User Guide

Gateway Guardian and CSM

Version 1.3
January 5, 2004

NETMASTER
Digital Security

Table of Contents

Installing the software and creating your first security device:

Configuring your security device to meet your specific needs:

Other topics:

Table of Figures

1 - Introduction

Congratulations on your purchase of a NetMaster Gateway Guardian product. Once installed, you will quickly realize what a revolutionary network security product Gateway Guardian is – and easy-to-install, easy-to-configure security system that will keep your network safe and running more efficiently.

This document is divided into several sections, beginning with several introductory chapters, followed by a few chapters on getting the software installed and your first security device up-and-running. The last two sections of this document provide more information on how to make additional configuration changes to meet your specific needs along with a few advanced features and functionality.

Please Note: This document can be used to proceed, step-by-step, through the process of obtaining (if you have not already done so) and installing the software, and initially configuring your first security device. To do so, simply follow the steps outlined in the sidebars entitled **Installation Step** as you read through the first few chapters of this document.

2 - NetMaster Security Products

Gateway Guardian Operating System (GG-OS)

NetMaster Gateway Guardian Operating System (GG-OS) is the core operating system that is at the heart of every NetMaster security device. It is a highly specialized operating system specifically tailored for security device implementations and is based on NetMaster's own Linux distribution. When used with the NetMaster CSM device management software (described below), no Linux knowledge is required to operate and manage GG-OS devices.

GG-OS System Requirements:

- Pentium-class computer system capable of booting from an IDE CDROM Drive (Pentium II or better recommended).
- 64MB RAM (96MB or more recommended)
- 500MB IDE Hard Drive (1GB recommended)
- Two PCI (or 3COM 3c509 ISA) Ethernet network cards
- IDE CDROM Drive

Centralized Security Management Console (CSM)

NetMaster CSM is a Java-based application running on any current Windows operating system (98/ME/2K/XP). This application is used to configure and manage any number of NetMaster security devices remotely; through the local area network or even over the Internet. It contains many wizards and other utilities to make managing your security devices and enforcing your information security policies as simple and easy as possible.

CSM System Requirements:

- Windows 98/ME/2000/XP Operating System
- Pentium II-class computer system.
- 128MB RAM
- 50MB Hard drive space (+100KB per configured device)
- Network connection between workstation running CSM and the computer system running GG-OS.

SecurityBlade (GG-Blade / GG-EXT)

SecurityBlades are incredibly energy-efficient devices – drawing less than 15 Watts of power from your PCI slot.

Due to customer demand for an integrated approach to network security, NetMaster has developed a very small device designed to have GG-OS embedded within it to become an all-in-one security device. These devices are offered in two form-factors: a PCI-card sized "peripheral" which can be mounted in any computer system having a PCI bus – effectively a computer within a computer, or an external "desktop" version about the same size as any textbook.

The internal, PCI-card sized version of the device (called GG-Blade) can be installed into any computer system with an available PCI 2.x-compliant PCI slot (almost every Pentium II-class or newer computer system is compliant with the PCI 2.x specification). GG-Blade only requires power from the host computer system. *There is no other interaction with the host computer system hardware or the operating system it is running.*

SecurityBlade System Requirements:

- Internal version requires a host computer system with PCI 2.x-compliant expansion slot.

3 – New and Enhanced Features

NetMaster CSM and GG-OS Version 2.0 build on the successful release and commercialization of the original Gateway Guardian, Firecard, and Inferno products. New or enhanced features in this version include:

- The process for locating and initially configuring new security devices on the network has been significantly modified to make it easier and faster than ever before. Users no longer have to change the IP of the local workstation or have a local DHCP Server available in order to configure the device. And, unlike many other network devices, console access or null-modem cables are not required either!

- GG-OS no longer requires any diskettes! GG-OS installs directly from a bootable CD and, once installed, runs directly from the internal system hard drive.

- GG-OS no longer needs to be rebooted to implement configuration changes or most software updates. This minimizes end-user impact due to system downtime.

- Significantly redesigned and improved user interface. Now better organized and more user-friendly.

- Significantly redesigned device status monitoring capability – via a "Status Web Server" and a built-in SNMP Agent. Authorized SNMP clients (such as NetMaster CSM) can retrieve device status information as required. Also, GG-OS can be configured to send SNMP Trap Messages to remote hosts configured and enabled to receive these messages. These messages can then be delivered via pager, cell phone text messaging, email, Windows popup messages, or other facility in order to alert the device administrator to specific events in real-time, as they occur. (This feature replaces, and is a significant enhancement to, the Active Alert system found in the first generation product.)

- Advanced Encryption Standard (AES – Rijndael) encryption algorithm for IPSEC VPN tunnels. (AES provides up to a 100% performance increase over 3DES-encrypted tunnels. See http://www.netmaster.com/products/fastervpn.shtml for more information.)

- Multi-homed external Ethernet interface. Up to 252 IP Addresses can now be assigned to the external interface. This allows multiple web servers, mail servers, etc. behind the NAT Mode firewall.

- Access to NetMaster SafetyNet[1] for free software updates for the life of the product version.

- Access Control Groups (users and/or network hosts) for Firewall and Bandwidth Management rulesets.

- Time-based Firewall rulesets using Access Control Groups.

SafetyNet provides automated software updates for NetMaster products. Any bug fixes, security patches, or product enhancements will be provided for free for the life of the product version being used. SafetyNet does not include product upgrades; however. In almost all cases, new product features will be released as part of a new product version and will require the purchase of an upgrade for a nominal fee.

4 - Software Installation

Installation Step:

1 – Obtain Software

Before you begin, you must have available and ready to use the NetMaster CSM and NetMaster GG-OS CD media. If these were not delivered to you, you will need to download them (as described to the right) and *burn* them to CD.

Software Downloads

All of NetMaster's software products can be downloaded via the website at http://www.netmaster.com/downloads. Most software products are downloadable as CDROM ISO Images that must be "burned" to CD before they can be used.

If you do not have a CD Writer or, for any other reason, require access to CD media, please contact NetMaster Sales via email at sales@netmaster.com or by telephone at +1 (604) 609-6384 to arrange to have a set of CD's to be shipped to you.

Installing GG-OS

Installation Step:

2 – Install NetMaster GG-OS

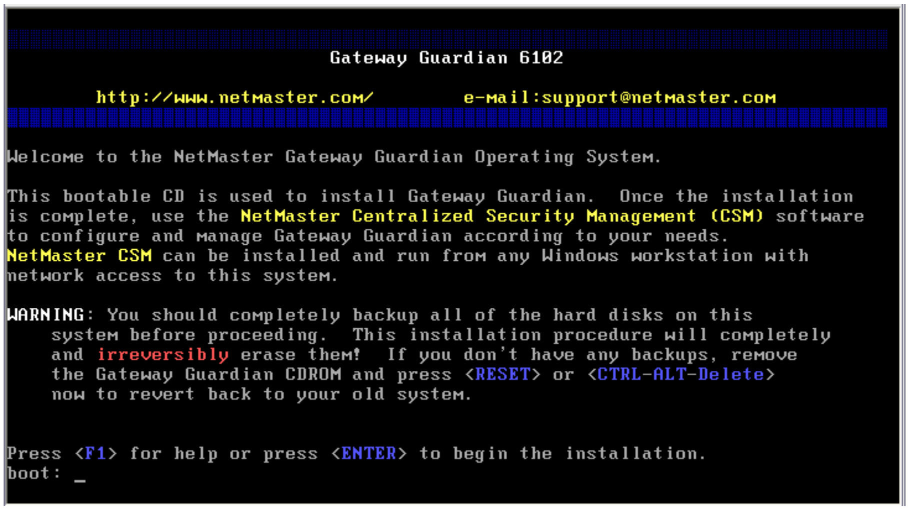
Install GG-OS onto a computer system having the necessary hardware requirements (see Section 2).

(This step is not required if you have purchased a NetMaster SecurityBlade as it already has the GG-OS software embedded onto it.)

GG-OS is NetMaster's security device operating system. This operating system can be installed onto a computer system meeting the minimum system requirements, replacing any existing operating system, applications, and data files previously installed, and turning it into a dedicated security appliance. For information on the minimum system requirements to run GG-OS, please refer to the GG-OS subsection located in the NetMaster Security Products section of this document.

Please Note: If you have purchased a NetMaster SecurityBlade device, it already has the GG-OS software embedded onto it and, therefore, you can skip down to the section entitled "Installing CSM".

Insert the GG-OS CD into the computer system and power it up. If the system is capable of and is configured to boot from the CDROM Drive, you will be presented with the GG-OS Installation screen as per the following screenshot. If this does not happen, you may need to reconfigure the computer system BIOS to re-order the boot-device sequence. Please consult your system or motherboard manufacturer's user manual for information on how to do this.



```
                        Gateway Guardian 6102

     http://www.netmaster.com/        e-mail:support@netmaster.com

Welcome to the NetMaster Gateway Guardian Operating System.

This bootable CD is used to install Gateway Guardian.  Once the installation
is complete, use the NetMaster Centralized Security Management (CSM) software
to configure and manage Gateway Guardian according to your needs.
NetMaster CSM can be installed and run from any Windows workstation with
network access to this system.

WARNING: You should completely backup all of the hard disks on this
    system before proceeding.  This installation procedure will completely
    and irreversibly erase them!  If you don't have any backups, remove
    the Gateway Guardian CDROM and press <RESET> or <CTRL-ALT-Delete>
    now to revert back to your old system.


Press <F1> for help or press <ENTER> to begin the installation.
boot: _
```

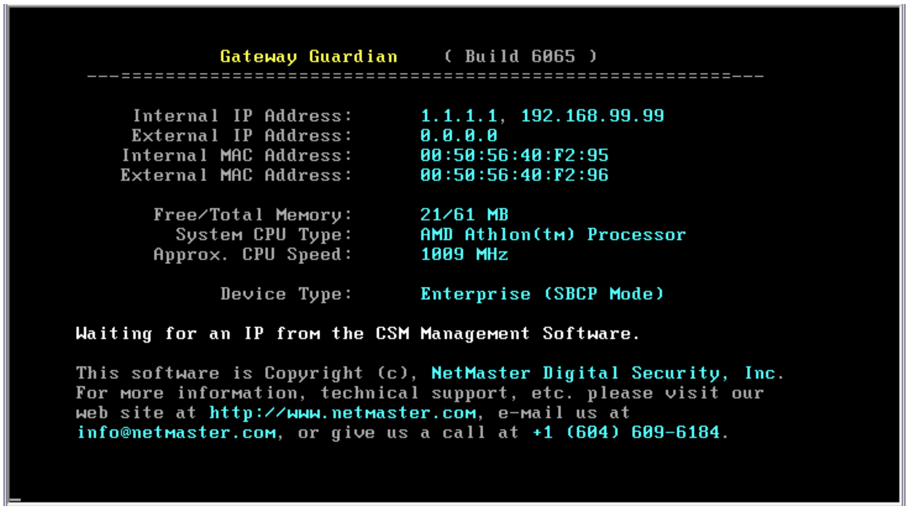
Figure 4-1: GG-OS CD Bootup Screen

As per the onscreen instructions, press the keyboard **<F1>** Function Key to view a help topic menu, or simply press **<ENTER>** to begin the installation process.

The entire GG-OS installation process is fully automated and only requires your input in a few places. The first is to read and accept the NetMaster End User License Agreement, the second is to specifically acknowledge and accept the fact that the system hard drive contents are about to be overwritten and replaced with the Gateway Guardian Operating System and, finally, to remove the CD and reboot the system to complete the installation process.

Before any permanent changes are made to the computer, the installation process will analyze the system configuration to ensure that it meets the minimum system requirements (i.e. RAM, Hard Drive type and size, and two compatible Ethernet cards). If the computer system does not meet the required minimums, the installation process will be aborted with an explanation as to why it cannot continue.

Once the installation is complete, be sure to remove the GG-OS CD from the system before rebooting the computer. The computer will proceed through its bootup sequence and, after a few minutes, will end up at the final screen as shown below.



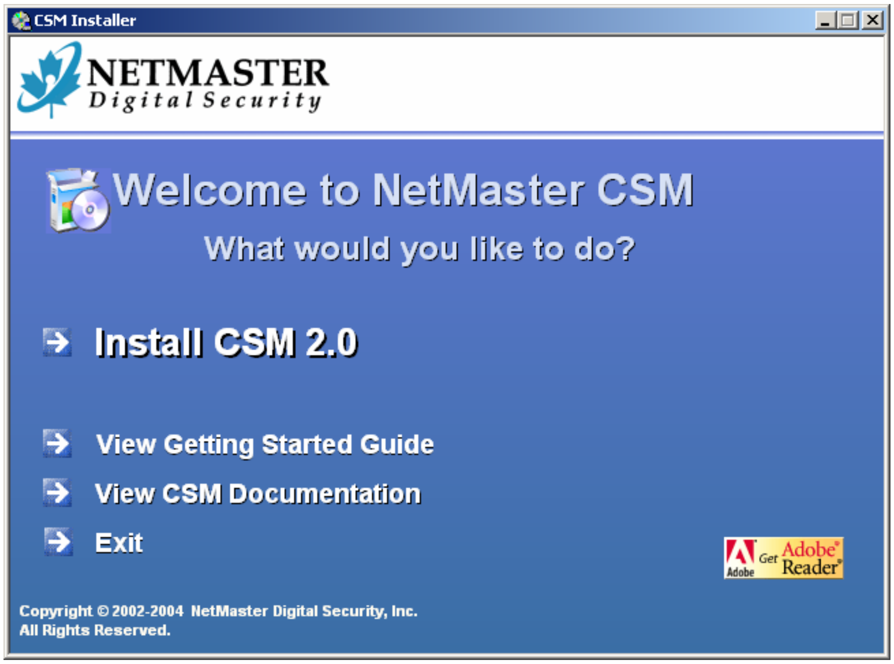
```
                 Gateway Guardian    ( Build 6065 )
       -------------------------------------------------------------

            Internal IP Address:      1.1.1.1, 192.168.99.99
            External IP Address:      0.0.0.0
           Internal MAC Address:      00:50:56:40:F2:95
           External MAC Address:      00:50:56:40:F2:96

              Free/Total Memory:      21/61 MB
                System CPU Type:      AMD Athlon(tm) Processor
              Approx. CPU Speed:      1009 MHz

                    Device Type:      Enterprise (SBCP Mode)

      Waiting for an IP from the CSM Management Software.

      This software is Copyright (c), NetMaster Digital Security, Inc.
      For more information, technical support, etc. please visit our
      web site at http://www.netmaster.com, e-mail us at
      info@netmaster.com, or give us a call at +1 (604) 609-6184.
```

Figure 4-2: GG-OS Startup Screen on Unconfigured Device

At this point, your GG-OS security device is now ready and waiting to be configured by the Centralized Security Management (CSM) console software. This process of configuring your security device will be covered in the “Creating a Security Device” section of this document.

Installing CSM

The NetMaster CSM CD has **autorun** functionality and, therefore, shortly after inserting this CD into your Windows-based computer, a menu system will pop up onscreen (as shown in Figure 3-3) from which you will be able to choose to install the CSM software. If you do not have **autorun** enabled on your CDROM Drive, use Windows Explorer to browse to your CDROM Drive and double-click the **autorun.exe** application to load the menu system.



Welcome to NetMaster CSM

What would you like to do?

Copyright © 2002-2004 NetMaster Digital Security, Inc.
All Rights Reserved.

Figure 4-3: CSM CD AutoRun Menu

Installation Step:

3 – Install NetMaster CSM

Install NetMaster CSM onto a computer system running Windows. (Typically, your local Windows workstation.)

Once the Welcome screen, as shown above in Figure 3-3, is displayed, click on **Install CSMv2** to begin the software installation process.

After asking a few questions, for instance where to install CSM onto your hard drive, the Installer will take a few minutes and continue through to completion.

5 - Introducing CSM

NetMaster CSM is the Centralized Security Management software used to initially configure and then maintain any number of NetMaster security devices. It contains many wizards and other utilities to make managing your security devices and enforcing your information security policies as easy as possible.

