Clavister SG4500 Series Getting Started Guide

Clavister SG4500 Series
Getting Started Guide

Published 2011-03-24

Table of Contents

List of Figures

Preface

Target Audience

The target audience for this guide is the administrator who has taken delivery of a packaged Clavister SG4500 Series appliance and is setting it up for the first time. The guide takes the user from unpacking and installation of the device through to power-up, including network connections and initial CorePlus configuration.

Text Structure

The text is divided into chapters and subsections. Numbered subsections are shown in the table of contents at the beginning of the document.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:

Note

This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasised or something that is not obvious or explicitly stated in the preceding text.

Tip

This indicates a piece of non-critical information that is useful to know in certain situations but is not essential reading.

Caution

This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important

This is an essential point that the reader should read and understand.

Warning

This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Text links

Where a "See section" link is provided in the main text, this can be clicked on to take the reader directly to that reference. For example, see *Section 3.6, "Troubleshooting Setup"*.

Web links

Web links included in the document are clickable. For example, *http://www.clavister.com*.

Trademarks

Certain names in this publication are the trademarks of their respective owners.

CorePlus is the trademark of Clavister AB.

Windows, *Windows XP*, *Windows Vista* and *Windows 7* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple and *Mac* are trademarks of Apple Inc. registered in the United States and/or other countries.

Chapter 1: Product Overview

- Unpacking the Product, page 7

- Interfaces and Ports, page 9

- The Keypad and Display, page 11

1.1. Unpacking the Product

This section details the unpacking of the SG4500 Series appliance. Open the packaging box used for shipping and carefully unpack the contents. The delivered product packaging should contain the following:

1. The Clavister SG4500 Series appliance.

2. A mounting kit for 19 inch racks.

3. An Ethernet cable.

4. A RS-232 null-modem cable.

5. A Power cord.

6. A CD-ROM containing:

    - Clavister software.

    - Product documentation in PDF format.

7. A printed guide for getting started.

Figure 1.1. An Unpacked Clavister SG4500 Series Appliance

Note: Missing items

If any items are missing from your package, please contact your reseller or distributor. All documentation can be freely downloaded in PDF format from the Clavister website.

End of Life Treatment

The SG4500 Series appliance is marked with the European *Waste Electrical and Electronic Equipment* (WEEE) directive symbol which is shown below.

The product, and any of its parts, should not be discarded of by means of regular refuse disposal. At end-of-life, the product and parts should be given to an appropriate service that deals with the removal of such specialist materials.

This also applies to any of the product's field-removable components.

1.2. Interfaces and Ports

This section is an overview of the SG4500 Series product's external design.

Note: Usage of the terms "interface" and "port"

*The terms **Ethernet interface** and **Ethernet port** are often used interchangeably. In this document, **interface** is used for Ethernet connections and **port** is used for non-Ethernet connections.*

Figure 1.2. Front View of the Clavister SG4500 Series.

The SG4500 Series features a number of connection ports. On the far right is the RS-232 console port and an LED display screen. To the left of these are a set of 10 Ethernet interfaces.

Each Ethernet interface has equal operational capacity and corresponds to a logical interface in the CorePlus software configuration. Going from left to right, the Ethernet interfaces are:

*   A set of 4 interfaces consisting of:

    i.   **2 x Small Form Pluggable Plus (SFP+) Ethernet interfaces** with logical CorePlus interface names **xsfp1** and **xsfp2**. These are for 10 Gigabit Ethernet links only.

    ii. **2 x Small Form Pluggable (SFP) Ethernet interfaces** with logical CorePlus interface names **sfp1** and **sfp2**. These are for 1 Gigabit Ethernet links only.
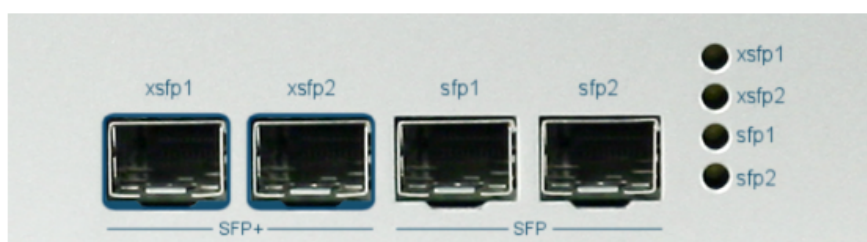
On the right of these interfaces is a vertical line of 4 LEDs which show the status for the interfaces. These LEDs are illuminated orange when a link is established.

*   **6 x RJ45 Gigabit Ethernet interfaces** with logical interface names **ge1** to **ge6**. These connections are capable of link speed auto-negotiation and can therefore operate with 10Base-T, 100Base-Tx, or 1000Base-T.
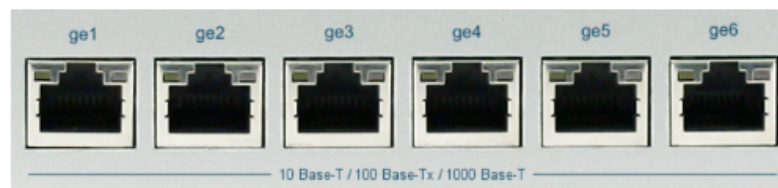
All **ge** interfaces support *Automatic MDI-X* and do not require a crossover cable for direct connection from another computer.

Status lights are located at the top-right and top-left of the **ge** interfaces. The top-left light flashes green to indicate data traffic. The top-right light shows the link speed and has the following states:

- Not lit (dark) if the link is 10 Mb.

- Green if the link is 100 Mb.

- Yellow if the link is 1 Gb.

USB Ports

Next to the RS-232 port are 2 USB ports. These ports are not used with the current version of CorePlus. The ports are intended for use with features planned for future CorePlus versions and are provided so that no hardware upgrade will be required in order to make use of those features after a software upgrade.

1.3. The Keypad and Display

The SG4500 Series features a keypad and display on the right hand front side of the hardware consisting of an LED display and 4 navigation buttons. The buttons are used to either move forwards or backwards through a sequential list of parameters which are always shown on the display while the power is on.

Pressing either the **Right** or **Upper** button will go forward in the display sequence. Pressing either the **Left** or **Lower** button will go backwards in the sequence. When the end of the display sequence is reached, the display cycles back to the beginning.

Figure 1.3. The SG4500 Series Keypad and Display

The sequence of information that is shown in the LED display is as follows:

- **Hardware Model information.**

  The model of the hardware is shown.

- **Status Information**

  This displays the message *Running* to indicate normal operation. If CorePlus is in 2 hour demonstration mode then this is indicated along with how much time is left before timeout. If CorePlus is in lockdown mode then this is shown.

- **CPU and Connections**

  This shows the CPU load and the total number of current state engine connections.

- **Data Throughput Information**

  The data throughput of the Clavister Security Gateway in bits per second and packets per second is shown. This is the total volume of all data traffic forwarded through the security gateway over a one second interval.

  These values are for raw data and include any overhead incurred with protocols such as IPsec. The actual throughput of, for example, unencrypted data flowing inside VPN tunnels, may be marginally less.

- **High Availability**

  This shows the HA mode (*master* or *slave*) and the HA status (*active* or *passive*).

  If the SG4500 Series is not part of a high availability cluster, this information is skipped.

- **Time Information**

  The date and time currently set in the hardware system clock is shown. If this is incorrect, it should be corrected through one of the administration interfaces.

- **Memory Information**

  This shows the current uptime (time since last restart), the total hardware RAM memory available to CorePlus and the current memory usage.

- **Anti-Virus Information**

  This shows the current signature count in the Anti-Virus database and the time of the last database update.

  If the CorePlus Anti-Virus subsystem is not activated, this information is skipped.

- **IDP Information**

  This shows the current signature count in the *Intrusion Detection and Prevention* (IDP) database and the time of the last database update.

  If the CorePlus IDP subsystem is not activated, this information is skipped.

- **Interface Information**

  This consists of multiple display sets of information, one for each physical Ethernet interface present. The information displayed for each interface is:

  i.   The logical CorePlus interface name.

  ii.   The current linkspeed.

  iii. If the link is full-duplex (*FD*) or half-duplex (*HD*). This is not shown if the linkspeed is Gigabit since it will always be full-duplex.

  iv.   The IP address assigned to the interface.

- **Hardware Monitor Information**

  This information consists of multiple sets of information, one for each sensor. Sensor information shows operating temperatures and fan speeds.

  Hardware monitoring must be enabled through one of the administration interfaces for this to be shown otherwise this information is skipped.

- **CorePlus Version**

  This shows the version of CorePlus which is currently running.

After the CorePlus version is displayed, going forward will cycle back to the first information displayed in the sequence which is the hardware model.

Chapter 2: Installation

2.1. Installation Guidelines

Follow these guidelines when installing your Clavister SG4500 Series appliance:

- **Safety**

  Take notice of the safety guidelines laid out in *Chapter 6, Safety Precautions*. These are specified in multiple languages.

- **Power**

  Make sure that the power source circuits are properly grounded and then use the power cord supplied with the appliance to connect it to the power source.

- **Using Other Power Cords**

  If your installation requires a different power cord than the one supplied with the appliance, be sure to use a cord displaying the mark of the safety agency that defines the regulations for power cords in your country. Such marks are an assurance that the cord is safe.

- **Power Overload**

  Ensure that the appliance does not overload the power circuits, wiring and over-current protection.

  To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the appliance and compare the total with the rating limit for the circuit. The maximum ratings for the SG4500 Series are listed in *Appendix A, Specifications*. Rating figures can also be found written on individual SG4500 Series PSU modules.

- **Surge Protection**

A third party surge protection device should be considered and is strongly recommended as a means to prevent electrical surges reaching the appliance. This is discussed again in *Section 2.4, "Connecting Power"*.

- **Temperature**

  Do not install the appliance in an environment where the operating ambient temperature could exceed the specified operating range (see *Appendix A, Specifications*).

  The recommended operating temperature range is "room temperature". That is to say, the temperature most commonly found in a modern office and in which humans feel comfortable. This is usually considered to be between 20 and 25 degrees Celsius (68 to 77 degrees Fahrenheit). Special rooms for computer equipment may use a lower range.

- **Airflow**

  Make sure that airflow around the sides and back of the appliance is not restricted.

- **Dust**

  Do not expose the appliance to environments with elevated dust levels. This is particularly important for the operation of the fans, both general cooling fans and the cooling fan found in SG4500 Series power supplies. Elevated dust levels can significantly reduce the operating lifetime of fans.

Note

*Detailed information concerning power supply range, operating temperature range etc. can be found at the end of this publication in **Appendix A, Specifications**.*

Flat Surface Installation

The SG4500 Series can be mounted on any appropriate stable, flat, level surface that can safely support the weight of the appliance and its attached cables.

Caution: Leave space around the appliance

Please ensure there is adequate space around the appliance for ventilation and access to operating switches and cable connectors. No other objects should be placed on top of the appliance.

Rack Installation

A rack mounted Clavister Security Gateway can be installed in most standard 19 inch equipment racks. To do this, fasten the appliance with screws suitable for the kind of rack you are using. The following mounting guidelines should be followed:

- A rack or cabinet used for mounting should be adequately secured to prevent it from becoming unstable and/or falling over.

- Devices installed in a rack or cabinet should be mounted as low as possible, with the heaviest devices at the bottom and progressively lighter devices installed above.

- Rear brackets should be used to support appliances at the rear.

Important: Use rear brackets for rack mounting

It is strongly recommended that the rear brackets included with the SG4500 Series are fitted and used to support the appliance from the back when rack mounted.

2.2. Installing SFP/SFP+ Modules

Small Form Pluggable (SFP) and *Small Form Pluggable Plus* (SFP+) modules can be sourced from different manufacturers. Shown below is a typical unit. The SG4500 Series does not come as standard with these modules and they must be purchased separately.

Figure 2.1. A Typical SFP/SFP+ Module

Figure 2.2. An Example of an SFP 1000 Base TX Module

Installation of the different types of modules is usually done in a similar way. For example, with the module shown above, insertion into the sockets is done with the label facing upwards. The module slides into position by gently pressing it inwards.

Figure 2.3. Installing an SFP/SFP+ Module

17

Note: Installation images are generic

The SFP/SFP+ installation images used here are generic and do not feature the SG4500 Series. However, the installation principles are the same on all Clavister hardware models that provide SFP or SFP+ support.

