.

   The IPsec VPN Logs screen displays.



```
2000-01-01 00:00:36: INFO:  IKE started
```

Figure 11-13 Need new screenshot

2. To view the most recent entries, click **refresh log**.
3. To delete all the existing log entries, click **clear log**.
4. Select the **SSL VPN Logs** tab to view SSL VPN log details.

Chapter 12
Troubleshooting

This chapter provides troubleshooting tips and information for your ProSafe Wireless-N VPN Firewall. After each problem description, instructions are provided to help you diagnose and solve the problem.

This chapter contains the following sections:

Basic Functions

After you turn on power to the VPN firewall, the following sequence of events should occur:

1. When power is first applied, verify the PWR LED is on.

2. After approximately two minutes, verify:

   a. The TEST LED is not lit.

   b. The LAN port LINK/ACT LEDs are lit for any local ports connected.

   c. The WAN port LINK/ACT LEDs are lit on the WAN port.

   If a port's LINK/ACT LED is lit, a link has been established to the connected device. If a LAN port is connected to a 1000 Mbps device, verify the port's SPEED LED is green. If the port is 100 Mbps, the LED will be amber. If the port is 10 Mbps, the LED will be off.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your VPN firewall is turned on:

- Verify the power adapter cord is properly connected to your VPN firewall and the power adapter is properly connected to a functioning power outlet.
- Verify you are using the 12VDC, 1.5A power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

LEDs Never Turn Off

When the firewall is turned on, the LEDs turns on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the firewall.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the firewall recovers.
- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 12-7.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Verify the Ethernet cable connections are secure at the firewall and at the hub or workstation.
- Verify the power is turned on to the connected workstation.
- Ensure you are using the correct cable:

  When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the firewall as described in the previous section.
- Ensure your PC’s IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC’s address should be in the range of 192.168.1.2 to 192.168.1.254.

> **Note:** If your PC’s IP address is shown as 169.254.x.x: Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.

- If your firewall’s IP address has been changed and you don’t know the current IP address, clear the firewall’s configuration to factory defaults. This will set the firewall’s IP address to 192.168.1.1. This procedure is explained in “Restoring the Default Configuration and Password” on page 12-7.

> **Tip:** If you don’t want to revert to the factory default settings and lose your configuration settings, you can reboot the firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the firewall’s LAN interface address.

- Ensure you are using the SSL *https://address* login rather than *http://address*.
- Ensure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Ensure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Verify CAPS LOCK is off when entering this information.

If the firewall does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your firewall is unable to access the Internet, you should first determine whether the firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your firewall must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and navigate to an external site such as www.netgear.com
2. Access the Main Menu of the firewall’s configuration at https://192.168.1.1
3. Under the Monitoring menu, click Router Status.
4. Check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your firewall is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your firewall.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem’s LEDs indicate that it has reacquired sync with the ISP, reapply power to your firewall.

If your firewall is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your PC's host name.
  Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to the Internet, and may check for your PC’s MAC address. In this case:
  – Inform your ISP that you have bought a new network device, and ask them to use the firewall’s MAC address; or

- – Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring the Internet Connection" on page 2-7.

If your firewall can obtain an IP address, but your PC is unable to load any Web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. You may configure your PC manually with DNS addresses, as explained in your operating system documentation.
- Your PC may not have the firewall configured as its TCP/IP gateway.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the Ping utility in your PC or workstation.

Testing the LAN Path to Your VPN Firewall

You can ping the firewall from your PC to verify that the LAN path to your firewall is set up correctly.

To ping the firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click **Start** and choose **Run**.
2. In the field provided, type "ping" followed by the IP address of the firewall; for example:

   ```
   ping 192.168.1.1
   ```
3. Click **OK.** A message, similar to the following, should display:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you will see this message:

   ```
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you will see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On" on page 12-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

`PING -n 10` <***IP address***>

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Verify your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel.
- Verify the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Verify your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring the Internet Connection" on page 2-7.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the VPN firewall's administration password to **password** and the IP address to **192.168.1.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the VPN firewall (see "Settings Backup and Firmware Upgrade" on page 9-13).
- Use the reset button (Factory Defaults) on the front panel of the VPN firewall. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the reset button on the rear panel of the VPN firewall.

To restore the factory defaults:

1. Press and hold the Factory Defaults (reset button) until the Test LED turns on and begins to blink (about 10 seconds).

   Use a slender pointed object, such as an ink pen or paper clip, to press and hold the reset button (Factory Defaults).

2. Release the reset button (Factory Defaults) and wait for the VPN firewall to reboot.

Problems with Date and Time

The Administration > Time Zone menu displays the current date and time of day. The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The VPN firewall has not yet successfully reached a Network Time Server. Verify your Internet access settings are configured correctly. If you have just completed configuring the VPN firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The VPN firewall does not automatically sense Daylight Savings Time. Check the Time Zone menu, and check or uncheck the box marked "Adjust for Daylight Savings Time".

Diagnostics Functions

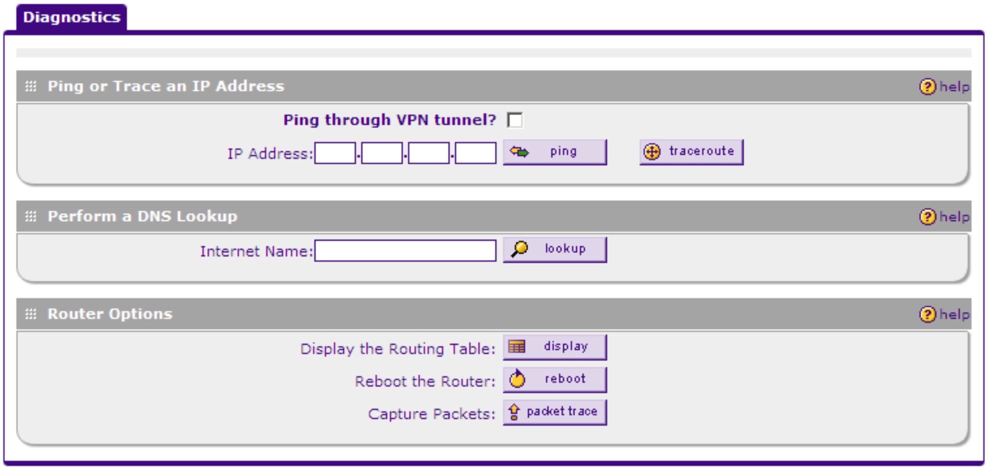
You can perform diagnostics such as pinging an IP address, performing a DNS lookup, displaying the routing table, rebooting the VPN firewall, and capturing packets.

1. Select **Monitoring** > **Diagnostics** from the main/submenu.

   The Diagnostics screen displays.

2. View the selections available in the Diagnostic screen and browse the descriptions listed in Table 12-1., "Diagnostics".

➡	**Note:** For normal operation, diagnostics are not required.



Diagnostics

Ping or Trace an IP Address

Ping through VPN tunnel? □

IP Address: [ ].[ ].[ ].[ ] ping traceroute

Perform a DNS Lookup

Internet Name: [ ] lookup

Router Options

Display the Routing Table: display

Reboot the Router: reboot

Capture Packets: packet trace

Figure 12-1

Table 12-1. Diagnostics

Item	Description
Ping or trace an IP address	Ping – Used to send a ping packet request to a specified IP address—most often, to test a connection. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen. If the specified address is intended to be reached through a VPN tunnel, check **Ping through VPN tunnel**.
	Traceroute – Lists all routers between the source (this device) and the destination IP address. The traceroute results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen.
Perform a DNS lookup	A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can request a DNS lookup to find the IP address.
Display the routing table	This operation will display the internal routing table, which can be used by Technical Support to diagnose routing problems.
Reboot the firewall	Used to perform a remote reboot (restart). You can use this if the firewall seems to have become unstable or is not operating normally.
	Note: Rebooting will break any existing connections either to the firewall (such as your management session) or through the firewall (for example, LAN users accessing the Internet). However, connections to the Internet will automatically be re-established when possible.
Packet trace	Packet Trace selects the interface and starts the packet capture on that interface.

Appendix A
Default Settings and Technical Specifications

You can use the reset button located on the rear panel to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, press and hold the reset button for approximately 10 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. router Default Configuration Settings

Feature		Default Behavior
Router Login		
	User Login URL	https://192.168.1.1
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Internet Connection		
	WAN MAC Address	Use Default address
	WAN MTU Size	1500
	Port Speed	AutoSense
Local Network (LAN)		
	Lan IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	RIP Direction	None
	RIP Version	Disabled
	RIP Authentication	Disabled
	DHCP Server	Enabled
	DHCP Starting IP Address	192.168.1.2
	DHCP Ending IP Address	192.168.1.100
Management		

Table A-1. router Default Configuration Settings (continued)

Feature		Default Behavior
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote Management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Denied
	Outbound (communications from the LAN to the Internet)	Allowed (all)
	Source MAC filtering	Disabled
	Stealth Mode	Enabled

Technical specifications for the ProSafe Wireless-N Security Router are listed in the following table.

Table A-2. router Technical Specifications

Feature		Specifications
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
Physical Specifications		
	Dimensions:	1.7 x 10 x 7.2 in.
	Weight:	2 kg (4.5 lb)

Table A-2. router Technical Specifications (continued)

Feature		Specifications
Environmental Specifications		
	Operating temperature:	0° to 40° C (32º to 104º F)
	Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions		
	Meets requirements of:	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN:	10BASE-T or 100BASE-Tx 1000BASE-T, RJ-45
	WAN:	10BASE-T or 100BASE-Tx 1000BASE-T, RJ-45

Table A-3. SSL VPN Technical Specifications

Parameter	Specification
Network Management	Web-based configuration and status monitoring
Concurrent Users Supported	10 tunnels
Encryption	DES, 3DES, AES, MD5, SHA-1
Authentication	Local User database, RADIUS, LDAP, MS Active Directory
Certificates supported	X.509, CRL
Electromagnetic Compliance	FCC Part 15 Class B, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications:	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access:	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN):	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index