The Graphical User Interface

Installation Step:

4 – Start CSM

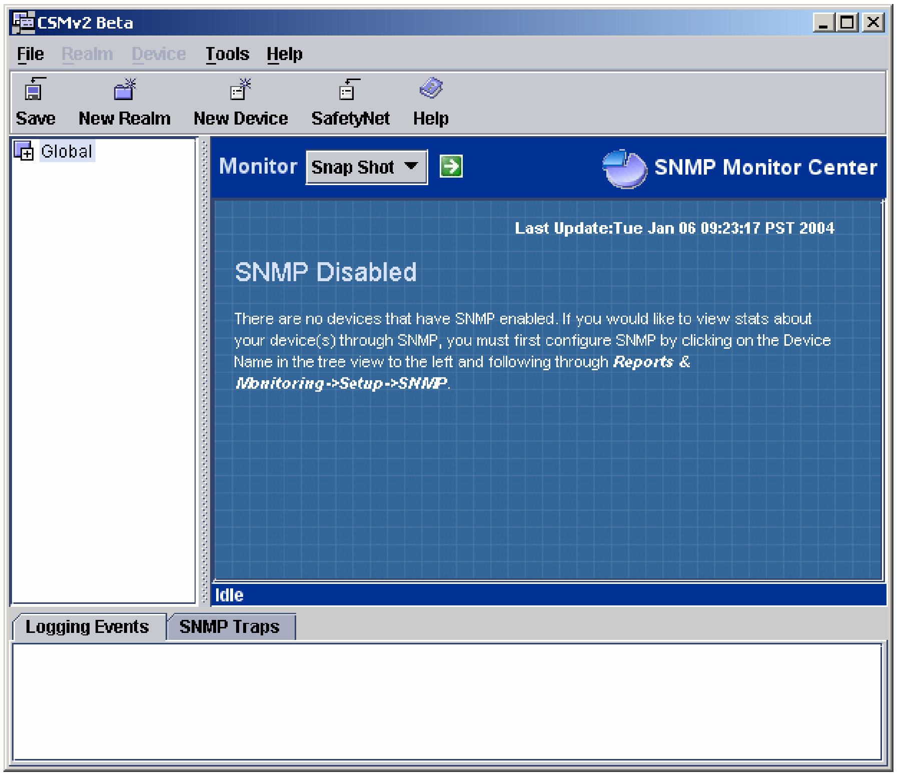
Find CSMv2 within the Programs → NetMaster folder off your Windows Start Menu and click on it to start the CSM application.

Once started, cancel the Configuration Wizard dialog in order to view the main CSM application window.

Once you have installed CSM onto your Windows-based computer system (as per the previous section), you can start the application by finding the **CSMv2** menu item within the **NetMaster** submenu off your Windows **Start Menu**.

The first time you start the application, CSM will start full-screen and an initial Configuration Wizard dialog will be displayed front-and-center.

For now, hit the Cancel button on the Configuration Wizard dialog. At this point, the main CSM application window should be displayed onscreen as shown below.



Last Update:Tue Jan 06 09:23:17 PST 2004

SNMP Disabled

There are no devices that have SNMP enabled. If you would like to view stats about your device(s) through SNMP, you must first configure SNMP by clicking on the Device Name in the tree view to the left and following through ***Reports & Monitoring->Setup->SNMP***.

Figure 5-1: Main CSM Console

The CSM main console, as shown above, is divided into 4 main areas:

1. The menu bar and toolbar along the top,
2. The tree view on the left,
3. The device settings detail view on the right, and
4. The Log Events viewer along the bottom.

Realms:

Realms are used to group Devices according to some pre-determined pattern; for instance, geographic location, customer, or other similar functional grouping. The topmost Realm is called "Global" and cannot be deleted. Each Realm can contain any number of other Realms and/or Devices.

The tree view on the left is used to easily organize and locate security devices being managed by CSM. This view can contain folders, called Realms, and security Devices. Simply double-click a Realm or Security Device to hide or display it's contents. See the sidebar for more information about Realms.

The device settings detail view on the right is used to monitor device status or view/modify device configuration details.

Once you have created a device (covered in Section 6) and have enabled remote logging for that device (covered in Section 10), any log events generated by the security device will be transmitted to CSM and displayed in the Log Events viewer at the bottom of the CSM main console.

Why Java?

NetMaster CSM is a Java-based application that is capable of running on any operating system having a compatible Java Runtime Environment (JRE) installed and available. At the time of this writing, CSM is designed to operate with JRE Version 1.4.1 and should remain forward-compatible with newer versions of the JRE as they become available.

As mentioned above, CSM is capable of running on any operating system – not just Windows – having a compatible JRE installed. While NetMaster does not currently provide an Installer application for other operating systems, CSM will run just fine in most cases. CSM has been known to run on Linux, Solaris, and Apple's OS X. This type of platform independence will allow NetMaster to respond quickly to user demand to provide full support for our software running on non-Windows operating systems.

6 - SafetyNet

Installation Step:

5 – Check SafetyNet

Click the **Check SafetyNet** button in the CSM Toolbar to download any software updates that may be available from NetMaster's website.

Software Updates

Internet security is an ever-moving target and, therefore, NetMaster is continually auditing and reviewing and updating it's software to reflect changing conditions, repair software deficiencies, and respond to security issues as they are discovered. SafetyNet is the system used to deploy these software updates as they are released.

NetMaster CSM is configured by default to check SafetyNet every time the application starts. This feature can be disabled by the end-user and, therefore, a **SafetyNet** button is located on the CSM toolbar to remind users to perform this activity on a regular basis.

Software Upgrades

Unlike software updates, software *upgrades* are not provided as part of SafetyNet. While a new product feature may occasionally be provided to customers via SafetyNet, most new product enhancements will only be available through a product upgrade that must be purchased for a nominal upgrade fee. Most major software manufacturers, including Microsoft and Symantec, use this approach in distributing software updates and upgrades to their customers.

How much does it cost?

SafetyNet, and all NetMaster software updates, are available for free for the life of the version of the product the customer has purchased.

7 - Creating a Security Device

This section will take you through configuring your first NetMaster security device. Upon completion, you will have a fully operational security device running with minimal services. The next section of this document will take you through the process of customizing your security device to meet specific needs or to implement advanced functionality.

In order to continue, you must have already installed NetMaster CSM and GG-OS (as described in Section 3). The Windows system running CSM and the computer running GG-OS must also be attached to the same physical Ethernet network segment.

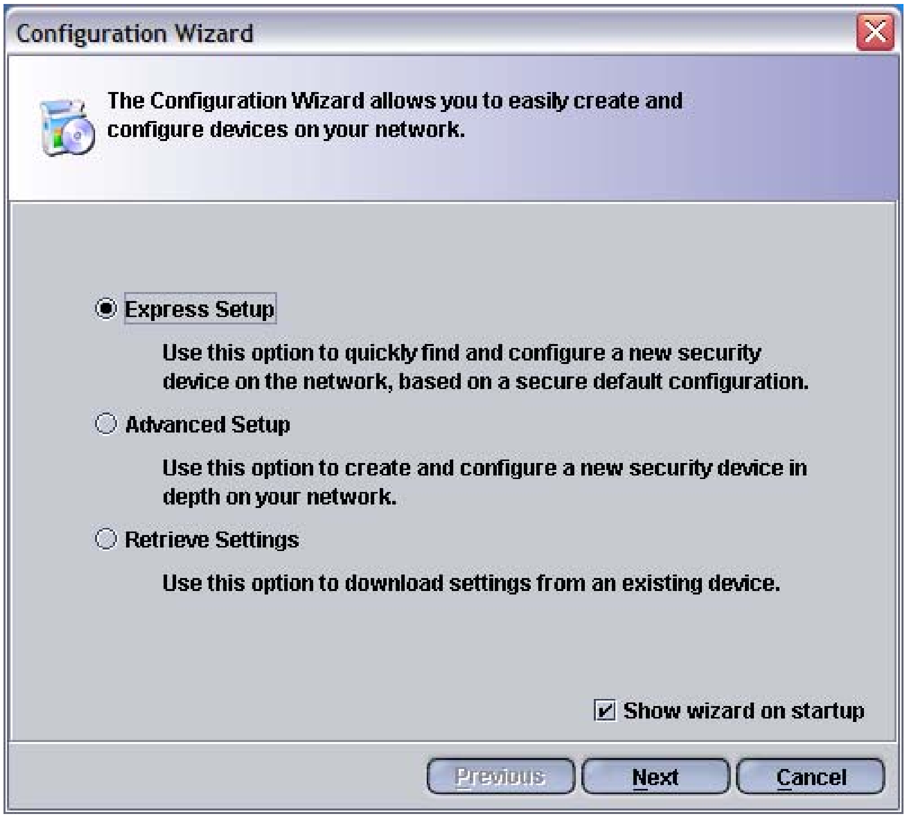
The Configuration Wizard

Installation Step:

6 – Creating a Device – Step 1

Press **Ctrl-W** to start the Configuration Wizard to begin the process of creating a security device within CSM.

When CSM is first loaded, it starts the Configuration Wizard (shown below) by default. You can disable this feature at any time by clicking the checkbox labeled "Show wizard on startup".



Configuration Wizard

The Configuration Wizard allows you to easily create and configure devices on your network.

● Express Setup

Use this option to quickly find and configure a new security device on the network, based on a secure default configuration.

○ Advanced Setup

Use this option to create and configure a new security device in depth on your network.

○ Retrieve Settings

Use this option to download settings from an existing device.

☑ Show wizard on startup

Figure 7-1: The Configuration Wizard

If you have CSM running and you don't see the Configuration Wizard as shown above, press **<Ctrl-W>** now to start it. Alternatively, you can start this wizard by clicking **Configuration Wizard** from the **Tools** menu.

As you can see from the screenshot above, there are three options to choose from within the Configuration Wizard:

1. **Express Setup:** Used to quickly configure a device to a usable state with minimal questions and interaction required of the user. Once the wizard is complete and the device has been created with CSM, the user will have full access to the device configuration parameters to customize them as required to meet any specific needs.
2. **Advanced Setup:** This option is similar to the Express Setup except the user is provided with additional choices and is asked several additional questions throughout the wizard to allow a more detailed initial configuration of the device. Just as above, once the wizard is complete, the user will be able to further modify device configuration parameters as required to meet any specific needs.
3. **Retrieve Settings:** This option allows the user to create a new device within CSM by retrieving a configuration from an active security device. This feature is useful in the event that CSM needs to be reinstalled at any time (and no backups are available).

Installation Step:

7 – Creating a Device – Step 2

Click **Next** to choose the **Express Setup** option.

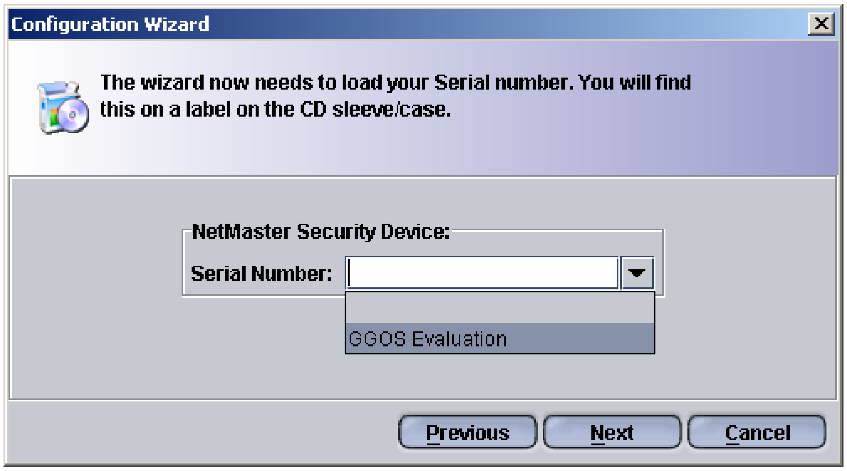
Click the **Next** button to select the **Express Setup** option and continue.

The next screen in the Configuration Wizard, shown below, requires that you fill in the device Serial Number provided to you by NetMaster. This Serial Number is uniquely keyed to each NetMaster product device-type.

Installation Step:

8 – Creating a Device – Step 3

Type in the security device **Serial Number** that was provided to you and click **Next** to continue.



The wizard now needs to load your Serial number. You will find this on a label on the CD sleeve/case.

NetMaster Security Device:

Serial Number:

GGOS Evaluation

Figure 7-2: Enter a Product Serial Number

You will find the Serial Number printed on a label attached to the back of the CD Jewel Case. If you are configuring a NetMaster SecurityBlade, you will also find the Serial Number printed on a label attached to the back of the PCI card (GG-Blade) or on the bottom of the device case (GG-EXT).

If you cannot find your Serial Number, please contact NetMaster Sales by telephone at +1 (604) 609-6184 or by email at sales@netmaster.com.

If you will only be using Gateway Guardian for **evaluation** purposes, click on the combo box's down-arrow and select "**GGOS Evaluation**" from the list that is displayed (as shown in Figure 7.2). Running Gateway Guardian in Evaluation Mode provides you with a security device that is fully functional in every way except that it ceases to function every 60 minutes. When this timeout occurs, you simply have to reboot the device in order to initiate another 60 minute evaluation period. You can repeat this process as many times as is necessary to fully evaluate the product.

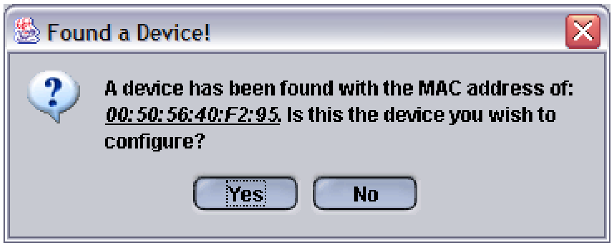
Once you have entered a valid Serial Number, click **Next** to continue.

At this point, the Configuration Wizard will now begin searching your local network using NetMaster's own SBCP technology (see sidebar for more information), looking for an unconfigured NetMaster Security Device. This process typically takes only a few seconds to locate your device, but can take up to several minutes during periods of high network activity. Once a device is found, a dialog box similar to the following will be displayed:

SBCP:

NetMaster's Security Blade Configuration Protocol (SBCP) was designed to make locating and initially configuring your NetMaster security device as easy as possible.

SBCP does not require any local workstation configuration changes, serial or null-modem cables, device console commands via a text-based user interface, or other cumbersome configuration methods that are so often required for network devices from other vendors.



A device has been found with the MAC address of: *00:50:56:40:F2:95*. Is this the device you wish to configure?

Figure 7-3: Found a Device!

The Ethernet MAC Address displayed within this dialog must match that of the NetMaster security device you are trying to configure. (The MAC Address of your security device is shown on the bootup screen of GG-OS and is printed on a label attached to the back of your GG-Blade/GG-EXT device.) The only time this MAC Address will *not* match the device you are trying to configure is if you are currently configuring more than one device at a time. (I.e. you have two unconfigured GG devices running on your local area network at the same time.)

Installation Step:

9 – Creating a Device – Step 4

If, for some reason, you are trying to configure more than one GG-OS device on the local subnet at the same time, ensure the MAC Address displayed here matches the MAC Address of the device you are intending to configure.

If the MAC Address displayed in this dialog is not the one you are wanting, click the **No** button and the Configuration Wizard will continue searching for other unconfigured GG devices on your local network.

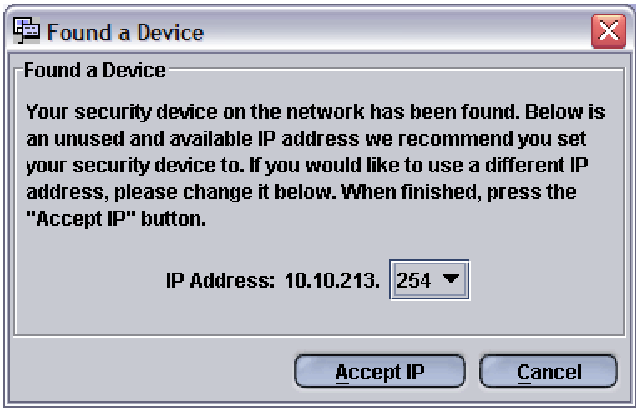
If the Configuration Wizard cannot find an unconfigured GG device on your network, an error dialog will pop up onscreen.