Important: Cover unused SFP and SFP+ interfaces with dust caps

The SG4500 Series SFP and SFP+ interfaces are covered with dust caps when the product is unpacked. These prevent dust entering theinterfaceopenings.

It is strongly recommended that dust caps are always used to cover ports when there is no module inserted. Otherwise, dust can build up inside the opening and potentially cause a malfunction.

2.3. Console Port Connection

The *serial console port* is a physical RS-232 port on the SG4500 Series hardware.

This port allows direct management connection to the appliance, either from a separate computer running console emulation software or from a console terminal. Serial console access can then be used for both management of CorePlus with CLI commands or to enter the *boot menu* in order to access SG4500 Series firmware loader options.

Tip: Skip this section for now if the web interface is used

This section can be initially skipped if initial CorePlus setup is done with the CorePlus Web Interface since neither boot menu or CLI access will be needed.

Figure 2.4. The SG4500 Series RS-232 Console Port

Issuing CLI Commands

CLI commands can be issued via the RS-232 console port for both initial CorePlus setup as well as for ongoing system administration.

The RS-232 console port need not be used if setup is done through a web browser as described in *Section 3.2, "Web Interface and Wizard Setup"*. If the RS-232 port is used for setup, no password is initially needed and the CLI commands required are described in *Section 3.4, "CLI Setup"*.

Note: Setting a console password

A serial console password need not be set. If this is the case, anyone with physical access to the serial console has full administrator rights.

If the SG4500 Series is not placed in a secure area, it is therefore advisable to set the console password. This is done using the console **boot menu** *and more detail on this can be found in the* **CorePlus Administrators Guide**.

An alternative to using the console port for CLI access is to connect via a physical Ethernet interface and using a Secure Shell (SSH) client on the workstation to issue CLI commands.

Equipment Required for Console Connection

To use the console port, the following is needed:

• A terminal or a computer with a serial port and the ability to emulate a terminal (for instance, the *Hyper Terminal* software included with some Microsoft Windows distributions could be used).

- The terminal console should have the following settings:

  - 9600 bps.

  - No parity.

  - 8 bits.

  - 1 stop bit.

  - No flow control.

- An RS-232 cable with appropriate terminating connectors. The SG4500 Series package includes an RS-232 null-modem cable.

Connection Steps

To connect a terminal to the console port, follow these steps:

1. Check that the console connection settings are configured as described above.

2. Connect one of the connectors on the RS-232 cable supplied, directly to the console port on the SG4500 Series.

3. Connect the other end of the cable to a console terminal or to the serial connector of a computer running console emulation software.

2.4. Connecting Power

This section describes connecting power to the SG4500 Series. Only an AC power source is supported by the product.

> ### *Important*
>
> *Please read the advisory information concerning electrical safety in **Chapter 6, Safety Precautions**.*

With the SG4500 Series there are double, hot-swappable PSUs and no On/Off switch. Power becomes available to the whole appliance as soon as it is made available to any of the installed PSUs. The back of the SG4500 Series is shown below with the two PSUs visible on the far left.

Figure 2.5. Rear View of the SG4500 Series

CorePlus will boot-up as soon as power is available to the appliance.

Operating the SG4500 Series with a Single PSU

The dual PSUs on the SG4500 Series provide power supply redundancy in the case of a single PSU failure. However, the SG4500 Series can operate correctly with only one power supply fitted. If a second PSU is not fitted then the second PSU slot must be filled with a special *PSU Filler Module* component. The filler module is necessary to prevent the alarm sounding because the hardware will detect only one active PSU.

It does not matter which of the two SG4500 Series PSU slots is fitted with the PSU and which is fitted with the filler module. It should also be remembered that the CorePlus *hardware monitoring* feature will consider a missing PSU to be a malfunctioned PSU and any CorePlus *Hardware Monitoring* alarms should be adjusted accordingly.

Connecting AC Power

To connect power, follow these steps:

1. Plug one end of the power adapter's power cord into the power receptacle on the back panel of the SG4500 Series. For the SG4500 Series, there can be two hot-swappable power supplies so the supplied power cords should be used to connect the both PSUs if two are installed.

2. Plug the other end of the power cord into a grounded power outlet.

3. With the SG4500 Series, the system starts as soon as the PSUs are connected to a power source and the power is applied.

If 2 PSUs are installed and there is a delay between switching on power to the first and then the second, the alarm may sound momentarily. The alarm will switch off when the both supplies are fully operational.

4. The SG4500 Series will boot up and CorePlus will start. After a brief period of time, CorePlus will be running and the appliance will be ready for initial configuration from a management workstation using either the *Web Interface* or the *Command Line Interface* (CLI) as the management interface.

   Initial configuration is discussed in detail in *Section 3.1, "Management Workstation Connection"*.

Important: Protecting Against Power Surges

It is strongly recommended that the purchase and use of a separate surge protection unit from a third party is considered. This is to ensure that computer hardware is protected from damage by electrical power surges.

Surge protection is particularly important in locations where there is a heightened risk of lightning strikes or where power grid spikes are more common.

Any surge protection unit should be installed exactly according to the manufacturer's instructions since correct installation of such units is vital for them to be effective.

Chapter 3: CorePlus Configuration

3.1. Management Workstation Connection

CorePlus Starts after Power Up

It is assumed you have now unpacked, positioned and powered up the SG4500 Series unit. If not, you should refer to the earlier chapters in this manual before continuing.

Clavister's CorePlus network security operating system is preloaded on the hardware and will automatically boot up after power is supplied.

The Default Management Interface

After first time startup, CorePlus makes management access available on a predefined Ethernet interface and assigns the private IP address *192.168.1.1* to it.

For the SG4500 Series, the default management interface is the **ge1** interface.

Alternative CorePlus Setup Methods

Initial CorePlus software configuration can be done in one of the following ways:

• **Through a web browser.**

   A standard web browser running on a standalone computer (also referred to as the

management workstation) can be used to access the CorePlus *Web Interface*. This provides an intuitive graphical interface for CorePlus management. When this interface is accessed for the first time, a *setup wizard* runs automatically to guide a new user through key setup steps. The wizard can be closed if the administrator wishes to go directly to the Web Interface to perform setup manually.

The wizard is recommended for its simplification of initial setup and is described in detail in *Section 3.2, "Web Interface and Wizard Setup"*.

- **Through a terminal console using CLI commands.**

  The setup process can alternatively be performed using console CLI commands and this is described in *Section 3.4, "CLI Setup"*. The CLI allows step by step control of setup and should be used by administrators who fully understand both the CLI and setup process.

  CLI access can be remote, across a network to a physical interface using a similar connection to that used with the Web Interface. Alternatively, CLI access can be through a console connected directly to the local RS-232 port on the SG4500 Series hardware. Direct console connection is described in *Section 2.3, "Console Port Connection"*.

Network Connection Setup

For setup using the Web Interface via a web browser or the CLI via SSH, we must first connect an Ethernet interface on an external workstation computer to an Ethernet interface on the SG4500 Series, as illustrated below.
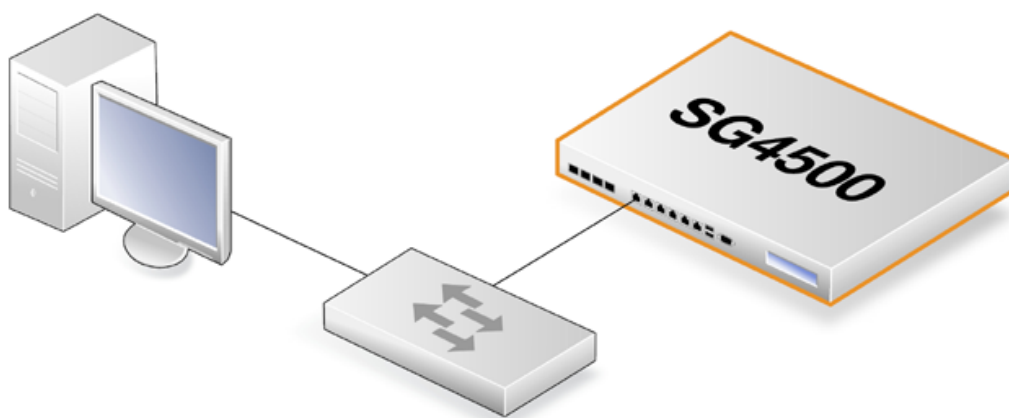
The default management Ethernet interface for the SG4500 Series is **ge1** and this should be connected to the same network as the management workstation (or a network accessible from the workstation via one or more switches). Typically the connection is made via a switch in the network, as shown in the illustration above, using regular Ethernet cables.

For connection to the public Internet, another interface should be connected to your ISP and this is referred to below and in the setup wizard as the *WAN* interface. In this guide, it is assumed that the physical **ge2** interface of the SG4500 Series is used for Internet connection although it could be any other unused interface.
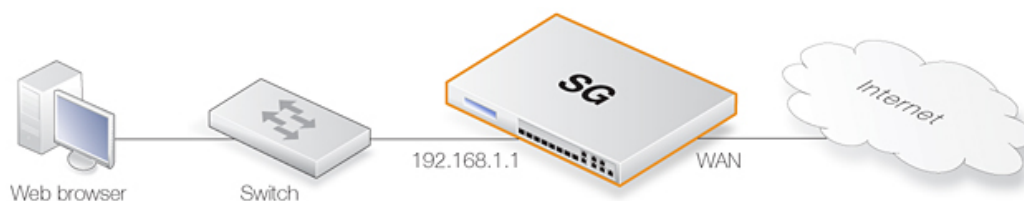
Using Crossover Cables

Connection to the management interface from the workstation can be done directly without a switch. This is usually done by using a crossover cable.

Note: A crossover cable is not necessary for Gigabit interfaces

*On the SG4500 Series, the **ge1** to **ge6** Ethernet ports support Automatic MDI-X and do not require a crossover cable. Direct connection with a regular cable is possible.*

Workstation Ethernet Interface Setup

Traffic will be able to flow between the designated workstation interface and the Clavister Security Gateway interface because they are on the same IP network. This means the workstation interface should be first assigned the following static IP addresses:

•   **IP address:** *192.168.1.30*

•   **Subnet mask:** *255.255.255.0*

•   **Default gateway:** *192.168.1.1*

Tip: Using another interface IP address

*The assigned IP address, **192.168.1.30**, could be another address from the **192.168.1.0/24** network as long as it is different from **192.168.1.1** which is the address used by CorePlus on its default management interface.*

To enter these settings on a Windows XP™ based PC, the following steps are needed:
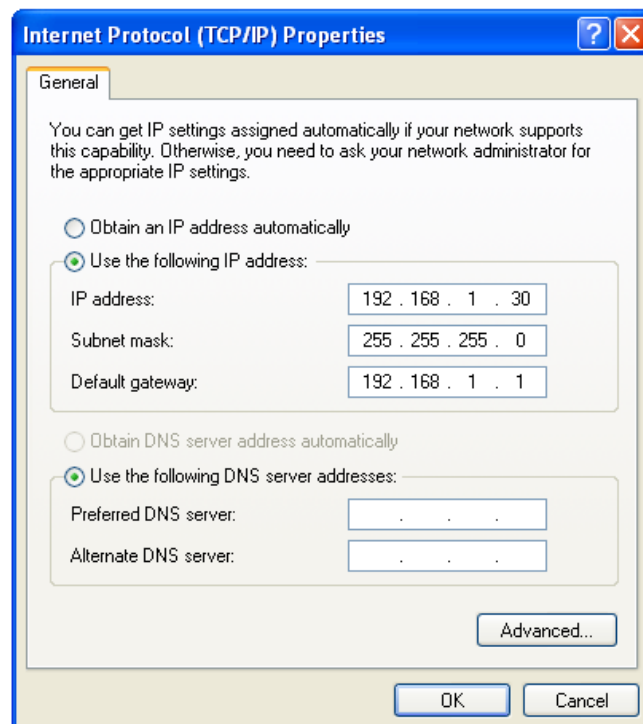
•   Click the **Start** button.

•   Right click on **My Network Places** and select **Properties**.

•   Right click the chosen Ethernet interface and select **Properties**.

