Clavister VMware VSG Series Getting Started Guide

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Published 2010-03-15

Clavister VMware VSG Series
Getting Started Guide

Published 2010-03-15

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. Clavister makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Clavister reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

List of Figures

Preface

Target Audience

The target audience for this guide is the administrator who wants to run the CorePlus network operating system under a VMware hypervisor. The guide takes the user from the installation of CorePlus through to start up of the software, including network connections and initial CorePlus configuration. The product name for CorePlus under VMware is the Clavister *Virtual Security Gateway* (VSG) Series.

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.

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 3.5, "Troubleshooting Setup"*.

Web links

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

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the 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.

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.

Chapter 1: Overview

CorePlus with VMware

By using the VMware product suite, it is possible to have a single computer running multiple, virtual Clavister Security Gateways with each virtual Clavister Security Gateway running a separate copy of CorePlus. This technique is referred to as *virtualization* and each virtual Clavister Security Gateway can be said to be running under a *VMware host* in its own *virtual machine*. This is the basis for the Clavister *Virtual Security Gateway* (VSG) product series.

Not only can CorePlus run in its own virtual machine under VMware, the management workstation that is used to administer CorePlus can also run under the same VMware installation. This workstation might be running InControl, the Web Interface or a CLI console through a secure shell client.

Referencing VMware Documentation

This guide describes the steps involved when installing CorePlus with VMware on x86 hardware as well as covering many of the issues that may be encountered with CorePlus running in a VMware virtual environment.

The guide tries to deal specifically with the subject of CorePlus running under VMware and unless relevant, does not detail the installation of VMware itself or issues which are related only to VMware. Pure VMware subjects are best explained by VMware's own, comprehensive product documentation which can be found at *http://www.vmware.com*.

Supported VMware Servers

CorePlus can run under the following VMware products for x86 hardware:

- VMware Server (the "classic" server).
- VMware ESXi Server.

The CorePlus installation files for these servers can be downloaded from the Clavister *Customer Web* which can be found at *https://clientweb.clavister.com*. These files are also available for download from the VMware virtual appliance web page at *http://www.vmware.com/appliances*.

Chapter 2: CorePlus Installation

As described in *Chapter 1, Overview*, the CorePlus installation files for VMware can be downloaded from the Clavister *Customer Web* or from the VMware virtual appliance web page.

CorePlus Installation with the VMware Server

The steps for CorePlus installation with the "classic" server and ESX are:

1. Unzip the Clavister distribution packet.
2. In VMware, go to **File > Open** and open the file *Other.vmx* from the unzipped packet.
3. Start the virtual machine.
4. When you receive the question "**Do you wish to create a new unique identifier**", answer using the **Create** option.

CorePlus Installation with the ESXi Server

The steps for CorePlus installation with the ESXi server are:

1. Unzip the Clavister distribution packet.
2. In the VMware infrastructure client, go to **File > Virtual Appliance > Import** and import the *.ovf* file from the unzipped packet.
3. Now complete the setup wizard with the appropriate settings. The virtual interfaces selected will be matched with the default interfaces defined in CorePlus. Extra virtual interfaces can be added later and can be used if the license allows them.
4. After the wizard completes, power on the ESXi virtual machine.

The VMware Console

When CorePlus starts, VMware will display a console which represents the console that is normally directly connected to the serial RS-232 port of a physical Clavister Security Gateway.

This console displays output from CorePlus exactly as it would be displayed with a non-virtual Clavister Security Gateway. It will show the initial startup sequence output and this can be interrupted, if required, by key presses to enter the boot menu. After startup, the VMware console can be used to issue CLI commands commands to configure CorePlus further.

Changing focus to the VMware console

VMware will keep focus in the console window after clicking it. Use the key combination ***Ctrl-Alt*** *to release focus.*

The Default Virtual Ethernet Interfaces

The standard CorePlus installation provides a number of virtual Ethernet interfaces. These act like E1000 NICs and can be connected to a physical Ethernet interface using the VMware *Bridged* option or to another virtual machine in the same host with the *Custom* option.

CorePlus assigns the following default names to the virtual interfaces:

- Interface names: *Ifn*. For example, the first interface is *If1*.
- IP address objects: *Ifn_ip*. For example, the first address object is *If1_ip*.
- Netmask IP objects: *Ifn_net*. For example, the first netmask is *If1_net*.

Connecting to the Virtual Clavister Security Gateway

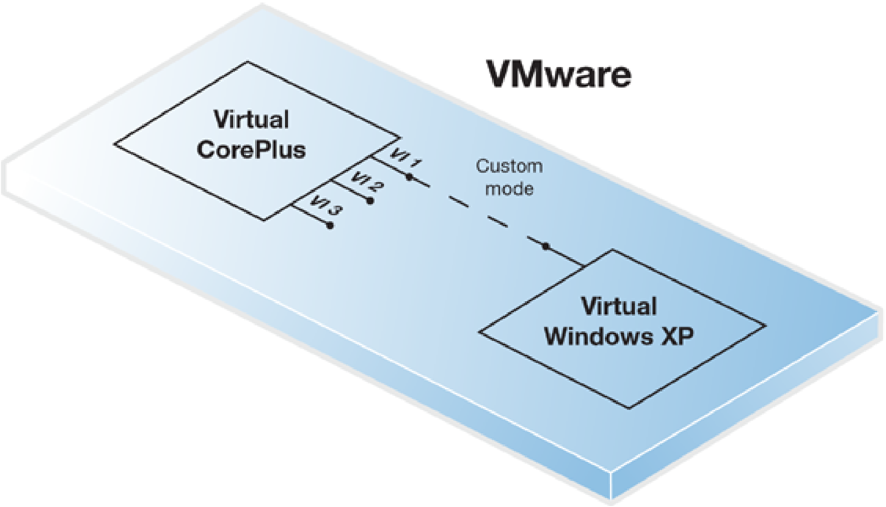
The first virtual Ethernet interface, *If1*, will be assigned the IP address *192.168.1.1* by CorePlus. This is the default CorePlus management interface and connection to it can be done from a web browser (using the CorePlus Web Interface) or SSH client (using the CorePlus CLI) just as it is done with a non-VMware installation.

The workstation running the web browser or SSH client can be one of the following:

- **A virtual workstation running under the same VMware host.**

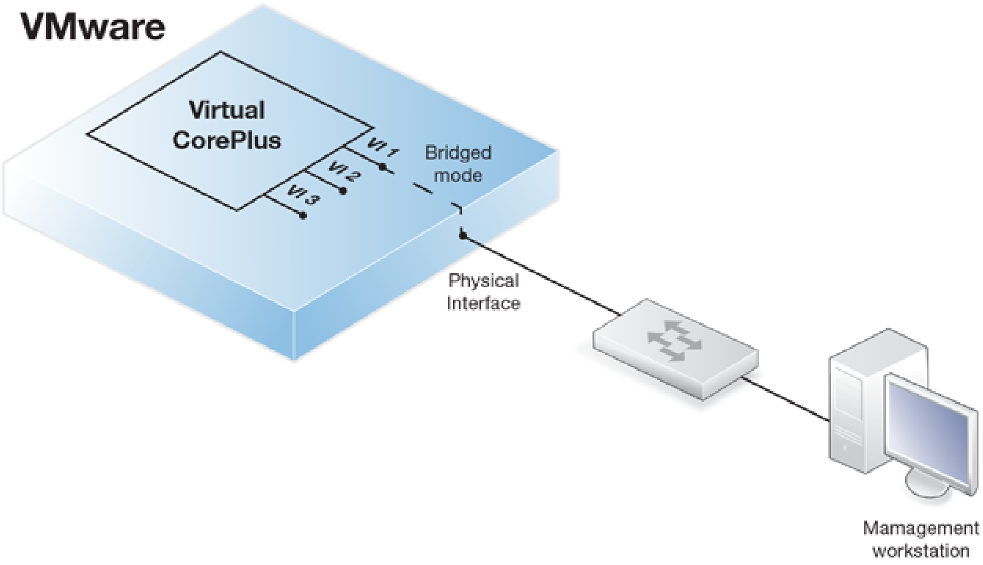
  In this case, the VMware *Custom* (not bridged) option can be used to connect the virtual Ethernet interface with a virtual Ethernet interface on the virtual workstation. The virtual workstation might be, for example, a Windows XP installation as shown below.

  For this option to function, VMware must be configured so that the virtual Ethernet interface on both CorePlus and the workstation are on the same virtual network.



- **A physically separate workstation computer.**

  In this case, VMware's *Bridged* mode should be used to connect the virtual Ethernet interface to a physical interface. Physical connection is then made between the physical interface and an interface on a physically separate workstation computer.



In both the above cases, the real or virtual workstation PC needs its connecting Ethernet interface configured with an IP address on the same network as the CorePlus interface. Once this is done, the management workstation and the Clavister Security Gateway can communicate and initial CorePlus setup can then be performed in exactly the same way as a non-virtual security gateway. This is described next in *Chapter 3, Configuring CorePlus*.

Setup with Multiple Virtual Clavister Security Gateways

When there are multiple virtual machines running CorePlus under one VMware host, the IP address of the management virtual Ethernet interface must be different for the different virtual machines if administration is to be done through the Web Interface or SSL client.

The recommended way to change the management interface IP address is to use the CorePlus console which is displayed by VMware after CorePlus starts. The CLI commands to do this are as follows:

1. Set the IP address of the default management interface *If1_ip*. In this example, it will be set to *10.0.0.1*:

   ```
   Device:/> set Address IP4Address If1_ip Address=10.0.0.1
   ```

2. Now set the network of the interface. This object has the name *If1_net*.

   ```
   Device:/> set Address IP4Address If1_net Address=10.0.0.0/24
   ```

3. As a check, the current management rule for HTTP access can be displayed:

   ```
   Device:/> show RemoteManagement RemoteMgmtHTTP
   ```

These steps should then be followed by an *activate* and then a *commit* command to deploy the changes.

These same steps could be performed through the Web Interface but as soon as the changes are committed, the administrator has 30 seconds to log back in to CorePlus before the changes are undone and CorePlus reverts to the previous configuration.

Generating a Unique *DeviceID*

The ready-to-run VMware virtual machine image provided by Clavister always has the same *DeviceID* and this causes problems for the InControl management client. The current ID can be displayed with the CLI command:

```
Device:/> show Device

         Property  Value                                 Remarks
 ----------------  ------------------------------------  ---------
             Name: Device
    ConfigVersion: 21                                    Read-only
       ConfigUser: admin                                 Read-only
    ConfigSession: WebUI                                 Read-only
         ConfigIP: 192.168.1.2                           Read-only
       ConfigDate: 2009-02-30 15:25:56                   Read-only
         DeviceID: 22b685f1-72e0-4124-b2a9-4c3d82834ae3  Read-only
          HWModel: SOFTWARE                              Read-only
  RegistrationKey: <empty>                               Read-only
   ProductionDate: <empty>                               Read-only
         HWSerial: <empty>                               Read-only
         Comments: <empty>
```

To generate a unique *DeviceID* for a virtual security gateway, the security gateways boot menu should be entered and the option to *Reset to base configuration* should be selected. This will generate a new ID. This should obviously be done as soon as a new virtual security gateway is created as any existing configuration will be lost.

Chapter 3: Configuring CorePlus

3.1. Management Workstation Connection

The Default Management Interface

After first time startup, CorePlus scans the available Ethernet interfaces and makes management access available on the first interface found and assigns the internal IP address *192.168.1.1* to it.

For a VMware installation, this is the *If1* 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 CorePlus interface using a similar connection to that used with the Web Interface. Alternatively, CLI access can be direct, through the VMware console window.

Network Connection Setup

For setup using the Web Interface or using remote CLI, we must first connect a workstation to CorePlus across a network. This workstation connection is already described previously in *Chapter 2, CorePlus Installation*.

The CorePlus management interface with VMware is *If1* and this should be connected to the same network as the management workstation (or a network accessible from the workstation via one or more routers). Typically the connection is made via a switch or hub in the network using a regular straight-through Ethernet cable. For connection to the public Internet, one of the other interfaces should be connected to your ISP and this is referred to below and in the setup wizard as the *WAN* interface.

Workstation Interface Setup

Traffic is 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 must be first assigned the following static IP addresses:

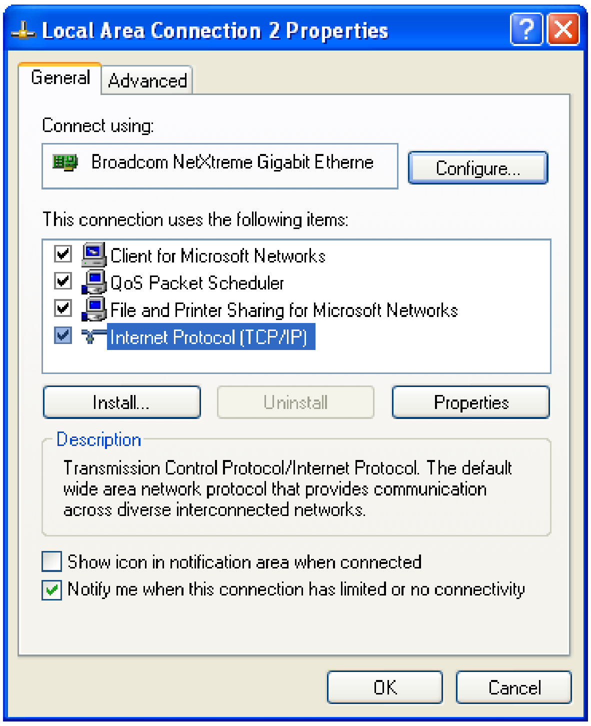
- **IP address:** *192.168.1.30*
- **Subnet mask:** *255.255.255.0*
- **Default gateway:** *192.168.1.1*

Tip
*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.*

To enter these settings on a PC running Windows XP, 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**.