If CSM is having trouble finding your unconfigured security device, consider the following:

- Does the security device appear to be operational?
    - If you are using GG-OS, did it completely bootup as per the screenshots found in Section 3?
    - If you are using GG-Blade/GG-EXT, are the link-lights lit up on the back of the device?
- If you are using GG-Blade/GG-EXT, did you wait long enough for the device to fully start before trying to locate it? (This can take 2-3 minutes from the time the host computer is powered on or from the time you pressed the reset button on the security device.)
- Are you running Personal Firewall software on the workstation running CSM, which might be blocking communications between CSM and the security device?
- Do you have both PCI Ethernet devices on the GG-OS device plugged into the network? (If you have one cable plugged into the local network and the other plugged into "the Internet" – i.e. a device provided by your ISP – try swapping the cables on the back of the GG-OS device and try again.)
- Are CSM and the security device attached to the same physical Ethernet network segment? (I.e. there cannot be any routers or bridges between them.)
- Are you running intelligent Ethernet switches that may be blocking certain types of broadcast traffic?
- Are you running intelligent Ethernet switches that may be separating your physical network into VLAN segments?

If the MAC Address displayed in the previous dialog matches that of the security device you are trying to configure, click **Yes** to continue.

At this point, CSM will scan your computer system configuration and the local area network to find an IP Address that is not currently being used. Once found, the following dialog box will be displayed, recommending an IP to be assigned to the security device.



Your security device on the network has been found. Below is an unused and available IP address we recommend you set your security device to. If you would like to use a different IP address, please change it below. When finished, press the "Accept IP" button.

IP Address: 10.10.213. 254

Figure 7-4: IP Address Recommendation

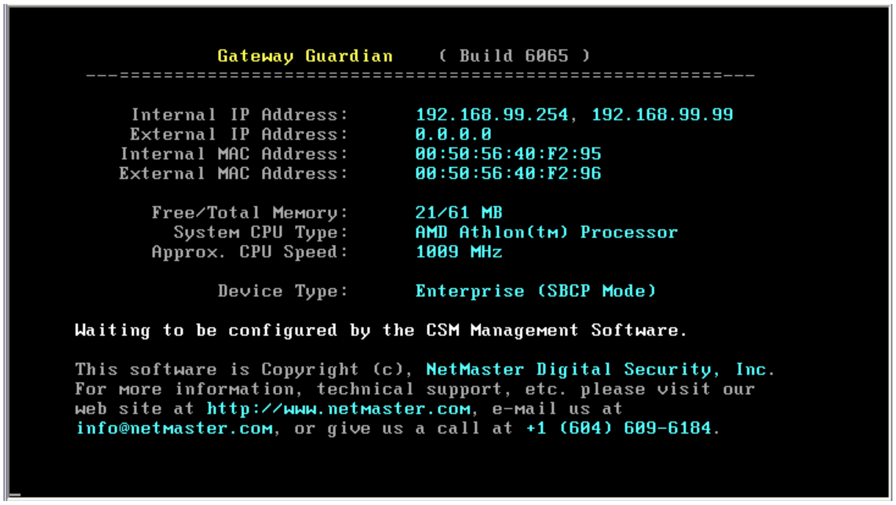
Installation Step:

10 – Creating a Device – Step 5

The recommended IP Address should be acceptable; however, make any changes if necessary.

In almost every case, the recommended IP Address should be chosen; however, you have the option to make any changes as necessary.

Once you click the **Accept IP** button, CSM will assign the IP Address to the unconfigured GG security device. If you are configuring a GG-OS device (versus the console-less GG-Blade / GG-EXT), you will notice that the console, as shown below, will refresh to reflect the IP Address assignment:



```
                  Gateway Guardian    ( Build 6065 )
       ---=======================================================---

           Internal IP Address:      192.168.99.254, 192.168.99.99
           External IP Address:      0.0.0.0
          Internal MAC Address:      00:50:56:40:F2:95
          External MAC Address:      00:50:56:40:F2:96

             Free/Total Memory:      21/61 MB
               System CPU Type:      AMD Athlon(tm) Processor
             Approx. CPU Speed:      1009 MHz

                   Device Type:      Enterprise (SBCP Mode)

      Waiting to be configured by the CSM Management Software.

      This software is Copyright (c), NetMaster Digital Security, Inc.
      For more information, technical support, etc. please visit our
      web site at http://www.netmaster.com, e-mail us at
      info@netmaster.com, or give us a call at +1 (604) 609-6184.
```

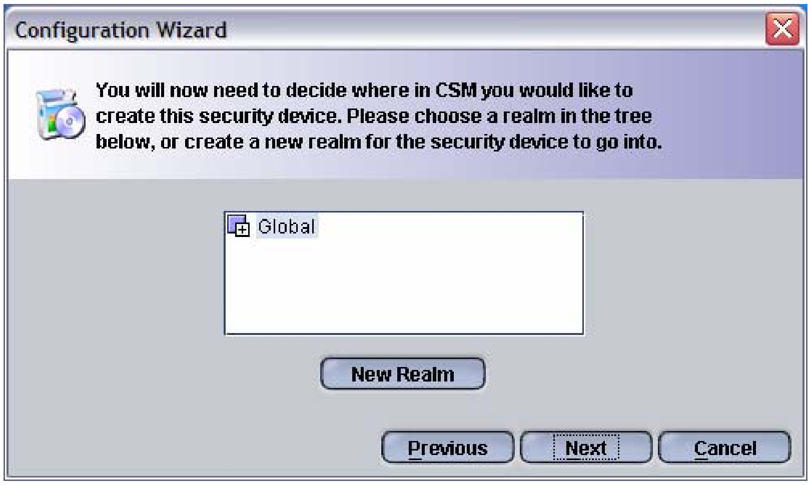
Figure 7-5: GG-OS has Accepted Assigned IP Address

The ensuing dialog of the Configuration Wizard (Figure 7-6) allows you to specify where in the Realm tree to create this new device. Realms are covered in more detail in Section 4; however, in summary, they're simply a way to organize and store devices according to your own, personal grouping system; for instance, geographic area. Realms are of most use to users who will be managing large numbers of devices. In a fresh installation of CSM, there will only be the Global Realm available. If you want to create a new Realm within which to place your new device, click the **New Realm** button to create new Realms as necessary.

Installation Step:

11 – Creating a Device – Step 6

Click **Next** to put this security device into the **Global** Realm otherwise, click **New Realm** to create any sub-Realm's as necessary within which to locate your device.



You will now need to decide where in CSM you would like to create this security device. Please choose a realm in the tree below, or create a new realm for the security device to go into.

Figure 7-6: Assign Device to a Realm

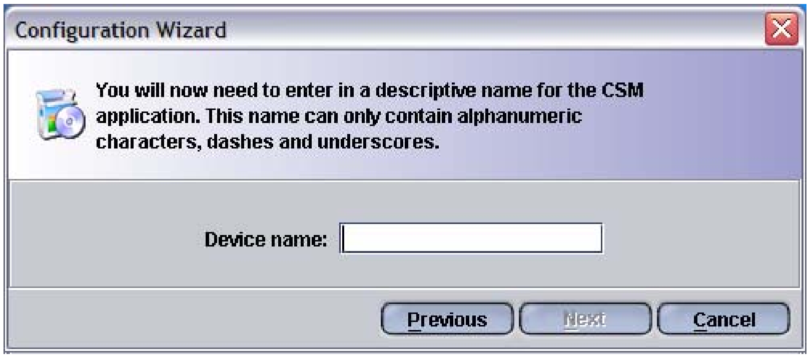
Once you have chosen a Realm within which to install the device, click the **Next** button to continue.

The next dialog in the Configuration Wizard asks that you give your new device a name. Typically, you should use a descriptive name such as "Vancouver" or "555_West_Hastings" to help you identify the physical location of the device.

Installation Step:

12 – Creating a Device – Step 7

Provide an appropriate name for your security device.



You will now need to enter in a descriptive name for the CSM application. This name can only contain alphanumeric characters, dashes and underscores.

Device name:

Figure 7-7: Name the Device

Device names cannot contains spaces and, therefore, as per the example above, replace any spaces with an underscore character.

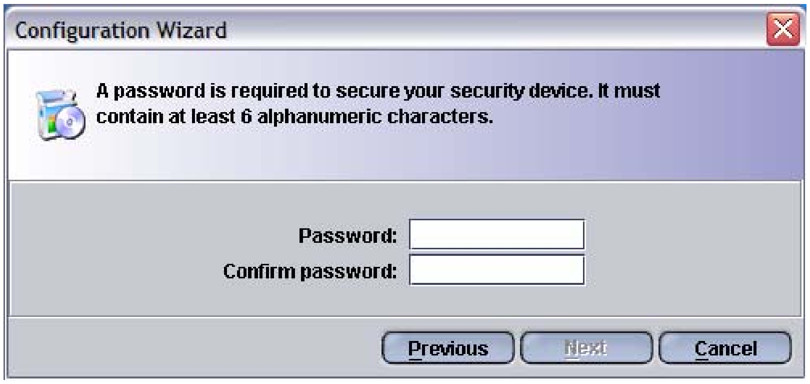
Once you have chosen a name for your device, click **Next** to continue.

The ensuing dialog in the Configuration Wizard requires that you provide an administration password for the device. This password is very important in that anyone who knows it will have full access and control of the security device. Passwords are case-sensitive and must be at least six characters in length.

Installation Step:

13 – Creating a Device – Step 8

Assign an Administration Password to the security device. This should be carefully guarded as anyone with access to this password will have full access to the security device and will be able to make configuration changes.



Configuration Wizard

A password is required to secure your security device. It must contain at least 6 alphanumeric characters.

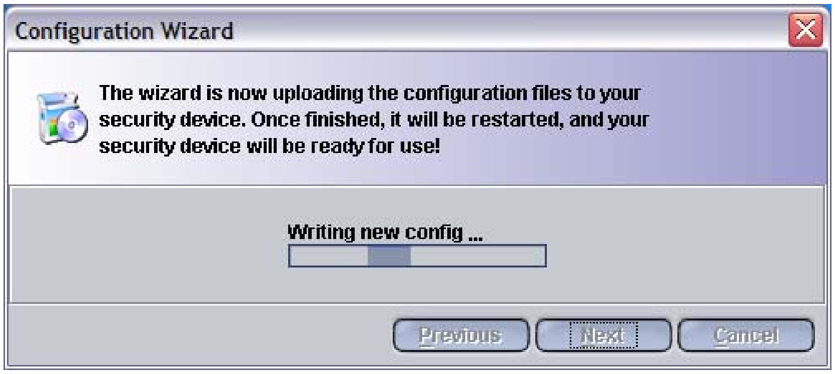
Password:

Confirm password:

Figure 7-8: Assign an Administration Password

Don't forget this password! You will need it later; any time you want to upload a new configuration to the device or retrieve settings from the device. If you are familiar with using SSH and the Linux command line, you can also use this password to log into your security device using SSH client software. (More on this in Section 12.)

At this point, the Configuration Wizard has all the information it needs to configure the device to a working state. The next screen in the Configuration Wizard, as shown below, is simply a way to monitor progress as the configuration is uploaded to the device and implemented. This process can take several minutes to complete.



Configuration Wizard

The wizard is now uploading the configuration files to your security device. Once finished, it will be restarted, and your security device will be ready for use!

Writing new config ...

Figure 7-10: Uploading New Configuration

Once the configuration upload process is complete, the new device configuration will immediately be implemented. If you are configuring a GG-OS device, you will notice the device console has been updated to reflect the uploaded configuration.

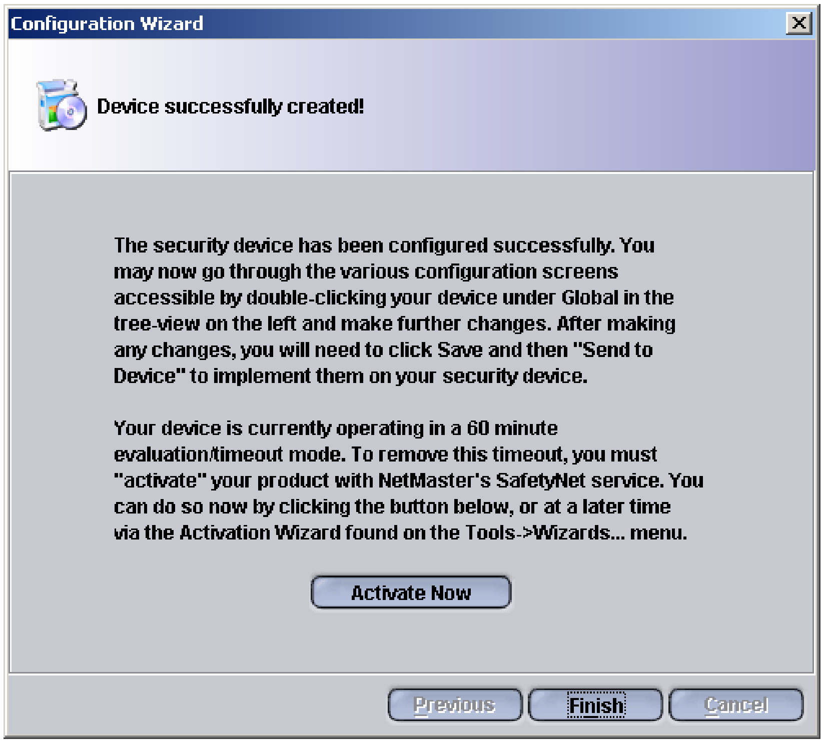
The next dialog in the Configuration Wizard, as shown below, will be displayed once the configuration upload process has been completed.

Installation Step:

14 – Creating a Device – Step 9

Click **Activate Now** if the workstation you are running CSM on currently has access to the Internet.

Otherwise, click **Finish** to complete the security device creation process and run the Activation Wizard at another time.



The security device has been configured successfully. You may now go through the various configuration screens accessible by double-clicking your device under Global in the tree-view on the left and make further changes. After making any changes, you will need to click Save and then "Send to Device" to implement them on your security device.

Your device is currently operating in a 60 minute evaluation/timeout mode. To remove this timeout, you must "activate" your product with NetMaster's SafetyNet service. You can do so now by clicking the button below, or at a later time via the Activation Wizard found on the Tools->Wizards... menu.

Figure 7-11: Configuration Wizard Success

As per the onscreen instructions, your security device is now operational but will be running in an Evaluation Mode until such time as you activate your product with SafetyNet.

Click on the **Activate Now** button to begin the Activation Wizard. This step can only be successful if the system you are running CSM on has access to the Internet (and, thus, NetMaster SafetyNet).

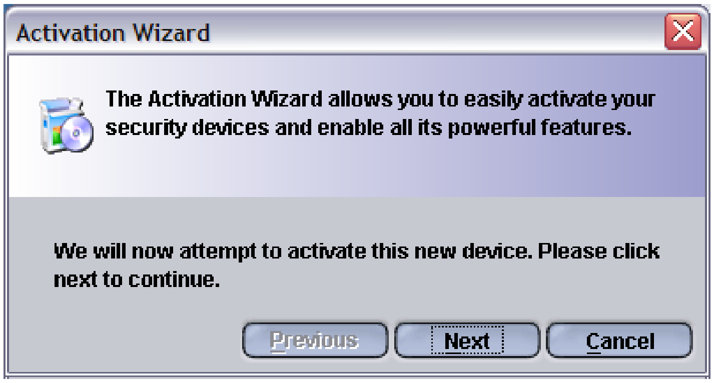
The Activation Wizard

NetMaster's Activation Wizard is used to validate your security device and it's Serial Number with SafetyNet. Until the device and Serial Number has been validated with SafetyNet, the security device will operate in a 60 minute Evaluation Mode and you will not be able to download software updates that may be available. After 60 minutes, the device will timeout and cease to function until it is rebooted. This will then begin another 60 minute evaluation period.

Activating a NetMaster product is a simple process as described below.

The Activation Wizard can be started in one of three ways; by clicking on the "**Activate Now**" button at the end of the Configuration Wizard (as shown in Figure 7-11), by clicking on the Activation Wizard menu item in the Tools Menu, or by pressing the **<Ctrl-A>** hotkey sequence.

The first dialog in the Activation Wizard is simply an introductory page.