•   Select **Internet Protocol (TCP/IP)** and click **Properties**.
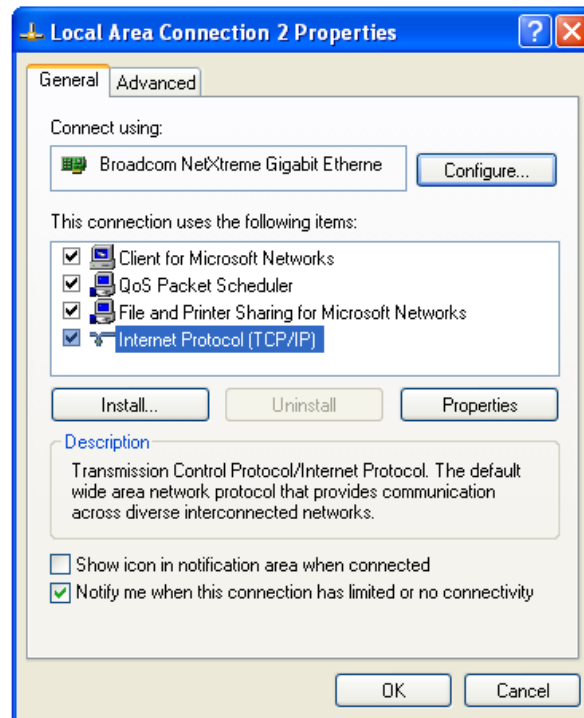
- Enter the IP addresses given above and click **OK**.

Note: DNS addresses can be entered later

To browse the Internet from the management workstation via the security gateway then it is possible to go back to the last step's properties dialog later and enter DNS server IP addresses. For now, they are not required.

IP Setup on Other Platforms

The following appendixes describe management workstation IP setup for other platforms:

- *Appendix C, Vista IP Setup*.

- *Appendix D, Windows 7 IP Setup*.

- *Appendix E, Apple Mac IP Setup*.

3.2. Web Interface and Wizard Setup

This chapter describes the setup when accessing the CorePlus for the first time through a web browser. The user interface accessed in this way is called the *Web Interface.*
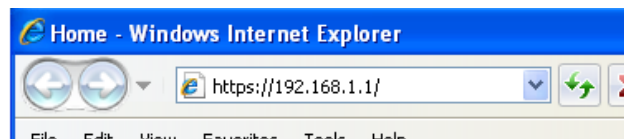
Note: Screenshot images are edited

Many of the screenshots in this section have had sections cut from the original image to aid readability. However, all of the relevant informational content has been preserved.

Connect By Browsing to *https://192.168.1.1*

Using a web browser, enter the address *https://192.168.1.1* into the navigation window as shown below.

Important: Disable any proxy server and turn off popup blocking

Make sure the web browser doesn't have a proxy server configured.

Any popup blocking in the browser should also be temporarily turned off to allow the setup wizard to run.

If there is no response from CorePlus and the reason is not clear, refer to the help checklist in *Section 3.6, "Troubleshooting Setup".*

The CorePlus Self-signed Certificate

When responding to an *https://* request, CorePlus sends a self-signed certificate which will not be initially recognized so it will be necessary to tell the browser to accept the certificate for this and future sessions. Different browsers handle this in slightly different ways. In Microsoft Internet Explorer the following error message will be displayed in the browser window.

To continue, tell IE to accept the certificate by clicking the following link which appears near the bottom of the browser window.

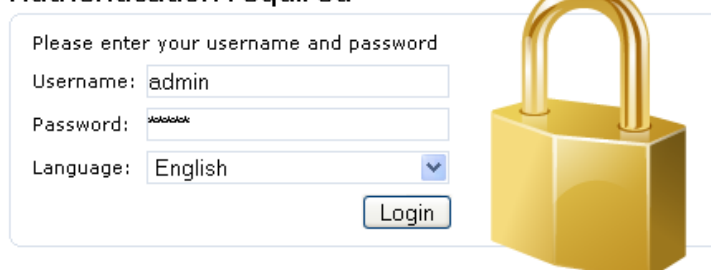In FireFox this procedure is called "*Add a security exception*".

The Login Dialog

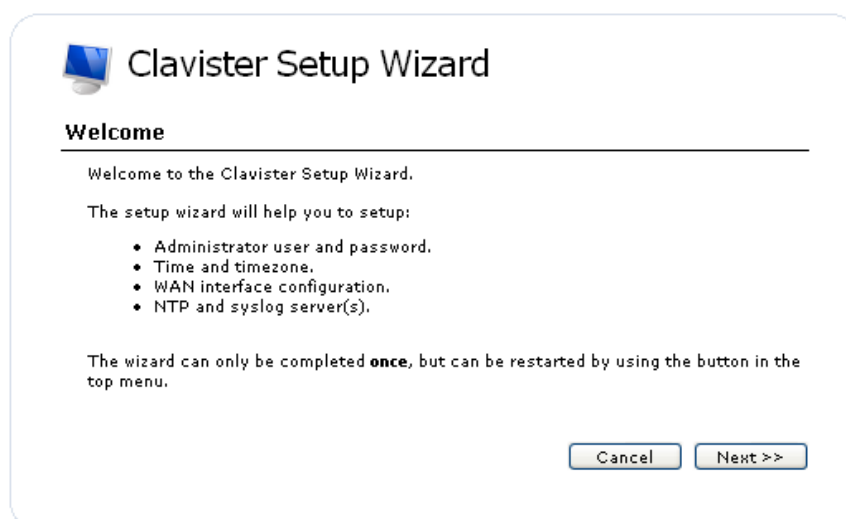CorePlus will next respond like a web server with the initial login dialog page as shown below.

The available Web Interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if CorePlus supports that language.

Logging In and the Setup Wizard

Now login with the username *admin* and the password *admin*. The Web Interface will appear and the CorePlus setup wizard should begin automatically. The first wizard dialog is the wizard welcome screen which should appear as shown below.

Cancelling the Wizard

The setup wizard can be cancelled at any point before the final *Activate* screen and run again by choosing the *Setup Wizard* option from the Web Interface toolbar. Once any configuration changes have been made and activated, either through the wizard, Web Interface or CLI, then the wizard cannot be run since the wizard requires that CorePlus has the factory defaults.

The Wizard Assumes Internet Access will be Configured

The wizard assumes that Internet access will be configured. If this is not the case, for example if the Clavister Security Gateway is being used in *Transparent Mode* between two internal networks, then the configuration setup is best done with individual Web Interface steps or through the CLI instead of through the wizard.

Advantages of the Wizard

The wizard makes setup easier because it automates what would otherwise be a more complex set of individual setup steps. It also reminds you to perform important tasks such as setting the date and time and configuring a log server.

The steps that the wizard goes through after the welcome screen are listed next.

Wizard step 1: Enter a new username and password

You will be prompted to enter a new administration username and password as shown below. It is recommended that this is always done and the new username/password is remembered (if these are forgotten, restoring to factory defaults will restore the original *admin*/*admin* combination). The password should be composed in a way which makes it difficult to guess.

Administrator user settings

Please enter a password for protecting the administrative interface of the unit.

Username: admin
Password: ********
Confirm Password: ********

Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.

Wizard step 2: Set the date and time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly in the fields shown below.

Time, time zone and daylight saving time settings

Setup the correct time and timezone settings for the firewall.

Date: 2009-09-01

Time: 14:39:44

[Set time and date]

Timezone settings

Time Zone: (GMT)

☑ Enable daylight saving time

Offset: 60   minutes
Start Date: March   1
End Date: October   1

Wizard step 3: Select the *WAN* interface

Next, you will be asked for the *WAN* interface that will be used to connect to your ISP for Internet access.

WAN interface settings

Select the interface that is connected to the ISP.

Interface: (None)

Wizard step 4: Select the *WAN* interface settings

This step selects how the WAN connection to the Internet will function. It can be one of *Manual configuration*, *DHCP*, *PPPoE* or *PPTP* as shown below.

These four different connection options are discussed next in the following subsections **4A** to **4D**.

- **4A. Static - manual configuration**

  Information supplied by the ISP should be entered in the next wizard screen. All fields need to be entered except for the *Secondary DNS server* field.

- **4B. DHCP - automatic configuration**

  All required IP addresses will automatically be retrieved from the ISP's DHCP server with this option. No further configuration is required for this so it does not have its own wizard screen.

- **4C. PPPoE settings**

  The username and password supplied by your ISP for PPPoE connection should be entered. The *Service* field should be left blank unless the ISP supplies a value for it.

PPPoE settings

PPP over Ethernet connections are used in many DSL and cable modem networks.
After authenticating, everything is automatic.

Username:

Password:

Confirm Password:

Service:

DNS servers are set automatically after connection with PPPoE.

- **4D. PPTP settings**

  The username and password supplied by your ISP for PPTP connection should be entered. If DHCP is to be used with the ISP then this should be selected, otherwise *Static* should be selected followed by entering the static IP address supplied by the ISP.

PPTP settings

PPTP over Ethernet connections are used in some DSL and cable modem networks.
You need account details, and possibly also IP configuration parameters of the actual
physical interface that the PPTP tunnel runs over. Your ISP should supply this
information.

PPTP tunnel parameters:

Username:

Password:

Confirm Password:

Remote Endpoint:

Physical interface parameters:

- ⦿ DHCP
- ◯ Static

  IP Address:

  Network:

  Gateway:

DNS servers are set automatically after connection with PPTP.

Wizard step 5: DHCP server settings

If the Clavister Security Gateway is to function as a DHCP server, it can be enabled here in the wizard on a particular interface or configured later.

The range of IP addresses that can be handed out must be specified in the form *n.n.n.n - n.n.n.n*, where *n* is a number between 0 and 255 and *n.n.n.n* is a valid IP address within a subnet local to the security gateway.

For example, the private IP address range *192.168.1.50 - 192.168.1.150* might be specified.

Wizard step 6: Helper server settings

Optional NTP and Syslog servers can be enabled here in the wizard or configured later. *Network Time Protocol* servers keep the system date and time accurate. Syslog servers can be used to receive and store log messages sent by CorePlus.

For the default gateway, it is recommended to specify the IP address assigned to the internal network interface. In this setup, this corresponds to *192.168.1.1*. The DNS server specified should be the DNS supplied by your ISP.

When specifying a hostname as a server instead of an IP address, the hostname should be prefixed with the string *dns:*. For example, the hostname *host1.company.com* should be entered as *dns:host1.company.com*.

Wizard step 7: Activate setup

The final step is to activate the setup by pressing the *Activate* button. After this step the Web Interface returns to its normal appearance and the administrator can continue to configure the system.
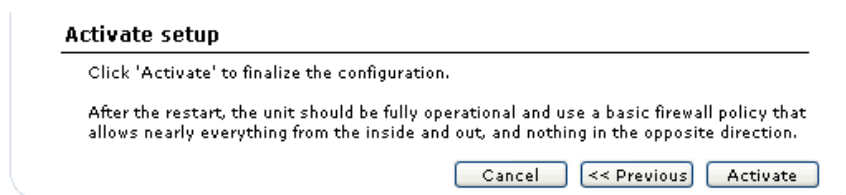
Running the Wizard Again

Once the wizard has been successfully finished and activated, it cannot be run again. The exception to this is if the Clavister Security Gateway has its factory defaults restored in which case the appliance will behave as though it were being started for the first time.

Uploading a License

If the wizard has been run or not, the Web Interface can now be used to upload a valid license to the Clavister Security Gateway. Without a license, CorePlus will run in *demonstration mode* which means that it will cease to function after two hours of operation (restarting the system will re-enable CorePlus for another two hours). The steps for license upload are:

• Using a web browser, browse to the *License Center* section of the Clavister website *https://www.clavister.com* and select the option **Register New License**.

  You will require your Clavister *Registration Key* to register (the key also referred to as the *License Number*. For the SG4500 Series, this key can be found written on a label on the underside or back of the appliance.

• The license center will also require a *MAC address* to associate with the Clavister license. This is the hardware Ethernet address associated with one of the Ethernet interfaces on the appliance. On the SG4500 Series, the MAC address of the default management interface can also be found written on the label on the underside or back of the hardware.

  Alternatively, a MAC address can be read from the output of the *ifstat* CLI command (this can be entered via the serial console CLI).

• Now download a valid *.lic* license file from the license center to the hard disk of the workstation.

• In the Web Interface menu bar, go to **Maintenance > Upgrade** and use the **Browse** button to select the license file, then upload it. As soon as the license is uploaded, demonstration mode will end and CorePlus will be restricted only by the limitations of the license.