Local Area Connection 2 Properties

General | Advanced

Connect using:

Broadcom NetXtreme Gigabit Etherne

This connection uses the following items:

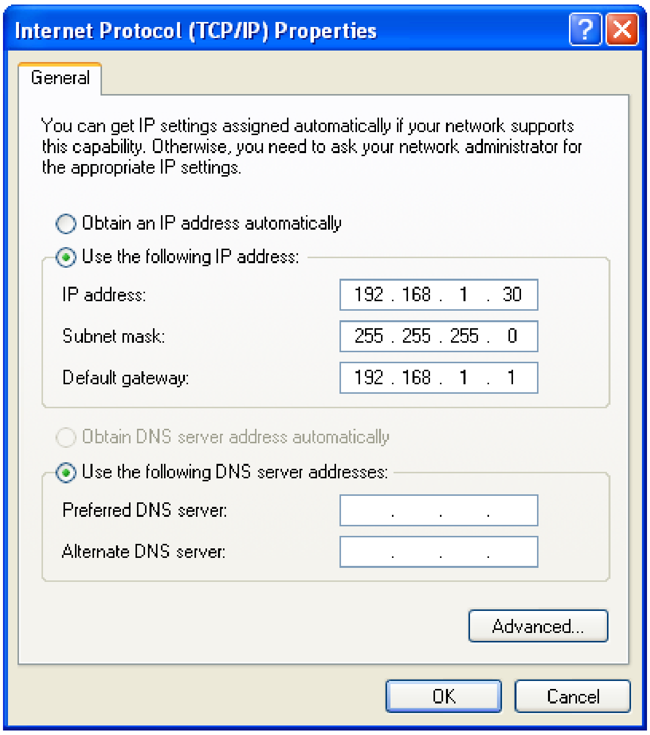
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

- Enter the IP addresses given above and click **OK**.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 30
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

IP Setup on Other Platforms

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

- ***Appendix A, Vista IP Setup***.

- ***Appendix B, Windows 7 IP Setup***.
- ***Appendix C, Apple Mac IP Setup***.

3.2. Web Interface and Wizard Setup

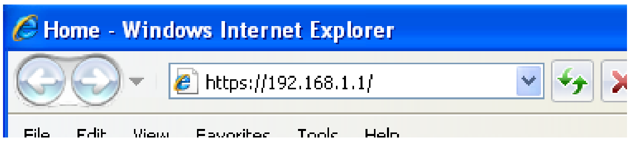
This chapter describes the setup when accessing CorePlus for the first time through a web browser. The user interface accessed in this way is called the Web Interface (also known as the WebUI).

Note

Many of the screenshots in this chapter have had whitespace removed from the original image to improve the readability. However, all of the informational content in the images has been preserved.

Connect By Surfing to *https://192.168.1.1*

Using a web browser (Internet Explorer or Firefox is recommended) enter the address *https://192.168.1.1* into the navigation window as shown below.



Check for a proxy server and turn off popup blocking.

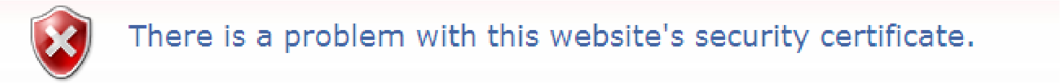
Make sure the web browser doesn't have a proxy server configured.

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 3.5, "Troubleshooting Setup"*.

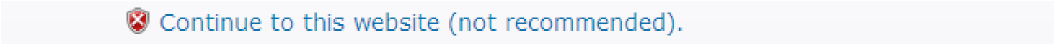
The CorePlus Self-signed Certificate

When responding to an *https://* request, CorePlus sends a self-signed certificate which will not be initially recognised 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.



There is a problem with this website's security certificate.

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

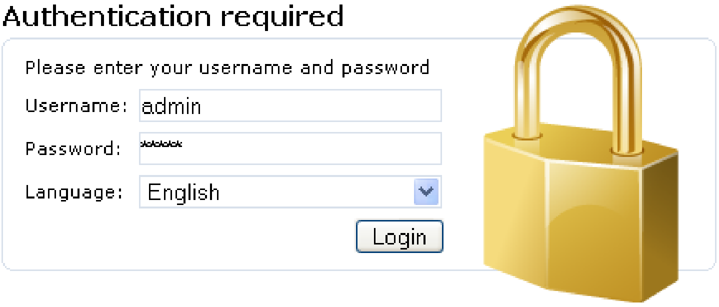


Continue to this website (not recommended).

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.



Authentication required

Please enter your username and password

Username: admin

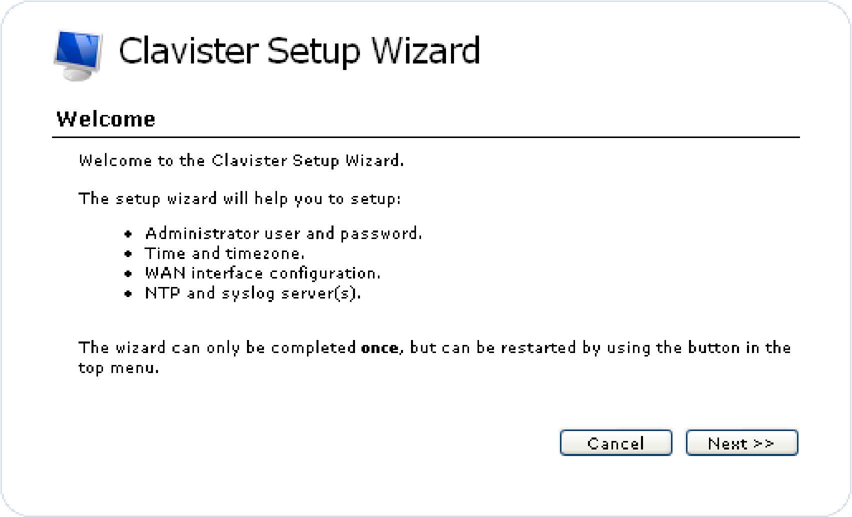
Password: *****

Language: English

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.



Clavister Setup Wizard

Welcome

Welcome to the Clavister Setup Wizard.

The setup wizard will help you to setup:

- Administrator user and password.
- Time and timezone.
- WAN interface configuration.
- NTP and syslog server(s).

The wizard can only be completed **once**, but can be restarted by using the button in the top menu.

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.

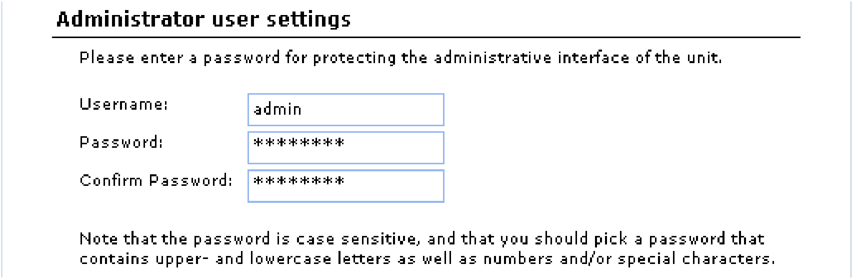
Advantages of the Wizard

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

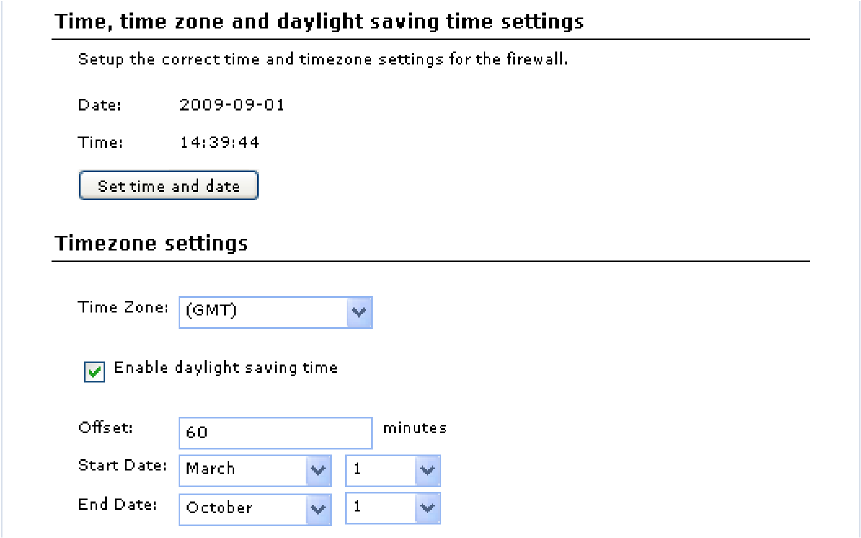
Please enter a password for protecting the administrative interface of the unit.

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

Timezone settings

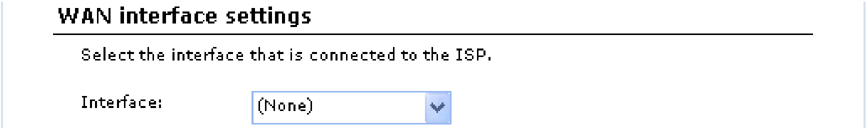
Time Zone: (GMT)

☑ 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.



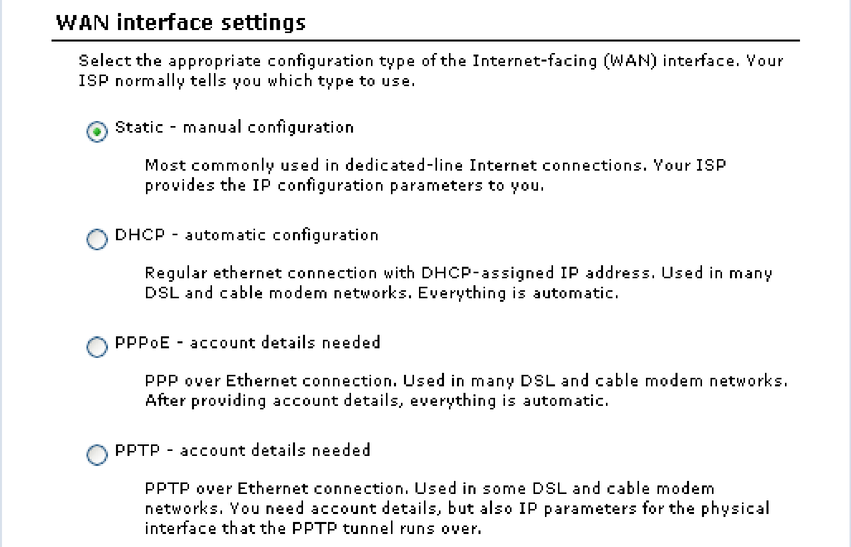
WAN interface settings

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.



WAN interface settings

Select the appropriate configuration type of the Internet-facing (WAN) interface. Your ISP normally tells you which type to use.

● Static - manual configuration

Most commonly used in dedicated-line Internet connections. Your ISP provides the IP configuration parameters to you.

○ DHCP - automatic configuration

Regular ethernet connection with DHCP-assigned IP address. Used in many DSL and cable modem networks. Everything is automatic.

○ PPPoE - account details needed

PPP over Ethernet connection. Used in many DSL and cable modem networks. After providing account details, everything is automatic.

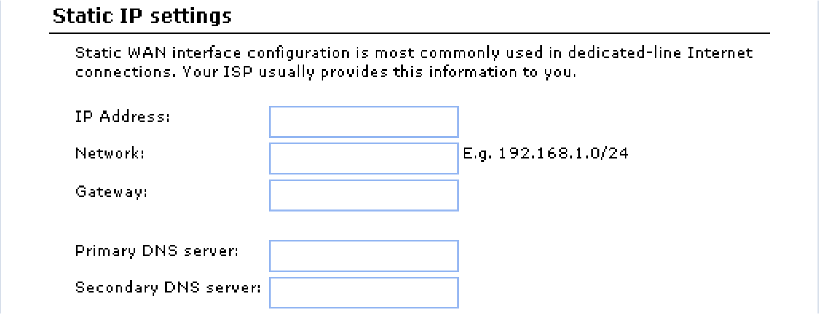
○ PPTP - account details needed

PPTP over Ethernet connection. Used in some DSL and cable modem networks. You need account details, but also IP parameters for the physical interface that the PPTP tunnel runs over.

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.



Static IP settings

Static WAN interface configuration is most commonly used in dedicated-line Internet connections. Your ISP usually provides this information to you.

IP Address:

Network: E.g. 192.168.1.0/24

Gateway:

Primary DNS server:

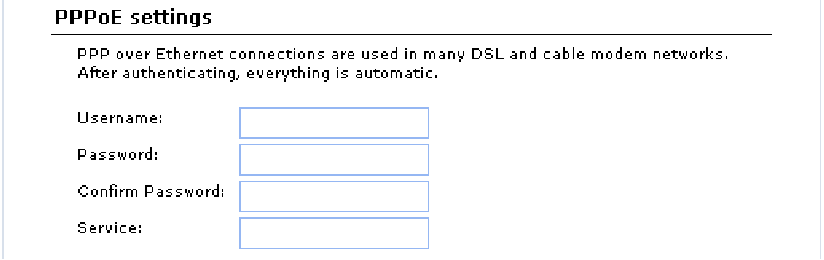
Secondary DNS server:

- **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

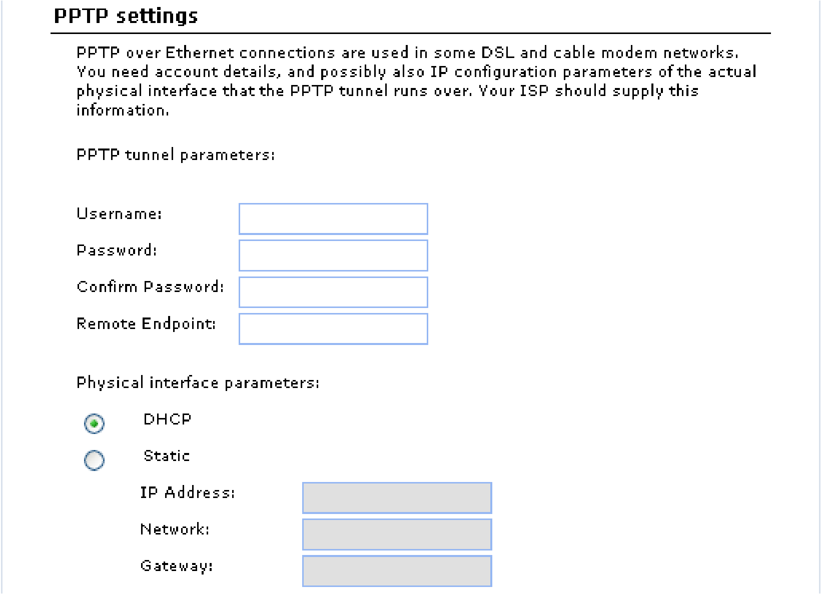
PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.

