Chapter 6
Virtual Private Networking
Using SSL Connections

The FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a pre-installed VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the FVS336G can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information is completed, the server and client can establish an encrypted connection. With support for 10 concurrent sessions, users can easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:
• “Understanding the Portal Options”
• “Planning for SSL VPN”
• “Creating the Portal Layout”
• “Configuring Domains, Groups, and Users”
• “Configuring Applications for Port Forwarding”
• “Configuring the SSL VPN Client”
• “Using Network Resource Objects to Simplify Policies”
• “Configuring User, Group, and Global Policies”

Understanding the Portal Options

The FVS336G’s SSL VPN portal can provide two levels of SSL service to the remote user:
• VPN Tunnel

The FVS336G can provide the full network connectivity of a VPN tunnel using the remote user’s browser in the place of a traditional IPsec VPN client. The SSL capability of the user’s browser provides authentication and encryption, establishing a secure connection to the VPN
firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote PC that will allow the remote user to virtually join the corporate network. The SSL VPN Client provides a PPP (point-to-point) connection between the client and the VPN firewall, and a virtual network interface is created on the user’s PC. The VPN firewall will assign the PC an IP address and DNS server IP addresses, allowing the remote PC to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions configured by the administrator.

• Port Forwarding

Like VPN Tunnel, Port Forwarding is a web-based client that installs transparently and then creates a virtual, encrypted tunnel to the remote network. However, Port Forwarding differs from VPN Tunnel in several ways. For example, Port Forwarding:

– Only supports TCP connections, not UDP or other IP protocols.
– Detects and reroutes individual data streams on the user’s PC to the Port Forwarding connection rather than opening up a full tunnel to the corporate network.
– Offers more fine grained management than VPN Tunnel. The administrator defines individual applications and resources that will be available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on the configuration by the administrator.

Planning for SSL VPN

To set up and activate SSL VPN connections, you will perform these basic steps in this order:

1. Edit the existing SSL Portal or create a new one.

   When remote users log in to the SSL VPN firewall, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create one or more authentication domains for authentication of SSL VPN users.

   When remote users log in to the SSL VPN firewall, they must specify a domain to which their login account belongs. The domain determines the authentication method to be used and the portal layout that will be presented, which in turn determines the network resources to which they will have access. Because you must assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

3. Create one or more groups for your SSL VPN users.
When you define the SSL VPN policies that determine network resource access for your SSL
VPN users, you can define global policies, group policies, or individual policies. Because you
must assign an authentication domain when creating a group, the group is created after you
have created the domain.

4. Create one or more SSL VPN user accounts.

Because you must assign a group when creating a SSL VPN user account, the user account is
created after you have created the group.

5. For port forwarding, declare the servers and services.

Create a list of servers and services that can be made available through user, group, or global
policies. You can also associate fully qualified domain names with these servers. The VPN
firewall will resolve the names to the servers using the list you have created.

6. For VPN tunnel service, configure the virtual network adapter.

In the VPN tunnel option, the VPN firewall creates a virtual network adapter on the remote PC
that will function as if it were on the local network. Configure the portal’s SSL VPN Client to
define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses.
Declare static routes or grant full access to the local network, subject to additional policies.

7. For simplifying policies, define network resource objects.

Network resource objects are groups of IP addresses, IP address ranges, and services. By
defining resource objects, you can more quickly create and configure network policies.

8. Configure the policies.

Policies determine access to network resources and addresses for individual users, groups, or
everyone.

Creating the Portal Layout

The SSL VPN Portal Layouts menu allows you to create a custom page that remote users will see
when they log into the portal. Because the page is completely customizable, it provides an ideal
way to communicate remote access instructions, support information, technical contact info, or
VPN-related news updates to remote users. The page is also well-suited as a starting page for
restricted users; if mobile users or business partners are only permitted to access a few resources,
the page you create will present only the resources relevant to these users.
Portal Layouts are applied by selecting from available portal layouts in the configuration of a Domain. When you have completed your Portal Layout, you can apply the Portal Layout to one or more authentication domains (see XREF to apply a Portal Layout to a Domain). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button adjacent to the portal layout name.

Note: The default portal address is \texttt{https://<IP\_Address>/portal/SSL-VPN}. The domain \texttt{geardomain} is attached to the SSL-VPN portal.

The VPN firewall administrator may define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the SSL VPN firewall by clicking the default button in the Action column of the List of Layouts, to the right of the desired portal layout.

To create a New Portal Layout:

1. Select VPN > SSL VPN from the main menu, and then select the Portal Layouts tab. The Portal Layouts screen will display.

2. Click Add. The Add Portal Layout screen is displayed.
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.

   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

![Login Screen](image)

**Figure 6-3**

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:

```html
<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.

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
</table>

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 Successful” 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 VPN 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 7-1.

### 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 VPN 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 menu, and then select the Port Forwarding tab. The Port Forwarding screen will display.

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>
<thead>
<tr>
<th>TCP Application</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Data (usually not needed)</td>
<td>20</td>
</tr>
<tr>
<td>FTP Control Protocol</td>
<td>21</td>
</tr>
<tr>
<td>SSH</td>
<td>22&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Telnet</td>
<td>23&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>SMTP (send mail)</td>
<td>25</td>
</tr>
</tbody>
</table>

Figure 6-4

Table 6-1. Port Forwarding Applications/TCP Port Numbers
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 6-4.
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.

### Table 6-1. Port Forwarding Applications/TCP Port Numbers (continued)

<table>
<thead>
<tr>
<th>TCP Application</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP (web)</td>
<td>80</td>
</tr>
<tr>
<td>POP3 (receive mail)</td>
<td>110</td>
</tr>
<tr>
<td>NTP (network time protocol)</td>
<td>123</td>
</tr>
<tr>
<td>Citrix</td>
<td>1494</td>
</tr>
<tr>
<td>Terminal Services</td>
<td>3389</td>
</tr>
<tr>
<td>VNC (virtual network computing)</td>
<td>5900 or 5800</td>
</tr>
</tbody>
</table>

a. Users can specify the port number together with the host name or IP address.
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 FVS336G 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 VPN 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 VPN 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 menu, and then select the SSL VPN Client tab. The SSL VPN Client screen will display.

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 Successful” message appears at the top of the tab.
VPN tunnel clients are now able to connect to the VPN 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 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 if 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 6-5.
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 Successful” 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 VPN firewall.

Restart the VPN 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 adjacent to the out-of-date route entry.
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 men, and then select the Resources tab. The Resources screen will display.

2. In the **Add New Resource** section, type the (qualified) resource name in the **Resource Name** field.

![Figure 6-6](image-url)
3. In the Service pull-down menu, select the type of service to which the resource will apply: either VPN Tunnel or Port Forwarding.

4. Click Add.

The “Operation Successful” 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.

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 6-7.

Figure 6-7
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 VPN 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 VPN 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 menu, and then select the Policies tab. The Policies screen will display.

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.
Adding a Policy

To add a policy, follow these steps:

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

![Policy Screen](image)

**Figure 6-9**

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.

   ![Query Options](image)

   **Note:** You should have already created the needed groups or users as described in “Adding Authentication Domains, Groups, and Users” on page 7-1.

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](image1)

Figure 6-10

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 6-13.

• 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](image2)

Figure 6-11

• 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.
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 8-10.