3.3. Manual Web Interface Setup

This section describes initial CorePlus configuration performed directly through the Web Interface, without using the setup wizard. Configuration is done as a series of individual steps, giving the administrator more direct control over the process. Even if the wizard is used, this section can also be read as a good introduction to using the Web Interface for configuring key aspects of CorePlus.

Ethernet Interfaces

The physical connection of external networks to the Clavister Security Gateway is through the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the SG4500 Series, the *ge1* interface is the default management interface. The other interfaces can be used as required. For this section, it is assumed that the *ge2* interface will be used for connection to the public Internet and the *ge3* interface will be used for connection to a protected, local network.

The Navigation Tree

The Web Interface presents the various components of CorePlus in a tree structure in the left-hand pane of the browser window.
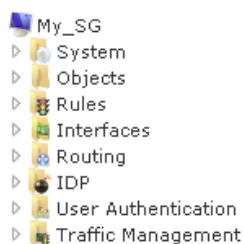
By clicking on the navigation tree we can expand its nodes to examine and change the properties of the various *settings*, *objects* and *rules* that make up a CorePlus configuration. A simple example of changing a configuration is discussed next.

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly. To do this, open the *System* node in the navigation tree.
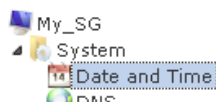
If we now click on the *Date and Time* node in the tree, the properties of the current date and time settings will appear in the central panel of the Web Interface.

By pressing the **Set Date and Time** button, a dialog appears that allows the exact time to be set.

A **Network Time Protocol** (NTP) servers can optionally be configured to maintain the accuracy of the system date and time and this will require public Internet access. Enabling this option is strongly recommended since it ensures the accuracy of the date and time. A typical NTP setup is shown below.

Note: The time server URL requires the "dns:" prefix

*When specifying a URL in CorePlus for the time server, the URL must have the prefix "**dns:**".*

Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in CorePlus configuration. Although changed values like this are saved by CorePlus, they do not become active until the entire saved configuration becomes the current and active configuration. We will look at how to do this next.

Activating Configuration Changes

To activate any CorePlus configuration changes made so far, we need to select the **Save and Activate** option from the **Configuration** menu (this process is also sometimes referred to as *deploying* a configuration).
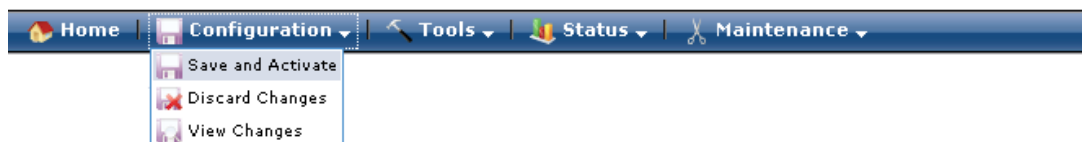
A dialog is then presented to confirm that the new configuration is to become the running configuration.

37

Save Configuration
Save and activate changes made to the configuration file.

Save and Activate

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

After clicking **OK**, CorePlus *reconfiguration* will take place and, after a short delay, the Web Interface will try and connect again to the security gateway.

Save and Activate

Saving configuration, please wait...

If no reconnection is detected by CorePlus within 30 seconds (this length of time is a setting that can be changed) then CorePlus will revert back to the original configuration. This is to ensure that the new configuration does not accidentally lock out the administrator. After reconfiguration and successful reconnection, a success message is displayed indicating successful reconfiguration.

Commit changes

Configuration successfully activated and committed.

Reconfiguration is a process that the CorePlus administrator may initiate often. Normally, reconfiguration takes a brief amount of time and causes only a slight delay in traffic throughput. Active user connections through the Clavister Security Gateway should rarely be lost.

> ### Tip: How frequently to commit changes
>
> *It is up to the administrator to decide how many changes to make before activating a new configuration. Sometimes, activating configuration changes in small batches can be appropriate in order to check that a small set of changes work as planned.*
>
> *However, it is not advisable to leave changes uncommitted for long periods of time, such as overnight, since any system outage will result in these edits being lost.*

Automatic Logout

If there is no activity through the Web Interface for a period of time (the default is 15 minutes), CorePlus will automatically log the user out. If they log back in through the same web browser session then they will return to the point they were at before the logout occurred and no saved (but not yet activated) changes are lost.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access. The setup wizard described in the previous chapter, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the Web Interface are discussed next.

A. Static - manual configuration

Manual configuration means that there will be a direct connection to the ISP and all the relevant IP addresses for the connecting interface are fixed values provided by the ISP which are entered into CorePlus manually.

Note: The interface DHCP option should be disabled

For static configuration of the Internet connection, the DHCP option must be disabled (the default) in the properties of the interface that will connect to the ISP.

The initial step is to set up a number of IP address objects in the CorePlus *Address Book*. Let us assume for this section that the physical interface used for Internet connection is *ge2*, the static IP address for this interface is to be *10.5.4.35*, the ISP's gateway IP address is *10.5.4.1*, and the network to which they both belong is *10.5.4.0/24*.

Note: Private IP addresses are used for example only

Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.

Let's now add the gateway *IP4 Address* object which we will call *wan_gw* and assign it the IP address *10.5.4.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Security Gateway. Go to **System > Objects > Address Book** in the Web Interface navigation tree.
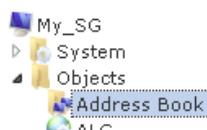
The current contents of the address book will be listed and will contain a number of predefined objects created by CorePlus after it scans the interfaces for the first time. The screenshot below shows the initial address book for the SG4500 Series.

Note: The all-nets address

*The IP address object **all-nets** is a wildcard address that should never be changed and can be used in many types of CorePlus rules to refer to any IP address or network range.*

All the interface related address objects are gathered together in an *address book folder* called *InterfaceAddresses*. By clicking on this folder, we open it and can view the addresses it contains. The first few default addresses in the folder are shown below.

By default on initial startup, two IP address objects are create automatically for each interface detected by CorePlus. One IP address object is named by combining the physical interface name with the suffix *_ip* and this is used for the IP address assigned to that interface. The other address object is named by combining the interface name with the suffix *_net* and this is the network to which the interface belongs.

Tip: Creating address book folders

New folders can be created when needed and provide a convenient way to group together related IP address objects. The folder name can be chosen to indicate the folder's contents.

Now click the **Add** button at the top left of the list and choose the *IP4 Address* option to add a new address to the folder.
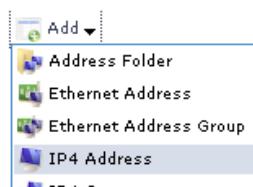
Enter the details of the object into the properties fields for the IP4 Address. Below, we have entered the IP address *10.5.4.1* for the address object called *wan_gw*. This is the IP of the ISP's router which acts as the gateway to the Internet.

Click the **OK** button to save the values entered.

Then set up *ge2_ip* to be *10.5.4.35*. This is the IP address of the *ge2* interface which will connect to the ISP's gateway.

Lastly, set the IP4 Address object *ge2_net* to be *10.5.4.0/24*. Both *ge2_ip* and *wan_gw* must belong to this network in order for the interface to communicate with the ISP.

Together, these 3 IP address objects will be used to configure the interface connected to the Internet which in this example is *ge2*. Select **Interfaces > Ethernet** in the navigation tree to

display a list of the physical interfaces. The first few lines of the interface list for the SG4500 Series are shown below.

Click on the interface in the list which is to be connected to the Internet. The properties for this interface will now appear and the relevant settings can be entered or changed.

Press **OK** to save the changes. Although changes are remembered by CorePlus, the changed configuration is not yet activated and won't be activated until CorePlus is told to activate the changed configuration.

Remember that DHCP should **not** be enabled when using static IP addresses and also that the IP address of the *Default Gateway* (which is the ISP's router) **must** be specified. As explained in more detail later, specifying the *Default Gateway* also has the additional effect of automatically adding a route for the gateway in the CorePlus routing table.

At this point, the connection to the Internet is configured but no traffic can flow to or from the Internet since all traffic needs a minimum of the following two CorePlus configuration objects to exist before it can flow through the Clavister Security Gateway:

•   An *IP rule* defined in a CorePlus *IP rule set* that explicitly allows traffic to flow from a given source network and source interface to a given destination network and destination interface.

•   A *route* defined in a CorePlus routing table which specifies on which interface CorePlus can find the traffic's destination IP address.

    If multiple matching routes are found, CorePlus uses the route that has the smallest (in other words, the narrowest) IP range.

We must therefore first define an IP rule that will allow through traffic from a designated source interface and source network. In this case let us assume we want to allow web browsing from the internal network *ge3_net* connected to the interface *ge3* to be able to access the public Internet.

To do this, we first go to **Rules > IP Rule Sets > main** in the navigation tree.

The empty *main* IP rule set will now appear. Press the **Add** button at the top left and select **IP Rule** from the menu.

The properties for the new IP rule will appear. In this example, we will call the rule *lan_to_wan*.

The rule *Action* is set to *NAT* (this is explained further below) and the *Service* is set to *http-all* which is suitable for most web browsing (it allows both HTTP and HTTPS connections). The interface and network for the source and destinations are defined in the *Address Filter* section of the rule.

General

Name:	lan_to_wan
Action:	NAT
Service:	http-all
Schedule:	(None)
RuleSet:	(None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	ge3	ge2
Network:	ge3_net	all-nets

The destination network in the IP rule is specified as the predefined IP4 Address object *all-nets*. This is used since we don't know to which IP address the web browsing will be done and this allows browsing to any IP address. IP rules are processed in a top down fashion, with the first matching rule being obeyed. An *all-nets* rule like this should be placed towards the bottom of the rule set since other rules with narrower destination addresses should trigger before it does.

Only one rule is needed since any traffic controlled by a *NAT* rule will be controlled by the CorePlus *state engine*. This means that the rule will allow *connections* that originate from the source network/destination and also implicitly allow any returning traffic that results from those connections.

In the above, we selected the service called *http_all* which is already defined in CorePlus. It is advisable to make the service in an IP rule as restrictive as possible to provide the best security possible. Custom service objects can be created and new service objects can be created which are combinations of existing services.

We could have specified the rule *Action* to be *Allow*, but only if all the hosts on the protected local network have public IP addresses. By using *NAT*, CorePlus will use the destination interface's IP address as the source IP. This means that external hosts will send their responses back to the interface IP and CorePlus will automatically direct the traffic back to the originating local host. Only the outgoing interface therefore needs to have a public IP address and the internal network topology is hidden.

To allow web browsing, DNS lookup also needs to be allowed in order to resolve URLs into IP addresses. The service *http_all* does not include the *DNS* protocol so we need a similar IP rule that allows this. This could be done with one IP rule that uses a custom service which combines the *HTTP* and *DNS* protocols but the recommended method is to create an entirely new IP rule that mirrors the above rule but specifies the service as *dns-all*. This method provides the most clarity when the configuration is examined for any problems. The screenshot below shows a new rule called *lan_to_wan_dns* being created to allow DNS.

This IP rule also specifies that the action for DNS requests is *NAT* so all DNS request traffic is sent out by CorePlus with the outgoing interface's IP address as the source IP.

For the Internet connection to work, we also need a *route* defined so that CorePlus knows on which interface the web browsing traffic should leave the Clavister Security Gateway. This route will define the interface where the network *all-nets* (in other words, any network) will be found. If we open the default *main* routing table by going to **Routing > Routing Tables > Main** in the navigation tree, the route needed should appear as below.

This required *all-nets* route is, in fact, added automatically after specifying the *Default Gateway* for a particular Ethernet interface which we did earlier after setting up the required IP4 Address objects.

Note: Disabling automatic route generation

*Automatic route generation is enabled and disabled with the setting "**Automatically add a default route for this interface using the given default gateway**" which can be found in the properties of the interface.*

As part of the setup, it is also recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address. Let's assume an IP address object called *wan_dns1* has already been defined in the address book which is the IP address for the first DNS server. By choosing **System > DNS** in the navigation tree, the DNS server dialog will open and this object from the address book can be assigned as the first server.

B. DHCP - automatic configuration

All the required IP addresses for Internet connection can, alternatively, be automatically retrieved from an ISP's DHCP server by enabling the **DHCP Client** option for the interface connected to the ISP. We enable this option by first selecting **Ethernet > Interfaces** in the navigation tree to display a list of all the interfaces.

Click the *ge2* interface in the list to display its properties.