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

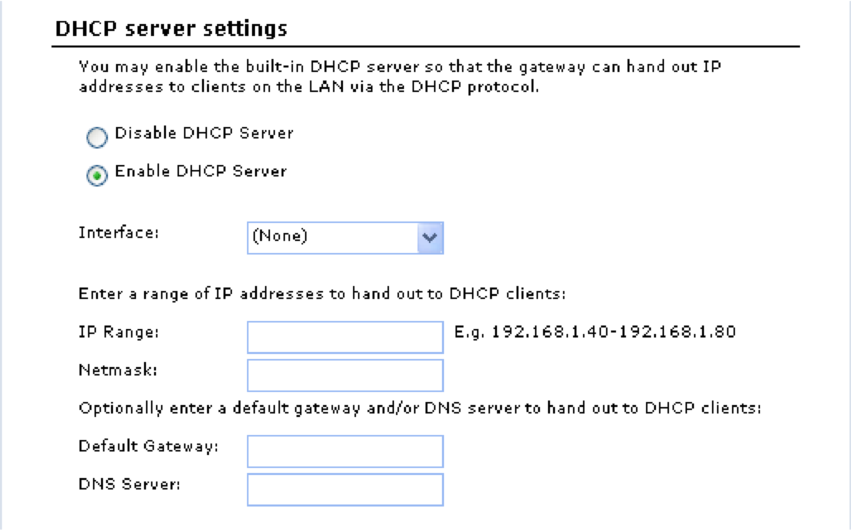
IP Address:	
Network:	
Gateway:	

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 *nn.nn.nn.nn - nn.nn.nn.nn*. For instance, the internal IP address range *192.168.1.50 - 192.168.1.150* might be specified.



DHCP server settings

You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.

○ Disable DHCP Server

● Enable DHCP Server

Interface: (None)

Enter a range of IP addresses to hand out to DHCP clients:

IP Range: E.g. 192.168.1.40-192.168.1.80

Netmask:

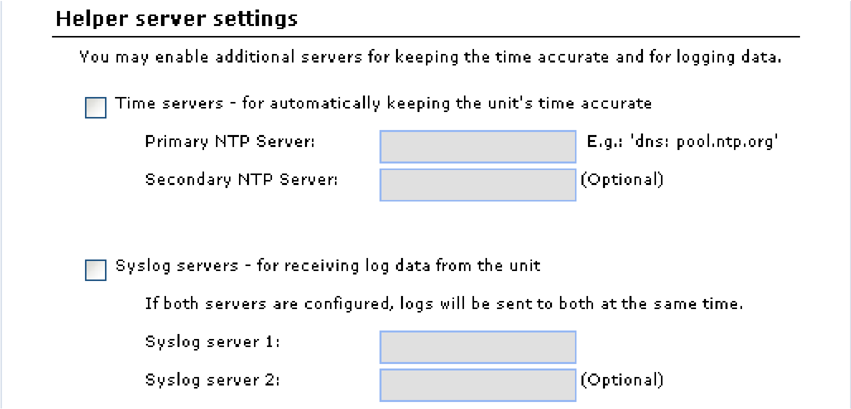
Optionally enter a default gateway and/or DNS server to hand out to DHCP clients:

Default Gateway:

DNS Server:

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.



Helper server settings

You may enable additional servers for keeping the time accurate and for logging data.

□ Time servers - for automatically keeping the unit's time accurate

Primary NTP Server: E.g.: 'dns: pool.ntp.org'

Secondary NTP Server: (Optional)

□ Syslog servers - for receiving log data from the unit

If both servers are configured, logs will be sent to both at the same time.

Syslog server 1:

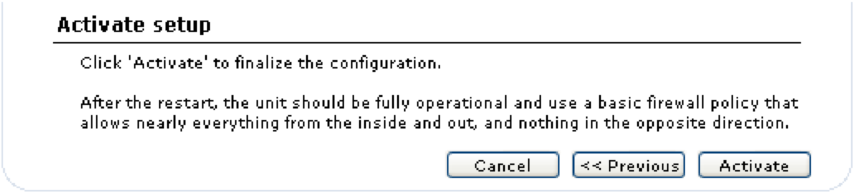
Syslog server 2: (Optional)

For the default gateway, it is recommended to specify the IP address *192.168.1.1* and 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.



Activate setup

Click 'Activate' to finalize the configuration.

After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.

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 unit 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 discussed in *Chapter 4, Licensing*.

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.

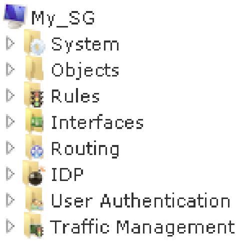
Ethernet Interfaces

The physical connection of external networks to the Clavister Security Gateway is through the various *Ethernet interfaces* which are provided by the hardware platform. With VMware, these are the *virtual interfaces* provided by the hypervisor. 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 CorePlus under VMware, the virtual *If1* interface is always the management interface. Assuming the normal VMware total of 3 virtual interfaces, the other two virtual interfaces will automatically be given the names *If2* and *If3* by CorePlus. For this section, we will assume that the *If2* interface will be used for connection to the public Internet and the *If3* interface will be used for connection to a protected, local network.

The Navigation Tree

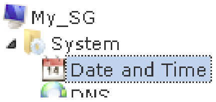
The Web Interface presents the various components of CorePlus in a tree structure in the left-hand pane of the browser window.



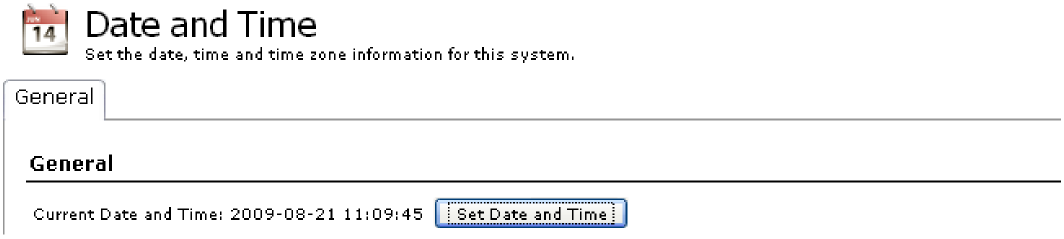
By clicking on the navigation tree we can expand its nodes to examine and change the properties of the various *settings*, *objects* and *rules* that make up a CorePlus configuration. A simple example of changing a configuration is discussed next.

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly. Even when running under VMware, each virtual security gateway maintains its own date and time and it is still important that this is set correctly for each gateway. 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.



Date and Time

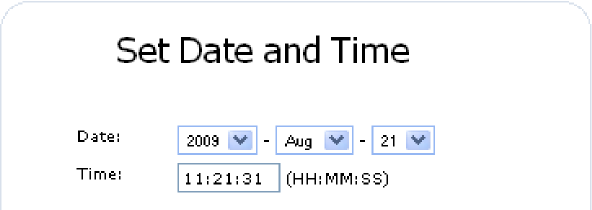
Set the date, time and time zone information for this system.

General

General

Current Date and Time: 2009-08-21 11:09:45

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

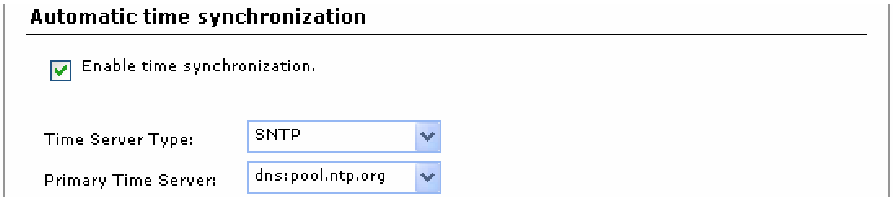


Set Date and Time

Date: 2009 - Aug - 21

Time: 11:21:31 (HH:MM:SS)

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.



Automatic time synchronization

☑ Enable time synchronization.

Time Server Type: SNTP

Primary Time Server: dns:pool.ntp.org

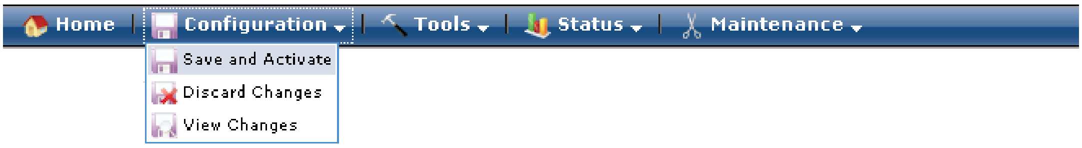
Note: The time server URL requires the "dns:" prefix

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

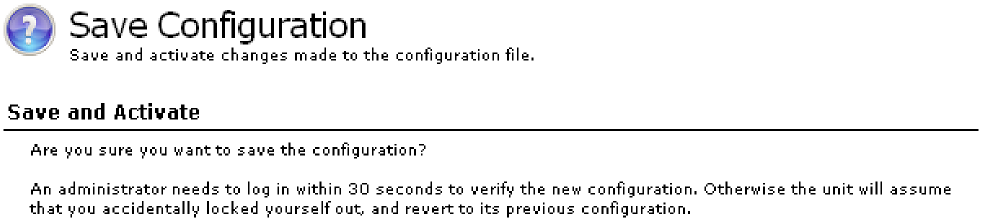
Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in CorePlus configuration. Although changed values like this are saved by CorePlus, they do not become active until the entire saved configuration becomes the current and active configuration.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



Save Configuration

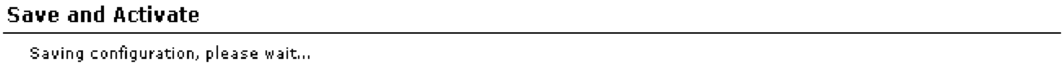
Save and activate changes made to the configuration file.

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.

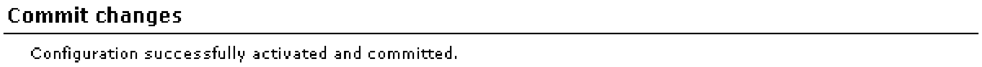
After clicking **OK**, CorePlus *reconfiguration* will take place and, after a short delay, the Web Interface will try and connect again to the security gateway.



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. It is, however, not advisable to leave changes uncommited 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

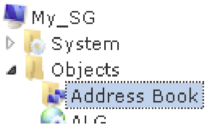
For static configuration of the Internet connection, the DHCP option must be disabled (the default) in the properties of the interface that will connect to the ISP.

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 *If2* 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.

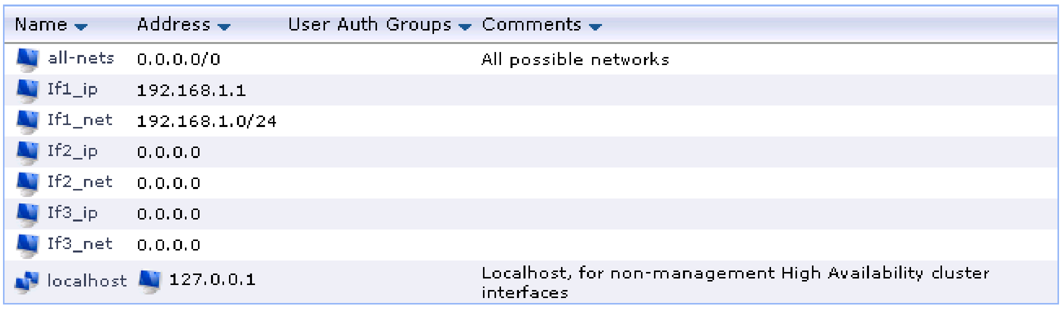
Let's now add the gateway *IP4 Address* object which we will call *wan_gw* and assign it the IP address *10.5.4.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Security Gateway. Go to **System > Objects > Address Book** in the Web Interface navigation tree.



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 VSG.

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.*



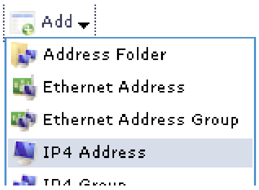
Name	Address	User Auth Groups	Comments
all-nets	0.0.0.0/0		All possible networks
If1_ip	192.168.1.1		
If1_net	192.168.1.0/24		
If2_ip	0.0.0.0		
If2_net	0.0.0.0		
If3_ip	0.0.0.0		
If3_net	0.0.0.0		
localhost	127.0.0.1		Localhost, for non-management High Availability cluster interfaces

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.

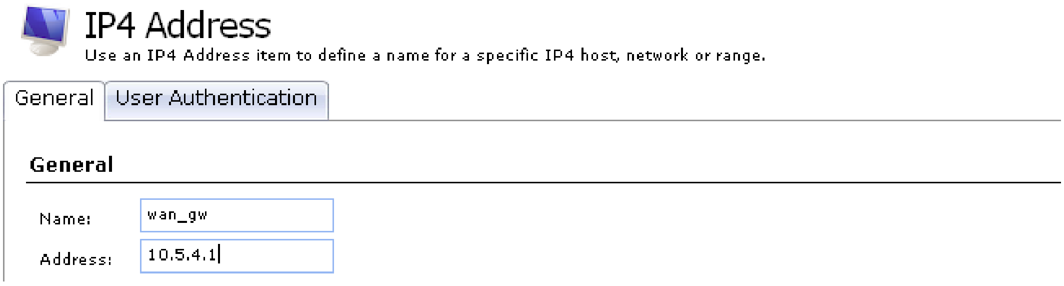
Tip: Creating address book folders

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.