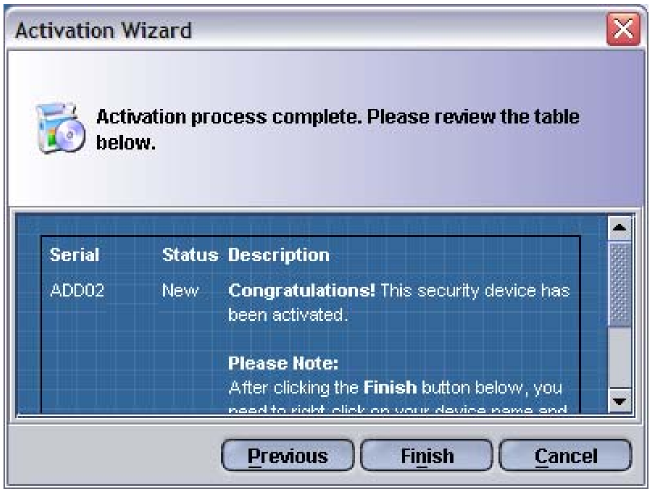
The Activation Wizard allows you to easily activate your security devices and enable all its powerful features.

We will now attempt to activate this new device. Please click next to continue.

Figure 7-12: Activation Wizard – Step 1

Click **Next** when you are ready to continue.

The second dialog in the Activation Wizard initiates communications with SafetyNet and passes several parameters back to NetMaster in order to validate your security device. If you security device information is valid and the device can be activated, you will see a results screen similar to the following:



Activation process complete. Please review the table below.

Serial	Status	Description
ADD02	New	**Congratulations!** This security device has been activated. **Please Note:** After clicking the **Finish** button below, you need to right click on your device name and

Figure 7-13: Activation Wizard – Step 2

This dialog identifies that your security device has now been activated. The bottom part of the results page above (which is partially hidden) reminds you to now send the configuration to the device in order to complete the device activation process.

Please Note: This activation process sends to NetMaster SafetyNet only the information necessary to activate your product. No personal or private information is ever sent at any time. If you would like more information on this process, please contact support@netmaster.com.

Once you have activated your security device using the Activation Wizard above, be sure to upload your new configuration to the device. Doing so will cancel the Evaluation Mode timer and your device will be fully operational.

Where to from here?

Installation Step:

15 – Creating a Device – Finish

Your security device is now up-and-running and should be fully functional in a typical office environment.

Once you have completed the initial configuration of your security device and the Configuration Wizard and Activation Wizards have been closed, you are now ready to make additional and advanced configuration changes to your device as required to suite your specific needs. These changes may include customized firewall rules, the implementation of a DHCP Server for your local area network, a secure VPN connection to a remote network, creation of bandwidth management rules, or any one of the other advanced features and functionality provided by your NetMaster security device. Each of these topics is covered in much more detail in the following sections of this document.

Right now would also be a good time to check **SafetyNet**, if you haven't already, and download any software updates that have been made available by NetMaster.

8 - Device Configuration

This section of the document will take you through the security device configuration options available under the **Device Configuration** menu of the device within the tree view of CSM. Within this menu is where all device operating system configuration parameters are set and maintained.

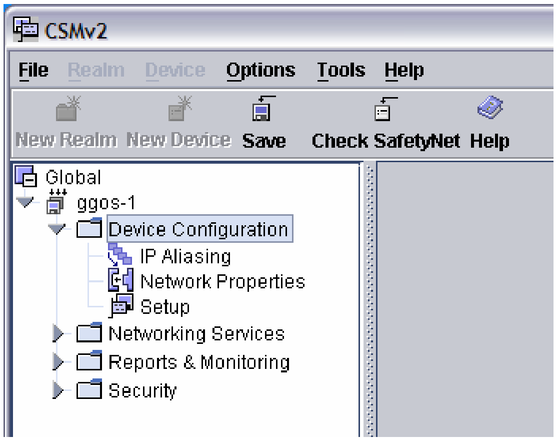


Figure 8-1: Device Configuration

IP Aliasing

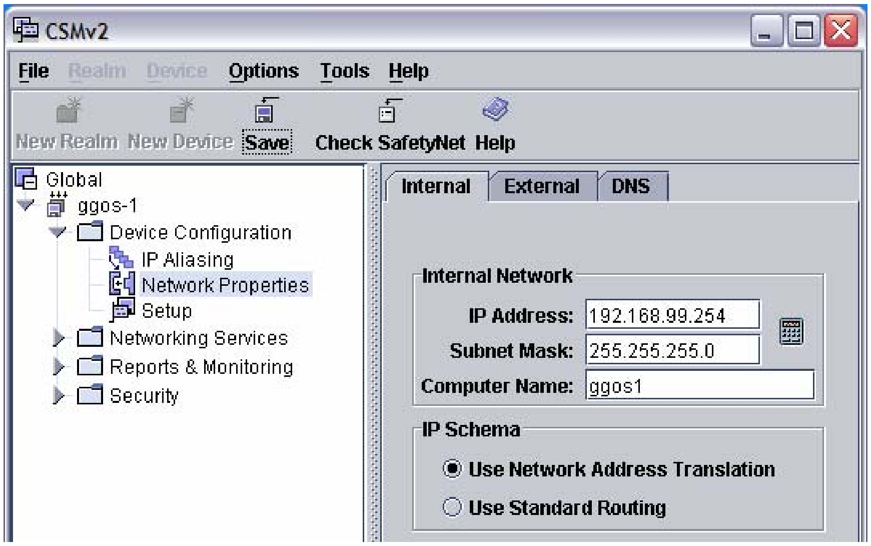
IP Aliasing, a feature often referred to as Multi-Homing, allows the NetMaster security device to bind multiple IP Addresses to the external Ethernet interface of the device. This module can be used to assign as many as 252 IP Addresses to the external interface. (Of the 254 available addresses in a Class C subnet, one is used as the main IP for the device. The other must be used for the Default Gateway.)

IP Aliasing is most often used in firewall implementations running in Network Address Translation Mode and having more than one web server, mail server, or other service located behind the firewall. For example in order to forward incoming web traffic to more than one web server located behind the firewall, each web server must have a unique IP Address assigned to it using this IP Aliasing module. Once this has been done, firewall rules can be implemented to forward all web traffic arriving at one IP Address to be forwarded to one of the web servers and all web traffic arriving at the other IP Address will be forwarded to the other web server.

Using IP Aliasing, any number of servers and services can be secured behind one NetMaster security device.

Network Properties

This device configuration option is where you can set the core IP Address information for the security device and is divided into three main areas: Internal, External, and DNS.



IP Address: 192.168.99.254
Subnet Mask: 255.255.255.0
Computer Name: ggos1

● Use Network Address Translation
○ Use Standard Routing

Figure 8-2: Network Properties – Internal

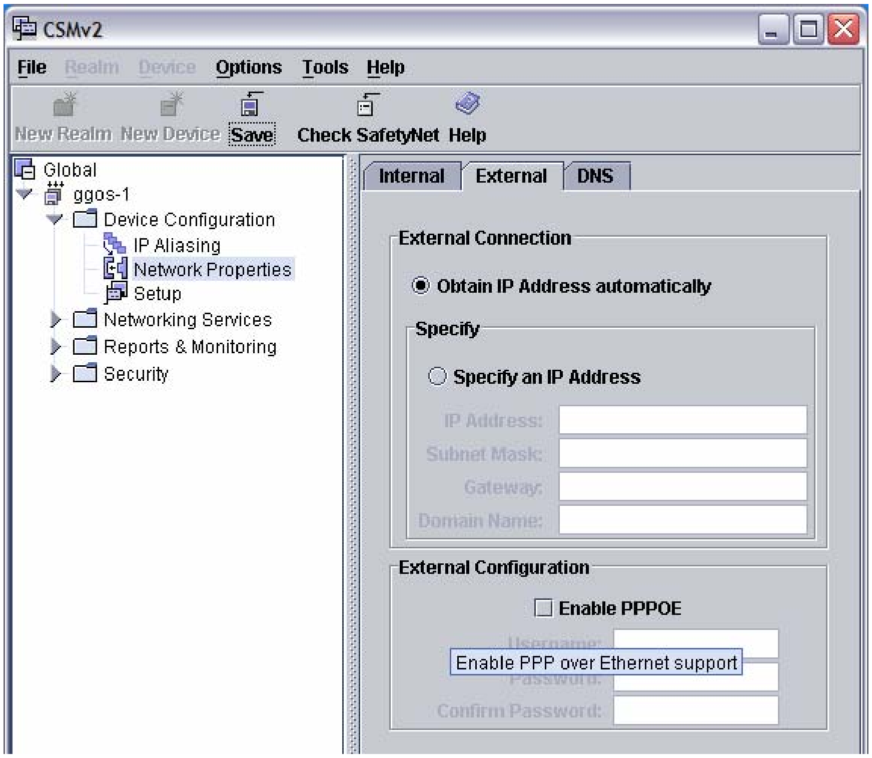
The **Internal** page is where you can set the IP Address information for the internal Ethernet interface of the security device. Also, here is where you can set the **IP Security Scheme** for your security device. Network Address Translation, or NAT, is almost always used; however, some security device implementations may require the use of a standard routing configuration.

- **Network Address Translation (NAT):** This operation mode configures the device to "translate" all outbound communications in order to appear to the remote end as coming from the device itself instead of the internal workstation where the communication has originated. There are several reasons for doing this, but the most common reasons are:
  - To hide the internal network configuration and number of internal workstations from the outside.
  - To minimize the number of "public" IP Addresses required. (With NAT, all internal network devices can use "private" IP Addresses that are not allowed to be used on the public Internet.)
  - To block the ability for external hosts to establish communications with internal network devices. (The only device that is accessible from the outside is the security device itself.)

- **Standard Routing:** This operation mode configures the device as a standard router albeit with a significant number of additional features and functionality. This mode is used when all internal hosts need to be routable from the external network.

The **External** page of the Network Properties menu item is used to configure the external Ethernet interface of the device. By default, the CSM Configuration Wizard sets up every device to automatically retrieve its external configuration from a remote device – such as the DHCP Server of your Internet Service Provider (ISP).

If your ISP has provided you with a "static" IP Address, or you would like to specify and assign your own IP Address to the external interface, or your ISP requires the use of PPP over Ethernet (PPPoE), use this page to fill in the details as necessary.



External Connection

● Obtain IP Address automatically

Specify

○ Specify an IP Address

IP Address:

Subnet Mask:

Gateway:

Domain Name:

External Configuration

☐ Enable PPPOE

Username:

Password:

Confirm Password:

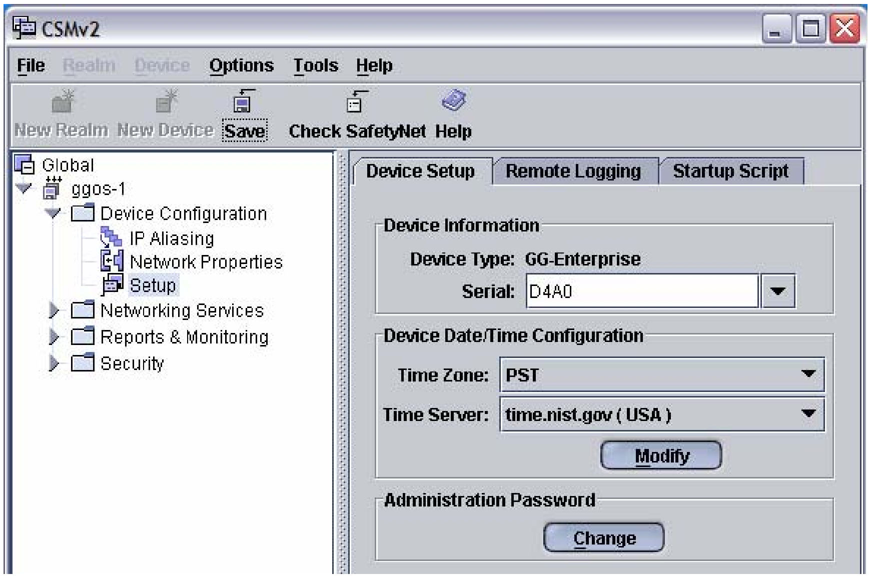
Enable PPP over Ethernet support

Figure 8-3: Network Properties – External

The third and final page of Network Properties is called **DNS** and is where you can specify which DNS Servers the device should use and be passed on to local network DHCP Clients if you have enabled the DHCP Server service (more information on the DHCP Server service can be found in Section 9). If your device is configured to retrieve an IP Address automatically for the external Ethernet interface, you do not need to provide this information, as it will be automatically configured for you.

Setup

The **Setup** configuration menu item is used to manage a fair number of device configuration details.



Device Type: GG-Enterprise

Serial: D4A0

Time Zone: PST

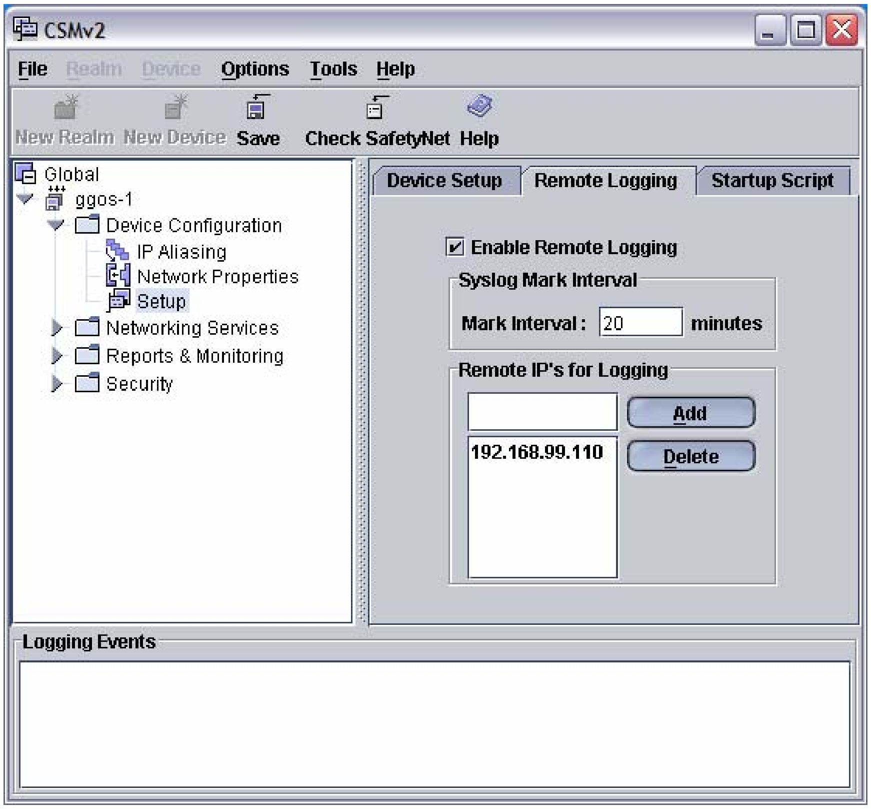
Time Server: time.nist.gov (USA)

Figure 8-4: Device Setup

The security device can be configured to automatically synchronize its system date and time with a remote time-server. Simply identify the time zone the device will be operating in and choose a Time Server to synchronize with. Alternatively, you can specify your own Time Server, if required, by clicking on the Modify button and adding your own Time Server to the list.

Any time you need to change the security device **Administration Password**, simply click on the **Change** button and provide the new password in the ensuing dialog box. (Be sure to remember to upload your new configuration to the device in order to activate the new password.)

The next page of the security device Setup can be used to enable and configure Remote Logging. By default, all remote logging is turned off; however, it should be enabled in most cases in order to remotely log various events detected on the security device.



☑ Enable Remote Logging

Syslog Mark Interval

Mark Interval : 20 minutes

Remote IP's for Logging

192.168.99.110

Logging Events

Figure 8-5: Remote Logging

To enable Remote Logging, click on the **Enable Remote Logging** checkbox and then type in the IP Address of a remote system that will be configured to accept logged events from the security device. The NetMaster CSM software is configured to accept log messages being sent from a security device. Any received messages will be appended to the **Logging Events** area located at the bottom of the CSM application window. Note, however, that CSM can only log events if there isn't already a "Syslog" service running on the local system. (This is very likely if you're running software such as the Kiwi Syslog Daemon for Windows, or if you're running CSM on a Linux or Mac OS X operating system.)