In the above screenshot, DHCP is enabled for this interface and this is the required setting if IP addresses are to be retrieved automatically. Usually, a DHCP *Host Name* does not need to be specified but can sometimes be used by an ISP to uniquely identify this Clavister Security Gateway as a particular DHCP client to the ISP's DHCP server.

On connection to the ISP, all required IP addresses are retrieved automatically from the ISP via DHCP and CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface *ge2*.

C. PPPoE setup

For PPPoE connection, we must create a PPPoE tunnel interface associated with the physical Ethernet interface. Assume that the physical interface is *ge2* and the PPPoE tunnel object created is called *wan_pppoe*. Go to **Interfaces > PPPoE** in the navigation tree and select **Add > PPPoE Tunnel**. These values can now be entered into the PPPoE Tunnel properties dialog.

General

Name:	wan_pppoe
Physical Interface:	ge2
Remote Network:	all-nets
Schedule:	(None)

Authentication

Username:	pppoe_username
Password:	••••••••••••••••••
Confirm Password:	
Service Name:	

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. If we go to **Routing > Routing Tables > Main** in the navigation tree we can see this route.

⊕ Route	🖥 wan_pppoe	🌐 all-nets	90	No	Direct route for network all-nets over interface wan_pppoe.

If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel we have defined.

D. PPTP setup

For PPTP connections, a PPTP client tunnel interface object needs to be created. Let us assume that the PPTP tunnel will be called *wan_pptp* with a remote endpoint *10.5.4.1* which has been defined as the IP4 Address object *pptp_endpoint*. Go to **Interfaces > PPTP/L2TP Clients** in the navigation tree and select **Add > PPTP/L2TP Client**. The values can now be entered into the properties dialog and the *PPTP* option should be selected.

General

Name: wan_pptp

Tunnel Protocol: PPTP

Remote Endpoint: pptp_endpoint

Remote Network: all-nets

Authentication

Username: pptp_password

Password: ••••••••••••

Confirm Password:

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

If we go to **Routing > Routing Tables > Main** in the navigation tree we can see this route.

⊕ Route	🟩 wan_pptp	🟦 all-nets		90	No	Direct route for network all-nets over interface wan_pptp.

If the PPTP tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source network and source interface (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First create an IP4 Address object which defines the address range to be handed out. Here, we will assume this is called *dhcp_range*. We will also assume that an IP4 Address object *dhcp_netmask* has been created which specifies the netmask.

We now create a DHCP server object called *dhcp_lan* which will only be available only on the *ge3* interface. To do this, go to **System > DHCP > DHCP Servers** and select **Add > DHCP Server**. We can now specify the server properties.

In addition it is important to specify the *Default gateway* for the server. This will be handed out to DHCP clients on the internal networks so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *ge3_ip*.

Also in the **Options** tab, we should specify the DNS address which is handed out with DHCP leases. This could be set, for example, to be the IP address object *dns1_address*.

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless at least one log server is set up to receive them and this is configured in CorePlus. *Syslog* is one of the most common server types.

First we create an IP4 Address object called, for example, *syslog_ip* which is set to the IP address of the server. We then configure the sending of log messages to a Syslog server from CorePlus by selecting **System > Log and Event Receivers** from the navigation tree and then choosing **Add > Syslog Receiver**.

The syslog server properties dialog will now appear. We give the server a name, for example *my_syslog*, and specify its IP address as the *syslog_ip* object.

> ### Tip: Address book object naming
>
> *The CorePlus address book is organized alphabetically so when choosing names for IP address objects it is best to have the descriptive part of the name first. In this case, use* **syslog_ip** *as the name and not* **ip_syslog**.

Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be very useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *ge3_net* network.

There can be several rule sets defined in CorePlus but there is only one rule set defined by default and this is called *main*. To add a rule to it, first select **Rules > IP Rule Sets > main** from the navigation tree.

The *main* rule set list contents are now displayed. Press the **Add** button and select **IP Rule**.
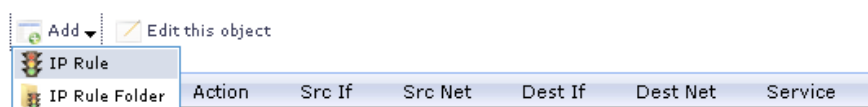
The properties for a new IP rule will appear and we can add a rule, in this case called *allow_ping_outbound*.

The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

The top-down nature of the IP rule set scanning has already been discussed earlier. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop

all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic.

General

Name:	Drop_All
Action:	Drop
Service:	all_services
Schedule:	(None)
RuleSet:	(None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	any	any
Network:	all-nets	all-nets

If the this rule us the only one defined, displaying the *main* IP rule set will be as shown below.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

Logging can now be enabled on this rule with the desired severity. Click the **Log Settings** tab, and click the **Enable logging** box. All log messages generated by this rule will be given the selected severity and which will appear in the text of the log messages. It is up to the administrator to choose the severity and depends on how they would like to classify the messages.

| General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors |

General

Select if logging should be enabled and what severity to use.

☑ Enable logging

Log with severity: Warning

Deleting Configuration Objects

If information is deleted from a configuration during editing then these deletes are indicated by a line scored through the list entry while the configuration is still not yet activated. The deleted entry only disappears completely when the changes are activated.

For example, we can delete the drop all IP rule created in the previous paragraph by right clicking the rule and selecting *Delete* in the context menu.

The rule now appears with a line scored through it.

We can reverse the delete by right clicking the rule again and choosing *Undo Delete*.

Uploading a License

Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Section 3.2, "Web Interface and Wizard Setup"*. This license can then be uploaded directly to CorePlus by selecting the **License** option from the **Maintenance** menu and then pressing the **Upload** button.

Now press the **Browse** button to select the file from the load file system and then the **Upload License** button to send it to CorePlus.

As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

3.4. CLI Setup

This chapter describes the setup steps using CLI commands instead of the setup wizard.

The CLI is accessible in two ways:

- Across the local network at default IP address *192.168.1.1* using an SSH (Secure Shell) client. The network connection setup is the same as that described in *Section 3.2, "Web Interface and Wizard Setup"* as is the way the workstation interface's static IP address must be set up so it is on the same network as the Clavister Security Gateway's interface.

  If there is a problem with workstation connection, a help checklist can be found in *Section 3.6, "Troubleshooting Setup"*.

- Using a terminal or computer running a console emulator connected directly to the local RS-232 console port on the SG4500 Series. Performing console port connection is described in the hardware installation manual for each Clavister hardware model.

The CLI commands listed below are grouped so that they mirror the options available in the setup wizard.

Confirming the Connection

Once connection is made to the CLI, pressing the **Enter** key will cause CorePlus to respond. The response will be a normal CLI prompt if connecting locally through the RS-232 console port and a username/password combination will not be required (a password for this console can be set later).

```
Device:/>
```

If connecting remotely through an SSH (Secure Shell) client, an administration username/password must first be entered and the initial default values for these are username *admin* and password *admin*. When these are accepted by CorePlus, a normal CLI prompt will appear and CLI commands can be entered.

Changing the Password

To change the administration username or password, use the *set* command to change the current CLI object category (sometimes referred to as the *object context*) to be the *LocalUserDatabase* called *AdminUsers*.

```
Device:/> cc LocalUserDatabase AdminUsers
Device:/AdminUsers>
```

> **Tip: Using tab completion with the CLI**
>
> *The tab key can be pressed at any time so that CorePlus gives a list of possible options in a command.*

Now set the username/password, which are case sensitive, to be the new chosen values for the user called *admin*. In the example below, we change to the username *new_name* and password *new_pass*.

```
Device:/AdminUsers> set User Admin Name=new_name Password=new_pass
```

The new username/password combination should be remembered and the password should be composed in a way which makes it difficult to guess. The next step is to return the CLI to the default top level of object categories.

```
Device:/AdminUsers> cc
Device:/>
```

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly using the *time* command. A typical usage might be:

```
Device:/> time -set 2008-06-24 14:43:00
```

Notice that the date is entered in *yyyy-mm-dd* format and the time is stated in 24 hour *hh:mm:ss* format.

Ethernet Interfaces

The connection of external networks to the Clavister Security Gateway is via the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the SG4500 Series, the *ge1* interface is the default management interface. The other interfaces can be used as desired. For the sake of example, it is assumed here that the *ge2* interface will be used for connection to the public Internet and the *ge3* interface will be used for connection to a protected, local network.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access with the CLI. The setup wizard described previously, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup.

D. PPTP setup.

The individual manual steps to configure these connection alternatives with the CLI are discussed next.

A. Static - manual configuration

We first must set or create a number of IP address objects. It's assumed here that the interface used for Internet connection is *ge2*, the ISP gateway IP address is *10.5.4.1*, the IP address for the connecting interface will be *10.5.4.35* and the network to which they belong is *10.5.4.0/24*.

> ### Note: Private IP addresses are used for example only

Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.

We first add the gateway IP address object which we will call *wan_gw*:

```
Device:/> add Address IP4Address wan_gw Address=10.5.4.1
```

This is the address of the ISP's gateway which is the first router hop towards the public Internet. If this IP object already exists, it can be given the IP address with the command:

```
Device:/> set Address IP4Address wan_gw Address=10.5.4.1
```

Now use this object to set the gateway on the *ge2* interface which is connected to the ISP:

```
Device:/> set Interface Ethernet ge2 DefaultGateway=wan_gw
```

Next, set the IP object *ge2_ip* which will be the IP address of the interface connected to the ISP:

```
Device:/> set IP4Address InterfaceAddresses/ge2_ip
          Address=10.5.4.35
```

Note: Qualifying the names of IP objects in folders

On initial startup of the SG4500 Series, CorePlus automatically creates and fills the **InterfaceAddresses** *folder in the CorePlus address book with the interface related IP address objects.*

When we specify an IP address object which is located in a folder, we must qualify the object's name with the name of the folder. When we specify, for example, the address **ge2_ip** *we must qualify it with the folder name* **InterfaceAddresses** *so the qualified name becomes* **InterfaceAddresses/ge2_ip***.*

If an object is not contained in a folder and is at the top level of the address book then no qualifying folder name is needed.

Now set the IP object *ge2_net* which will be the IP network of the connecting interface:

```
Device:/> set IP4Address InterfaceAddresses/ge2_net
          Address=10.5.4.0/24
```

It is recommended to verify the properties of the *ge2* interface with the command:

```
Device:/> show Interface Ethernet ge2
```

The typical output from this will be similar to the following:

```
           Property  Value
   ------------------------  ------------------------
              Name:  ge2
                IP:  InterfaceAddresses/ge2_ip
           Network:  InterfaceAddresses/ge2_net
    DefaultGateway:  wan_gw
         Broadcast:  10.5.4.255
         PrivateIP:  <empty>
             NOCHB:  <empty>
               MTU:  1500
            Metric:  100
       DHCPEnabled:  No
```

```
         EthernetDevice:  0:ge2  1:<empty>
        AutoSwitchRoute:  No
AutoInterfaceNetworkRoute:  Yes
   AutoDefaultGatewayRoute:  Yes
   ReceiveMulticastTraffic:  Auto
     MemberOfRoutingTable:  All
               Comments:  <empty>
```

Setting the default gateway on the interface has the additional effect that CorePlus automatically creates a route in the default *main* routing table that has the network *all-nets* routed on the interface. This means that we do not need to explicitly create this route.

Even though an *all-nets* route is automatically added, no traffic can flow without the addition of an *IP rule* which explicitly allows traffic to flow. Let us assume we want to allow web browsing from the protected network *ge3_net* on the interface *ge3*. A simple rule to do this would have an *Action* of *Allow* and would be defined with the following commands.