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Name: wan_gw

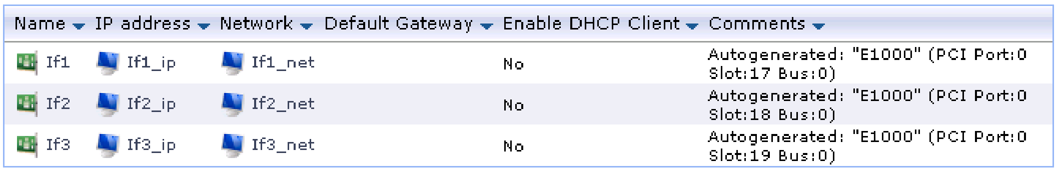
Address: 10.5.4.1

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

Then set up *If2_ip* to be *10.5.4.35*. This is the IP address of the *If2* interface which will connect to the ISP's gateway.

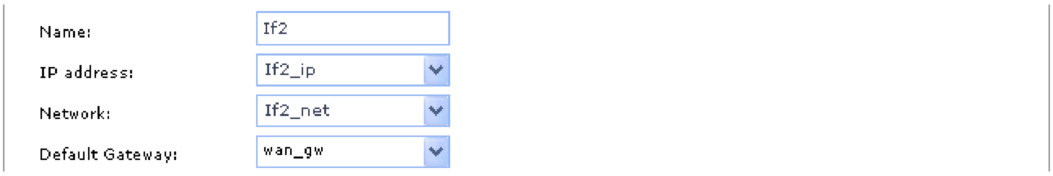
Lastly, set the IP4 Address object *If2_net* to be *10.5.4.0/24*. Both *If2_ip* and *wan_gw* must belong to this network in order for the interface to communicate with the ISP.

Together, these 3 IP address objects will be used to configure the interface connected to the Internet which in this example is *If2*. Select **Interfaces** > **Ethernet** in the navigation tree to display a list of the physical interfaces.



Name	IP address	Network	Default Gateway	Enable DHCP Client	Comments
If1	If1_ip	If1_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:17 Bus:0)
If2	If2_ip	If2_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:18 Bus:0)
If3	If3_ip	If3_net		No	Autogenerated: "E1000" (PCI Port:0 Slot:19 Bus:0)

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.



Name: If2

IP address: If2_ip

Network: If2_net

Default Gateway: wan_gw

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:

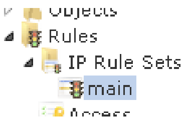
- An *IP rule* defined in a CorePlus *IP rule set* that explicitly allows traffic to flow from a given source network and source interface to a given destination network and destination interface.

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

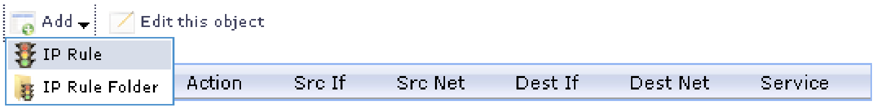
  If multiple matching routes are found, CorePlus uses the route that has the smallest (in other words, the narrowest) IP range.

We must therefore first define an IP rule that will allow traffic from a designated source interface and source network. In this case let us assume we want to allow web surfers on the internal network *If3_net* connected to the interface *If3* to be able to access the public Internet.

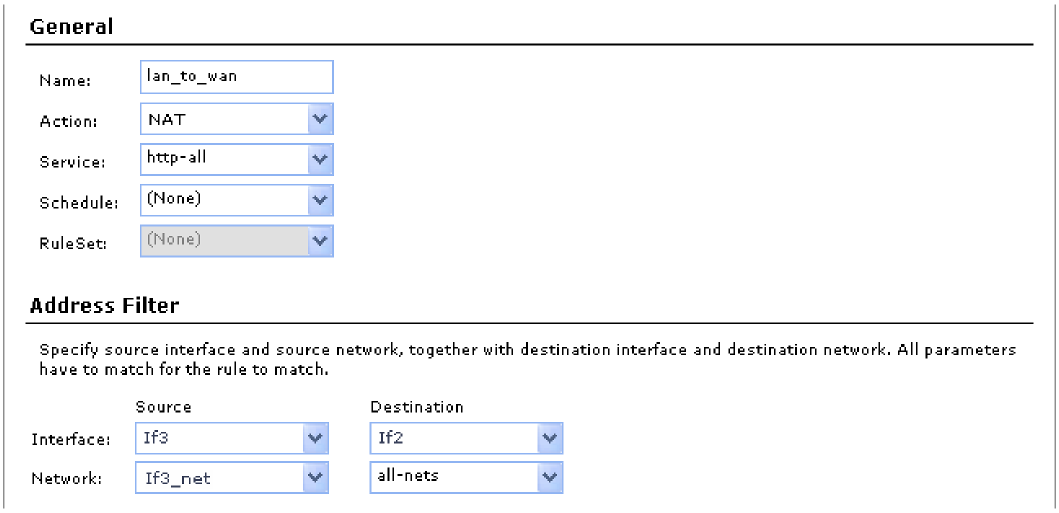
To do this, we first go to **Rules > IP Rule Sets > main** in the navigation tree.



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 surfing (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:	If3	If2
Network:	If3_net	all-nets

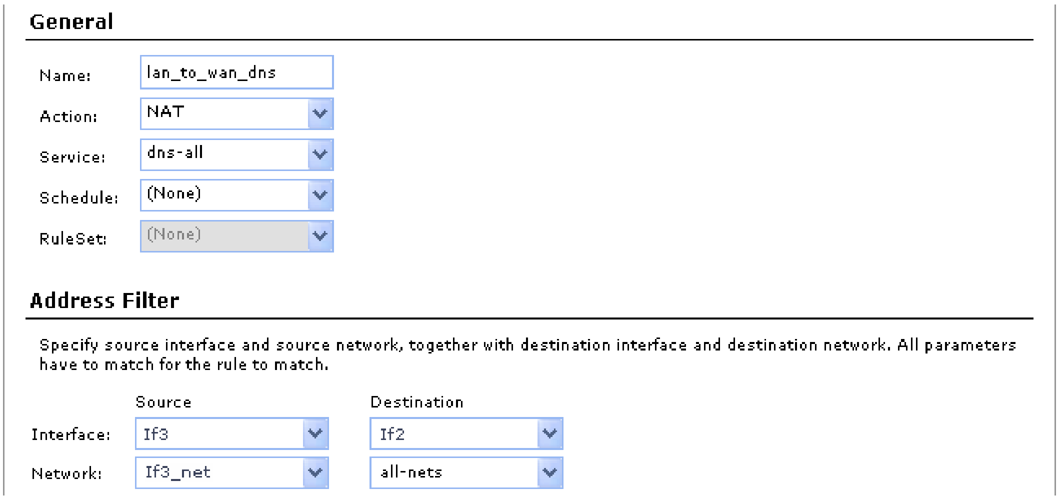
The destination network in the IP rule is specified as the predefined IP4 Address object *all-nets*. This is used since we don't know to which IP address the web surfing will be done and this allows surfing to any IP address. IP rules are processed in a top down fashion, with the first matching rule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



General

Name: lan_to_wan_dns

Action: NAT

Service: dns-all

Schedule: (None)

RuleSet: (None)

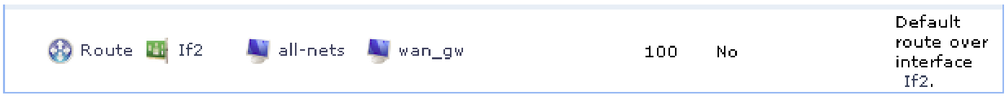
Address Filter

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:	If3	If2
Network:	If3_net	all-nets

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 surfing traffic should leave the Clavister Security Gateway. This route will define the interface where the network *all-nets* 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.



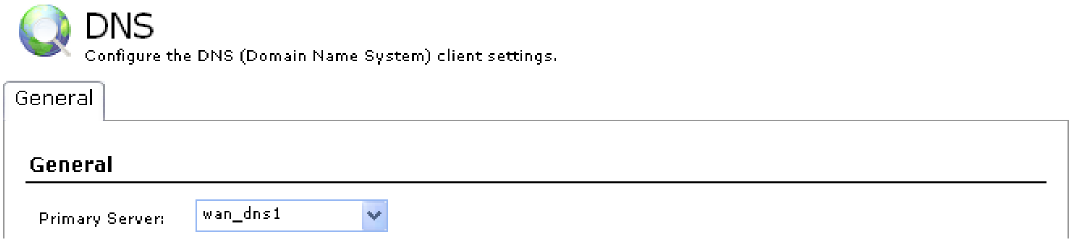
Route	If2	all-nets	wan_gw	100	No	Default route over interface If2.

This required *all-nets* route is, in fact, added automatically after specifing 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.



DNS

Configure the DNS (Domain Name System) client settings.

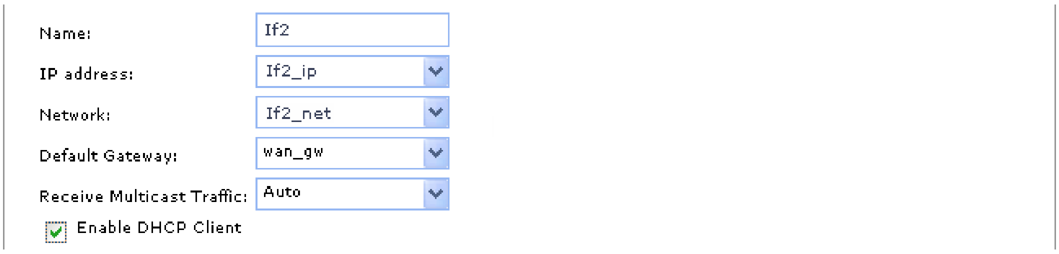
General

Primary Server: wan_dns1

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 *If2* interface in the list to display its properties.



Name: If2

IP address: If2_ip

Network: If2_net

Default Gateway: wan_gw

Receive Multicast Traffic: Auto

☑ Enable DHCP Client

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.

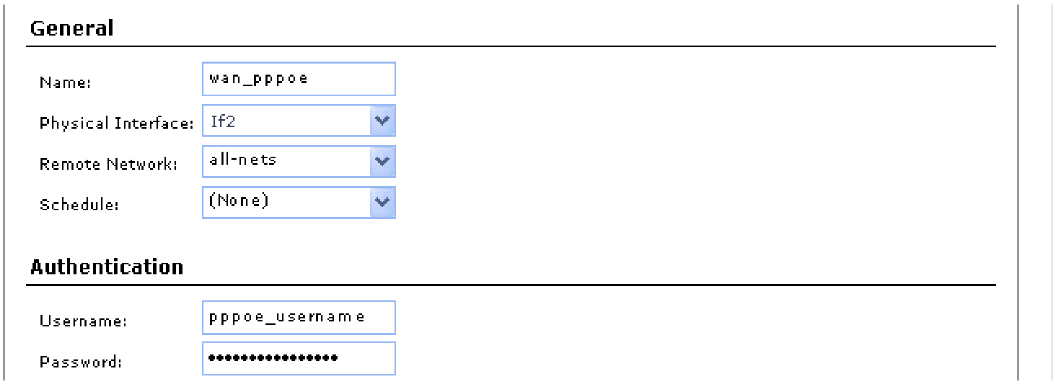
On connection to the ISP, all required IP addresses are retrieved automatically from the ISP via DHCP and CorePlus automatically sets the relevant address objects in the address book with this information.

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 *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface *If2*.

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 *If2* 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: If2

Remote Network: all-nets

Schedule: (None)

Authentication

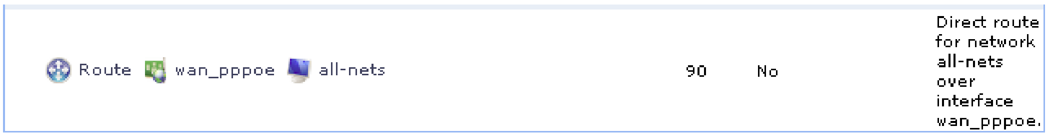
Username: pppoe_username

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



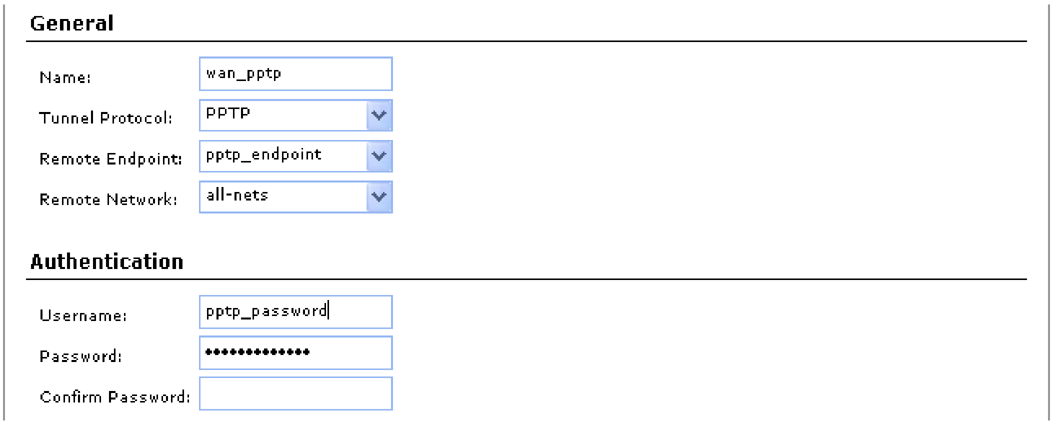
Route	wan_pppoe	all-nets	90	No	Direct route for network all-nets over interface wan_pppoe.

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 *If3_net* and interface *If3*) 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 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: ••••••••••••••

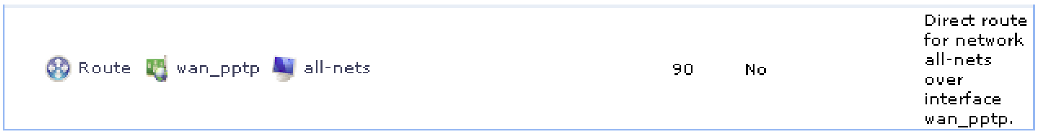
Confirm Password:

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.