Type the IP Address of the computer running CSM into the text field located beside the Add button and click **Add** to identify to the remote security device that this host is authorized to receive event messages. The next time you upload configuration changes to the security device, you should begin to see event messages being logged into the **Logging Events** area located at the bottom of the CSM application window.

The third page of the security device Setup module can be used to identify and special startup commands that need to be run once the system startup is complete. This is an advanced feature and is typically only used for system debugging purposes. However, if you are familiar with the inner workings of the Gateway Guardian Operating System and have a good understanding of Linux/Unix shell scripting, you can use this facility to add your own commands to be executed at system startup.

9 - Security Configuration

This section of the document will take you through the security device configuration options available under the **Security** menu of the device within the tree view of CSM. Within this menu is where all core security features of the product are configured and managed.

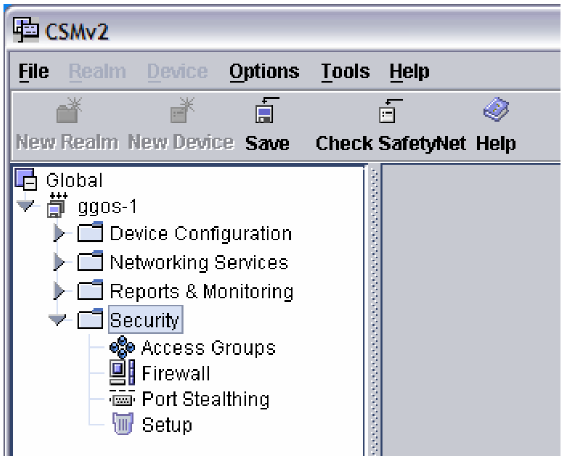
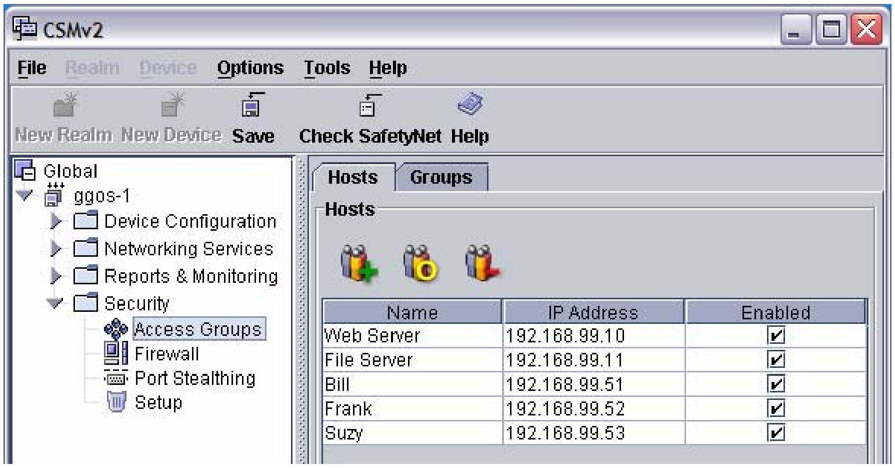


Figure 9-1: Security Configuration

Access Groups

Access Groups allow you to combine network users, servers, and other devices into functional groupings that you can then apply access policies to. Both firewall rules and bandwidth management rules can be applied to Access Groups. Access Groups can also have time-based firewall rules applied to them, whereby the rules created against the group will only be in effect during the times/days specified.



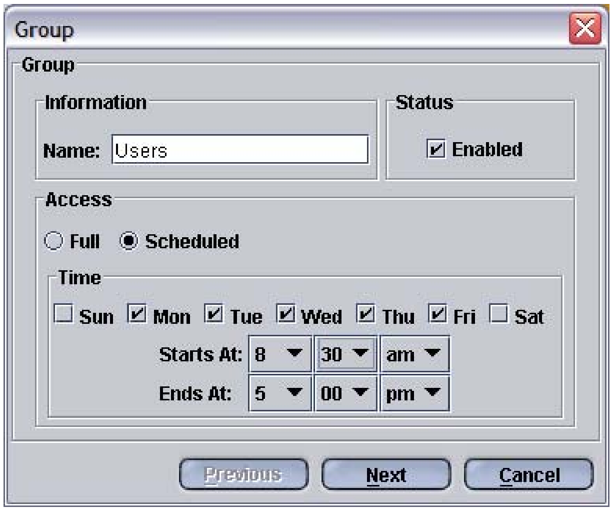
Name	IP Address	Enabled
Web Server	192.168.99.10	☑
File Server	192.168.99.11	☑
Bill	192.168.99.51	☑
Frank	192.168.99.52	☑
Suzy	192.168.99.53	☑

Figure 9-2: Access Control Groups

Before you can create Access Control Groups, you need to define the network users, servers, and other devices that you will be assigning to the various groups that you create. This can be accomplished using the **Hosts** page of this module as shown above in Figure 8-2.

Once all the necessary entries have been made in the Hosts page, click the **Groups** tab to view the Groups page of this module.

Clicking the Add Group button will display a dialog box similar to the following within which a group can be named and you can define whether this group will be used to define time-based rulesets.



Name: Users

☑ Enabled

○ Full ● Scheduled

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

Starts At: 8 30 am

Ends At: 5 00 pm

Figure 9-3: Creating an Access Control Group – Step 1

Once the group has been named and any required changes to the access schedule have been made, click **Next** to proceed to the next step in the process of creating an Access Control Group.

The next dialog, as shown in Figure 8-4, is used to assign the users, servers and other network devices created previously to the Group being created.

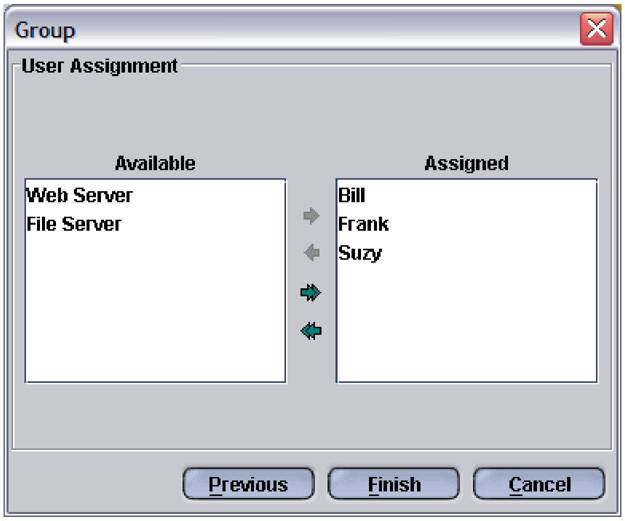


Figure 9-4: Assigning Users/Hosts to a Group

Move the entries from one list box to another until all of the desired users, servers, and other network devices are listed on the **Assigned** side. Click **Finish** to close the dialog and create the Access Control Group.

Firewall

This module is used to define and implement the access security policies for traffic passing through the security device. This module provides the core functionality for the device and, as the name implies, is what makes it a firewall.

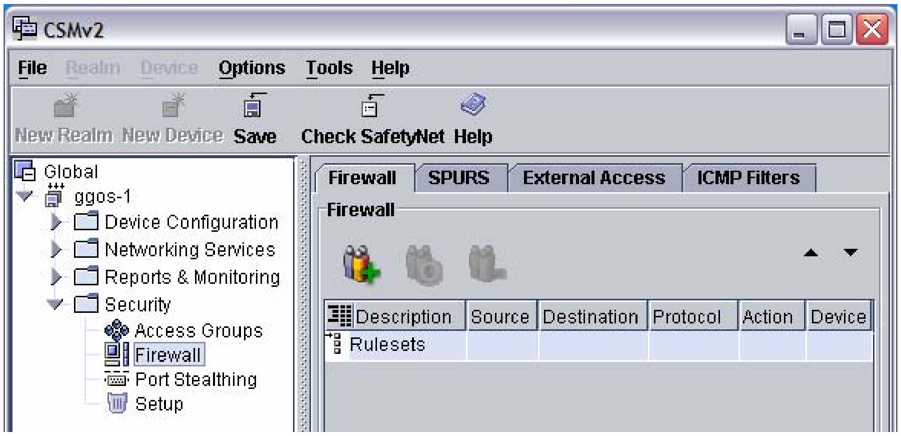
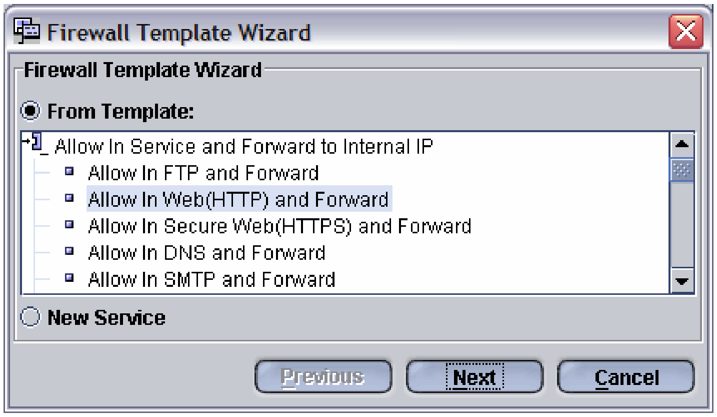


Figure 9-5: Device Firewall Module

This module is broken up into several sections including **Firewall**, **SPURS**, **External Access**, and **ICMP Filters.**

The **Firewall** page of this plugin is where all Global Firewall Rulesets are defined. Each ruleset is defined using a two-step wizard as shown below:


Firewall Template Wizard

Firewall Template Wizard

● From Template:

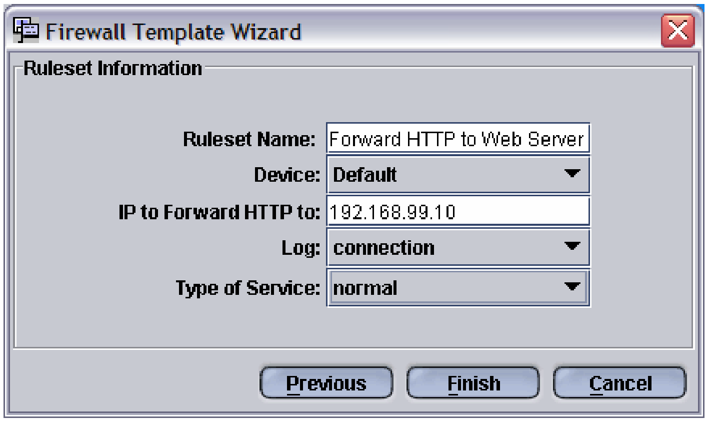
- Allow In Service and Forward to Internal IP
  - Allow In FTP and Forward
  - Allow In Web(HTTP) and Forward
  - Allow In Secure Web(HTTPS) and Forward
  - Allow In DNS and Forward
  - Allow In SMTP and Forward

○ New Service

Figure 9-6: Firewall Ruleset Wizard – Step 1

The first stage of the Wizard is to choose a ruleset from the list provided. Hundreds of pre-defined rulesets have been defined for you; however, if you cannot find one matching what you need to accomplish, simply click on the radio button labelled "New Service" and click **Next** to define your own set of rules.

Once you have found the ruleset template meeting your requirements, double-click on it to move to the next dialog in the wizard. (Alternatively, simply click **Next** to continue to the next dialog….)


Firewall Template Wizard

Ruleset Information

Ruleset Name: Forward HTTP to Web Server
Device: Default
IP to Forward HTTP to: 192.168.99.10
Log: connection
Type of Service: normal

Figure 9-7: Firewall Ruleset Wizard – Step 2

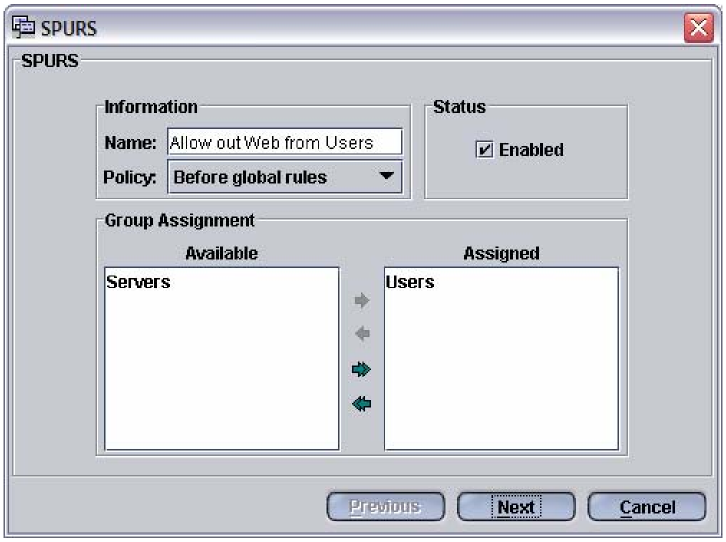
Once you have selected a pre-defined ruleset template, you must provide additional information in order to implement the ruleset. In Figure 8-7 above, the "Allow in Web and Forward" ruleset template has been configured to forward any incoming HTTP data on the external interface on to the web server located at 192.168.99.10. In addition, all connections made to the web server through the firewall will be logged.

Click **Finish** on this dialog to create the ruleset and close the Wizard.

Once you have returned to CSM, you will notice that a ruleset consists of several individual firewall rules; sometimes as many as 5 or more. As you can see, using Firewall Ruleset Templates makes things significantly easier for the administrator to implement data access and security policies.

The **SPURS** (Security Policy User Rule Set) page is where all firewall rulesets to be assigned to Access Control Groups are defined. Via the time settings defined within Access Control Groups (see beginning of this section), firewall rules defined here can be time-based rulesets.

A two-step wizard is used in defining a SPURS entry. The first dialog of the wizard, as shown in Figure 8-8, is used to name the SPURS, define what Access Control Groups this ruleset is to be applied against, and whether the firewall policies defined (in the next step) are to be applied before the Global Firewall Rules, or after. In most cases, SPURS are applied before the Global Rules.

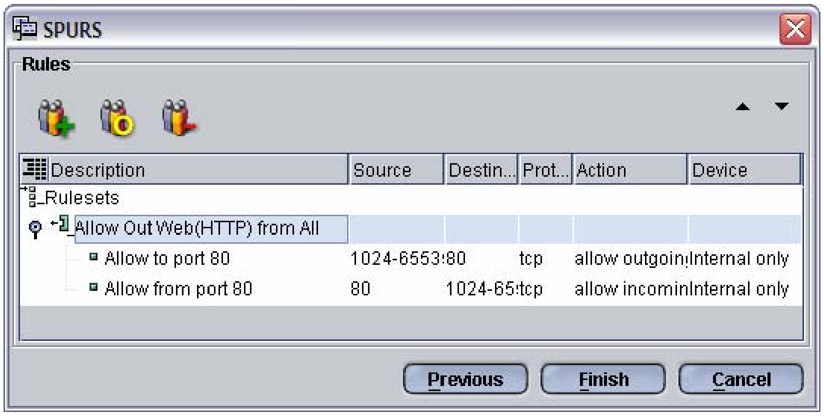


Name: Allow out Web from Users
Policy: Before global rules
☑ Enabled

Figure 9-8: Create a Security Policy User Rule Set (SPURS)

Once you have provided a name for the SPURS entry and identified what Access Control Groups to apply the ruleset against, click **Next** to continue.

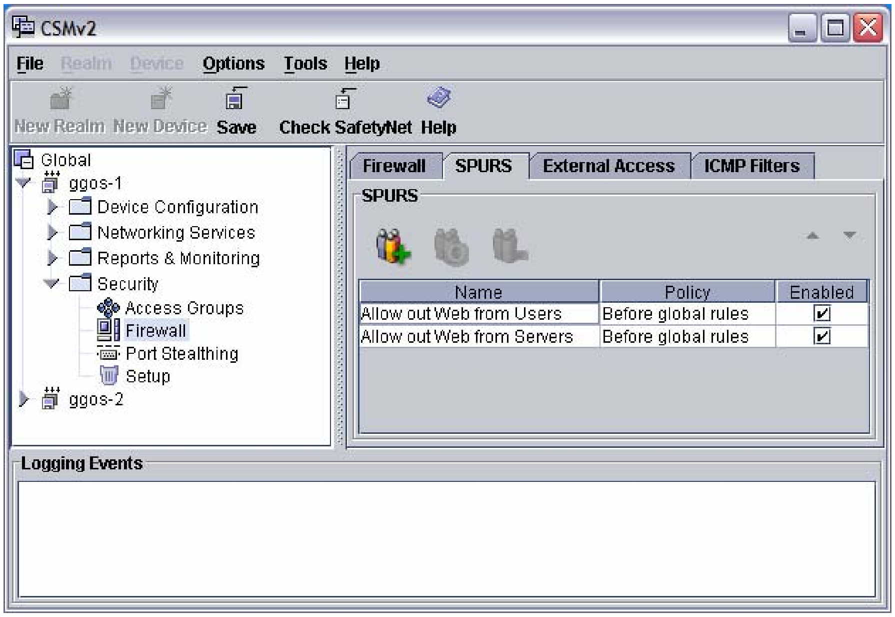
The next dialog displayed when creating a SPURS entry is shown below in Figure 8-9. This dialog is used to assign firewall rulesets to the SPURS entry and works the same way as when defining global firewall rulesets as described earlier in this section.