Firstly, we must change the current CLI context to be the default *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Additional IP rule sets can be defined which is why we do this, with the rule set *main* existing by default. Notice that the CLI prompt changes to reflect the current context:

```
Device:/main>
```

Now add an IP rule called *lan_to_wan* to allow the traffic through to the public Internet:

```
Device:/main> add IPRule name=lan_to_wan
              Action=Allow SourceInterface=ge3
              SourceNetwork=InterfaceAddresses/ge3_net
              DestinationInterface=ge2
              DestinationNetwork=all-nets
              Service=http-all
```

This IP rule would be correct if the internal network hosts have public IP addresses but in most scenarios this will not be true and internal hosts will have private IP addresses. In that case, we must use NAT to send out traffic so that the apparent source IP address is the IP of the interface connected to the ISP. To do this we simply change the *Action* of the above command from *Allow* to *NAT*:

```
Device:/main> add IPRule name=lan_to_wan
              Action=NAT SourceInterface=ge3
              SourceNetwork=InterfaceAddresses/ge3_net
              DestinationInterface=ge2
              DestinationNetwork=all-nets
              Service=http-all
```

The service used in the IP rule is *http-all* which will allow most web browsing but does not include the DNS protocol to resolve URLs into IP addresses. To solve this problem, a custom service could be used in the above rule which combines *http-all* with the *dns-all* service. However, the recommended method which provides the most clarity to a configuration is to create a separate IP rule for DNS:

```
Device:/main> add IPRule name=lan_to_wan_dns
              Action=NAT SourceInterface=ge3
              SourceNetwork=InterfaceAddresses/ge3_net
              DestinationInterface=ge2
              DestinationNetwork=all-nets
              Service=dns-all
```

It is recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address. If we assume an IP address object called *dns1_address* has already been defined for the first DNS server, the command to specify the first DNS server is:

```
Device:/> set DNS DNSServer1=dns1_address
```

Assuming a second IP object called *dns2_address* has been defined, the second DNS server is specified with:

```
Device:/> set DNS DNSServer2=dns2_address
```

B. DHCP - automatic configuration

All required IP addresses can alternatively be automatically retrieved from the ISP's DHCP server by enabling DHCP on the interface connected to the ISP. If the interface on which DHCP is to be enabled is *ge2*, then the command is:

```
Device:/> set Interface Ethernet ge2 DHCPEnabled=Yes
```

Once the required IP addresses are retrieved with DHCP, CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process. Automatic route generation is a setting for each interface that can be manually enabled and disabled.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore manually define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface *ge2*.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface *ge2*, is assumed to be connected to the ISP in the command shown below which creates a PPPoE tunnel object called *wan_ppoe*:

```
Device:/> add Interface PPPoETunnel wan_ppoe
             EthernetInterface=ge2 username=pppoe_username
             Password=pppoe_password Network=all-nets
```

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password*.

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it,

and this is automatically created in the *main* routing table when the tunnel is defined. If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that we have defined.

D. PPTP setup

For PPTP connection, first create the PPTP tunnel interface. It is assumed below that we will create a PPTP tunnel object called *wan_pptp* with the remote endpoint *10.5.4.1*:

```
Device:/> add Interface L2TPClient wan_pptp Network=all-nets
            username=pptp_username Password=pptp_password
            RemoteEndpoint=10.5.4.1 TunnelProtocol=PPTP
```

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint.

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

As with all automatically added routes, if the PPTP tunnel object is deleted then this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *ge3_net* and interface *ge3*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

Activating and Committing Changes

After any changes are made to a CorePlus configuration, they will be saved as a new configuration but will not yet be activated. To activate all the configuration changes made since the last activation of a new configuration, the following command must be issued:

```
Device:/> activate
```

Although the new configuration is now activated, it does not become permanently activated until the following command is issued within 30 seconds following the *activate*:

```
Device:/> commit
```

The reason for two commands is to prevent a configuration accidentally locking out the administrator. If a lock-out occurs then the second command will not be received and CorePlus will revert back to the original configuration after the 30 second time period (this time period is a

setting that can be changed).

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First define an IP address object which has the address range that can be handed out. Here, we will use the IP range *192.168.1.10-192.168.1.20* as an example and this will be available on the *ge3* interface which is connected to the protected internal network *ge3_net*.

```
Device:/> add Address IP4Address dhcp_range
            Address=192.168.1.10-192.168.1.20
```

The DHCP server is then configured with this IP address object on the appropriate interface. In this case we will call the created DHCP server object *dhcp_lan* and assume the DHCP server will be available on the *ge3* interface:

```
Device:/> add DHCPServer dhcp_lan IPAddressPool=dhcp_range
            Interface=ge3 Netmask=255.255.255.0
            DefaultGateway=InterfaceAddresses/ge3_ip
            DNS1=dns1_address
```

It is important to specify the *Default gateway* for the DHCP server since this will be handed out to DHCP clients on the internal network so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *ge3_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can optionally be configured to maintain the accuracy of the system date and time. The command below sets up synchronization with the two NTP servers at hostname *pool.ntp.org* and IP address *10.5.4.76*:

```
Device:/> set DateTime TimeSyncEnable=Yes
            TimeSyncServer1=dns:pool.ntp.org
            TimeSyncServer2=10.5.4.76
```

The prefix *dns:* is added to the hostname to identify that it must resolved to an IP address by a DNS server (this is a convention used in the CLI with some commands).

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless a server is set up to receive them and *Syslog* is the most common server type. If the Syslog server's address is *195.11.22.55* then the command to create a log receiver object called *my_syslog* which enables logging is:

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *ge3_net* network. The commands to allow this are as follows.

Firstly, we must change the current CLI context to be the *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Now add an IP rule called *allow_ping_outbound* to allow ICMP pings to pass:

```
Device:/main> add IPRule name=allow_ping_outbound
             Action=NAT SourceInterface=ge3
             SourceNetwork=InterfaceAddresses/ge3_net
             DestinationInterface=ge2
             DestinationNetwork=all-nets
             Service=ping-outbound
```

The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

Scanning of the IP rule set is done in a top-down fashion. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic. The command for creating this rule is:

```
Device:/main> add IPRule name=drop_all
             Action=Drop SourceInterface=any
             SourceNetwork=any
             DestinationInterface=any
             DestinationNetwork=all-nets
             Service=all_services
```

Uploading a License

Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Section 3.2, "Web Interface and Wizard Setup"*. This license can then be uploaded directly to CorePlus using a *Secure Copy* (SCP) client (see the CorePlus Administrators Guide for more details of using SCP). As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

3.5. Downgrading to 8.nn

The SG4500 Series comes preinstalled with a 9.nn CorePlus version and this cannot be downgraded since the hardware does not support 8.nn versions

3.6. Troubleshooting Setup

This appendix deals with connection problems that might occur when connecting a management workstation to a Clavister Security Gateway.

If the management interface does not respond after the Clavister Security Gateway has powered up and CorePlus has started, there are a number of simple steps to troubleshoot basic connection problems:

1. Check that the correct interface is being used.

The most obvious problem is that the wrong Clavister Security Gateway interface has been used for the initial connection. Only the first interface found by CorePlus is activated for the initial connection from a browser after CorePlus starts for the first time.

2. Check that interface characteristics match.

If a Clavister Security Gateway's interface characteristics are configured manually then the interface on a switch to which it is connected should be configured with the same characteristics. For instance, the link speeds and half/full duplex settings must match. If they don't, communication will fail. This problem will not occur if the interfaces are set for automatic configuration on both sides and automatic is always the Clavister factory default setting.

3. Check that the workstation IP is configured correctly.

The second most obvious problem is if the IP address of the workstation running the web browser is not configured correctly.

4. Is the management interface properly connected?

Check the link indicator lights on the management interface. If they are dark then there may be a cable problem.

5. Check the cable type connected to the management interface.

Is the management interface connected directly to the management workstation or another router or host? In this case, an Ethernet "cross-over" cable may be needed for the connection, depending on the capabilities of the interface.

6. Using the *ifstat* CLI command.

To investigate a connection problem further, connect the a console to the RS-232 port on the Clavister Security Gateway after CorePlus starts. When you press the enter key, CorePlus should respond with the a standard CLI prompt. Now enter the following command a number of times:

```
Device:/> ifstat <if-name>
```

Where *<if-name>* is the name of the management interface. This will display a number of counters for that interface. The *ifstat* command on its own can list the names of all the interfaces.

If the *Input* counters in the hardware section of the output are not increasing then the error is likely to be in the cabling. However, it may simply be that the packets are not getting to the Clavister Security Gateway in the first place. This can be confirmed with a packet sniffer if it is available.

If the *Input* counters are increasing, the management interface may not be attached to the correct physical network. There may also be a problem with the routing information in any connected hosts or routers.

7. Using the *arpsnoop* CLI command.

A final diagnostic test is to try using the console command:

```
Device:/> arpsnoop -all
```

This will show the *ARP* packets being received on the different interfaces and confirm that the correct cables are connected to the correct interfaces.

3.7. Going Further with CorePlus

After initial setup is complete, the administrator is ready to go further with configuring CorePlus to suit the requirements of a particular networking scenario. The reference documentation provided for this consists of the following manuals:

- The CorePlus Administrators Guide

- The CLI Reference Guide

- The Log Reference Guide

The CorePlus Administrators Guide

This guide is a comprehensive description of all CorePlus features and includes a detailed table of contents with a comprehensive index to quickly locate particular topics.

Examples of the setup for various scenarios are included but screenshots are kept to a minimum since the user has a variety of management interfaces to choose from.

Basic CorePlus Objects and Rules

At minimum, the new administrator should first acquaint themselves with the CorePlus *Address Book* for defining IP address objects and with the CorePlus *IP rule set* for defining IP rules which can allow or block traffic types and which are also used to set up NAT address translation.

IP rules also demonstrate the way *Security Policies* are set up in CorePlus by identifying the targeted traffic through combinations of the source/destination interface/network combined with protocol type. By default, no IP rules are defined so all traffic is dropped. At least one IP rule needs to be defined before traffic can traverse the Clavister Security Gateway.

In addition to IP rules, *routes* need to be defined so that traffic can be sent on the correct interface to reach its final destination.

ALGs

Once the address book and IP rules are understood, the various ALGs will probably be of interest for managing higher level protocols such as HTTP. For example, for management of web browsing, the HTTP ALG provides a number of important features such as content filtering.

VPN Setup

A common requirement is to quickly setup VPN networks based on Clavister Security Gateways. The CorePlus Administrators Guide includes an extensive VPN section and as part of this, a *VPN Quick Start* section which goes through a checklist of setup steps for nearly all types of VPN scenarios.

Included with the quick start section is a checklist for troubleshooting and advice on how best to deal with the networking complications that can arise with certificates.

Log Messages

By default, certain events will generate log messages and at least one log server should be configured in CorePlus to capture these messages although a *memlog* feature is provided which

captures recent log messages in hardware memory. The administrator should review what events are important to them and at what severity. The *CorePlus Log Reference Guide* provides a complete listing of the log messages that CorePlus is capable of generating.

The CLI Reference Guide

The *CLI Reference Guide* provides a complete listing of the available CLI commands with their options. A CLI overview is also provided as part of the *CorePlus Administrators Guide*.

CorePlus Education Courses

For details about classroom and online CorePlus education as well as CorePlus certification, visit the Clavister company website at *http://www.clavister.com* or contact your local sales representative.

Staying Informed

Clavister maintains an RSS feed of announcements that can be subscribed to at *https://forums.clavister.com/rss-feeds/announcements/*. It is recommended to subscribe to this feed so that you receive notifications when new releases of CorePlus versions are available for download and installation. Alternatively, announcements can be read directly from the Clavister forums which can be found at *https://forums.clavister.com/*.

Chapter 4: Product Maintenance

• Replacing PSUs, page 65

• Replacing Fan Modules, page 69

Replacing SG4500 Series Modules

The SG4500 Series allows on-site, hot-swap replacement of both its dual power supply units (PSUs) as well as any of its 3 cooling fan modules. This chapter describes the onsite removal and installation of both PSUs and fan modules.

4.1. Replacing PSUs

The SG4500 Series has dual hot-swappable PSUs, both of which supply power in normal, redundant operation. As described earlier, the appliance will operate correctly with only one power supply but that configuration provides no redundancy.

Single PSU Operation

The SG4500 Series does not need both PSUs fitted. The appliance can operate correctly with just one PSU fitted. If this is the case, the second PSU slot should be filled with a special *PSU Filler Module*. This module also has the effect of disabling the PSU failure alarm which will be automatically activated if one PSU slot is left completely empty.

> ### Tip: Any slot can be used for a single PSU
>
> *In a single PSU configuration, it is not important which of the two PSU slots contains the PSU and which contains the Filler Module. Either slot can be used for either function.*

Dual PSU Operation

When both PSUs are fitted, PSU redundancy is provided. If a PSU fails then the security gateway will continue to function and the faulty PSU can be changed on-site through a simple procedure provided that a spare PSU is available.

