Chapter 9
Monitoring System Performance

This chapter describes the full set of system monitoring features of your ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN. 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 ports, LAN ports, and VPN tunnels.

This chapter contains the following sections:

- “Enabling the Traffic Meter”
- “Activating Notification of Events and Alerts”
- “Viewing Firewall Logs”
- “Viewing Router Configuration and System Status”
- “Monitoring the Status of WAN Ports”
- “Monitoring Attached Devices”
- “Reviewing the DHCP Log”
- “Monitoring Active Users”
- “Viewing Port Triggering Status”
- “Monitoring VPN Tunnel Connection Status”
- “Reviewing the VPN Logs”

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 one or both WAN ports.

To monitor traffic limits on each of the WAN ports:

1. Select Monitoring > Traffic Meter from the main menu, and then the WAN1 Traffic Meter tab. The WAN1 Traffic Meter screen will display.
Enable the traffic meter by clicking the Yes radio box under Do you want to enable Traffic Metering on WAN1? The traffic meter will record the volume of Internet traffic passing through the WAN1. 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.
• **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 a 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 4-25).

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.

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.

7. Click the WAN2 Traffic Meter tab and repeat this process to configure the Traffic Meter for the WAN2 port.

---

**Note:** Both incoming and outgoing traffic are included in the limit.
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 VPN firewall 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 4-19), 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 > Firewall Logs & E-mail from the main menu. 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.
Figure 9-2
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.

<table>
<thead>
<tr>
<th>Numerical Code</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency: System is unusable</td>
</tr>
<tr>
<td>1</td>
<td>Alert: Action must be taken immediately</td>
</tr>
<tr>
<td>2</td>
<td>Critical: Critical conditions</td>
</tr>
<tr>
<td>3</td>
<td>Error: Error conditions</td>
</tr>
<tr>
<td>4</td>
<td>Warning: Warning conditions</td>
</tr>
<tr>
<td>5</td>
<td>Notice: Normal but significant conditions</td>
</tr>
<tr>
<td>6</td>
<td>Informational: Informational messages</td>
</tr>
<tr>
<td>7</td>
<td>Debug: Debug level messages</td>
</tr>
</tbody>
</table>

**Viewing Firewall Logs**

To view the Firewall logs:

1. Select Monitoring > Firewall Logs & E-mail from the main menu. 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 9-1.

**Table 9-1. Firewall Logs Field Descriptions**

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

**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 > Router Status from the main menu. The Router Status screen is displayed.
The following information is displayed:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>This is the Account Name that you entered in the Basic Settings page.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>This is the current software the router is using. This will change if you upgrade your router.</td>
</tr>
<tr>
<td>LAN Port</td>
<td>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.</td>
</tr>
</tbody>
</table>
Monitoring the Status of WAN Ports

You can monitor the status of both of the WAN connections, the Dynamic DNS Server connections, and the DHCP Server connections. To monitor the status of the WAN ports:

1. Select Network > WAN Settings from the main menu. The WAN1 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 WAN1 port.
3. To get a status report on the WAN2 port, click the WAN2 ISP Settings tab, and then click the WAN Status link.
Monitoring Attached Devices

The **LAN Groups** screen contains a table of all IP devices that the VPN firewall has discovered on the local network.

To view the LAN Groups screen:

1. Select Network > LAN Setup from the main menu, and then select the LAN Groups tab. The LAN Groups screen will display.

2. 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 VPN 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 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.
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 9-2. Known PCs and Devices options

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the PC. The MAC address is a low-level network identifier which is fixed at manufacture.</td>
</tr>
<tr>
<td>Group</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note:** If the VPN firewall is rebooted, the table data is lost until the VPN firewall rediscovers the devices.
Reviewing the DHCP Log

To review the most recent entries in the DHCP log:

1. Select Network > LAN Setup from the main menu, and then click the LAN Setup tab. The LAN Setup screen will display.

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

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 menu. The Active Users screen is displayed.

![Active Users Table]

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

The status window displays the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description___________________________________________________________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>The name of the port triggering rule associated with this entry.</td>
</tr>
<tr>
<td>LAN IP Address</td>
<td>The IP address of the PC currently using this rule.</td>
</tr>
<tr>
<td>Open Ports</td>
<td>The Incoming ports which are associated with this rule. Incoming traffic using one of these ports will be sent to the IP address above.</td>
</tr>
<tr>
<td>Time Remaining</td>
<td>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.</td>
</tr>
</tbody>
</table>
Monitoring VPN Tunnel Connection Status

To review the status of current VPN tunnels:

1. Select VPN > Connection Status from the main menu, and then select the IPsec VPN Connection Status tab. The **IPsec Connection Status** screen is displayed.

![IPsec Connection Status](image)

**Figure 9-11**

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

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

2. Select the SSL VPN Connection Status tab. The SSL VPN Connection Status screen will display

![SSL VPN Connection Status](image)

**Figure 9-12**
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 menu, and select the IPsec VPN Logs tab. The IPsec VPN Logs screen will display.

![IPSec VPN Logs](image)

**Figure 9-13**

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

3. Select the SSL VPN Logs tab to view SSL VPN log details.