Description	Source	Destin...	Prot...	Action	Device
Rulesets					
Allow Out Web(HTTP) from All					
Allow to port 80	1024-6553	80	tcp	allow outgoin	Internal only
Allow from port 80	80	1024-65	tcp	allow incomin	Internal only

Figure 9-9: Assigning Firewall rules to a SPURS entry

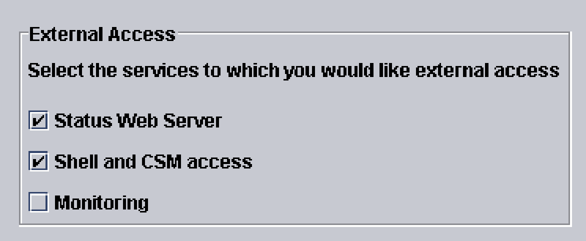
Once the necessary firewall rulesets have been applied to the SPURS entry, click **Finish** to close the dialog and return to the main CSM application window. The SPURS entry you have defined will be displayed as shown in Figure 8-10.



Name	Policy	Enabled
Allow out Web from Users	Before global rules	☑
Allow out Web from Servers	Before global rules	☑

Figure 9-10: Security Policy User Rulesets (SPURS)

The **External Access** page, as partially shown in Figure 8-8, provides a quick way to implement several commonly used firewall rulesets. Security device users must be able to quickly and easily define whether external hosts should be permitted to access the security device's Status Web Server or Administration Access functions. These options are disabled by default, which means that the security device cannot be monitored or configured from outside the network (i.e. over the Internet). If these functions need to be accessible from the external network, simply click the appropriate checkbox to enable the feature.


External Access

Select the services to which you would like external access

☑ Status Web Server

☑ Shell and CSM access

☐ Monitoring

Figure 9-11: External Access to Common Functions

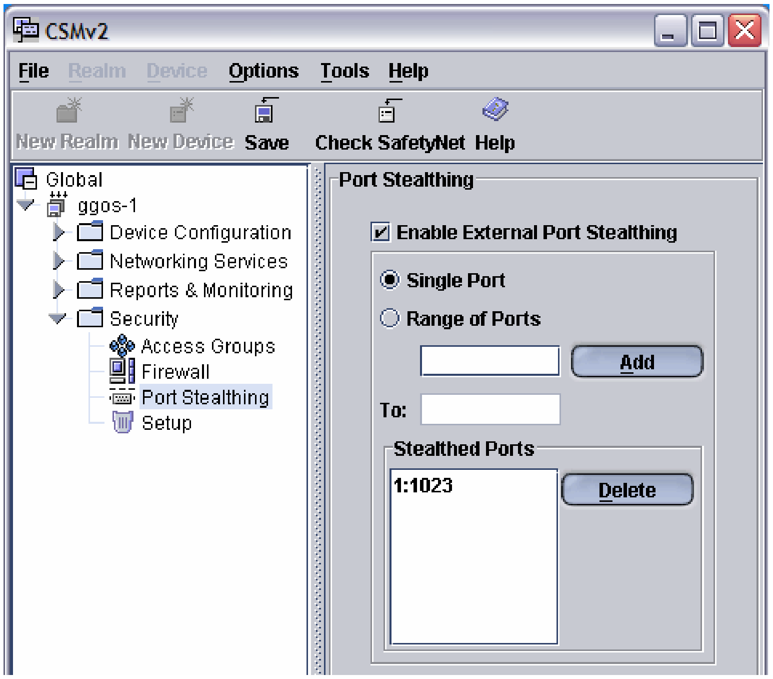
The **ICMP Filters** page provides the device administrator detailed control over how ICMP traffic is handled by the security device. This is an advanced feature and the defaults, as configured, should only be modified under very special circumstances.

Port Stealthing

Port Stealthing is an important part of every security device and is used to hide your security device from "prying eyes" in the outside world.

Would-be hackers utilize port-scanning software to find devices on the Internet. This software tries connecting to various ports at the specified IP Addresses to determine, first, if a device exists at that IP Address and, if so, then tries to determine what type of device it is. (In order to determine whether it's worthy of additional consideration.)

The port stealthing feature of the security device works to ensure that port-scanning software cannot detect that something even exists at the IP Address being scanned. This feature significantly reduces the chances that a probe or attack will be launched against your security device and, thus, your network.



Port Stealthing

☑ Enable External Port Stealthing

● Single Port

○ Range of Ports

Stealthed Ports

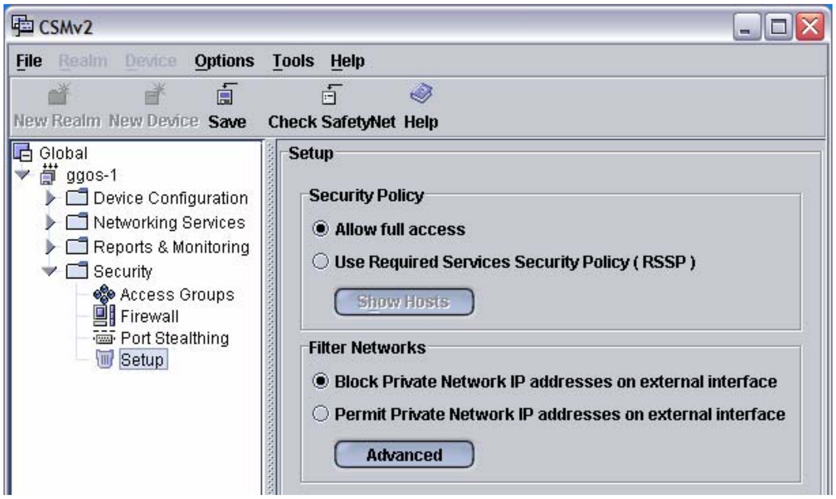
1:1023

Figure 9-12: Port Stealthing

By default, your security device is configured to stealth the so-called Privileged Ports ranging from 1 through 1023. All other ports (1024 through 65534) are considered unprivileged ports and are typically bypassed by port-scanning software.

Setup

This module is used to define two important aspects of the security policy implementation for your security device.



Setup

Security Policy

● Allow full access

○ Use Required Services Security Policy (RSSP)

Filter Networks

● Block Private Network IP addresses on external interface

○ Permit Private Network IP addresses on external interface

Figure 9-13: Security Setup

The **Security Policy** setting, as shown in Figure 8-10 above, is a critical and fundamental part of how your security device is deployed and functioning on your network.

By default, **Allow full access** is enabled. This setting allows all users, workstations, servers, and other network devices full access to the external network (the Internet).

The other setting, **Required Services Security Policy (RSSP)**, varies from the above in that if this feature is enabled, by default, all of the users, workstations, servers, and other network devices will be ***denied*** access to the external network unless explicitly allowed to do so via firewall rules that have been defined within the Firewall module. RSSP is the basis for a ***"least privilege policy"*** for Internet access.

Please Note: With either of these settings, the security device is configured, by default, to deny all incoming connection requests from the external network to the device itself or the internal network. In other words, this **Security Policy** setting does not create any "holes" through your firewall from the outside in. This setting only defines what's allowed, by default, from the inside out.

The other parameter defined with this plugin is **Filter Networks**. By default the security device is configured to ignore any incoming traffic originating from Private Class IP Addresses. (As defined in RFC XXXX.) If, however, you are using the security device on your local network to secure one network segment from another, you may need to modify this setting to permit Private Class IP's on the external interface.

The **Advanced** button can be used to modify the list of defined Private Class IP subnets.

10 - Networking Services

This section of the document will take you through the security device configuration options available under the **Networking Services** menu of the device within the tree view of CSM. Within this menu is where all device operating system services are configured and maintained.

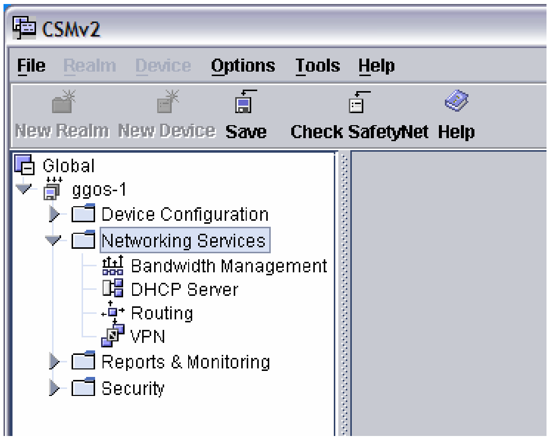


Figure 10-1: Networking Services

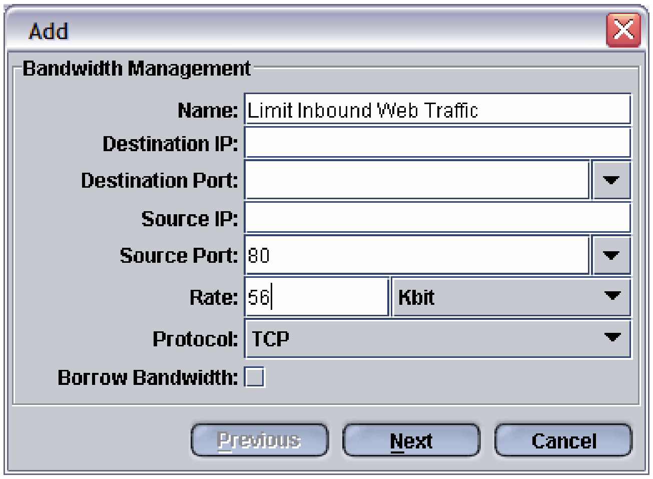
Bandwidth Management

The Bandwidth Management module is used to control the traffic flowing through the security device; in and out of the local network. Bandwidth usage can be controlled on either a protocol or a per-user basis. In other words, a particular network user's usage patterns can be controlled or limited, or the same can be done with a particular Internet protocol, such as streaming audio.

Bandwidth Management allows you to set up different bandwidth limits for various regions of your network. You can configure Bandwidth Management by a source or destination IP Address, by source or destination Port, by protocol (TCP or UDP), or by any combination of each of these parameters.

Bandwidth Management is an important aspect of good network design. Any organization having a dedicated Internet connection may often want to limit or control the amount of bandwidth being used in particular areas. For example, you may want to allow your web and mail servers to have full access to the Internet bandwidth at all times, but restrict all network users (except for yourself, of course) to the equivalent of a 128Kbit ISDN feed for all web surfing activity.

Creating a Bandwidth Management rule is accomplished via a two-step wizard as shown below.



Add

Bandwidth Management

Name: Limit Inbound Web Traffic
Destination IP:
Destination Port:
Source IP:
Source Port: 80
Rate: 56 Kbit
Protocol: TCP
Borrow Bandwidth: ☐

Figure 10-2: Bandwidth Management Wizard – Step 1

This first page of the Bandwidth Management wizard allows you to define various parameters of the bandwidth management ruleset. The screenshot shown in Figure 9-2 above demonstrates the settings required to set the maximum amount of incoming web traffic on port 80 to 56Kbps – equivalent to the speed of an analog modem!

Enabling the Borrow Bandwidth checkbox at the bottom of the dialog, will allow the managed IP Address or Port traffic to use more than the allotted bandwidth if extra bandwidth is currently available and not being used elsewhere. As other traffic begins to saturate the connection, the managed IP Address or Port will be, once again, shaped down to their maximum allowable data rate. If this checkbox is disabled, as it is by default, the managed IP Address or Port will never receive more than it's allotted bandwidth as specified in the data Rate field.

Once the necessary fields have been filled out as required, click the **Next** button to continue.

The next dialog of the Bandwidth Management wizard, as shown below in Figure 9-3, allows you to specify what Access Groups (see Section 8) to apply the Bandwidth Management rule to.

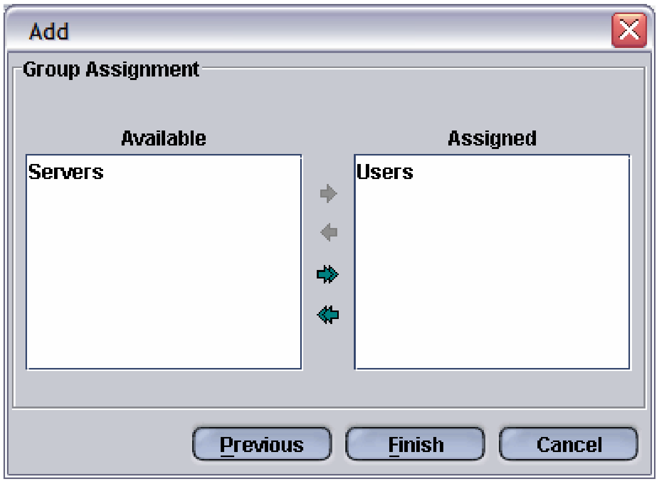


Figure 10-3: Bandwidth Management Wizard – Step 2

By default, Bandwidth Management rules that you create will be assigned to Everybody; however, you can modify this as necessary to suite your specific needs.

Click **Finish** to implement the Bandwidth Management rule.

DHCP Server

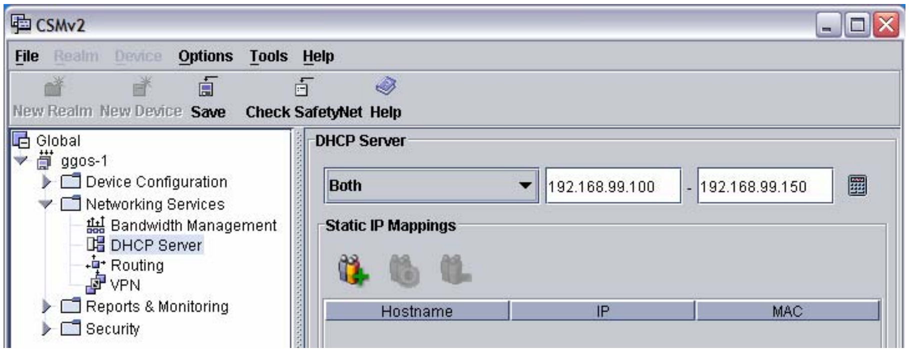
Maintaining IP Address assignments for workstations, servers, and other devices on any sized network can quickly become almost unmanageable. DHCP (the Dynamic Host Configuration Protocol) allows you to easily connect devices to your network without client-level configuration. GG-OS can act as a DHCP Server for your network, automatically configuring all DHCP Clients with appropriate IP Address, Subnet Mask, Default Gateway, Domain Name, and DNS Server information.

Your security device can also act as a DHCP Client on the external network, automatically retrieving IP Address and other network settings from your Internet Service Provider's DHCP Server. While operating as a DHCP Client on the external network and a DHCP Server on the internal network, your security device will pass along various configuration settings received from your ISP, such as a Domain Name and DNS Server IP Addresses, to your internal network hosts.

Alternatively if your security device is configured with a static IP Address on the external interface and you have manually provided Domain Name and DNS Server IP Address values, these too will be passed along to internal network DHCP Clients while the device is operating as a DHCP Server.

DHCP Clients can be assigned IP Addresses in one of two ways. Either dynamically from a pool of available IP's, or statically by having specific

IP's matched to the client's MAC Address. Static mappings are useful for printers and other such devices that you would like to remain relatively static; however, also want to easily change at any time from one central console. Mapping workstations to static IP addresses also makes managing and controlling Access Control Groups easier.