> ### Note: Spare PSUs can be ordered
>
> *Spare PSUs can be ordered from your local sales representative so they can be ready when needed.*

The PSU

The SG4500 Series PSU is a self-contained power supply unit that slides into either of two slots located at the rear of the appliance.

Figure 4.1. A PSU Module

The PSU features a black handle which should be used for lifting as well as for applying pressure when inserting or pulling out the module. To the top-left of the handle is a locking switch which should be pressed to one side to disengage the lock when removing the PSU from a slot.

The PSU does not have an Off/On switch and comes into operation as soon as a power cord is inserted and external power is applied.

> ### Important: Dusty environments reduce PSU fan lifetimes
>
> *SG4500 Series PSU fans are designed to work in environments with reasonable air quality. Elevated dust levels in the surrounding air can substantially reduce the operating lifetimes of PSU fan modules.*

Using CorePlus Hardware Monitoring to Detect Failure

The *Hardware Monitoring* (HWM) functions of CorePlus should be used to remotely monitor the hardware state of the SG4500 Series and associated PSUs. If only one PSU is operating then this is shown through such monitoring regardless if this is intentional and a PSU filler module occupies an empty PSU slot.

PSU failure in a single PSU system will result in a total loss of hardware functionality. For this reason, dual redundant PSUs are the recommended configuration.

Local PSU Failure Indicators

If two PSUs are fitted to provide redundancy and there is a single PSU failure, a loud, continuous, audible alarm sound will be heard coming from the appliance. The alarm can be switched off by pressing the red button located to the right of the PSUs. This button is indicated on the image shown below.
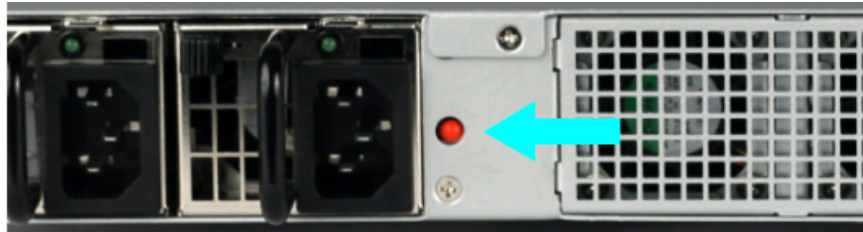
Figure 4.2. The Alarm Reset Button

In normal operation there is a green LED light that is illuminated on the back of each PSU. This LED will not be illuminated if its PSU has failed. This LED is indicated on the image shown below.

Figure 4.3. The PSU Status LED

Swapping a PSU

To swap a failed PSU:

1. Switch off the power source to the faulty PSU. This may be done by simply unplugging the power cable from a wall socket.

2. Remove the power supply cord from the PSU.

3. Firmly put two fingers around the PSU handle while using another finger to push the locking switch horizontally to one side. This is shown in the image below.

4. Once the locking switch is moved to the side and the lock disengaged, gently pull out the failed PSU until it is clear of the appliance and place it to one side.

5. After grasping the replacement PSU's handle with two fingers, gently slide it into the now empty PSU slot until it clicks into place. The locking switch need not be pushed. Inward

67

pressure should be applied only through the black handle.

6. Insert a power cord into the new PSU.

7. Apply the power source to the new PSU. This may be done by just plugging the power cord into a wall socket.

8. The new PSU's green light will illuminate, indicating normal operation and the audible alarm will stop if it hasn't already been switched off.

Tip: Having spare PSUs onsite

Having spare PSUs onsite and available will mean no delay if replacements are required. These can be ordered from your local sales representative.

4.2. Replacing Fan Modules

The SG4500 Series has three individual and independent fan modules that can be hot-swapped onsite. A fan module is shown below.

Figure 4.4. An Individual Fan Module

The Recommended Replacement Interval

All fan modules are liable to wear from mechanical movement and fan failure can lead to much more serious failures from the overheating of electronic components. Although fan modules are built for prolonged use, it is nevertheless a recommended precaution to replace them every three years.

> *Important: Dusty environments reduce fan lifetimes*
>
> *SG4500 Series fans are designed to work in environments with reasonable air quality. Elevated dust levels in the surrounding air can substantially reduce the operating lifetimes of fan modules.*

Identifying Failure

There are two ways of identifying fan failure:

- **Hardware Monitoring through CorePlus**

  By using the *hardware monitoring* feature of CorePlus it is possible to examine fan speeds and also to have alarms set should a fan speed fall below a particular value.

- **Manual Inspection**

  Complete fan failure can be seen by simple manual inspection of the fan to check if it is still spinning. There are no other external physical indicators on a fan module to signal failure.

Replacement Procedure

The following steps should be followed to replace a fan module:

1. Unscrew by hand the retaining screw at the right of the metal grill covering the fans.

> ### Caution: Keep away from spinning fans
>
> *Keep fingers, tools and any loose objects well away from the fans that are still spinning.*

2. Pull back the grill from the right side.

The grill pivots out on two locating tabs and can be pulled completely away to expose the three fans modules.

3. The fans are secured in place by a simple spring mechanism on each module's left and right side and this will release the module if sufficient outward, even force is applied.

   Each module has an inward facing bracket on its outer right and left front side. A thumb from either hand should be placed simultaneously behind each bracket and outward pressure applied to release and pull out the module. The image below shows just one thumb in place behind one of the brackets in order to provide a clearer view.

4. A new fan module can now be pushed into the empty space by placing fingers on each of the same left and right brackets. It will click into place when it is level with the other 2 modules. Be sure to push in the module slowly and squarely without forcing it into the empty slot.

5. If power to the appliance is on, the fan will begin to spin immediately.

6. Replace the metal grill by locating its two tabs into the locating holes on the left and secure it by screwing back the retaining screw by hand. The retaining screw requires just moderate hand tightening and extra tightening with a tool is not required.

Tip: Having spare fan modules onsite

Having spare fan modules onsite and available will mean no delay if replacements are required. These can be ordered from your local sales representative.

Chapter 5: Warranty Service

Limitation of Warranty

Clavister warrants to the customer of the SG4500 Series Appliance that the Hardware components will be free from defects in material and workmanship under normal use for a period of two (2) years from the Start Date (as defined below). The warranty will only apply to failure of the product if Clavister is informed of the failure not later than two (2) years from the Start Date or thirty (30) days after that the failure was or ought to have been noticed by the customer.

The warranty will not apply to products from which serial numbers have been removed or to defects resulting from unauthorized modification, operation or storage outside the environmental specifications for the product, in-transit damage, improper maintenance, defects resulting from use of third-party software, accessories, media, supplies, consumables or such items not designed for use with the product, or any other misuse. Any replacement Hardware will be warranted for the remainder of the original warranty period or thirty days, whichever is longer.

Note that the term *Start Date* means the earlier of the product registration date **OR** ninety (90) days following the day of shipment by Clavister.

Obtaining Warranty Service with an RMA

Warranty service can be obtained within the warranty period with the following steps:

1. Obtain a *Return Material Authorization* (RMA) number from Clavister. This **must** be obtained before the product is sent back.

   The Clavister RMA request form can be found online at (clickable link):

   http://www.clavister.com/support/support-center/

   If the Purchaser's circumstances require special handling of warranty correction, then at the time of requesting the RMA number, the Purchaser may also propose suitable special procedures.

2. The defective product **MUST** be packaged securely in the original packaging or other suitable shipping packaging to ensure that it will not be damaged in transit.

3. The RMA number must be clearly marked on the outside of the package.

4. The package is then shipped to Clavister with all the costs of mailing/shipping/insurance

paid by the Purchaser. The address for shipping is:

Clavister AB
Sjögatan 6J
891 60 Örnsköldsvik
SWEDEN

If the product has not yet been registered with the Clavister through it's client web, a proof of purchase (such as a copy of the dated purchase invoice) must be provided with the shipped product.

An RMA Number Must Be Obtained Before Shipping

Any package returned to Clavister without an RMA number will be rejected and shipped back to the Purchaser at the Purchaser's expense. Clavister reserves the right in such a case to levy a reasonable handling charge in addition to mailing and/or shipping costs.

Data on the Hardware

Note that Clavister is not responsible for any of the purchaser's software, firmware, information, or memory data contained in, stored on, or integrated with any product returned to Clavister pursuant to this warranty.

Contacting Clavister

Should there be a problem with the online form then Clavister support can be contacted by email at: *support@clavister.com*.

Hardware Replacement Procedures

Details of the procedures to follow when replacing old Clavister hardware with new hardware can be found in the separate Clavister document:

Hardware Replacement Guide for CorePlus 9.nn.

Customer Remedies

Clavister's entire liability according to this warranty shall be, at Clavister's option, either return of the price paid, or repair or replacement of the Hardware that does not meet Clavister's limited warranty and which is returned to Clavister with a copy of your receipt.

Limitations of Liability

Refer to the legal statement at the beginning of the guide for a statement of liability limitations.

Chapter 6: Safety Precautions

Safety Precautions

Clavister SG4500 Series devices are *Safety Class I* products and have protective ground terminals. There must be an uninterrupted safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.

- LAN cables may occasionally be subject to hazardous transient voltage (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

There are no user-serviceable parts inside these products. Only service-trained personnel can perform any adjustment, maintenance or repair.

Säkerhetsföreskrifter

Dessa produkter är säkerhetsklassade enligt klass I och har anslutningar för skyddsjord. En obruten skyddsjord måste finnas från strömkällan till produktens nätkabelsanslutning eller nätkabel. Om det finns skäl att tro att skyddsjorden har blivit skadad, måste produkten stängas av och nätkabeln avlägnas till dess att skyddsjorden har återställts.

För LAN-kablage gäller dessutom att:

- om LAN:et täcker ett område som betjänas av mer än ett strömförsörjningssystem måste deras respektive skyddsjord vara ihopkopplade.

- LAN kablage kan vara föremål för farliga spänningstransienter (såsom blixtnedslag eller störningar i elnätet). Hantera metallkomponenter i förbindelse med nätverket med försiktighet.

Det finns inga delar i produkten som kan lagas av användaren. All service samt alla justeringar, underhåll eller reparationer får endast utföras av behörig personal.

Informations concernant la sécurité

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entree, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soint convenablement interconnectées.

- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Hinweise zur Sicherheit

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, dass der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfasst, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, dass die Sicherheitserdungen fest untereinander verbunden sind.

- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetz werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedieningspersonal durchgeführt werden.

Considerazioni sulla sicurezza

Questo prodotte è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;

- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Consideraciones sobre seguridad

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentacíon eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.

- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Appendix A: Specifications

Below are the key hardware specifications for Clavister SG4500 Series installation.

Dimensions, Weight and MTBF

Height x Width x Depth (mm)	44 x 440 x 500
Hardware Weight	9.0 kg
Hardware Form Factor	1U
19 inch Rack Mountable	Yes
MTBF	1 x PSU: 124,708 hours 2 x PSU: 324,491 hours

Regulatory and Safety Standards

Safety	UL, CE
EMC	FCC class A, CE class A, VCCI class A

Environmental

Humidity	20% to 95% noncondensing
Operational Temperature	0 to 45° C
Vibration	0.41 Grms2 (3-500 Hz)
Shock	30 G

Power Specifications

Power Supply (AC)	100-240V, 47-63 Hz
Typical Consumption (W)	1 x PSU: 101 W 2 x PSU: 127 W
BTU	1 x PSU: 345 BTU 2 x PSU: 434 BTU
PSU Rated Power (W)	275 W per installed PSU

Further information

For complete product specifications refer to: *http://www.clavister.com*

Appendix B: Declarations of Conformity

CE
DECLARATION OF CONFORMITY

We, the manufacturer,
Clavister AB
Sjögatan 6J
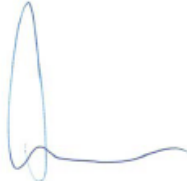SE-891 60 ÖRNSKÖLDSVIK
SWEDEN

Declares that the product
Product Description   : Network security appliance
Model Designation   : Clavister Security Gateway 4500 Series

Is in compliance with the essential requirements and other relevant provisions of the following directives:
Electromagnetic Compatibility Directive   (2004/108/EC)

The product is compatible with the following norms / standards:

EN 55022	(2006 Class A)
EN 61000-3-2	(2006)
EN 61000-3-3	(1995, A1:2001, A2:2005)
EN 55024	(1998, A1:2001, A2:2003)
IEC 61000-4-2	(1995, A2:2000)
IEC 61000-4-3	(2002)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(1995, A1:2000)
IEC 61000-4-6	(1996, A1:2000)
IEC 61000-4-8	(1993, A1:2000)
IEC 61000-4-11	(1994, A1:2000)
AS/NZS CISPR 22	(2006 Class A)

Manufacturer/Authorised representative

Peter Johansson, CEO
Örnsköldsvik, 2010-10-01

Certificate No.:   CLA-APP-SG4500-CEDOC-A001

CLAVISTER.