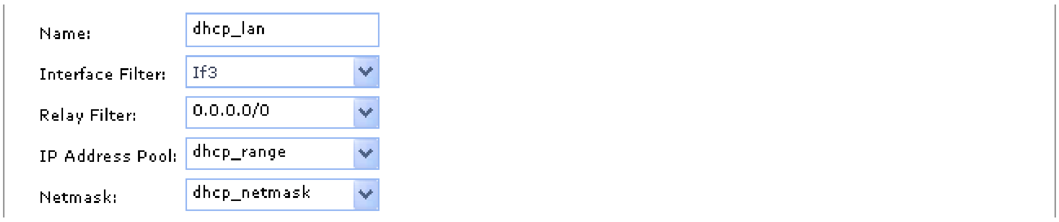
At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source network and source interface (in this example, the network *If3_net* and interface *If3*) 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 *If3* interface. To do this, go to **System** > **DHCP** > **DHCP Servers** and select **Add** > **DHCP Server**. We can now specify the server properties.



Name: dhcp_lan

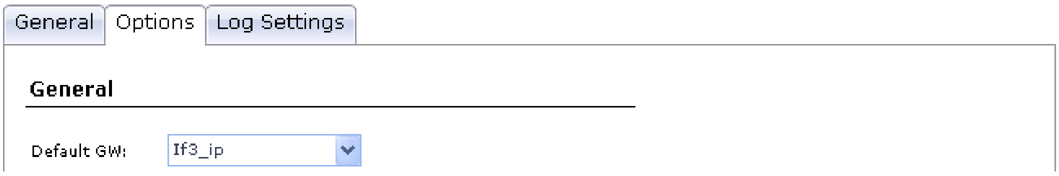
Interface Filter: If3

Relay Filter: 0.0.0.0/0

IP Address Pool: dhcp_range

Netmask: dhcp_netmask

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, *If3_ip*



General

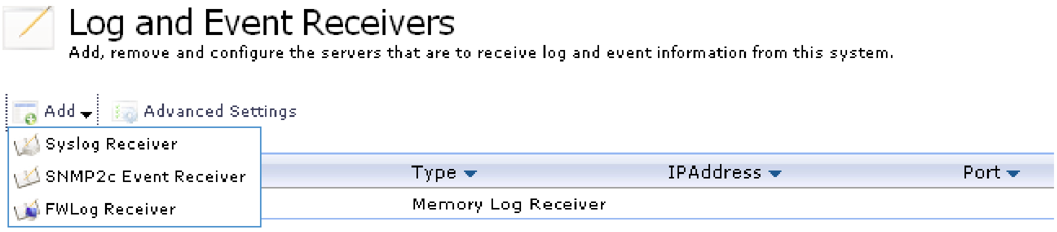
Default GW: If3_ip

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**.

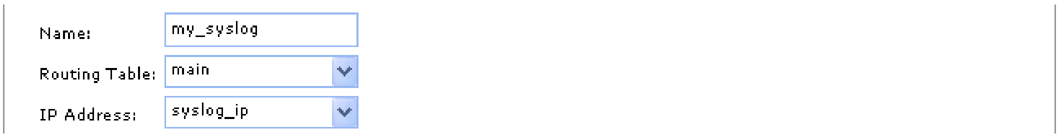


Log and Event Receivers

Add, remove and configure the servers that are to receive log and event information from this system.

Type	IPAddress	Port
Memory Log 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.



Name: my_syslog

Routing Table: main

IP Address: syslog_ip

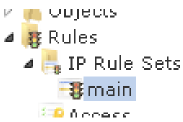
Tip: Address book object naming

*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**.*

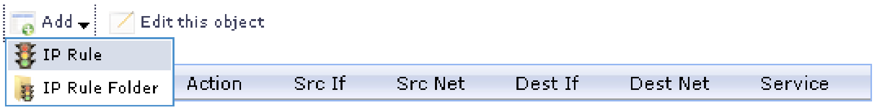
Allowing ICMP *Ping* Requests

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 *If3_net* network.

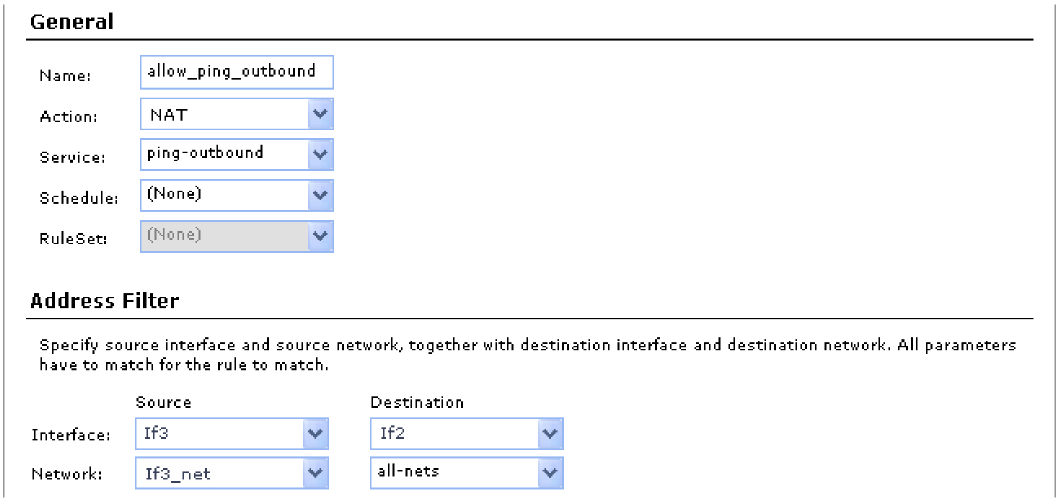
There can be several rule sets defined in CorePlus but there is only one rule set defined by default and this is called *main*. To add a rule to it, first select **Rules** > **IP Rule Sets** > **main** from the navigation tree.



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*.



General

Name:	allow_ping_outbound
Action:	NAT
Service:	ping-outbound
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:	If3	If2
Network:	If3_net	all-nets

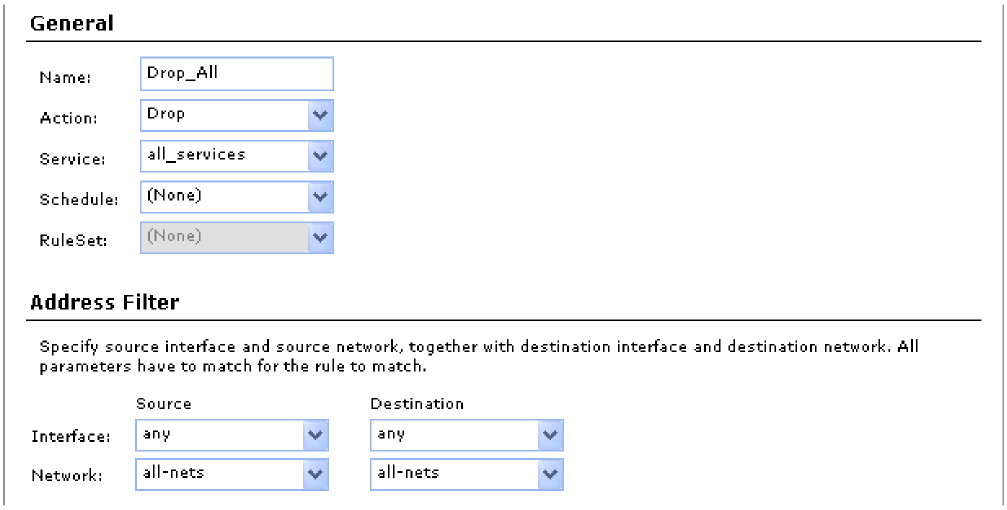
The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back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

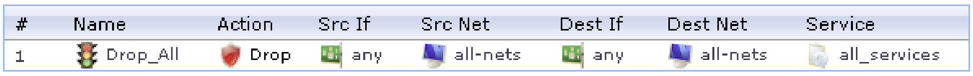
Name:	Drop_All
Action:	Drop
Service:	all_services
Schedule:	(None)
RuleSet:	(None)

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.

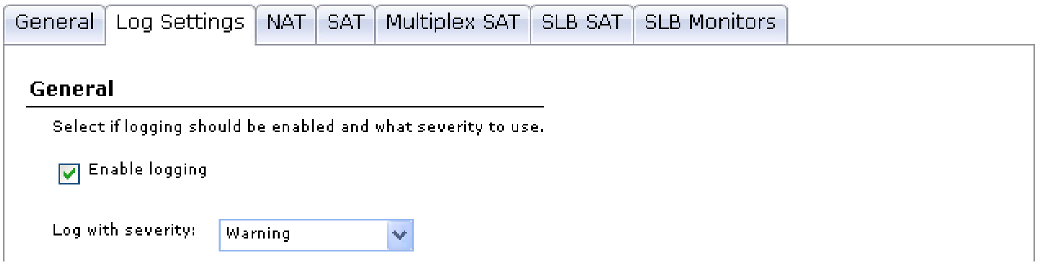
	Source	Destination
Interface:	any	any
Network:	all-nets	all-nets

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

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

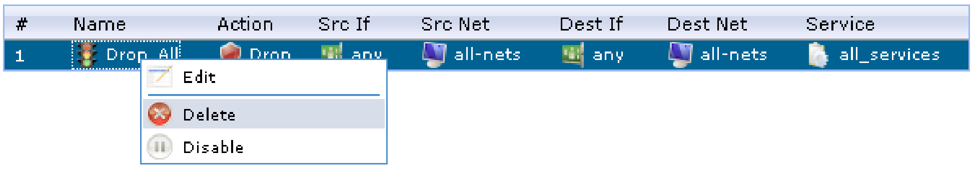
☑ Enable logging

Log with severity: Warning

Deleting Configuration Objects

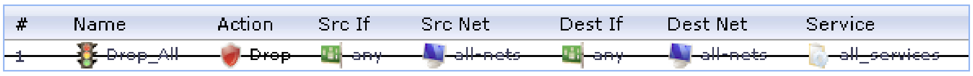
If information is deleted from a configuration during editing then these deletes are indicated by a line scored through the list entry while the configuration is still not yet activated. The deleted entry only disappears completely when the changes are activated.

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.



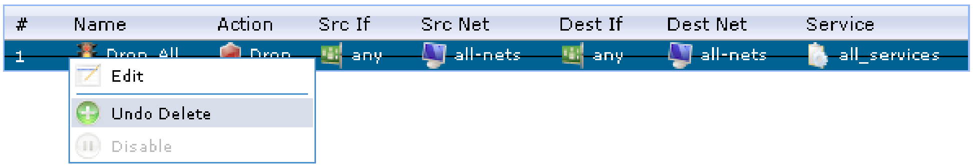
#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

The rule now appears with a line scored through it.



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

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

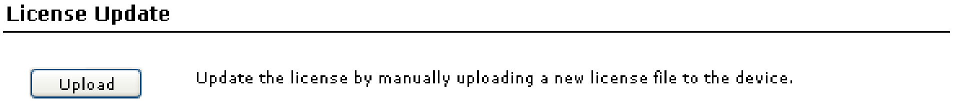


#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	Drop_All	Drop	any	all-nets	any	all-nets	all_services

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.

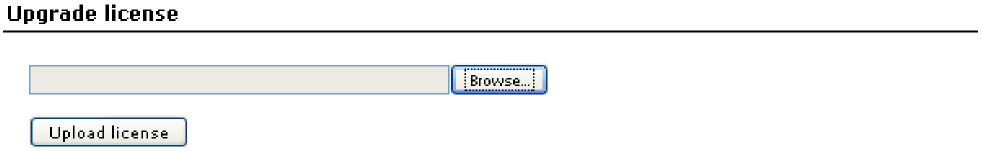
To do this, download a license as described in the last part of *Section 3.2, "Web Interface and Wizard Setup"*. This license can then be uploaded directly to CorePlus by selecting the **License** option from the **Maintenance** menu and then pressing the **Upload** button.



License Update

Update the license by manually uploading a new license file to the device.

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.



Upgrade license

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 3.5, "Troubleshooting Setup"*.

- Via the local CorePlus console. With VMware, the CorePlus console is the same as the virtual machine console.

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 you are using the VMware virtual machine console 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 refered 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. With VMware, connection is via the *virtual interfaces* provided by the hypervisor. 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 CorePlus under VMware, the virtual *If1* interface is always the management interface. Assuming a total of 3 virtual interfaces, the other two interfaces will be given the names *If2* and *If3* by CorePlus. For the sake of example, we will assume that the *If2* interface will be used for connection to the public Internet and the *If3* 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 *If2*, 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 *If2* interface which is connected to the ISP:

```
Device:/> set Interface Ethernet If2 DefaultGateway=wan_gw
```

Next, set the IP object *If2_ip* which will be the IP address of the interface connected to the ISP:

```
Device:/> set IP4Address If2_ip Address=10.5.4.35
```

Now set the IP object *If2_net* which will be the IP network of the connecting interface:

```
Device:/> set IP4Address If2_net Address=10.5.4.0/24
```

It is recommended to verify the properties of the *If2* interface with the command:

```
Device:/> show Interface Ethernet If2
```

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

```
                  Property  Value
 --------------------------  --------------------------
                      Name:  If2
                        IP:  If2_ip
                   Network:  If2_net
            DefaultGateway:  wan_gw
                 Broadcast:  10.5.4.255
                 PrivateIP:  <empty>
                     NOCHB:  <empty>
                       MTU:  1500
                    Metric:  100
               DHCPEnabled:  No
            EthernetDevice:  0:If2  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 surfing from the protected network *If3_net*. on the interface *If3*. 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 rulesets 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 allows the traffic through to the public Internet:

```
Device:/main> add IPRule name=lan_to_wan
                Action=Allow SourceInterface=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                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=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                DestinationNetwork=all-nets
                Service=http-all
```

The service used in the IP rule is *http-all* which will allow most web surfing 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=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                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 *If2* then the command is:

```
Device:/> set Interface Ethernet If2 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 *If3_net* and interface *If3*) to flow to the destination network *all-nets* and the destination interface *If2*.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface *If2* 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=If2 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 *If3_net* and interface *If3*) 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 *If3_net* and interface *If3*) 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 *If3* interface which is connected to the protected internal network *If3_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 *If3* interface:

```
Device:/> add DHCPServer dhcp_lan IPAddressPool=dhcp_range
                Interface=If3 Netmask=255.255.255.0
                DefaultGateway=If3_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, *If3_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 *If3_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=If3
                SourceNetwork=If3_net
                DestinationInterface=If2
                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 repsonses 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. 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 interface has been used for the initial connection to the management workstation. 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 the workstation IP is configured correctly.

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

3. Using the *ifstat* CLI command.

To investigate a connection problem further, use the VMware console after CorePlus starts. When you press the enter key with the console, 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 CorePlus management interface. By default this is the VMware *If1* interface. This command will display a number of counters for that interface. The *ifstat* command on its own can list the names of all the VMware 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.

4. 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 connections have been made to the correct interfaces.

Chapter 4: Licensing

Each virtual copy of CorePlus running under VMware requires a unique license (*.lic*) file to be associated with it and this can be downloaded from the Clavister Customer Web before uploading to the virtual Clavister Security Gateway.

Retrieving a License

To retrieve a license, the Customer Web system will require the input of a unique *registration key* which is supplied by Clavister after a license is purchased.

When retrieving a license from the Clavister Customer Web, a MAC address associated with the VMware virtual machine will be required. VMware assigns unique virtual MAC addresses to the interfaces for each virtual machine and these can be queried by first using the console command:

```
Device:/> ifstat
```

This gives the list of virtual interface names. To get the MAC address of any one of these, use the command:

```
Device:/> ifstat <interface_name>
```

The MAC address has the field name *HW address*.

Examining the License Contents

The contents of a Clavister license (*.lic*) file can be examined by opening it in a standard text editor. CorePlus licenses for VMware contain the line:

```
Virtual Hardware: Yes
```

The license contents also specifies how many virtual interfaces are available on one virtual machine. The default value can be upgraded by purchasing the appropriate license.

Uploading a License

A CorePlus license for VMware is uploaded to the installed virtual CorePlus in the same way as a normal non-virtual installation. In the Web Interface menu bar, select **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.

VMware and CorePlus Lockdown Mode

When CorePlus is run in demonstration mode (that is to say, without a valid license), it will operate for two hours before it enters *lockdown mode*.

When CorePlus enters *lockdown mode* under VMware, it will consume all VMware resources. When this happens it is necessary to shutdown the CorePlus virtual machine instance since nothing further can be done with CorePlus itself until it is restarted. In other words, restarting CorePlus should **only** be done via the VMware management interface once *lockdown mode* is entered.

General information about CorePlus licensing can be found in the *CorePlus Administrators Guide*.

Chapter 5: System Management

Upgrades Under VMware

When running CorePlus under a VMware server, upgrades of CorePlus can be done just as they are done on a single physical computer, by installing upgrade packages through the normal CorePlus user interfaces. It is not necessary to create a new virtual machine for a new version.

Virtual Network Performance

When using a VMware virtual network, traffic throughput can be lowered slightly when using the VMware *custom* (non-bridged) mode to connect a virtual interface through a virtual network to another virtual interface. This is because of the processing overhead involved in implementing the virtual network.

To avoid this performance penalty and achieve throughput which is close to "wirespeed", it is recommended to use VMware *bridged* mode to connect virtual CorePlus interfaces directly to physical Ethernet interfaces.

Resource Allocation

VMware allows the administrator the option to guarantee as well as limit resource allocation for each virtual process. Guaranteeing the resources available to a single virtual gateway can be important in order to avoid a situation where other virtual security gateways consume all available resources because they may be under a sustained security attack or processing may have frozen. For the same reasons, limiting the resources consumed by a single virtual security gateway can also be advisable.

Multicore Processing

When running VMware under multicore processors, it is possible to force one virtual machine into a separate core in order to improve performance

When running the standard VMware server under Microsoft Windows, the Windows *Set affinity* command can be used to do this. This command is reached by displaying a list of processes in the task manager and then right clicking on the particular VMware process that will be allocated to a single core.

With ESX or ESXi, VMware is the base operating system and forcing a virtual machine to use a separate core is done through the VMware administration interface.

Increasing the Number of Virtual Interfaces

It is possible to increase the number of virtual interfaces available with CorePlus with the following steps:

1. Add the extra virtual interface(s) in VMware. All virtual interfaces must be configured to be an *E1000* device.

   VMware product versions themselves may have a maximum number of virtual interfaces that can be added and this will limit additions.

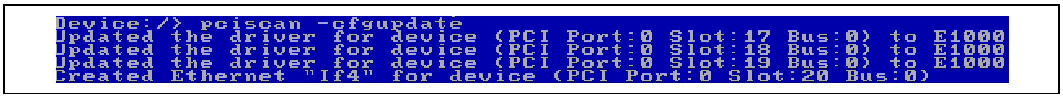
   When adding a virtual interface in VMware, make sure the option *Connect at power on* is enabled for the interface in *Virtual Machine Properties* before starting the virtual machine.

2. Acquire a new license that allows the extra interfaces and upload it to CorePlus.

3. If CorePlus has not yet detected all interfaces, run the CLI command *pciscan* so that any new interfaces are added to the configuration. The full CLI command is:

   ```
   Device:/> pciscan -cfgupdate
   ```

   An example console showing the *pciscan* command being used to add the new interface *If4* to a CorePlus configuration is shown below.