Both 192.168.99.100 - 192.168.99.150

Figure 10-4: DHCP Server Configuration

The DHCP Server service is not enabled by default. To enable it, simply click the mode in which you would like to operate in from the dropdown list box at the upper-right of the DHCP Server module. Make sure the DHCP Lease range you've specified falls within the same subnet range as the IP you've assigned to the internal network interface of your security device.

Static Routing

This module is important to every network configuration having more than one router attached to it. In some larger network topologies, the security device may be the Internet access point for a large network made up of many smaller networks. The security device must have a static route defined for each remote subnet in order to be able to route traffic for each of those subnets.

Virtual Private Networking

Virtual Private Networking (VPN) is the process of providing secure, encrypted data communications between two remote networks using a public, or otherwise untrusted, network between the two endpoints. In most cases, this public network is the Internet. Before VPN's were available, organizations had to resort to "leased-line" communications in order to connect remote networks together; which often proved prohibitively expensive. VPN's are proven, reliable, and cost-effective alternatives to leased-line implementations.

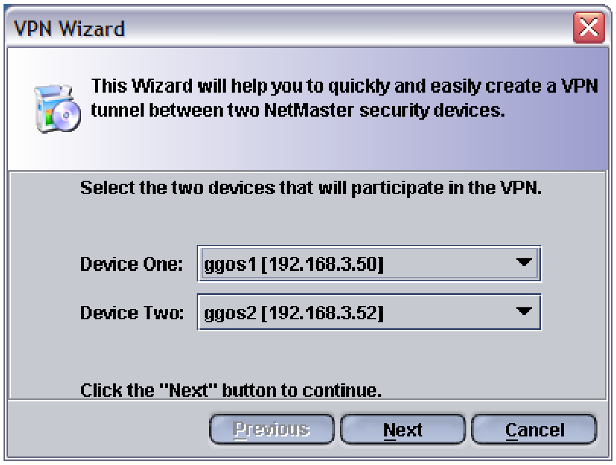
All of NetMaster's security devices provide fully IPSEC-compliant VPN services. IPSEC compliancy means that our products are easily configured to interoperate with other, third-party IPSEC-compliant devices.

VPN tunnels can be created between any number of disparate networks (network-to-network) or between a remote endpoint (client-to-network) "Road-Warrior" running VPN software such as what is integrated into Windows 2000/XP, or provided by a third-party, such as SSH Sentinel.

VPN Wizard:

In order to use the VPN Wizard to configure a VPN Tunnel between two devices, CSM must be properly synchronized with each of the devices. This synchronization is necessary because the devices themselves provide some of the information used in creating the tunnel.

Configuring a VPN tunnel between two security devices being managed within CSM is a simple, one-step process using the VPN Wizard. To create a VPN tunnel between two security devices, select **VPN Wizard** from the **Tools** menu, or hit **Ctrl-Z**, and the Wizard (Figure 9-5) will be displayed.



This Wizard will help you to quickly and easily create a VPN tunnel between two NetMaster security devices.

Select the two devices that will participate in the VPN.

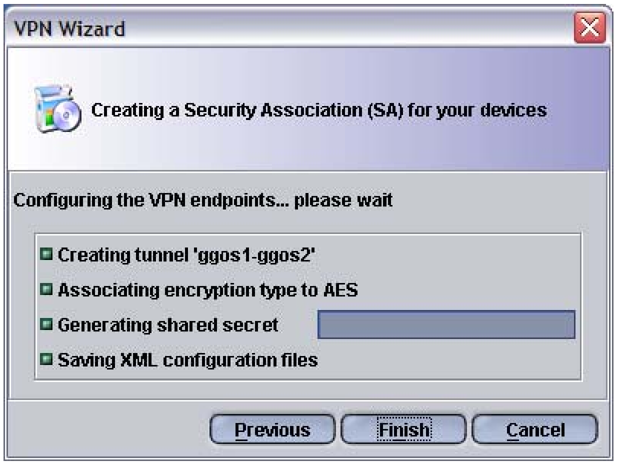
Device One: ggos1 [192.168.3.50]

Device Two: ggos2 [192.168.3.52]

Click the "Next" button to continue.

Figure 10-5: VPN Wizard – Step 1

Configuring a VPN tunnel between two security devices is as easy as selecting the two devices to be connected via the tunnel and clicking the **Next** button to continue. The ensuing dialog, as shown in Figure 9-6, simply shows the status as the VPN tunnel is created.



Creating a Security Association (SA) for your devices

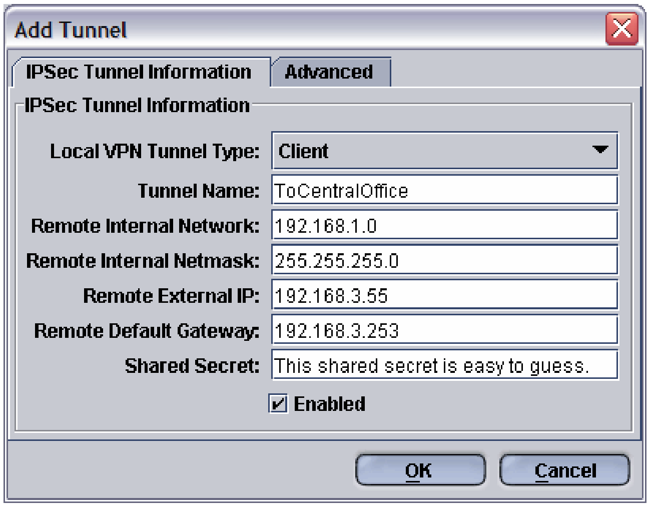
Configuring the VPN endpoints... please wait

- Creating tunnel 'ggos1-ggos2'
- Associating encryption type to AES
- Generating shared secret
- Saving XML configuration files

Figure 10-6: VPN Wizard – Step 2

Once the VPN tunnel creation process is complete, simply click **Finish** to continue.

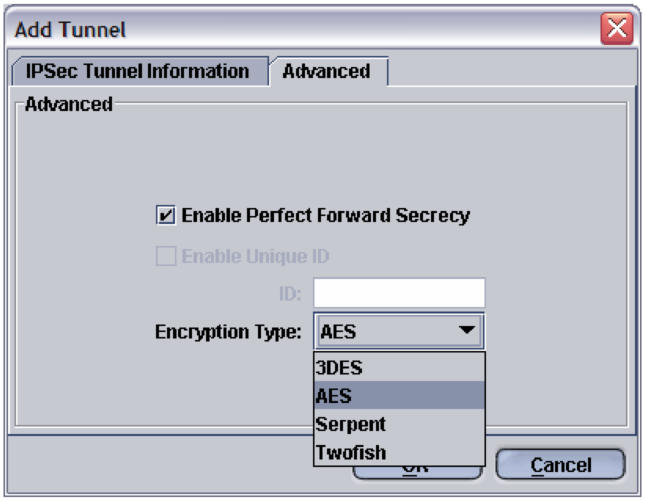
You can also create VPN tunnels manually. This is required when creating a network-to-network VPN tunnel between a NetMaster security device and a third-party IPSEC-compliant VPN device. To manually create a VPN tunnel, you must use the Add Tunnel button in the VPN module. This will display a dialog box, as shown in Figure 9-7, within which you must provide the necessary details to establish the connection to the remote VPN device. NetMaster has various White-papers on it's Technical Support website, providing additional information on configuring VPN tunnels with various third-party IPSEC-compliant VPN devices.



Local VPN Tunnel Type: Client
Tunnel Name: ToCentralOffice
Remote Internal Network: 192.168.1.0
Remote Internal Netmask: 255.255.255.0
Remote External IP: 192.168.3.55
Remote Default Gateway: 192.168.3.253
Shared Secret: This shared secret is easy to guess.
☑ Enabled

Figure 10-7: Manual VPN Tunnel Configuration – 1

When manually configuring a VPN tunnel, there are several advanced options available, which are used to customize the IPSEC tunnel parameters as necessary to establish a connection with the remote VPN device.



☑ Enable Perfect Forward Secrecy
☐ Enable Unique ID
ID:
Encryption Type: AES

Figure 10-8: Manual VPN Tunnel Configuration – 2

As per the dialog above, you'll note that four VPN tunnel encryption types are supported; 3DES, AES (Rijndael), Serpent, and Twofish. Triple-DES (3DES) is, by far, the most common VPN encryption algorithm and is provided for backward-compatibility with most third-party VPN products that do not support the newer encryption standards – AES and Twofish.

AES is the preferred VPN encryption algorithm as it can provide up to 100% tunnel performance increases over 3DES-encrypted tunnels.

The Rijndael, Serpent, and Twofish encryption algorithms were all standards competing to become the new Advanced Encryption Standard (AES). The Rijndael algorithm was eventually selected to become the AES. NetMaster's products still provide the Serpent and Twofish algorithms for end-user implementations requiring it.

11 - Reports and Monitoring

This section of the document will take you through the security device configuration options available under the **Reports and Monitoring** menu of the device within the tree view of CSM. Within this menu is where you can configure various features used to monitor your security device.

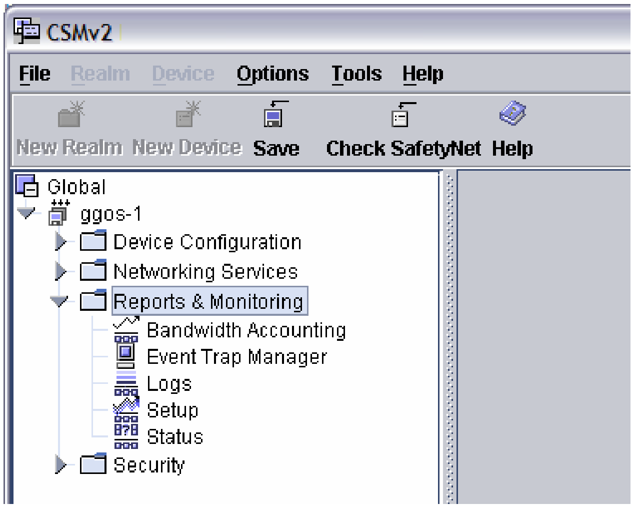


Figure 11-1: Reports and Monitoring

Bandwidth Accounting

The Bandwidth Accounting module is used to track the amount of data that has passed through the security device.

Event Trap Manager

NetMaster CSM incorporates the Simple Network Management Protocol (SNMP) in order to generate SNMP Traps to quickly alert system administrator(s) as monitored events occur or are detected on the security device. This is an extremely powerful feature of Gateway Guardian and CSM and provides the system administrator with the ability to quickly respond to these events as they occur.

Gateway Guardian uses a proprietary event trap analyser that sends SNMP Traps based on particular signature patterns as recorded by the system logger. Defining these signature patterns and enabling an SNMP Trap is a two-step process using the Event Trap Manager:

- Create a Service Signature Pattern for the particular daemon process to be monitored.

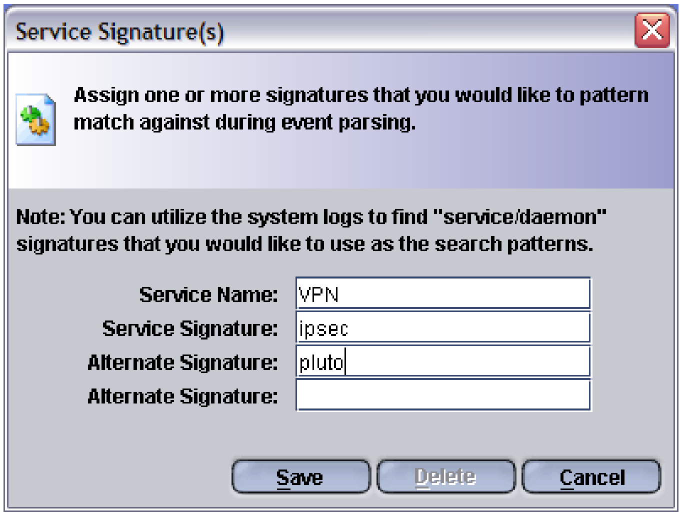
- Create an **Event Signature Pattern** to be associated with the Service Signature Pattern created above and point it to a system running an SNMP Trap Manager (such as NetMaster CSM, or HP OpenView, CA NetCenter, etc.).

Configuring Service Signature Patterns:

The Event Trap Manager monitors the information being logged to the security device system logger (syslog), looking for patterns matching the criteria defined within the Services tab of the Event Trap Manager plugin. This pattern is typically associated by the service/daemon, and can be viewed in the "Logging Events" window within CSM. Some common patterns include:

- **ssh** for the Secure Shell service
- **ipsec** for the VPN system service
- **cron** for the Cron system scheduling service
- **DENY** for any logged firewall Deny rules.
- **ACCEPT** for any logged firewall Accept rules.

Configuring a Service Signature is accomplished by clicking on the **Create New Service Signature** link within the Services tab of the Event Trap Manager module. Clicking this link will display a dialog box as shown in Figure 10-2.



Assign one or more signatures that you would like to pattern match against during event parsing.

Note: You can utilize the system logs to find "service/daemon" signatures that you would like to use as the search patterns.

Service Name: VPN
Service Signature: ipsec
Alternate Signature: pluto
Alternate Signature:

Figure 11-2: Create an SNMP Trap Service Signature

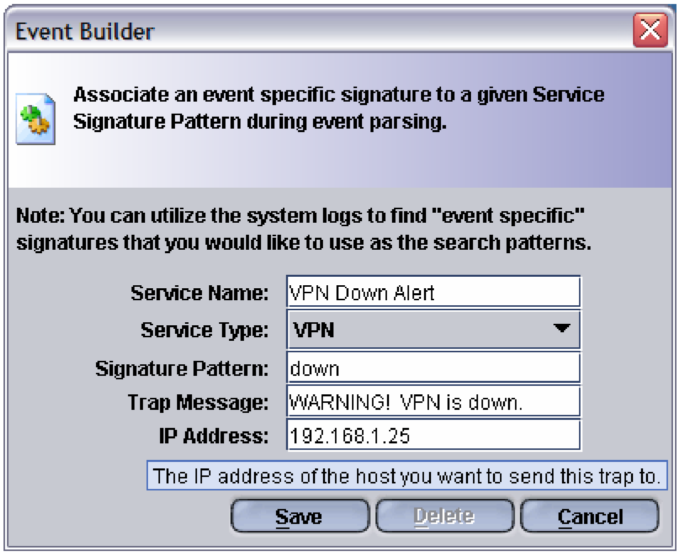
Fill in the fields as necessary and click **Save** to close the dialog and create the service signature pattern.

Once you have created a Service Signature, you must then create and associate one or more Event Signature Patterns to it. This is covered in the following section.

Configuring Event Signature Patterns

Once you have created a Service Signature Pattern, you need to assign Event Signature Patterns to it. These Event Signatures allow you to define the Event Signature Pattern (i.e. what pattern to look for in the logged event) and what trap message to send and where to send it.

Configuring an Event Signature is accomplished by clicking on the **Create New Event** link within the Events tab of the Event Trap Manager module. Clicking this link will display a dialog box as shown in Figure 10-3.



Associate an event specific signature to a given Service Signature Pattern during event parsing.

Note: You can utilize the system logs to find "event specific" signatures that you would like to use as the search patterns.

Service Name: VPN Down Alert
Service Type: VPN
Signature Pattern: down
Trap Message: WARNING! VPN is down.
IP Address: 192.168.1.25

The IP address of the host you want to send this trap to.

Figure 11-3: Create an SNMP Trap Event Signature

Fill in the fields as appropriate and click **Save** to close the dialog and create the event.