DECLARATION OF CONFORMITY

We, the manufacturer,
　　　　Clavister AB
　　　　Sjögatan 6J
　　　　SE-891 60 ÖRNSKÖLDSVIK
　　　　SWEDEN

Declares that the product
　　　　Product Description　　　　: Network security appliance
　　　　Model Designation　　　　: Clavister Security Gateway 4500 Series

Is in compliance with the essential requirements and other relevant provisions of the following:
　　　　FCC CFR Title 47 Part 15 Subpart B　　　　Federal Communication Commission
　　　　　　　　　　　　　　　　　　　　　　　　Code of Federal Regulations
　　　　　　　　　　　　　　　　　　　　　　　　Telecommunications, Radio frequency devices,
　　　　　　　　　　　　　　　　　　　　　　　　unintentional radiators

　　　　Canadian Standards Association　　　　Spectrum Management and
　　　　Standard ICES-003　　　　　　　　　　 Telecommunications Policy Interference-
　　　　　　　　　　　　　　　　　　　　　　　　Causing Equipment Standard, Digital Apparatus

The product is compatible with the following norms / standards:
　　　　FCC CFR Title 47 Part 15 Subpart B Class A
　　　　CSA ICES-003

Manufacturer/Authorised representative

Peter Johansson, CEO
Örnsköldsvik, 2010-10-01

Appendix C: Vista IP Setup

If a PC running Microsoft Vista is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

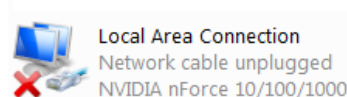The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Vista are as follows:

1. Press the Windows **Start** button.

2. Select the **Control Panel** from the start menu.

3. Select **Network & Sharing Center** from the control panel.

Network and Sharing Center
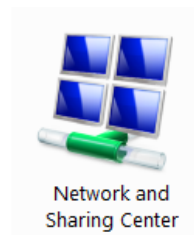
4. Select the **Manage network connections** option.
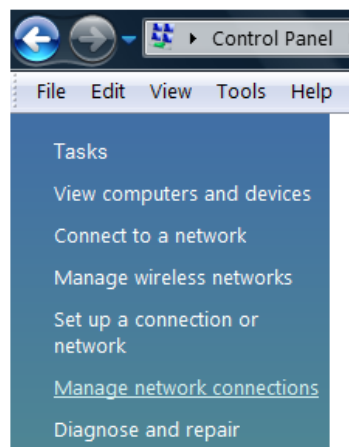
5. A list of the Ethernet interface connections will appear. Select the interface that will connect to the security gateway.
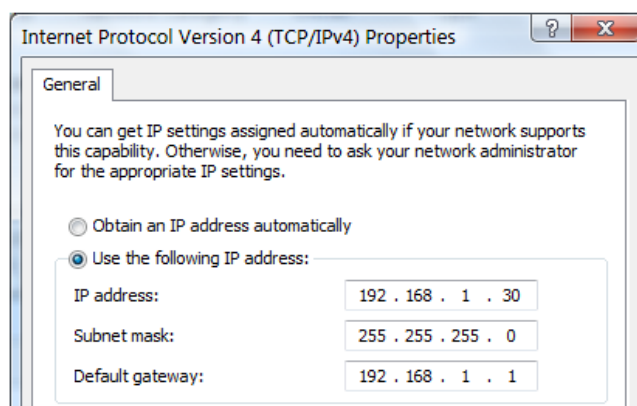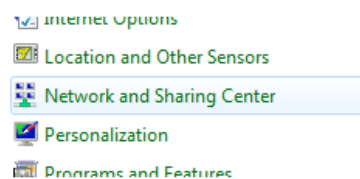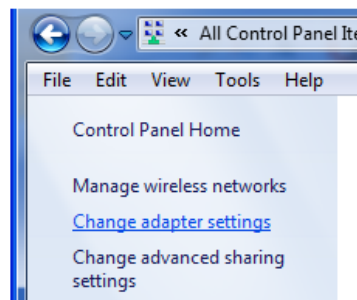

6. The properties for the selected interface will appear.

Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4).*

7.   In the properties dialog, select the option **Use the following IP address** and enter the following values:

   •   **IP Address:** *192.168.1.30*

   •   **Subnet mask:** *255.255.255.0*

   •   **Default gateway:** *192.168.1.1*

DNS addresses can be entered later once Internet access is established.

8.   Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

82

Appendix D: Windows 7 IP Setup

If a PC running Microsoft Windows 7 is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Windows 7 are as follows:

1. Press the Windows **Start** button.

2. Select the **Control Panel** from the start menu.

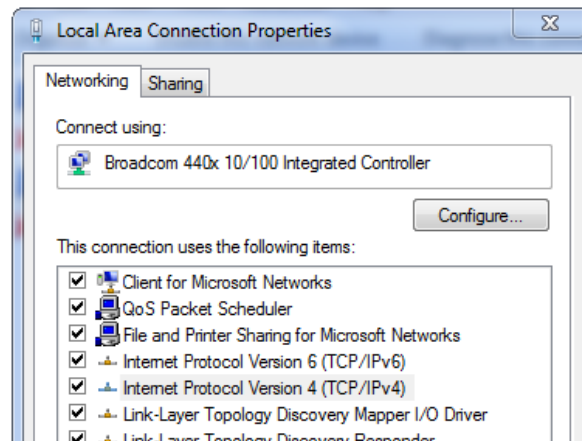3. Select **Network & Sharing Center** from the control panel.

4. Select the **Change adapter settings** option.

5. A list of adapters will appear and will include the Ethernet interfaces. Select the interface that will connect to the security gateway.
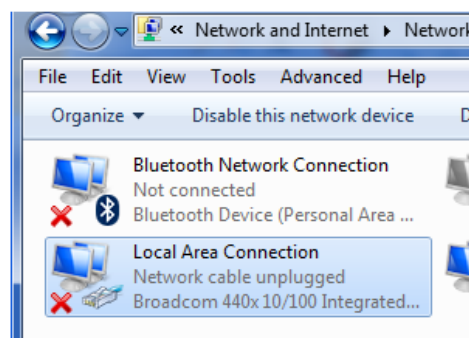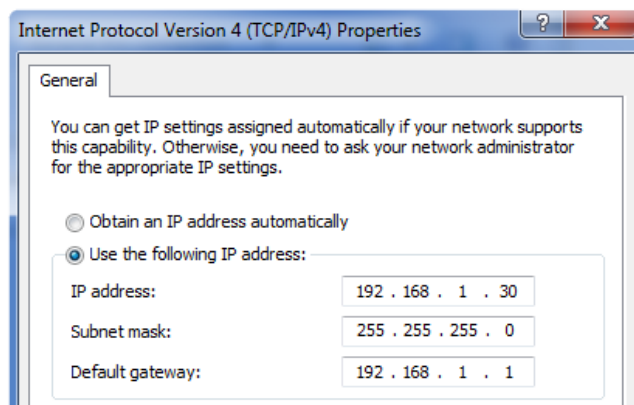

6. The properties for the selected interface will appear.

Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4)*.

7. In the properties dialog, select the option **Use the following IP address** and enter the following values:

    *   **IP Address:** *192.168.1.30*

    *   **Subnet mask:** *255.255.255.0*

    *   **Default gateway:** *192.168.1.1*

DNS addresses can be entered later once Internet access is established.

8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

Appendix E: Apple Mac IP Setup

An Apple Mac can be used as the management workstation for initial setup of a Clavister Security Gateway. To do this, a selected Ethernet interface on the Mac must be configured correctly with a static IP. The setup steps for this with Mac OS X are:

1. Go to the **Apple Menu** and select **System Preferences**.
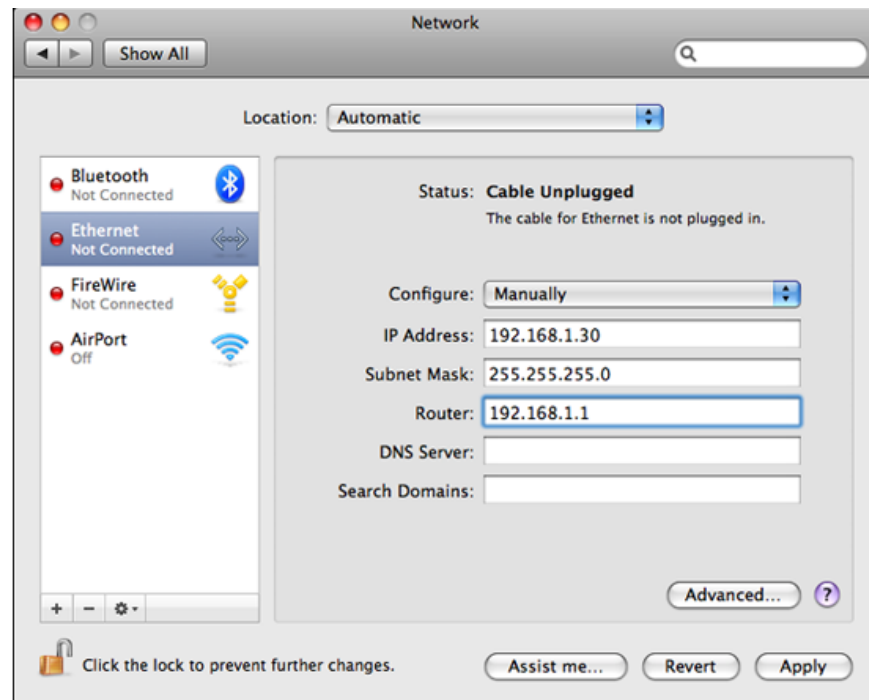
2. Click on **Network**.

3. Select **Ethernet** from the left sidebar menu.

4. Select **Manually** in the **Configure** pull down menu.
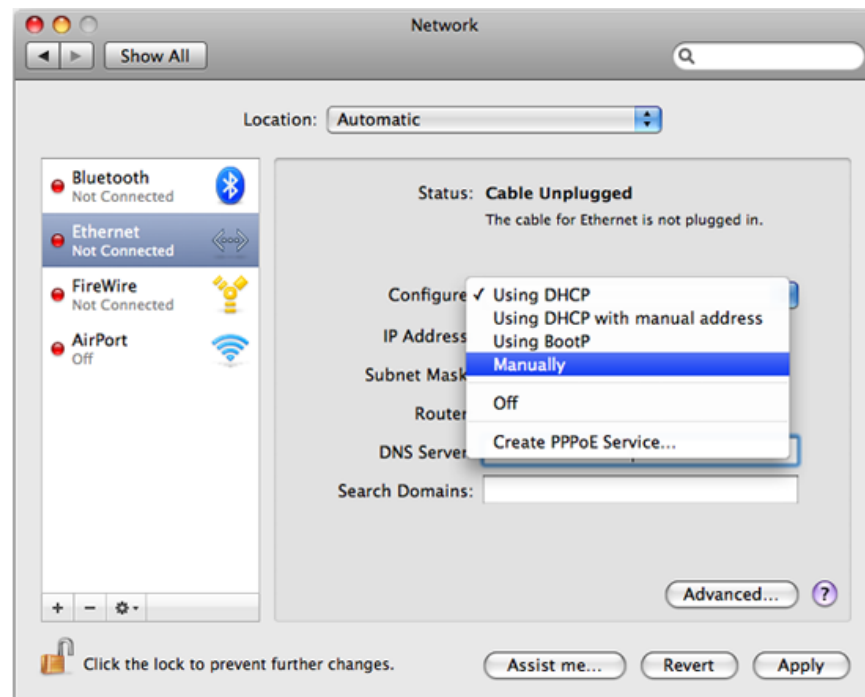
5.   Now set the following values:

   •   **IP Address:** *192.168.1.30*

   •   **Subnet Mask:** *255.255.255.0*

   •   **Router:** *192.168.1.1*

6.   Click **Apply** to complete the static IP setup.

86

CLAVISTER