```
Device:/> pciscan -cfgupdate
Updated the driver for device (PCI Port:0 Slot:17 Bus:0) to E1000
Updated the driver for device (PCI Port:0 Slot:18 Bus:0) to E1000
Updated the driver for device (PCI Port:0 Slot:19 Bus:0) to E1000
Created Ethernet "If4" for device (PCI Port:0 Slot:20 Bus:0)
```

4. The CLI commands *activate* followed by *commit* should then be entered to save the updated configuration.

Chapter 6: Separating VLANs

The Problem

In VMware ESX or ESXi installations, there may be a number of virtual machines set up which we want to connect together on a single *virtual network*. To do this, we define them as belonging to a single *port group* on a *virtual switch* with the port group having a particular *VLAN ID*. The virtual machines now act as though they are connected together on a single virtual network.

Suppose that we now have a second set of virtual machines similarly connected to the same virtual switch through another port group.

All the virtual machines from both groups may also need to communicate with a virtual Clavister Security Gateway. That security gateway would also be connected to the virtual switch through another port group on the switch. This arrangement is illustrated in the diagram below. The boxes labelled "VM" represent the various virtual machines.

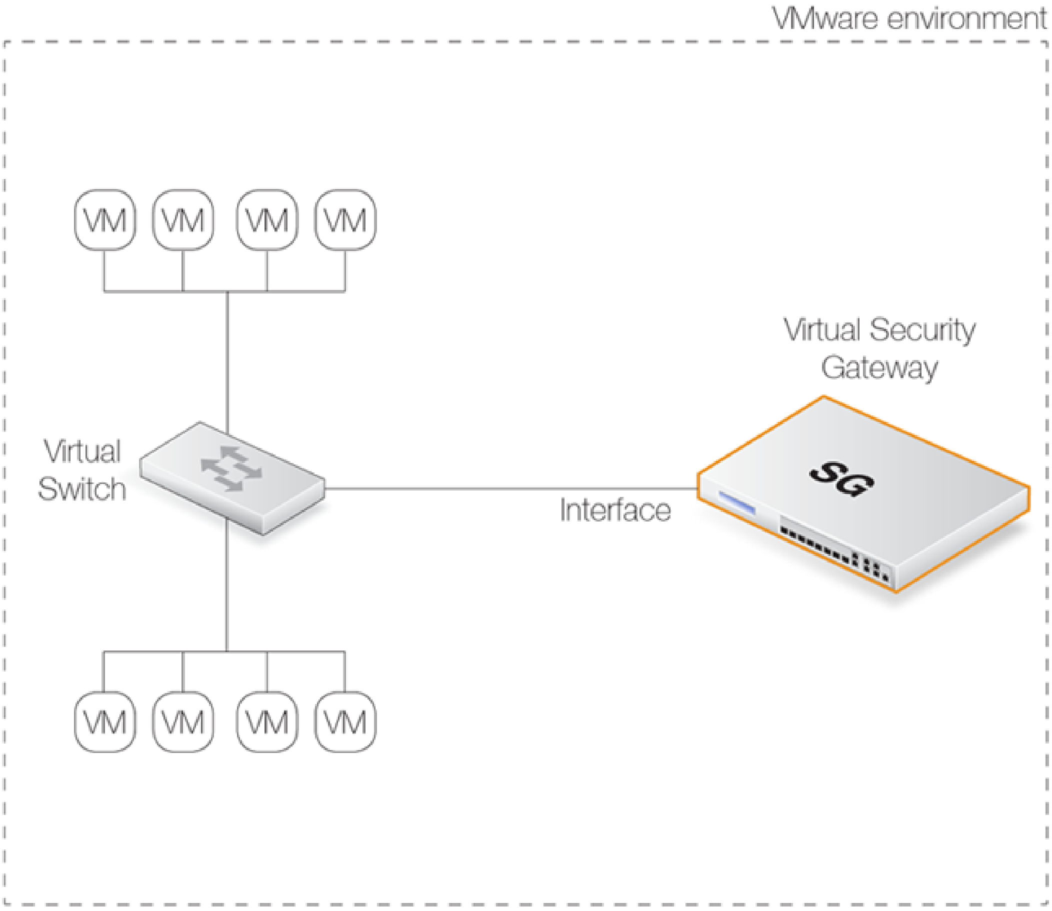


Figure 6.1. Connecting VLANs

The virtual switch will normally allow the two groups of virtual machines to communicate with each other. However, what is often required is that they should communicate with each other only through the virtual Clavister Security Gateway so all traffic can be under the control of CorePlus.

The Solution

The way to achieve separation is by using unique VLAN IDs for the two groups of virtual machines and a third VLAN for connection to the Clavister Security Gateway. The diagram below illustrates this arrangement.

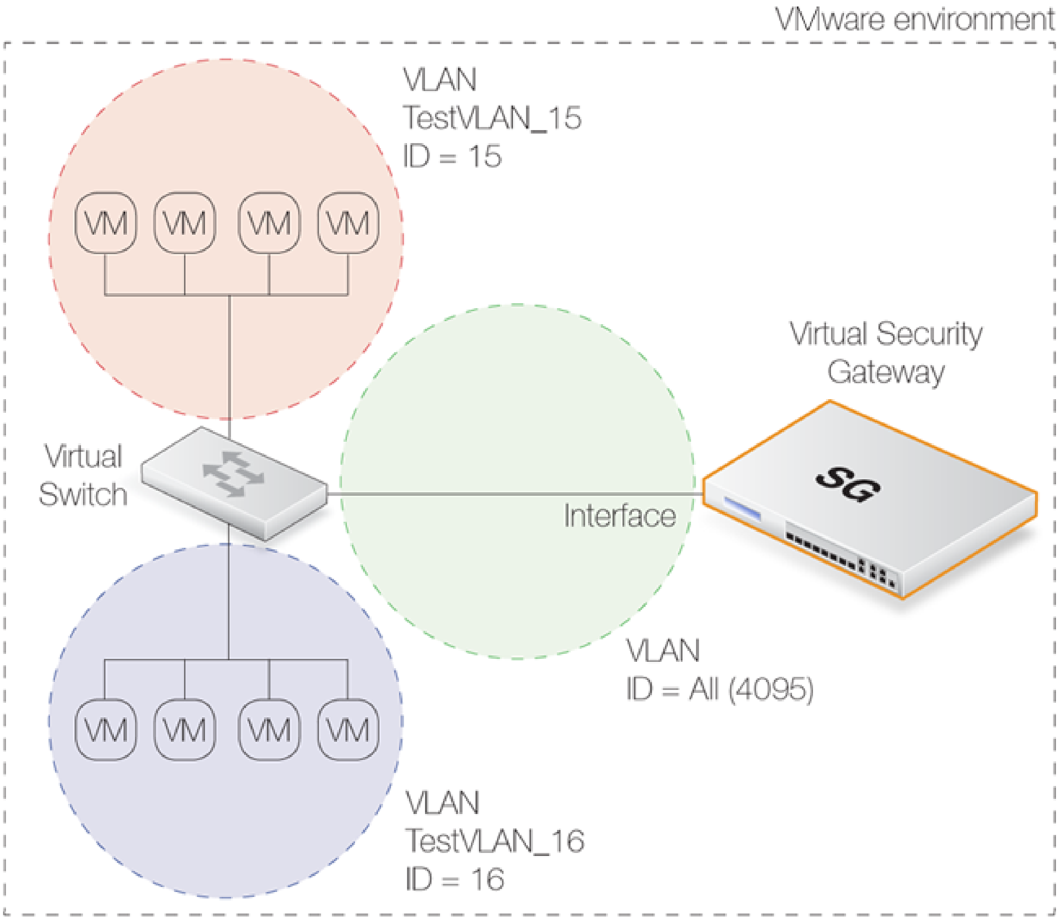


Figure 6.2. Separating VLANs

The key points for this solution are:

1. Each port group for the two groups of virtual machines must be given a unique VLAN ID.

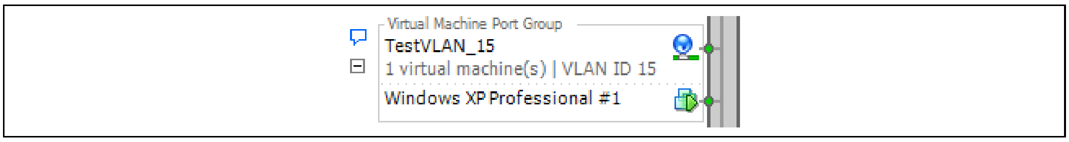
   One of the two networks of virtual machines in the illustration is set up to be a VLAN called *TestVLAN_15* with the VLAN ID *15*. The other is set up to be a VLAN called *TestVLAN_16* with the VLAN ID *16*. Using different IDs means that the two VLANs cannot communicate with each other.

2. The virtual machine port group on the virtual switch that connects to the security gateway should allow all VLAN ID's to exist in this port group. This is done by specifying the VLAN ID to be *4095* in the infrastructure client (this ID is displayed by the client as the VLAN ID *ALL*). Only the connected interface of the security gateway should exist in this group and this acts as a VLAN *trunk* (all VLAN IDs can exists on the trunk).

3. Each VLAN ID on the virtual switch requires a corresponding *VLAN Interface* object defined in CorePlus for the connecting interface and with the same VLAN ID.

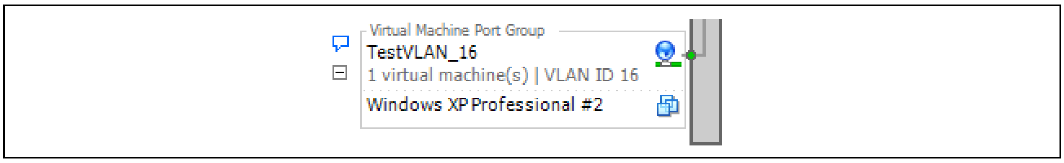
   In other words, create one CorePlus VLAN Interface objects for the VLAN *TestVLAN_15* with the ID *15* and create a second for VLAN *TestVLAN_16* with the ID *16*. Both VLAN Interfaces are configured on the interface that connects to the virtual switch. This allows CorePlus to communicate with these VLANs.

In the VMware infrastructure client, the virtual switch will contain two *virtual machine port group*s and these are shown in the partial screen shots below. The first port group is for *TestVLAN_15*:



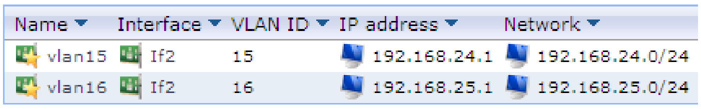
Virtual Machine Port Group
TestVLAN_15
1 virtual machine(s) | VLAN ID 15
Windows XP Professional #1

The second port group is for *TestVLAN_16*:



Virtual Machine Port Group
TestVLAN_16
1 virtual machine(s) | VLAN ID 16
Windows XP Professional #2

Below is a partial screenshot that shows the VLAN setup in CorePlus when viewed through the Web Interface. The virtual interface *if2* is connected to the virtual switch.



Name	Interface	VLAN ID	IP address	Network
vlan15	If2	15	192.168.24.1	192.168.24.0/24
vlan16	If2	16	192.168.25.1	192.168.25.0/24

The IP addresses used for the VLANs, *192.168.24.1* and *192.168.25.1*, are randomly chosen internal IP addresses. The clients attached to VLAN *vlan15* must therefore be configured with the default gateway *192.168.24.1*. The clients on *vlan16* must have the default gateway *192.168.25.1*.

Advantages of this Approach

The key advantage of this approach of using VLANs is that all traffic flow between the virtual machines and CorePlus occurs inside the virtual VMware network setup and none needs to leave the virtual environment to enter the "real world". This has clear benefits in terms of performance and control.

If Internet access is through the virtual Clavister Security Gateway then that traffic would obviously leave the virtual environment.

VMware References

VMware themselves discuss this approach under the paragraph heading *Fully Collapsed DMZ* in a VMware document entitled *DMZ Virtualization with VMware Infrastructure*. The approach is described as "*virtualizing the entire DMZ*".

Chapter 7: Creating Virtual Machines

It is not normally necessary to create a new virtual machine from scratch in VMware since CorePlus is downloadable from the Clavister customer web in a form that is ready to import into VMware and virtual machine creation is automatic. An alternative to this for ESX and ESXi is to:

- Download the standard CorePlus *ISO* file image for non-VWare software installation from the Clavister Customer Web.
- Create a new VMware virtual machine suitable for running CorePlus.
- Start the new virtual machine.
- Import the *ISO* image file into the virtual machine and then start it.

After downloading the *ISO* file image, the following sections describe the remaining steps.

Creating an ESX/ESXi Virtual Machine

To create a new virtual machine for CorePlus, the steps are:

1. Start the VMware option *Create a new virtual machine* from the *Getting started* tab in the infrastructure client. A wizard will start.
2. Select the *Custom* option.
3. Give the new virtual machine a suitable name.
4. Select the resource for the virtual machine and press *Next*. The resource is the VMware host that will be used in a cluster.
5. Select the data store to use.
6. Select the *Guest O/S* to be *Other 64 bit*.
7. Select the number of processors to be *1*.
8. Select the memory size to be at least *256* Mbytes and press *Next*. The allowable memory size may be greater depending on the CorePlus license purchased.
9. Select the network adaptors to use. The network adaptors will be the interfaces of the security gateway. There can be up to 4 adaptors but all must be of the type *E1000*.
10. Select the storage adaptor types to be *SCSI adaptor bus logic*.

11. Create a new virtual disk.
12. Set the disk capacity to be exactly 2 GBytes.
13. The advanced options dialog appears next. Skip this by pressing *Next*.
14. A summary of the virtual machine will be displayed. Press *Finish* if all the settings are correct.

Importing the ISO File

The next set of steps imports the CorePlus *ISO* file into the newly created virtual machine.

1. In the VMware navigation menu, select the virtual machine just created and edit its settings.
2. Under the *Hardware* tab, go to the *CD/DVD Drive* and enable the option *Datastore ISO File*.
3. Press the *Browse* button and select the CorePlus *ISO* file to be imported.
4. Enable the *Connect at power on* option and press *OK*.

Starting the Security Gateway

Now start CorePlus running:

1. Start the virtual machine and select the *Console* tab.
2. Select the option *Transfer system from CD*. This will place the CorePlus executable on the virtual disk created earlier.
3. A blue console screen now appears which lists the available virtual disks. Select the disk created earlier.
4. At the question *Transfer system to disk?*, enter *Yes*.
5. At the message *Press any key to reboot*, press any key.

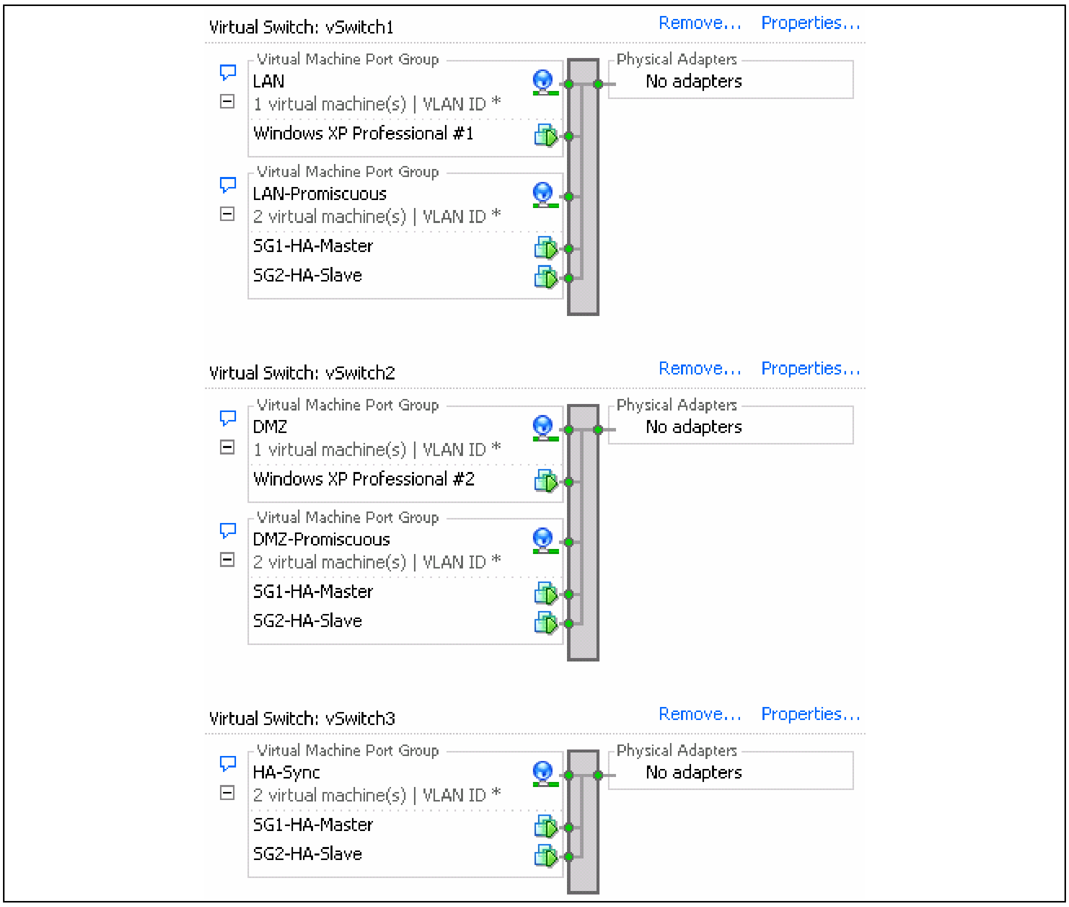
CorePlus will now reboot in the virtual machine and the console displayed will show the boot up sequence and can be used to enter CLI commands.

Chapter 8: VMware HA Setup

This section provides the extra information needed to correctly set up an HA cluster under VMware, where both Clavister Security Gateways in the cluster are running in separate VMware virtual machines.

The initial setup of the two separate Clavister Security Gateways is done as normal so they are initially working as separate units. Before running the *HA Setup Wizard* on each unit to create the HA cluster, it is first necessary to correctly configure the VMware virtual networking to emulate the hardware connections that would normally be present between the master and slave units. The key to this, is to create VMware *virtual switches* so that the pairs of matching interfaces from the security gateways in the cluster are connected together via a group in a virtual switch operating in *promiscuous mode*.

Below is a screenshot which shows the setup in the *Configuration* section of the VMware infrastructure client for an ESXi server:



Virtual Switch: vSwitch1 Remove... Properties...

Virtual Machine Port Group
LAN
1 virtual machine(s) | VLAN ID *
Windows XP Professional #1

Virtual Machine Port Group
LAN-Promiscuous
2 virtual machine(s) | VLAN ID *
SG1-HA-Master
SG2-HA-Slave

Physical Adapters
No adapters

Virtual Switch: vSwitch2 Remove... Properties...

Virtual Machine Port Group
DMZ
1 virtual machine(s) | VLAN ID *
Windows XP Professional #2

Virtual Machine Port Group
DMZ-Promiscuous
2 virtual machine(s) | VLAN ID *
SG1-HA-Master
SG2-HA-Slave

Physical Adapters
No adapters

Virtual Switch: vSwitch3 Remove... Properties...

Virtual Machine Port Group
HA-Sync
2 virtual machine(s) | VLAN ID *
SG1-HA-Master
SG2-HA-Slave

Physical Adapters
No adapters

Figure 8.1. VMware Virtual Switch Setup with HA

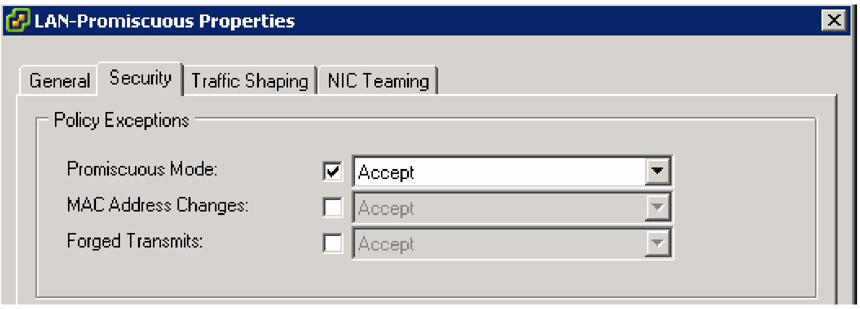
The image shows the setup for virtual switches number 1 to 3. Virtual switch 0 is not shown since this is for the management workstation. The purpose of the 3 virtual switches is described next:

Switch 1

If we look at *Switch 1* in the screenshot, there are two groups defined within the switch:

- The first is the *LAN* group which connects the normal networks outside the Clavister Security Gateway to the **LAN** interface of the cluster.

- The second group is the *LAN-Promiscuous* group and this connects together the **LAN** ports on the two security gateways. As the group name indicates, this group must operate in *promiscuous mode* which means that the switch does not use ARP requests to determine which host is found on which interface. Instead, traffic is sent to all connected interfaces.



Policy Exceptions

Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

Figure 8.2. Setting Promiscuous Mode in VMware

Switch 2

The structure of *Switch 2* is the same as *Switch 1* but this time it is the **DMZ** interfaces of the two security gateways which are being connected together in the second promiscuous group. The first group, again, is used for connection if external networks which will connect to the security gateway via the **DMZ** interface of the cluster.

Switch 3

Switch 3 is a virtual switch with only one group. This is used to link together the *Sync* interfaces of each security gateway.

Chapter 9: FAQ

This appendix collects together answers to a selection of *Frequently Asked Questions* that can be helpful in solving various issues with CorePlus running under VMware.

Question Summary

1. The 2 hour CorePlus demonstration mode time limit has expired. What do I do?
2. Are upgrades of CorePlus done differently under VMware?
3. How do I release focus from the VMware console window?
4. Do all my virtual interfaces have to be configured as E1000 NICs?
5. How do I manage multiple virtual security gateways?
6. How do I change the CorePlus device ID?
7. How do I separate different virtual networks?

Questions and Answers

1. The 2 hour CorePlus demonstration mode time limit has expired. What do I do?

CorePlus will not respond after it enters *lockdown mode* after 2 hours and will consume all the VMware resources. In this situation, the VMware virtual machine must be stopped and then restarted so that CorePlus restarts and enters a new 2 hour evaluation period.

2. Are upgrades of CorePlus done differently under VMware?

No. CorePlus upgrades are performed under VMware just as they would be in non-VMware environments.

3. How do I release focus from the VMware console window?

VMware keeps focus in the console window. To click outside the console wondow, press the key combination **Ctrl-Alt** .

4. Do all my virtual interfaces have to be configured as E1000 NICs?

Yes. CorePlus will not work with virtual interfaces that are not configured as an E1000.

5. How do I achieve management access to multiple virtual security gateways?

The IP address of the management virtual Ethernet interface must be different for the different virtual security gateways running under a single hypervisor.

6. How do I change the CorePlus device ID?

The ready-to-run VMware virtual machine image provided by Clavister always has the same *DeviceID* and this causes problems for the InControl management client. To generate a unique ID for a virtual security gateway, enter the boot menu and select the option to reset to the default configuration.

7. How do I separate different virtual networks?

If different sets of virtual machines are connected to a virtual switch through different port groups, they can be separated by making them VLANs with different VLAN IDs. This is described further in *Chapter 6, Separating VLANs*.

8. After restarting CorePlus, where is the new virtual network adaptor that was added?

Go to *Virtual Machine Properties* in the VMware client and view the network adapter to verify that the checkbox *Connect at power on* is enabled before starting the virtual machine. If the added interface is still not detected by CorePlus, enter the CLI command:

```
Device:/> pciscan –cfgupdate
```

This will scan for any new interfaces. Then save the updated configuration with the command:

```
Device:/> activate
```

Followed by:

```
Device:/> commit
```

Appendix A: Vista IP Setup

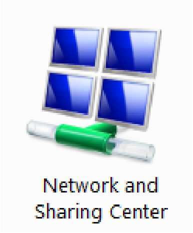
If a PC running Microsoft Vista is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address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

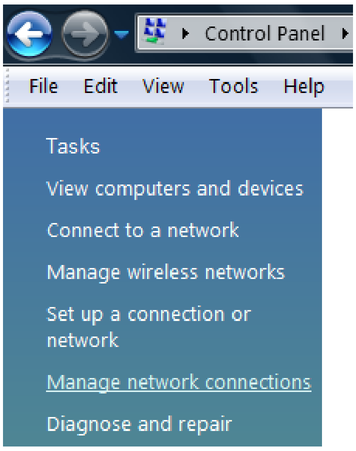
1. Press the Windows **Start** button.

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

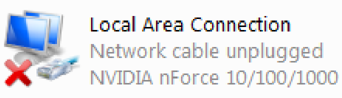
3. Select **Network & Sharing Center** from the control panel.



4. Select the **Manage network connections** option.

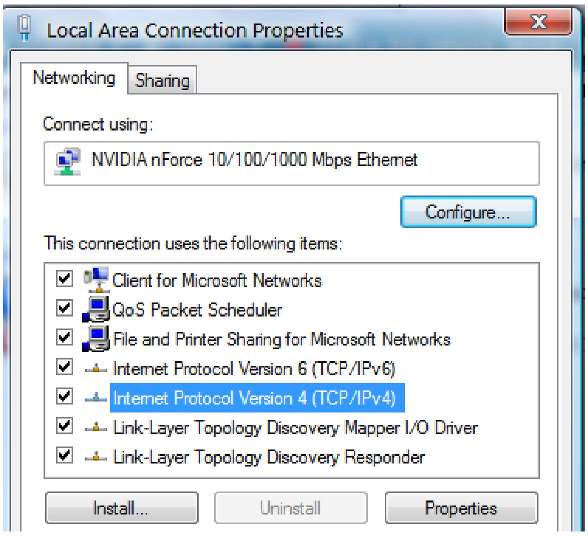


5. A list of the Ethernet interface connections will appear. Select the interface that will connect to the security gateway.



Local Area Connection
Network cable unplugged
NVIDIA nForce 10/100/1000

6. The properties for the selected interface will appear.



Connect using:

NVIDIA nForce 10/100/1000 Mbps Ethernet

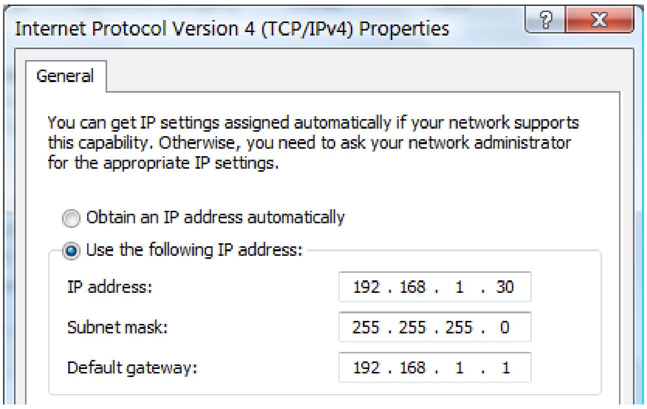
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

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*



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

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 B: Windows 7 IP Setup

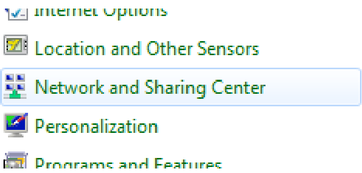
If a PC running Microsoft Windows 7 is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address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

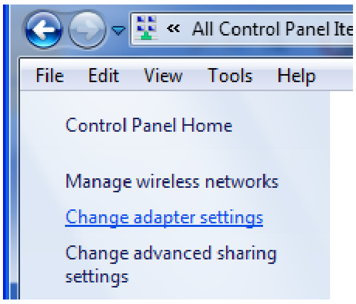
1. Press the Windows **Start** button.

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

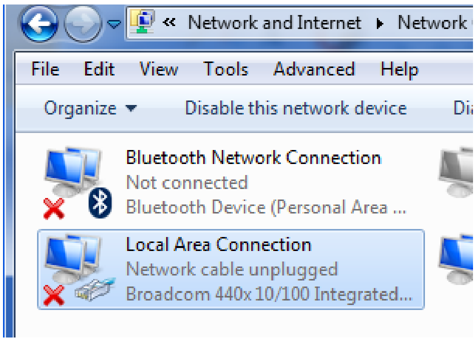
3. Select **Network & Sharing Center** from the control panel.



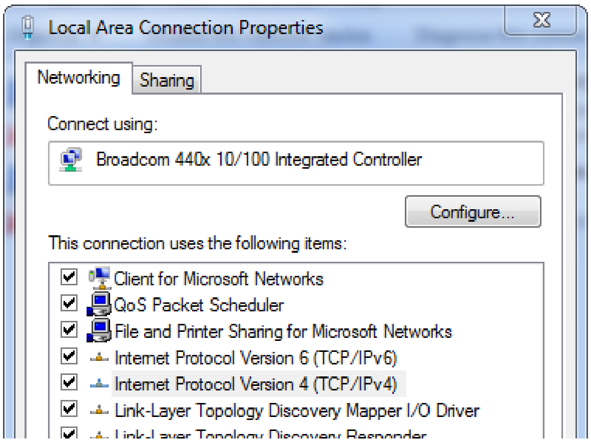
4. Select the **Change adapter settings** option.



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


« Network and Internet ▸ Network
File Edit View Tools Advanced Help
Organize ▾ Disable this network device Di
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Local Area Connection
Network cable unplugged
Broadcom 440x 10/100 Integrated...

6. The properties for the selected interface will appear.



Connect using:

Broadcom 440x 10/100 Integrated Controller

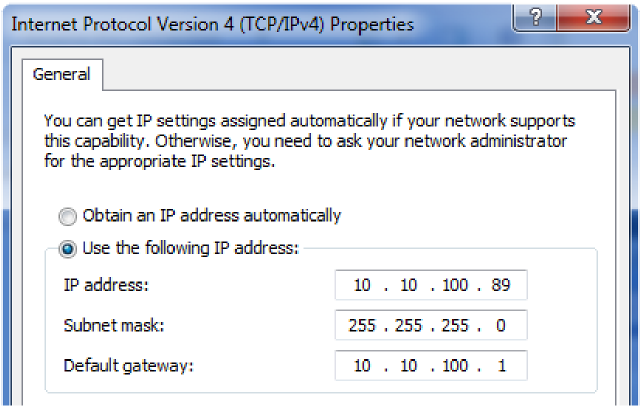
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

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*



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 100 . 89

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 100 . 1

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

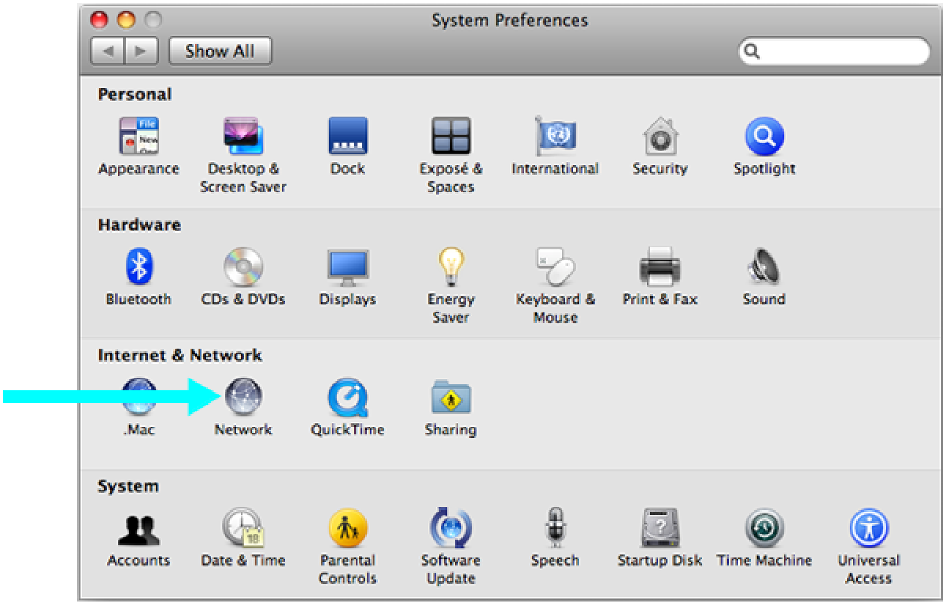
8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

Appendix C: 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:

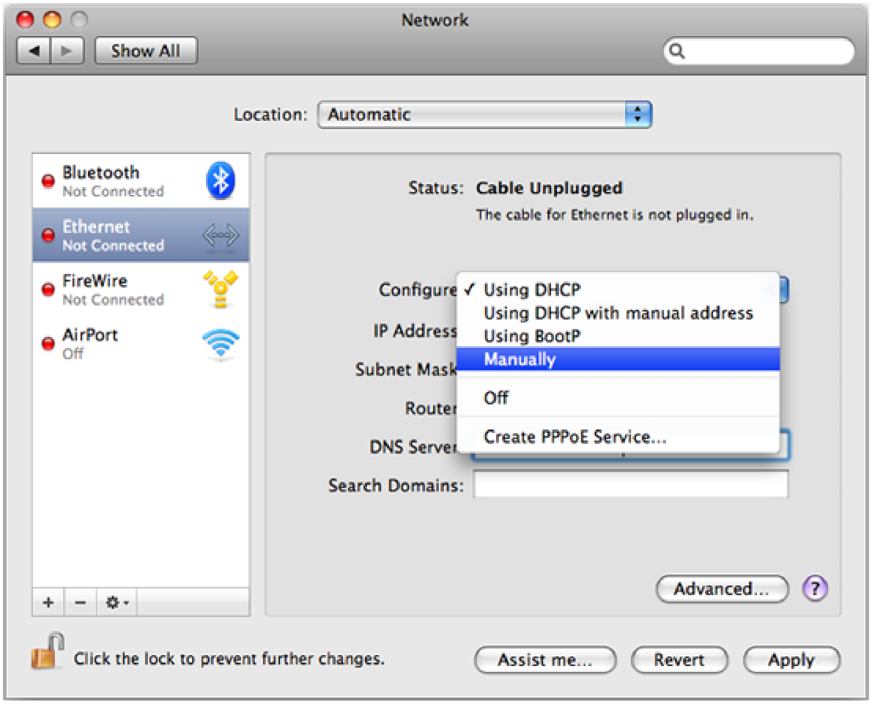
1. Go to the **Apple Menu** and select **System Preferences**.

2. Click on **Network**.



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

4. Select **Manually** in the **Configure** pull down menu.


Location: Automatic

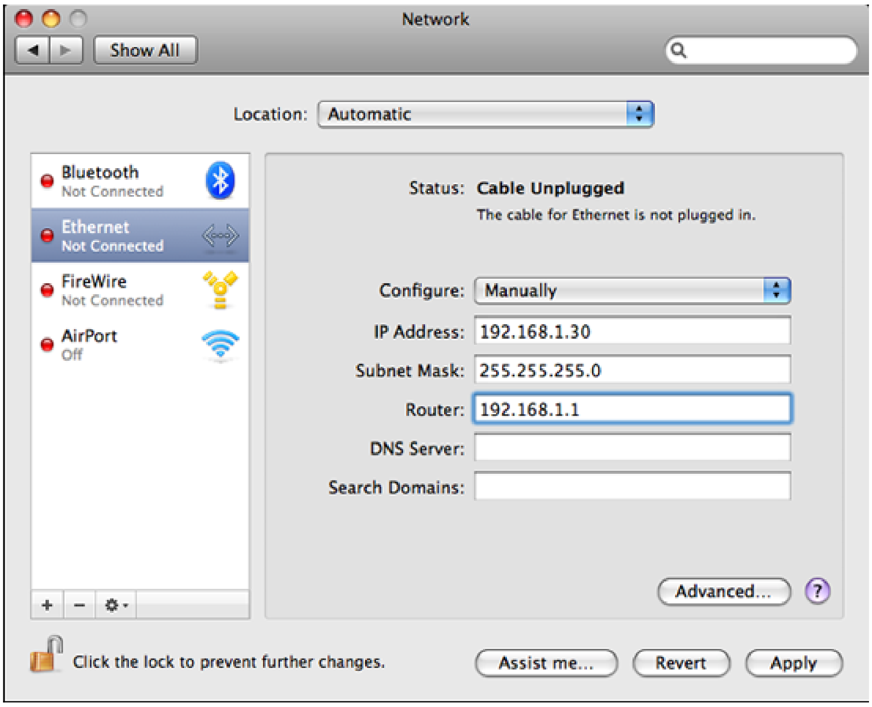
Status: Cable Unplugged

The cable for Ethernet is not plugged in.

Click the lock to prevent further changes.

5. Now set the following values:

   - **IP Address:** *192.168.1.30*
   - **Subnet Mask:** *255.255.255.0*
   - **Router:** *192.168.1.1*



Location: Automatic

Bluetooth
Not Connected

Ethernet
Not Connected

FireWire
Not Connected

AirPort
Off

Status: **Cable Unplugged**
The cable for Ethernet is not plugged in.

Configure: Manually
IP Address: 192.168.1.30
Subnet Mask: 255.255.255.0
Router: 192.168.1.1
DNS Server:
Search Domains:

Click the lock to prevent further changes.

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

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com