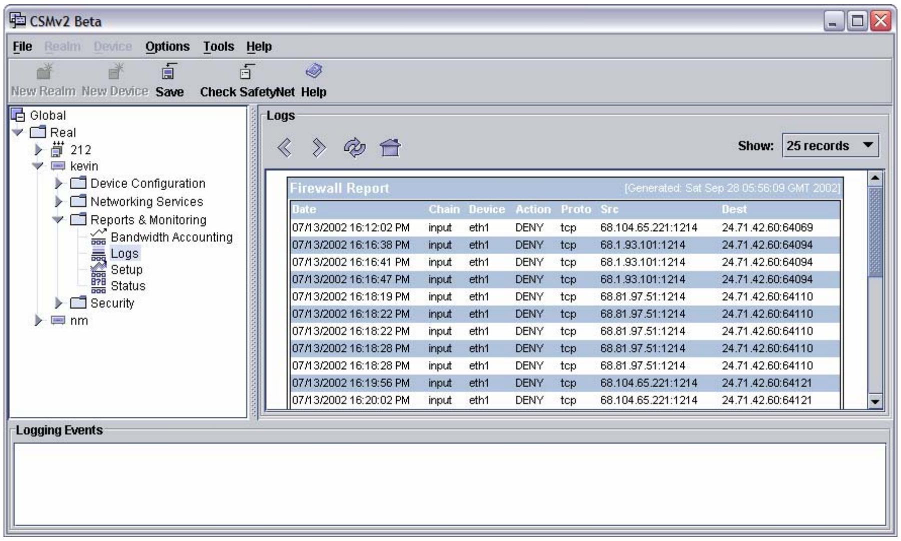
Once the new configuration has been uploaded to the security device, it will begin monitoring system events and will start sending SNMP Traps every time an event occurs that matches a defined pattern.

If the system running NetMaster CSM is the one specified to send Trap messages to, it will begin receiving these messages within the **SNMP Traps** window at the bottom of the CSM application. (Please note: SNMP Trap messages can only be received while CSM is running. Any messages sent by the security device while CSM is not running will be lost.)

Logs

Your security device can be configured to log event information by sending it to CSM. (How to configure this is covered in Section 7.) When CSM receives this information, it is parsed and stored in various device-specific log files at the operating system level. CSM also displays this information in the Log Events area located at the bottom of the main CSM window.

If your security device has been configured to transmit log event information to CSM, it will be stored for later parsing and viewing. For example, within the Logs module, you can view any captured firewall events within a Firewall report, an example of which is displayed below in Figure 10-2.



Firewall Report [Generated: Sat Sep 28 05:56:09 GMT 2002]

Date	Chain	Device	Action	Proto	Src	Dest
07/13/2002 16:12:02 PM	input	eth1	DENY	tcp	68.104.65.221:1214	24.71.42.60:64069
07/13/2002 16:16:38 PM	input	eth1	DENY	tcp	68.1.93.101:1214	24.71.42.60:64094
07/13/2002 16:16:41 PM	input	eth1	DENY	tcp	68.1.93.101:1214	24.71.42.60:64094
07/13/2002 16:16:47 PM	input	eth1	DENY	tcp	68.1.93.101:1214	24.71.42.60:64094
07/13/2002 16:18:19 PM	input	eth1	DENY	tcp	68.81.97.51:1214	24.71.42.60:64110
07/13/2002 16:18:22 PM	input	eth1	DENY	tcp	68.81.97.51:1214	24.71.42.60:64110
07/13/2002 16:18:22 PM	input	eth1	DENY	tcp	68.81.97.51:1214	24.71.42.60:64110
07/13/2002 16:18:28 PM	input	eth1	DENY	tcp	68.81.97.51:1214	24.71.42.60:64110
07/13/2002 16:18:28 PM	input	eth1	DENY	tcp	68.81.97.51:1214	24.71.42.60:64110
07/13/2002 16:19:56 PM	input	eth1	DENY	tcp	68.104.65.221:1214	24.71.42.60:64121
07/13/2002 16:20:02 PM	input	eth1	DENY	tcp	68.104.65.221:1214	24.71.42.60:64121

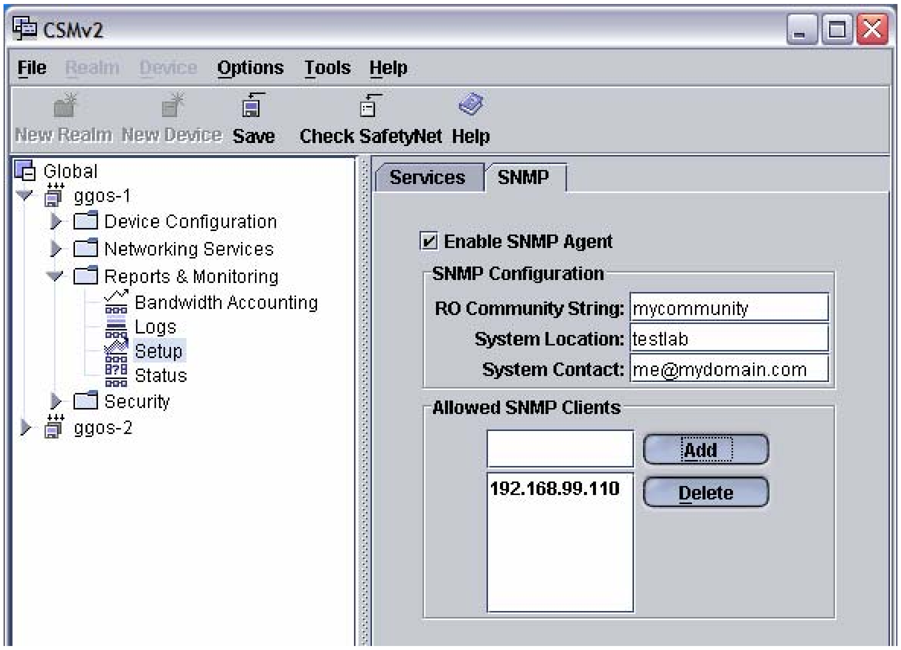
Figure 11-4: Logged Firewall Events

Setup

The Reports and Monitoring Setup module has two pages:

The first page, **Services**, can be used to modify various parameters regarding the system status monitoring system (Status Web Server) configuration. These parameters typically do not need to be modified from their default values.

The second page, **SNMP**, is used to enable and configure the SNMP Agent installed on the security device and used for monitoring purposes.



☑ Enable SNMP Agent

RO Community String: mycommunity

System Location: testlab

System Contact: me@mydomain.com

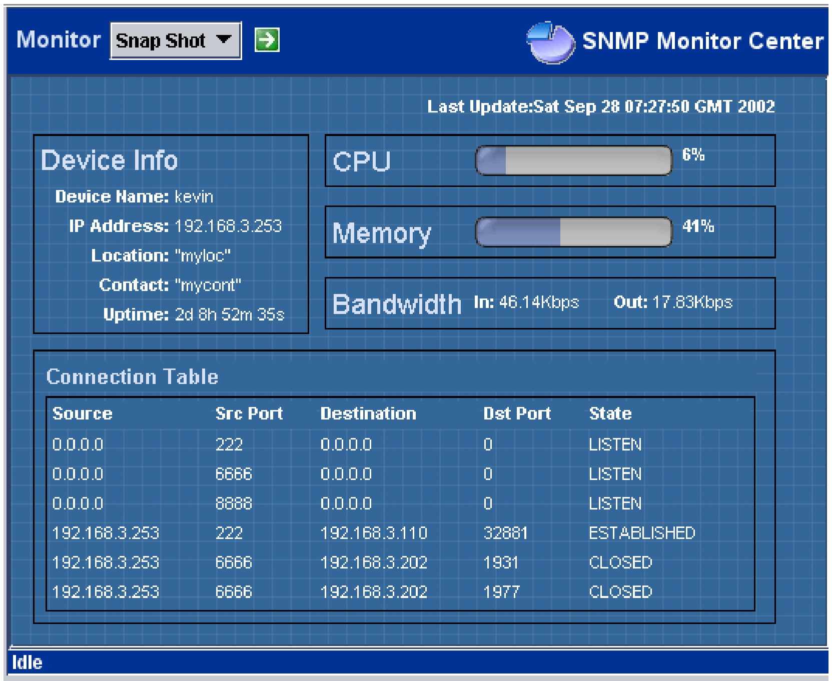
192.168.99.110

Figure 11-5: SNMP Agent Configuration

Configuring the SNMP Agent is a fairly straightforward process. The three parameters under **SNMP Configuration** are fairly arbitrary; however, the SNMP Community String must match the community string of a managed network containing other SNMP-enabled devices. Most importantly, you must add the IP Address of each remote administration workstation that is authorized to access the SNMP Agent on the security device into the **Allowed SNMP Clients** list box. All SNMP access to the NetMaster security device is Read-Only as it is only used for monitoring the device.

Once you have enabled and configured the **SNMP Agent**, you will be able to monitor various device status information details using CSM or a third-party SNMP Client – such as HP OpenView or CA NetCenter.

To view device status information via SNMP within CSM, click on the device name within the tree view on the left within CSM. From the screen displayed, as shown in Figure 10-4, you have two ways to monitor the device; via a one-time snapshot which compares two snapshots 15 seconds apart, or by polling the system every 30 seconds.



Last Update:Sat Sep 28 07:27:50 GMT 2002

Device Info

Device Name: kevin
IP Address: 192.168.3.253
Location: "myloc"
Contact: "mycont"
Uptime: 2d 8h 52m 35s

CPU 6%

Memory 41%

Bandwidth **In:** 46.14Kbps **Out:** 17.83Kbps

Connection Table

Source	Src Port	Destination	Dst Port	State
0.0.0.0	222	0.0.0.0	0	LISTEN
0.0.0.0	6666	0.0.0.0	0	LISTEN
0.0.0.0	8888	0.0.0.0	0	LISTEN
192.168.3.253	222	192.168.3.110	32881	ESTABLISHED
192.168.3.253	6666	192.168.3.202	1931	CLOSED
192.168.3.253	6666	192.168.3.202	1977	CLOSED

Figure 11-6: System Device Details via SNMP

You can view the summary status of all devices having the SNMP Agent enabled at each of the Realm levels within CSM. Each Realm level can be used to monitor the devices contained within the Realm and any of its sub-Realms. You can use the Global Realm to access a summary status view of all devices configured within CSM.

Status

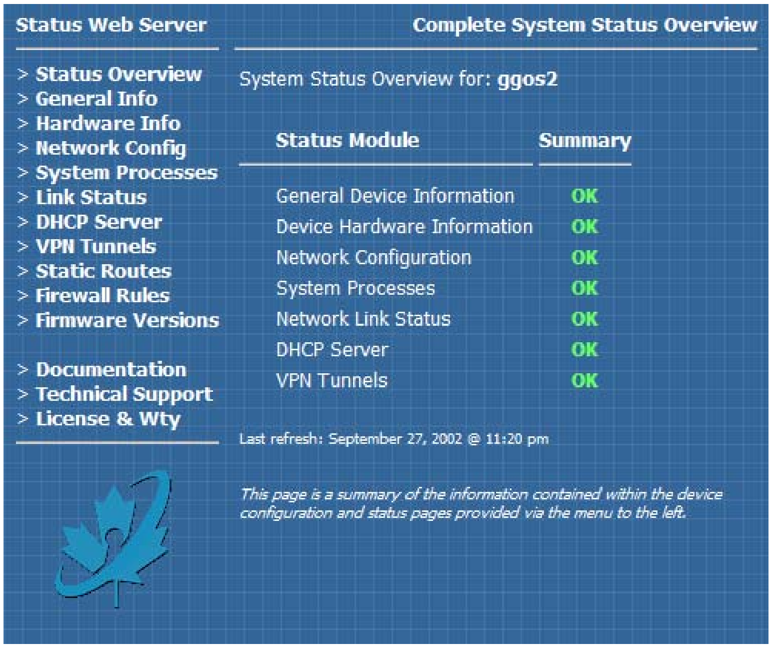
NetMaster's security devices include a comprehensive status monitoring system to provide information on the configuration and status of various system functions and features of the running system. This status information is accessible from within the CSM device management software; however is also available via any common web browser.

To access the device status system within CSM, simply click the Status module and the device status menu should automatically appear in the display window on the right.

To access the device status system from outside of CSM, simply load up your web browser and type the following into the Location bar:

http://ip.of.security.device:8888

Replace "ip.of.security.device" with the Internal IP Address of your NetMaster security device. Alternatively, if you have enabled External Access to your Status Web Server (see Figure 8-8 in Section 8), you can replace “ip.of.security.device” with the External IP Address of your NetMaster security device.



Complete System Status Overview

System Status Overview for: **ggos2**

Status Module	Summary
General Device Information	OK
Device Hardware Information	OK
Network Configuration	OK
System Processes	OK
Network Link Status	OK
DHCP Server	OK
VPN Tunnels	OK

Last refresh: September 27, 2002 @ 11:20 pm

This page is a summary of the information contained within the device configuration and status pages provided via the menu to the left.

Figure 11-7: System Status Overview

The main system status overview screen, as shown in Figure 10-x above, provides a complete overview of every monitored parameter in the security device. If a problem was discovered in any of the functional areas listed onscreen, a red WARNING message would be displayed. WARNING labels are linked objects and, when clicked, will take you directly to the necessary status page to determine what the exact problem is.

The device status monitoring system analyzes and reports on almost a dozen different functional areas of the security device. Click through the menu on the left side of the status window to see various system configuration parameters and current system status details.

Hint for Security Device Administrators

If your main workstation is running Windows and you have Active Desktop enabled, create a new desktop web object with the URL http://192.168.99.253:8888/cgi-bin/modules/overview and have it automatically displayed on your system desktop at all times. This page automatically refreshes every 5 minutes and, therefore, you will always have instant access to a snapshot of the current system status – right at your fingertips. (Be sure to replace the IP Address above with the appropriate IP Address for your device.)

12 – Advanced Functions and Features

GG-OS System Console

The GG-OS bootup screen is just one of several console screens available to monitor system status and configuration. To access alternate console screens, simply press **Alt** and one of the function keys, **F1** through **F12** to access the other consoles. The various console screens available include:

- **F1:** The main bootup console, showing configuration details.
- **F3:** System Log (syslog) output.
- **F4:** TCP Connections – both active and closed
- **F5:** Bandwidth throughput statistics
- **F6:** TCP/UDP protocol application statistics
- **F7:** Packet distribution by size statistics
- **F8:** Per-device traffic usage statistics
- **F9-F12:** System Login Shell Consoles

The last four consoles, F9 through F12, provide access to the GG-OS command line. Use the system administration password provided in Section 6 when creating the device to access the command line. This is an advanced feature and should only be used by Administrators that are familiar with the Unix/Linux command-line environment.

The system login shell consoles and the ability to Secure Shell into the device (see below) are not features required during normal maintenance and administration of your security device. These features have been provided to the system administrator solely as a means to "get into the backend" if it's absolutely required for some strange reason.

Using Secure Shell (SSH)

GG-OS is based on a Linux kernel and, therefore, contains a Linux command-line environment that you can access remotely via any SSH client software. If you are running Linux or another Unix or Unix-like operating system, you most likely have an SSH client already installed and available. If you are running Windows, you will need to download and install and SSH client. One such client is PuTTY, a freeware SSH client that you can download from:

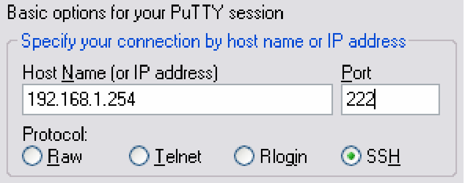
http://www.chiark.greenend.org.uk/~sgtatham/putty/

While most SSH Server Daemon implementations run on TCP port 22, the GG-OS SSH Daemon runs on TCP port 222 to avoid conflicts with regular SSH traffic that may be forwarded through the security device. Therefore, you must remember to specify port 222 as the destination port during any attempted SSH communications with GG-OS. For example:

Using a Unix/Linux SSH client, you will need to run:

```
ssh –p 222 root@<ip.of.security.device>
```

If you are using PuTTY on Windows, you will need to specify an SSH connection and then specify that the connection is to be made on port 222 as per the following:



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.254

Port: 222

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Figure 12-1: Using the PuTTY SSH Client for Windows

There is one thing you must be careful of when configuring PuTTY as per the above. First, type in the IP Address of your security device. Second, click the Protocol you want to use (SSH). Third, override the default Port value (22) with 222. (If you type in the port number first and then click SSH, PuTTY will override your port setting back to the SSH default of 22 – which can easily be missed as you try to establish your connection.)

The ability to Secure Shell into the device and the system login shell consoles (described on the previous pages) are not features required during normal maintenance and administration of your security device. These features have been provided to the system administrator solely as a means to "get into the backend" if it's absolutely required for some strange reason.

For More Information

Please send an email to
evaluations@netmaster.com
or call the number below.

NetMaster Digital Security
Suite 300
1055 West Hastings St.
Vancouver, BC
Canada V6E 2E9
604-609-6184
www.netmaster.com